TLP:AMBER

ASM-VP REPORT

GLESEC

July 26, 2023

TLP AMBER
ASM-VP REPORT

About this report

This is a SKYWATCH report that presents the most up-to-date information for the ASM-VP as displayed in the service dashboard.

Assets

MSS-VME

Overview

Vulnerability Level

14%

Discovered Hosts

63

Vulnerable Hosts

43

Executive Summary Vulnerability Severity Distribution

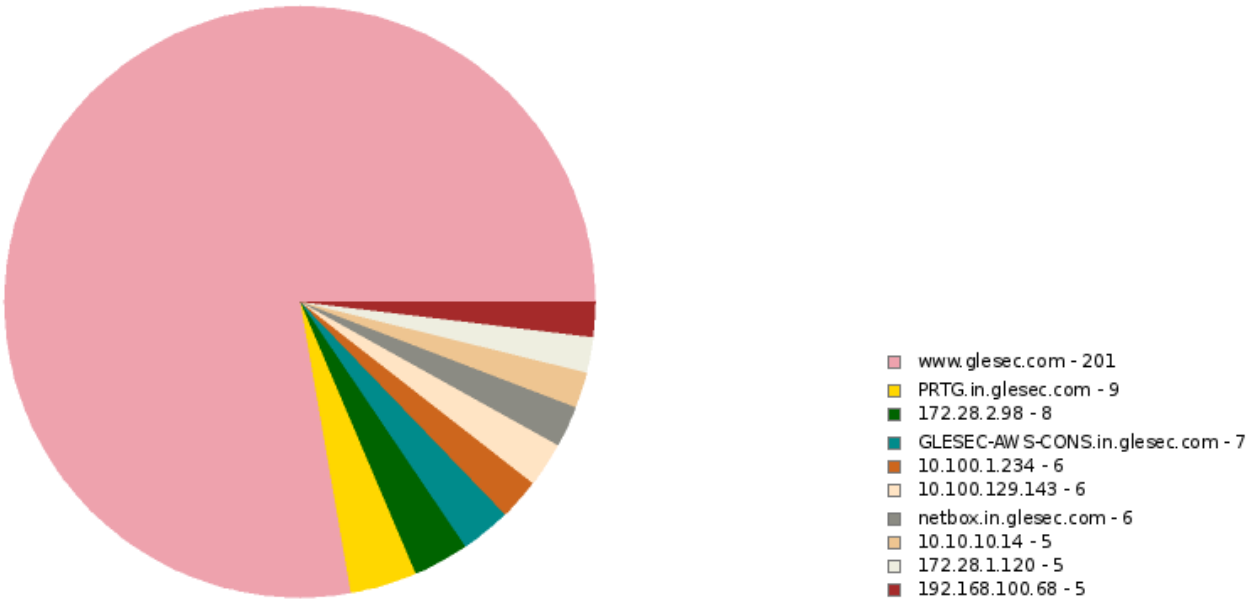
Scanner	critical	high	medium	low
GLESEC	1	4	119	24
GLESEC WEB SERVERS	0	0	2	1
Domain Scan: skywatch.glesec.com	0	0	2	2
Domain Scan: www.glesec.com	12	0	0	187

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

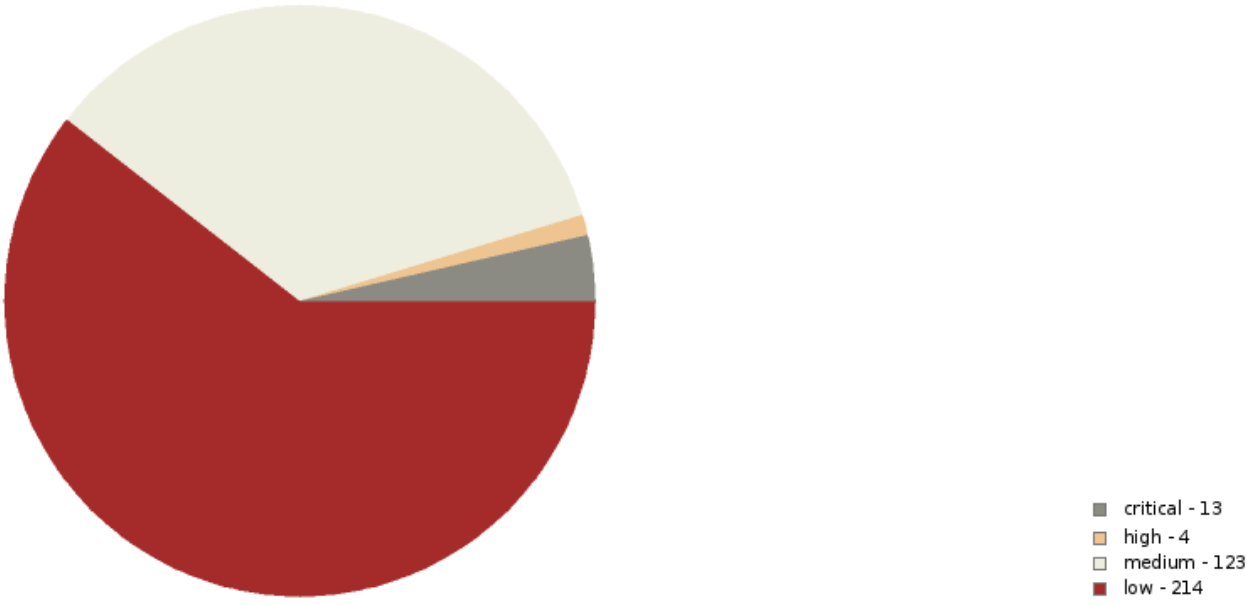
ASM-VP REPORT

GLESEC 07/26/2023

Most Vulnerable Host *



Vulnerability Distribution



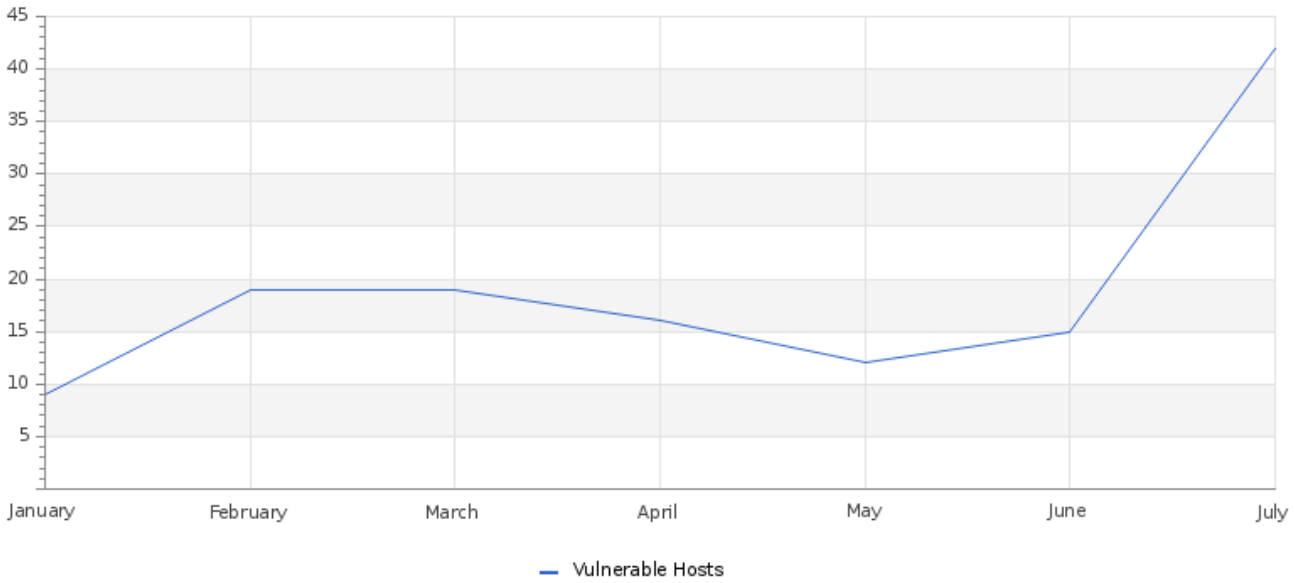
LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

Top 10 Most Common Vulnerabilities

Vulnerability
Cookie manipulation (DOM-based)
Client-side JSON injection (DOM-based)
Cross-site scripting (DOM-based)
SSL Certificate Cannot Be Trusted
Client-side HTTP parameter pollution (reflected)
SSL Self-Signed Certificate
Microsoft Windows Unquoted Service Path Enumeration
Web Server Allows Password Auto-Completion
Strict transport security not enforced
Splunk Enterprise and Universal Forwarder < 9.00 Improper Certificate Validation

History

Vulnerable Host History

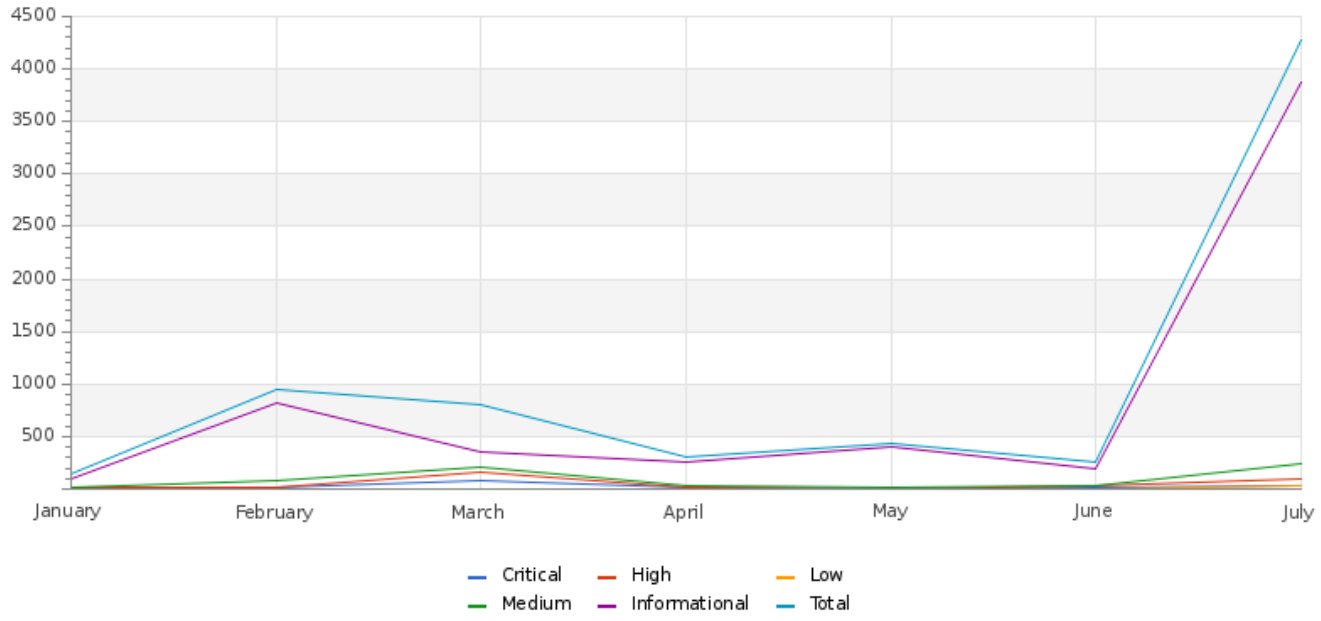


LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

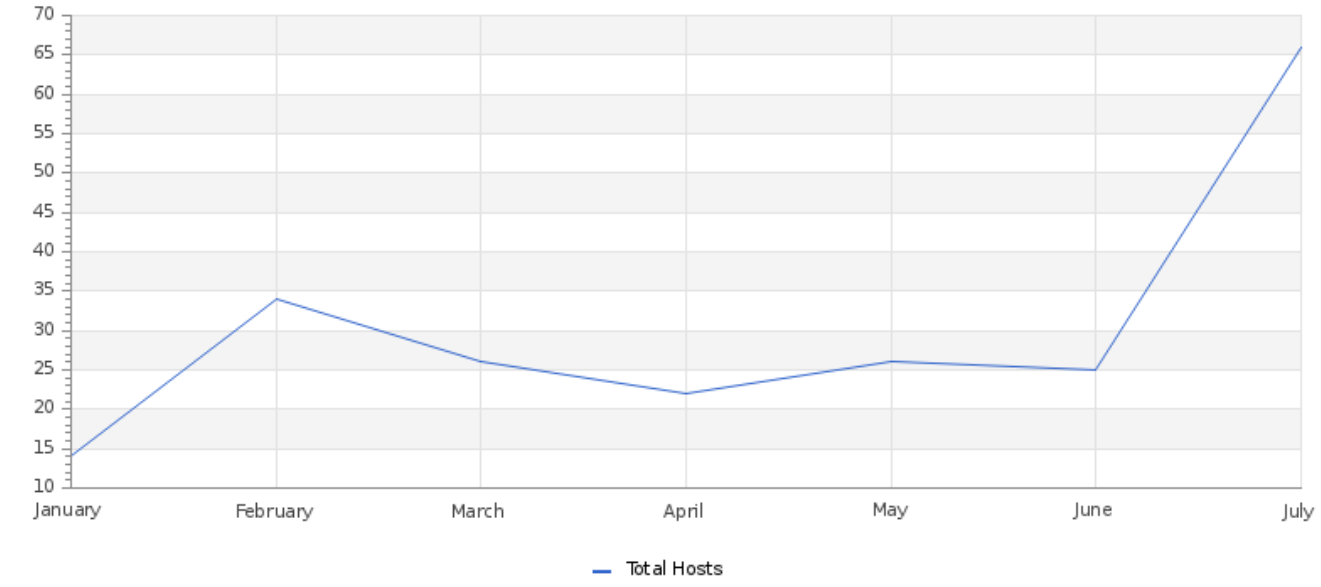
ASM-VP REPORT

GLESEC 07/26/2023

Vulnerability Severity History



Discovered Host History



LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

Vulnerabilities Compared To Previous Month

dest	Previous	Current
10.10.10.14	6	5
10.100.1.185	2	2
10.100.1.234	6	6
10.100.129.14	2	2
10.100.129.143	6	6
172.28.1.119	3	2
172.28.1.120	4	5
172.28.1.65	1	1
172.28.1.85	2	2
172.28.2.124	2	2
172.28.2.65	3	2
172.28.2.92	2	2
172.28.2.98	8	8
192.168.52.28	4	4
GMSA-LAB.in.glesec.com	5	12
GOC-USA-WALL.in.glesec.com	4	3
GOCUSAWS02.in.glesec.com	9	5
PRTG.in.glesec.com	4	9
USASYSTEMSWS01.in.glesec.com	4	4
USASYSTEMSWS02.in.glesec.com	4	5
USASYSTEMSWS03.in.glesec.com	4	3
dc-01.in.glesec.com	5	3
dc-02.in.glesec.com	5	3
goc-usa-sw.in.glesec.com	2	2
netbox.in.glesec.com	7	6
skywatch.glesec.com	1	1
www.glesec.com	2	2

Open Port Monitoring

Open Ports

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

TLP:AMBER

ASM-VP REPORT

GLESEC 07/26/2023

ip	hostname	port	status	protocol	service
66.22.79.162	skywatch.glesec.com	80	open	tcp	www
66.22.79.162	skywatch.glesec.com	443	open	tcp	www
172.28.2.98		123	open	udp	No Service Detected
172.28.2.98		135	open	tcp	epmap
172.28.2.98		137	open	udp	No Service Detected
172.28.2.98		445	open	tcp	cifs
172.28.2.98		1900	open	udp	No Service Detected
172.28.2.98		3389	open	udp	No Service Detected
172.28.2.98		3389	open	tcp	No Service Detected
172.28.2.98		4155	open	tcp	No Service Detected
172.28.2.98		5040	open	tcp	No Service Detected
172.28.2.98		5050	open	udp	No Service Detected
172.28.2.98		5120	open	tcp	No Service Detected
172.28.2.98		5353	open	udp	No Service Detected
172.28.2.98		5985	open	tcp	www
172.28.2.98		7680	open	tcp	No Service Detected
172.28.2.98		9593	open	tcp	No Service Detected
172.28.2.98		9594	open	tcp	No Service Detected
172.28.2.98		9595	open	tcp	No Service Detected
172.28.2.98		9595	open	udp	No Service Detected
172.28.2.98		33354	open	udp	No Service Detected
172.28.2.98		33354	open	tcp	No Service Detected
172.28.2.98		33355	open	udp	No Service Detected
172.28.2.98		33370	open	udp	No Service Detected
172.28.2.98		33370	open	tcp	No Service Detected
172.28.2.98		33371	open	udp	No Service Detected
172.28.2.98		38293	open	udp	No Service Detected
172.28.2.98		44343	open	tcp	www
172.28.2.98		47001	open	tcp	No Service Detected
172.28.2.98		49664	open	tcp	dce
172.28.2.98		49665	open	tcp	dce
172.28.2.98		49666	open	tcp	dce
172.28.2.98		49667	open	tcp	dce
172.28.2.98		49669	open	tcp	dce
172.28.2.98		49671	open	tcp	dce

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

ASM-VP REPORT

GLESEC 07/26/2023

ip	hostname	port	status	protocol	service
172.28.2.98		49711	open	tcp	dce
172.28.2.98		52098	open	tcp	dce
172.28.2.98		52980	open	udp	No Service Detected
172.28.2.98		54089	open	udp	No Service Detected
172.28.2.98		55388	open	udp	No Service Detected
172.28.2.98		55734	open	udp	No Service Detected
172.28.2.98		57358	open	udp	No Service Detected
172.28.2.98		57450	open	udp	No Service Detected
172.28.2.98		58543	open	udp	No Service Detected
172.28.2.98		61519	open	udp	No Service Detected
192.168.100.173	PRTG.in.glesec.com	80	open	tcp	www
192.168.100.173	PRTG.in.glesec.com	123	open	udp	No Service Detected
192.168.100.173	PRTG.in.glesec.com	135	open	tcp	epmap
192.168.100.173	PRTG.in.glesec.com	137	open	udp	No Service Detected
192.168.100.173	PRTG.in.glesec.com	138	open	udp	No Service Detected
192.168.100.173	PRTG.in.glesec.com	139	open	tcp	smb
192.168.100.173	PRTG.in.glesec.com	443	open	tcp	www
192.168.100.173	PRTG.in.glesec.com	445	open	tcp	cifs
192.168.100.173	PRTG.in.glesec.com	500	open	udp	No Service Detected
192.168.100.173	PRTG.in.glesec.com	3389	open	udp	No Service Detected
192.168.100.173	PRTG.in.glesec.com	3389	open	tcp	No Service Detected
192.168.100.173	PRTG.in.glesec.com	4155	open	tcp	www
192.168.100.173	PRTG.in.glesec.com	4500	open	udp	No Service Detected
192.168.100.173	PRTG.in.glesec.com	5120	open	tcp	No Service Detected
192.168.100.173	PRTG.in.glesec.com	5985	open	tcp	www
192.168.100.173	PRTG.in.glesec.com	6162	open	tcp	dce
192.168.100.173	PRTG.in.glesec.com	6183	open	tcp	dce
192.168.100.173	PRTG.in.glesec.com	6184	open	tcp	No Service Detected
192.168.100.173	PRTG.in.glesec.com	6190	open	tcp	dce
192.168.100.173	PRTG.in.glesec.com	6290	open	tcp	No Service Detected
192.168.100.173	PRTG.in.glesec.com	23560	open	tcp	www
192.168.100.173	PRTG.in.glesec.com	47001	open	tcp	www
192.168.100.173	PRTG.in.glesec.com	49664	open	tcp	dce
192.168.100.173	PRTG.in.glesec.com	49665	open	tcp	dce
192.168.100.173	PRTG.in.glesec.com	49667	open	tcp	dce

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

ASM-VP REPORT

GLESEC 07/26/2023

ip	hostname	port	status	protocol	service
192.168.100.173	PRTG.in.glesec.com	49669	open	tcp	dce
192.168.100.173	PRTG.in.glesec.com	49670	open	tcp	dce
192.168.100.173	PRTG.in.glesec.com	49771	open	tcp	dce
192.168.100.173	PRTG.in.glesec.com	49772	open	tcp	dce
192.168.100.173	PRTG.in.glesec.com	49901	open	tcp	dce
10.4.0.61	skywatch-dev.glesec.com	80	open	tcp	www
10.4.0.61	skywatch-dev.glesec.com	443	open	tcp	www
172.28.1.120		123	open	udp	No Service Detected
172.28.1.120		135	open	tcp	epmap
172.28.1.120		137	open	udp	netbios
172.28.1.120		138	open	udp	No Service Detected
172.28.1.120		139	open	tcp	smb
172.28.1.120		445	open	tcp	cifs
172.28.1.120		1900	open	udp	No Service Detected
172.28.1.120		5040	open	tcp	No Service Detected
172.28.1.120		5050	open	udp	No Service Detected
172.28.1.120		5120	open	tcp	No Service Detected
172.28.1.120		5353	open	udp	No Service Detected
172.28.1.120		5355	open	udp	No Service Detected
172.28.1.120		5985	open	tcp	www
172.28.1.120		7680	open	tcp	No Service Detected
172.28.1.120		9593	open	tcp	No Service Detected
172.28.1.120		9594	open	tcp	No Service Detected
172.28.1.120		9595	open	udp	No Service Detected
172.28.1.120		9595	open	tcp	www
172.28.1.120		33354	open	udp	No Service Detected
172.28.1.120		33354	open	tcp	No Service Detected
172.28.1.120		33355	open	udp	No Service Detected
172.28.1.120		33370	open	udp	No Service Detected
172.28.1.120		33370	open	tcp	No Service Detected
172.28.1.120		33371	open	udp	No Service Detected
172.28.1.120		38293	open	udp	No Service Detected
172.28.1.120		44343	open	tcp	www
172.28.1.120		47001	open	tcp	No Service Detected
172.28.1.120		49664	open	tcp	dce

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

ASM-VP REPORT

GLESEC 07/26/2023

ip	hostname	port	status	protocol	service
172.28.1.120		49665	open	tcp	dce
172.28.1.120		49666	open	tcp	dce
172.28.1.120		49667	open	tcp	dce
172.28.1.120		49668	open	tcp	dce
172.28.1.120		49669	open	tcp	dce
172.28.1.120		49672	open	tcp	dce
172.28.1.120		50392	open	udp	No Service Detected
172.28.1.120		51886	open	udp	No Service Detected
172.28.1.120		53124	open	tcp	dce
172.28.1.120		56781	open	udp	No Service Detected
172.28.2.114	GOCUSAWS02.in.glesec.com	123	open	udp	No Service Detected
172.28.2.114	GOCUSAWS02.in.glesec.com	135	open	tcp	epmap
172.28.2.114	GOCUSAWS02.in.glesec.com	137	open	udp	No Service Detected
172.28.2.114	GOCUSAWS02.in.glesec.com	445	open	tcp	cifs
172.28.2.114	GOCUSAWS02.in.glesec.com	1536	open	tcp	dce
172.28.2.114	GOCUSAWS02.in.glesec.com	1537	open	tcp	dce
172.28.2.114	GOCUSAWS02.in.glesec.com	1538	open	tcp	dce
172.28.2.114	GOCUSAWS02.in.glesec.com	1539	open	tcp	dce
172.28.2.114	GOCUSAWS02.in.glesec.com	1541	open	tcp	dce
172.28.2.114	GOCUSAWS02.in.glesec.com	1544	open	tcp	dce
172.28.2.114	GOCUSAWS02.in.glesec.com	1584	open	tcp	dce
172.28.2.114	GOCUSAWS02.in.glesec.com	1900	open	udp	No Service Detected
172.28.2.114	GOCUSAWS02.in.glesec.com	3389	open	tcp	No Service Detected
172.28.2.114	GOCUSAWS02.in.glesec.com	3389	open	udp	No Service Detected
172.28.2.114	GOCUSAWS02.in.glesec.com	4155	open	tcp	No Service Detected
172.28.2.114	GOCUSAWS02.in.glesec.com	4551	open	tcp	dce
172.28.2.114	GOCUSAWS02.in.glesec.com	5040	open	tcp	No Service Detected
172.28.2.114	GOCUSAWS02.in.glesec.com	5050	open	udp	No Service Detected
172.28.2.114	GOCUSAWS02.in.glesec.com	5120	open	tcp	No Service Detected
172.28.2.114	GOCUSAWS02.in.glesec.com	5353	open	udp	No Service Detected
172.28.2.114	GOCUSAWS02.in.glesec.com	5985	open	tcp	www
172.28.2.114	GOCUSAWS02.in.glesec.com	7680	open	tcp	No Service Detected
172.28.2.114	GOCUSAWS02.in.glesec.com	9593	open	tcp	No Service Detected
172.28.2.114	GOCUSAWS02.in.glesec.com	9594	open	tcp	No Service Detected
172.28.2.114	GOCUSAWS02.in.glesec.com	9595	open	tcp	No Service Detected

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

ASM-VP REPORT

GLESEC 07/26/2023

ip	hostname	port	status	protocol	service
172.28.2.114	GOCUSAWS02.in.glesec.com	9595	open	udp	No Service Detected
172.28.2.114	GOCUSAWS02.in.glesec.com	33354	open	tcp	No Service Detected
172.28.2.114	GOCUSAWS02.in.glesec.com	33354	open	udp	No Service Detected
172.28.2.114	GOCUSAWS02.in.glesec.com	33355	open	udp	No Service Detected
172.28.2.114	GOCUSAWS02.in.glesec.com	33370	open	udp	No Service Detected
172.28.2.114	GOCUSAWS02.in.glesec.com	33370	open	tcp	No Service Detected
172.28.2.114	GOCUSAWS02.in.glesec.com	33371	open	udp	No Service Detected
172.28.2.114	GOCUSAWS02.in.glesec.com	38293	open	udp	No Service Detected
172.28.2.114	GOCUSAWS02.in.glesec.com	44343	open	tcp	www
172.28.2.114	GOCUSAWS02.in.glesec.com	47001	open	tcp	No Service Detected
172.28.2.114	GOCUSAWS02.in.glesec.com	50899	open	udp	No Service Detected
172.28.2.114	GOCUSAWS02.in.glesec.com	51285	open	udp	No Service Detected
172.28.2.114	GOCUSAWS02.in.glesec.com	53258	open	udp	No Service Detected
172.28.2.77	GOC-USA-WALL.in.glesec.com	123	open	udp	No Service Detected
172.28.2.77	GOC-USA-WALL.in.glesec.com	135	open	tcp	epmap
172.28.2.77	GOC-USA-WALL.in.glesec.com	137	open	udp	No Service Detected
172.28.2.77	GOC-USA-WALL.in.glesec.com	445	open	tcp	cifs
172.28.2.77	GOC-USA-WALL.in.glesec.com	1900	open	udp	No Service Detected
172.28.2.77	GOC-USA-WALL.in.glesec.com	4155	open	tcp	No Service Detected
172.28.2.77	GOC-USA-WALL.in.glesec.com	5040	open	tcp	No Service Detected
172.28.2.77	GOC-USA-WALL.in.glesec.com	5050	open	udp	No Service Detected
172.28.2.77	GOC-USA-WALL.in.glesec.com	5120	open	tcp	No Service Detected
172.28.2.77	GOC-USA-WALL.in.glesec.com	5353	open	udp	No Service Detected
172.28.2.77	GOC-USA-WALL.in.glesec.com	5985	open	tcp	www
172.28.2.77	GOC-USA-WALL.in.glesec.com	7680	open	tcp	No Service Detected
172.28.2.77	GOC-USA-WALL.in.glesec.com	9593	open	tcp	No Service Detected
172.28.2.77	GOC-USA-WALL.in.glesec.com	9594	open	tcp	No Service Detected
172.28.2.77	GOC-USA-WALL.in.glesec.com	9595	open	tcp	No Service Detected
172.28.2.77	GOC-USA-WALL.in.glesec.com	9595	open	udp	No Service Detected
172.28.2.77	GOC-USA-WALL.in.glesec.com	33354	open	tcp	No Service Detected
172.28.2.77	GOC-USA-WALL.in.glesec.com	33354	open	udp	No Service Detected
172.28.2.77	GOC-USA-WALL.in.glesec.com	33355	open	udp	No Service Detected
172.28.2.77	GOC-USA-WALL.in.glesec.com	33370	open	udp	No Service Detected
172.28.2.77	GOC-USA-WALL.in.glesec.com	33370	open	tcp	No Service Detected
172.28.2.77	GOC-USA-WALL.in.glesec.com	33371	open	udp	No Service Detected

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

TLP:AMBER

ASM-VP REPORT

GLESEC 07/26/2023

ip	hostname	port	status	protocol	service
172.28.2.77	GOC-USA-WALL.in.glesec.com	38293	open	udp	No Service Detected
172.28.2.77	GOC-USA-WALL.in.glesec.com	44343	open	tcp	www
172.28.2.77	GOC-USA-WALL.in.glesec.com	47001	open	tcp	No Service Detected
172.28.2.77	GOC-USA-WALL.in.glesec.com	49664	open	tcp	dce
172.28.2.77	GOC-USA-WALL.in.glesec.com	49665	open	tcp	dce
172.28.2.77	GOC-USA-WALL.in.glesec.com	49666	open	tcp	dce
172.28.2.77	GOC-USA-WALL.in.glesec.com	49667	open	tcp	dce
172.28.2.77	GOC-USA-WALL.in.glesec.com	49668	open	tcp	dce
172.28.2.77	GOC-USA-WALL.in.glesec.com	49672	open	tcp	dce
172.28.2.77	GOC-USA-WALL.in.glesec.com	61054	open	udp	No Service Detected
172.28.2.77	GOC-USA-WALL.in.glesec.com	61726	open	udp	No Service Detected
172.28.2.77	GOC-USA-WALL.in.glesec.com	61762	open	tcp	dce
172.28.2.77	GOC-USA-WALL.in.glesec.com	63153	open	udp	No Service Detected
66.22.79.163	www.glesec.com	80	open	tcp	www
66.22.79.163	www.glesec.com	443	open	tcp	www
172.28.2.113	GMSA-LAB.in.glesec.com	80	open	tcp	www
172.28.2.113	GMSA-LAB.in.glesec.com	123	open	udp	No Service Detected
172.28.2.113	GMSA-LAB.in.glesec.com	135	open	tcp	epmap
172.28.2.113	GMSA-LAB.in.glesec.com	137	open	udp	netbios
172.28.2.113	GMSA-LAB.in.glesec.com	138	open	udp	No Service Detected
172.28.2.113	GMSA-LAB.in.glesec.com	139	open	tcp	smb
172.28.2.113	GMSA-LAB.in.glesec.com	443	open	tcp	No Service Detected
172.28.2.113	GMSA-LAB.in.glesec.com	445	open	tcp	cifs
172.28.2.113	GMSA-LAB.in.glesec.com	2179	open	tcp	No Service Detected
172.28.2.113	GMSA-LAB.in.glesec.com	3389	open	udp	No Service Detected
172.28.2.113	GMSA-LAB.in.glesec.com	3389	open	tcp	No Service Detected
172.28.2.113	GMSA-LAB.in.glesec.com	5120	open	tcp	No Service Detected
172.28.2.113	GMSA-LAB.in.glesec.com	5985	open	tcp	www
172.28.2.113	GMSA-LAB.in.glesec.com	6160	open	tcp	dce
172.28.2.113	GMSA-LAB.in.glesec.com	6162	open	tcp	dce
172.28.2.113	GMSA-LAB.in.glesec.com	6163	open	tcp	dce
172.28.2.113	GMSA-LAB.in.glesec.com	6190	open	tcp	dce
172.28.2.113	GMSA-LAB.in.glesec.com	6290	open	tcp	No Service Detected
172.28.2.113	GMSA-LAB.in.glesec.com	6600	open	tcp	No Service Detected
172.28.2.113	GMSA-LAB.in.glesec.com	11731	open	tcp	dce

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

TLP:AMBER

ASM-VP REPORT

GLESEC 07/26/2023

ip	hostname	port	status	protocol	service
172.28.2.113	GMSA-LAB.in.glesec.com	47001	open	tcp	No Service Detected
172.28.2.113	GMSA-LAB.in.glesec.com	49664	open	tcp	dce
172.28.2.113	GMSA-LAB.in.glesec.com	49665	open	tcp	dce
172.28.2.113	GMSA-LAB.in.glesec.com	49666	open	tcp	dce
172.28.2.113	GMSA-LAB.in.glesec.com	49667	open	tcp	dce
172.28.2.113	GMSA-LAB.in.glesec.com	49668	open	tcp	dce
172.28.2.113	GMSA-LAB.in.glesec.com	49669	open	tcp	dce
172.28.2.113	GMSA-LAB.in.glesec.com	49726	open	tcp	dce
172.28.2.113	GMSA-LAB.in.glesec.com	49863	open	tcp	dce
172.28.2.108	GMSA-LAB.in.glesec.com	80	open	tcp	www
172.28.2.108	GMSA-LAB.in.glesec.com	123	open	udp	No Service Detected
172.28.2.108	GMSA-LAB.in.glesec.com	135	open	tcp	epmap
172.28.2.108	GMSA-LAB.in.glesec.com	137	open	udp	netbios
172.28.2.108	GMSA-LAB.in.glesec.com	138	open	udp	No Service Detected
172.28.2.108	GMSA-LAB.in.glesec.com	139	open	tcp	smb
172.28.2.108	GMSA-LAB.in.glesec.com	443	open	tcp	No Service Detected
172.28.2.108	GMSA-LAB.in.glesec.com	445	open	tcp	cifs
172.28.2.108	GMSA-LAB.in.glesec.com	2179	open	tcp	No Service Detected
172.28.2.108	GMSA-LAB.in.glesec.com	3389	open	udp	No Service Detected
172.28.2.108	GMSA-LAB.in.glesec.com	3389	open	tcp	No Service Detected
172.28.2.108	GMSA-LAB.in.glesec.com	5120	open	tcp	No Service Detected
172.28.2.108	GMSA-LAB.in.glesec.com	5985	open	tcp	www
172.28.2.108	GMSA-LAB.in.glesec.com	6160	open	tcp	dce
172.28.2.108	GMSA-LAB.in.glesec.com	6162	open	tcp	dce
172.28.2.108	GMSA-LAB.in.glesec.com	6163	open	tcp	dce
172.28.2.108	GMSA-LAB.in.glesec.com	6190	open	tcp	dce
172.28.2.108	GMSA-LAB.in.glesec.com	6290	open	tcp	No Service Detected
172.28.2.108	GMSA-LAB.in.glesec.com	6600	open	tcp	No Service Detected
172.28.2.108	GMSA-LAB.in.glesec.com	11731	open	tcp	dce
172.28.2.108	GMSA-LAB.in.glesec.com	47001	open	tcp	No Service Detected
172.28.2.108	GMSA-LAB.in.glesec.com	49664	open	tcp	dce
172.28.2.108	GMSA-LAB.in.glesec.com	49665	open	tcp	dce
172.28.2.108	GMSA-LAB.in.glesec.com	49666	open	tcp	dce
172.28.2.108	GMSA-LAB.in.glesec.com	49667	open	tcp	dce
172.28.2.108	GMSA-LAB.in.glesec.com	49668	open	tcp	dce

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

TLP:AMBER

ASM-VP REPORT

GLESEC 07/26/2023

ip	hostname	port	status	protocol	service
172.28.2.108	GMSA-LAB.in.glesec.com	49669	open	tcp	dce
172.28.2.108	GMSA-LAB.in.glesec.com	49726	open	tcp	dce
172.28.2.108	GMSA-LAB.in.glesec.com	49863	open	tcp	dce
172.28.2.108	GMSA-LAB.in.glesec.com	61414	open	udp	No Service Detected
192.168.51.15	dc-02.in.glesec.com	53	open	tcp	dns
192.168.51.15	dc-02.in.glesec.com	53	open	udp	dns
192.168.51.15	dc-02.in.glesec.com	88	open	udp	No Service Detected
192.168.51.15	dc-02.in.glesec.com	88	open	tcp	No Service Detected
192.168.51.15	dc-02.in.glesec.com	123	open	udp	ntp
192.168.51.15	dc-02.in.glesec.com	135	open	tcp	epmap
192.168.51.15	dc-02.in.glesec.com	137	open	udp	No Service Detected
192.168.51.15	dc-02.in.glesec.com	389	open	tcp	ldap
192.168.51.15	dc-02.in.glesec.com	389	open	udp	No Service Detected
192.168.51.15	dc-02.in.glesec.com	445	open	tcp	cifs
192.168.51.15	dc-02.in.glesec.com	464	open	tcp	No Service Detected
192.168.51.15	dc-02.in.glesec.com	464	open	udp	No Service Detected
192.168.51.15	dc-02.in.glesec.com	500	open	udp	No Service Detected
192.168.51.15	dc-02.in.glesec.com	593	open	tcp	http
192.168.51.15	dc-02.in.glesec.com	636	open	tcp	ldap
192.168.51.15	dc-02.in.glesec.com	647	open	tcp	No Service Detected
192.168.51.15	dc-02.in.glesec.com	3268	open	tcp	ldap
192.168.51.15	dc-02.in.glesec.com	3269	open	tcp	ldap
192.168.51.15	dc-02.in.glesec.com	3389	open	tcp	No Service Detected
192.168.51.15	dc-02.in.glesec.com	3389	open	udp	No Service Detected
192.168.51.15	dc-02.in.glesec.com	4155	open	tcp	No Service Detected
192.168.51.15	dc-02.in.glesec.com	4500	open	udp	No Service Detected
192.168.51.15	dc-02.in.glesec.com	5120	open	tcp	No Service Detected
192.168.51.15	dc-02.in.glesec.com	5985	open	tcp	www
192.168.51.15	dc-02.in.glesec.com	6162	open	tcp	dce
192.168.51.15	dc-02.in.glesec.com	6183	open	tcp	dce
192.168.51.15	dc-02.in.glesec.com	6184	open	tcp	No Service Detected
192.168.51.15	dc-02.in.glesec.com	6190	open	tcp	dce
192.168.51.15	dc-02.in.glesec.com	6290	open	tcp	No Service Detected
192.168.51.15	dc-02.in.glesec.com	9389	open	tcp	No Service Detected
192.168.51.15	dc-02.in.glesec.com	47001	open	tcp	No Service Detected

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

ASM-VP REPORT

GLESEC 07/26/2023

ip	hostname	port	status	protocol	service
192.168.51.15	dc-02.in.glesec.com	49664	open	tcp	dce
192.168.51.15	dc-02.in.glesec.com	49665	open	tcp	dce
192.168.51.15	dc-02.in.glesec.com	49666	open	tcp	dce
192.168.51.15	dc-02.in.glesec.com	49667	open	tcp	dce
192.168.51.15	dc-02.in.glesec.com	49668	open	tcp	dce
192.168.51.15	dc-02.in.glesec.com	49670	open	tcp	ncacn_http
192.168.51.15	dc-02.in.glesec.com	49671	open	tcp	dce
192.168.51.15	dc-02.in.glesec.com	49676	open	tcp	dce
192.168.51.15	dc-02.in.glesec.com	49750	open	tcp	dce
192.168.51.15	dc-02.in.glesec.com	49762	open	tcp	dce
192.168.51.15	dc-02.in.glesec.com	49773	open	tcp	dce
192.168.51.15	dc-02.in.glesec.com	49873	open	tcp	dce
172.28.2.124		80	open	tcp	www
172.28.2.124		443	open	tcp	www
172.28.2.124		5060	open	tcp	No Service Detected
172.28.2.89	goc-usa-sw.in.glesec.com	80	open	tcp	www
172.28.2.89	goc-usa-sw.in.glesec.com	443	open	tcp	www
172.28.2.89	goc-usa-sw.in.glesec.com	5060	open	tcp	No Service Detected
172.28.2.92		80	open	tcp	www
172.28.2.92		443	open	tcp	www
172.28.2.92		5060	open	tcp	No Service Detected
192.168.51.51		22	open	tcp	ssh
192.168.51.51		80	open	tcp	www
192.168.51.51		443	open	tcp	www
192.168.51.51		5432	open	tcp	postgresql
192.168.51.51		8081	open	tcp	www
172.28.2.65		22	open	tcp	ssh
172.28.2.65		53	open	tcp	dns
172.28.2.65		80	open	tcp	www
172.28.2.65		443	open	tcp	www
10.100.129.14		443	open	tcp	www
172.28.1.91		22	open	tcp	ssh
10.100.1.185		443	open	tcp	www
10.4.0.51	gmp.glesec.com	80	open	tcp	www
10.4.0.51	gmp.glesec.com	443	open	tcp	www

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

TLP:AMBER

ASM-VP REPORT

GLESEC 07/26/2023

ip	hostname	port	status	protocol	service
10.10.10.2		53	open	tcp	dns
10.4.0.2		53	open	tcp	dns
172.28.2.109	GMSA-LAB.in.glesec.com	80	open	tcp	www
172.28.2.109	GMSA-LAB.in.glesec.com	123	open	udp	No Service Detected
172.28.2.109	GMSA-LAB.in.glesec.com	135	open	tcp	epmap
172.28.2.109	GMSA-LAB.in.glesec.com	137	open	udp	netbios
172.28.2.109	GMSA-LAB.in.glesec.com	138	open	udp	No Service Detected
172.28.2.109	GMSA-LAB.in.glesec.com	139	open	tcp	smb
172.28.2.109	GMSA-LAB.in.glesec.com	443	open	tcp	No Service Detected
172.28.2.109	GMSA-LAB.in.glesec.com	445	open	tcp	cifs
172.28.2.109	GMSA-LAB.in.glesec.com	2179	open	tcp	No Service Detected
172.28.2.109	GMSA-LAB.in.glesec.com	3389	open	udp	No Service Detected
172.28.2.109	GMSA-LAB.in.glesec.com	3389	open	tcp	No Service Detected
172.28.2.109	GMSA-LAB.in.glesec.com	5120	open	tcp	No Service Detected
172.28.2.109	GMSA-LAB.in.glesec.com	5985	open	tcp	www
172.28.2.109	GMSA-LAB.in.glesec.com	6160	open	tcp	dce
172.28.2.109	GMSA-LAB.in.glesec.com	6162	open	tcp	dce
172.28.2.109	GMSA-LAB.in.glesec.com	6163	open	tcp	dce
172.28.2.109	GMSA-LAB.in.glesec.com	6190	open	tcp	dce
172.28.2.109	GMSA-LAB.in.glesec.com	6290	open	tcp	No Service Detected
172.28.2.109	GMSA-LAB.in.glesec.com	6600	open	tcp	No Service Detected
172.28.2.109	GMSA-LAB.in.glesec.com	11731	open	tcp	dce
172.28.2.109	GMSA-LAB.in.glesec.com	47001	open	tcp	No Service Detected
172.28.2.109	GMSA-LAB.in.glesec.com	49664	open	tcp	dce
172.28.2.109	GMSA-LAB.in.glesec.com	49665	open	tcp	dce
172.28.2.109	GMSA-LAB.in.glesec.com	49666	open	tcp	dce
172.28.2.109	GMSA-LAB.in.glesec.com	49667	open	tcp	dce
172.28.2.109	GMSA-LAB.in.glesec.com	49668	open	tcp	dce
172.28.2.109	GMSA-LAB.in.glesec.com	49669	open	tcp	dce
172.28.2.109	GMSA-LAB.in.glesec.com	49726	open	tcp	dce
172.28.2.109	GMSA-LAB.in.glesec.com	49863	open	tcp	dce
172.28.2.109	GMSA-LAB.in.glesec.com	56467	open	udp	No Service Detected
192.168.52.28		80	open	tcp	www
192.168.52.28		123	open	udp	No Service Detected
192.168.52.28		135	open	tcp	epmap

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

ASM-VP REPORT

GLESEC 07/26/2023

ip	hostname	port	status	protocol	service
192.168.52.28		137	open	udp	No Service Detected
192.168.52.28		138	open	udp	No Service Detected
192.168.52.28		139	open	tcp	smb
192.168.52.28		443	open	tcp	www
192.168.52.28		445	open	tcp	cifs
192.168.52.28		3389	open	udp	No Service Detected
192.168.52.28		3389	open	tcp	No Service Detected
192.168.52.28		5120	open	tcp	No Service Detected
192.168.52.28		5985	open	tcp	www
192.168.52.28		6162	open	tcp	dce
192.168.52.28		6183	open	tcp	dce
192.168.52.28		6184	open	tcp	No Service Detected
192.168.52.28		6190	open	tcp	dce
192.168.52.28		6290	open	tcp	No Service Detected
192.168.52.28		8530	open	tcp	www
192.168.52.28		8531	open	tcp	No Service Detected
192.168.52.28		47001	open	tcp	No Service Detected
192.168.52.28		49664	open	tcp	dce
192.168.52.28		49665	open	tcp	dce
192.168.52.28		49667	open	tcp	dce
192.168.52.28		49668	open	tcp	dce
192.168.52.28		49669	open	tcp	dce
192.168.52.28		49782	open	tcp	dce
192.168.52.28		49793	open	tcp	dce
192.168.52.28		49816	open	tcp	dce
192.168.52.28		51729	open	tcp	dce
192.168.50.114	dc-01.in.glesec.com	53	open	tcp	dns
192.168.50.114	dc-01.in.glesec.com	53	open	udp	dns
192.168.50.114	dc-01.in.glesec.com	88	open	udp	No Service Detected
192.168.50.114	dc-01.in.glesec.com	88	open	tcp	No Service Detected
192.168.50.114	dc-01.in.glesec.com	123	open	udp	ntp
192.168.50.114	dc-01.in.glesec.com	135	open	tcp	epmap
192.168.50.114	dc-01.in.glesec.com	137	open	udp	No Service Detected
192.168.50.114	dc-01.in.glesec.com	389	open	tcp	ldap
192.168.50.114	dc-01.in.glesec.com	389	open	udp	No Service Detected

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

ASM-VP REPORT

GLESEC 07/26/2023

ip	hostname	port	status	protocol	service
192.168.50.114	dc-01.in.glesec.com	445	open	tcp	cifs
192.168.50.114	dc-01.in.glesec.com	464	open	tcp	No Service Detected
192.168.50.114	dc-01.in.glesec.com	464	open	udp	No Service Detected
192.168.50.114	dc-01.in.glesec.com	593	open	tcp	http
192.168.50.114	dc-01.in.glesec.com	636	open	tcp	ldap
192.168.50.114	dc-01.in.glesec.com	3268	open	tcp	ldap
192.168.50.114	dc-01.in.glesec.com	3269	open	tcp	ldap
192.168.50.114	dc-01.in.glesec.com	3389	open	udp	No Service Detected
192.168.50.114	dc-01.in.glesec.com	3389	open	tcp	No Service Detected
192.168.50.114	dc-01.in.glesec.com	4155	open	tcp	No Service Detected
192.168.50.114	dc-01.in.glesec.com	5120	open	tcp	No Service Detected
192.168.50.114	dc-01.in.glesec.com	5985	open	tcp	www
192.168.50.114	dc-01.in.glesec.com	6162	open	tcp	dce
192.168.50.114	dc-01.in.glesec.com	6183	open	tcp	dce
192.168.50.114	dc-01.in.glesec.com	6184	open	tcp	No Service Detected
192.168.50.114	dc-01.in.glesec.com	6190	open	tcp	dce
192.168.50.114	dc-01.in.glesec.com	6290	open	tcp	No Service Detected
192.168.50.114	dc-01.in.glesec.com	9389	open	tcp	No Service Detected
192.168.50.114	dc-01.in.glesec.com	47001	open	tcp	No Service Detected
192.168.50.114	dc-01.in.glesec.com	49664	open	tcp	dce
192.168.50.114	dc-01.in.glesec.com	49665	open	tcp	dce
192.168.50.114	dc-01.in.glesec.com	49666	open	tcp	dce
192.168.50.114	dc-01.in.glesec.com	49667	open	tcp	dce
192.168.50.114	dc-01.in.glesec.com	49668	open	tcp	dce
192.168.50.114	dc-01.in.glesec.com	49674	open	tcp	ncacn_http
192.168.50.114	dc-01.in.glesec.com	49675	open	tcp	dce
192.168.50.114	dc-01.in.glesec.com	49676	open	tcp	dce
192.168.50.114	dc-01.in.glesec.com	49695	open	tcp	dce
192.168.50.114	dc-01.in.glesec.com	49702	open	tcp	dce
192.168.50.114	dc-01.in.glesec.com	49820	open	tcp	dce
192.168.50.114	dc-01.in.glesec.com	49886	open	tcp	dce
192.168.52.48	netbox.in.glesec.com	22	open	tcp	ssh
192.168.52.48	netbox.in.glesec.com	68	open	udp	No Service Detected
192.168.52.48	netbox.in.glesec.com	80	open	tcp	www
192.168.52.48	netbox.in.glesec.com	443	open	tcp	www

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

ASM-VP REPORT

GLESEC 07/26/2023

ip	hostname	port	status	protocol	service
192.168.52.48	netbox.in.glesec.com	6162	open	tcp	No Service Detected
192.168.52.48	netbox.in.glesec.com	10050	open	tcp	No Service Detected
172.28.1.119		135	open	tcp	epmap
172.28.1.119		445	open	tcp	cifs
172.28.1.119		3389	open	tcp	No Service Detected
172.28.1.119		9593	open	tcp	No Service Detected
172.28.1.119		9594	open	tcp	No Service Detected
172.28.1.119		9595	open	tcp	No Service Detected
10.100.129.143		443	open	tcp	www
10.100.1.234		443	open	tcp	www
172.28.1.65		22	open	tcp	No Service Detected
172.28.1.65		53	open	tcp	dns
172.28.1.65		80	open	tcp	www
172.28.1.65		443	open	tcp	www
172.28.1.65		5666	open	tcp	No Service Detected
172.28.1.85		80	open	tcp	www
172.28.1.85		443	open	tcp	www
172.28.2.95		80	open	tcp	www
172.28.2.95		5060	open	tcp	No Service Detected
172.28.1.89		135	open	tcp	epmap
172.28.2.91		80	open	tcp	No Service Detected
172.28.2.91		443	open	tcp	No Service Detected
172.28.2.91		631	open	tcp	No Service Detected
172.28.2.91		8080	open	tcp	No Service Detected
172.28.2.91		9100	open	tcp	No Service Detected
172.28.1.87		67	open	udp	No Service Detected
172.28.1.87		80	open	tcp	No Service Detected
172.28.1.87		137	open	udp	No Service Detected
172.28.1.87		138	open	udp	No Service Detected
172.28.1.87		139	open	tcp	smb
172.28.1.87		161	open	udp	snmp
172.28.1.87		427	open	udp	No Service Detected
172.28.1.87		443	open	tcp	No Service Detected
172.28.1.87		445	open	tcp	cifs
172.28.1.87		515	open	tcp	No Service Detected

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

ip	hostname	port	status	protocol	service
172.28.1.87		631	open	tcp	No Service Detected
172.28.1.87		1865	open	tcp	No Service Detected
172.28.1.87		9100	open	tcp	No Service Detected
10.100.0.2		53	open	tcp	dns
172.28.1.86		80	open	tcp	www
172.28.1.86		443	open	tcp	www

Penetration Tab

Recent Scans

Scan Date	Scanned Domain	Scan Duration	Pages Scanned
2023-07-24 13:58:07	www.glesec.com	6:37:00	780/452
2023-07-20 15:14:04	www.glesec.com	1:46:54	795/468
2023-07-25 15:46:26	www.glesec.com	5:42:17	801/472

Vulnerability Counts

Total Vulnerabilities	High Vulnerabilities	Medium Vulnerabilities	Low Vulnerabilities	Informational Vulnerabilities
27	0	7	14	6
18	0	7	7	4
19	0	7	7	5

Vulnerable Pages

16

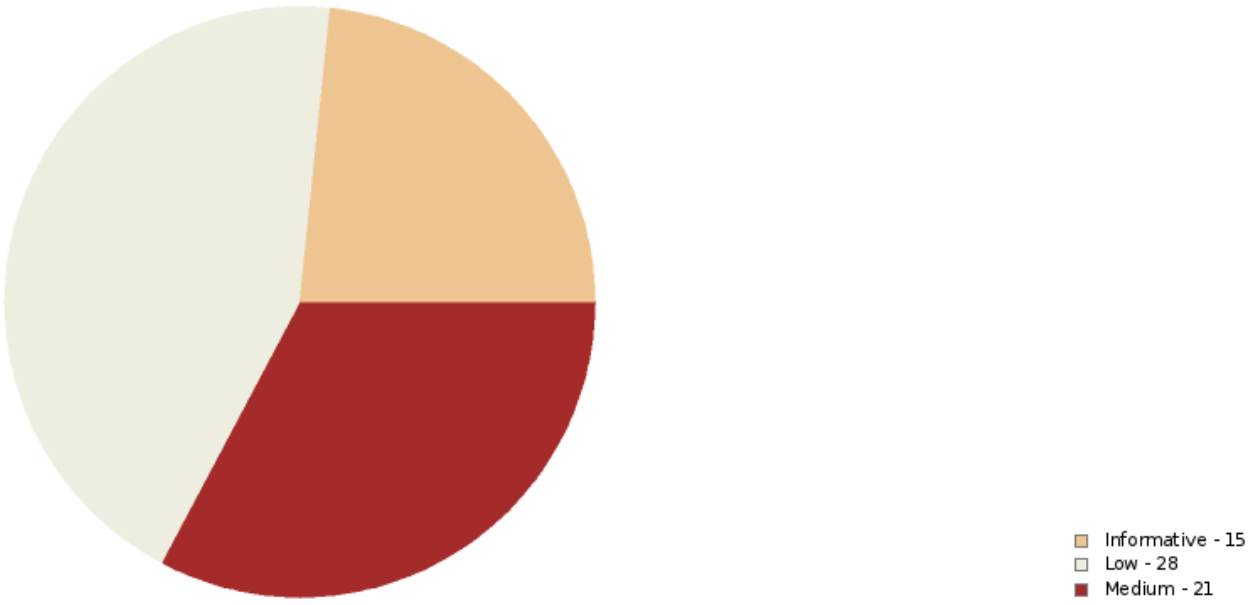
LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

TLP:AMBER

ASM-VP REPORT

GLESEC 07/26/2023

Risk Distribution



Vulnerabilities

url	vuln_name	severity
https://www.glesec.com/	ClickJacking - X-Frame-Options header missing	Low
https://www.glesec.com/	WordPress - User Disclosure	Medium
https://www.glesec.com/	jQuery - CVE-2020-23064	Medium
https://www.glesec.com/	jQuery - CVE-2020-11023	Medium
https://www.glesec.com/	jQuery - CVE-2020-11022	Medium
https://www.glesec.com/	jQuery - CVE-2019-11358	Medium
https://www.glesec.com/	jQuery - CVE-2015-9251	Medium
https://www.glesec.com/wp-content/plugins/the-events-calendar/common/vendor/composer/installed.json	Development configuration files	Medium
https://www.glesec.com/events/action{new_param0}	Possible External IP Disclosure	Low

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

ASM-VP REPORT

GLESEC 07/26/2023

url	vuln_name	severity
https://www.glesec.com/calendar/action{new_param0}	Possible External IP Disclosure	Low
https://www.glesec.com/{new_param0}?	Possible External IP Disclosure	Low
https://www.glesec.com/	No SPF record found	Low
https://www.glesec.com/	HTTP Strict Transport Security (HSTS) not implemented	Low
https://www.glesec.com/	CSP header not implemented	Low
https://www.glesec.com/	CSP header not implemented	Low
https://www.glesec.com/	ClickJacking - X-Frame-Options header missing	Low
https://www.glesec.com/	WordPress - User Disclosure	Medium
https://www.glesec.com/	jQuery - CVE-2020-23064	Medium
https://www.glesec.com/	jQuery - CVE-2020-11023	Medium
https://www.glesec.com/	jQuery - CVE-2020-11022	Medium
https://www.glesec.com/	jQuery - CVE-2019-11358	Medium
https://www.glesec.com/	jQuery - CVE-2015-9251	Medium
https://www.glesec.com/wp-content/plugins/the-events-calendar/common/vendor/composer/installed.json	Development configuration files	Medium
https://www.glesec.com/calendar/action{new_param0}	Subresource Integrity (SRI)	Low
https://www.glesec.com/	Subresource Integrity (SRI)	Low
https://www.glesec.com/test/	Subresource Integrity (SRI)	Low
https://www.glesec.com/test/	Possible External IP Disclosure	Low

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

TLP:AMBER

ASM-VP REPORT

GLESEC 07/26/2023

url	vuln_name	severity
https://www.glesec.com/terminator-antivirus-killer-is-a-vulnerable-windows-drive r-in-disguise/	Possible External IP Disclosure	Low
https://www.glesec.com/sitemap.xml	Possible External IP Disclosure	Low
https://www.glesec.com	WAF detected	Informative
https://www.glesec.com/.well-known/security.txt	Security.txt file is missing	Informative
https://www.glesec.com/new-terminator-iocs/	Possible Social Security Number Disclosure	Informative
https://www.glesec.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fwww.glesec.com%2F&format=xml	Possible Secret Key Found	Informative
https://login.microsoftonline.com:443/glesec.com/v2.0/.well-known/openid-configu ration	Microsoft Azure - Domain Tenant ID	Informative
https://www.glesec.com/	TLS/SSL certificate expired in less than 90 days	Low
https://www.glesec.com/calendar/action{new_param0}	Subresource Integrity (SRI)	Low
https://www.glesec.com/calendar/action{new_param0}	Possible External IP Disclosure	Low
https://www.glesec.com/	No SPF record found	Low
https://www.glesec.com/	HTTP Strict Transport Security (HSTS) not implemented	Low
https://www.glesec.com/	CSP header not implemented	Low
https://www.glesec.com/	ClickJacking - X-Frame-Options header missing	Low
https://www.glesec.com/	WordPress - User Disclosure	Medium
https://www.glesec.com/	jQuery - CVE-2020-23064	Medium
https://www.glesec.com/	jQuery - CVE-2020-11023	Medium
https://www.glesec.com/	jQuery - CVE-2020-11022	Medium

ASM-VP REPORT

GLESEC 07/26/2023

url	vuln_name	severity
https://www.glesec.com/	jQuery - CVE-2019-11358	Medium
https://www.glesec.com/	jQuery - CVE-2015-9251	Medium
https://www.glesec.com/wp-content/plugins/the-events-calendar/common/vendor/composer/installed.json	Development configuration files	Medium
https://www.glesec.com	WAF detected	Informative
https://www.glesec.com/.well-known/security.txt	Security.txt file is missing	Informative
https://www.glesec.com/terminator-antivirus-killer-is-a-vulnerable-windows-drive r-in-disguise/	Possible Social Security Number Disclosure	Informative
https://www.glesec.com/author/matthewdavid/	Possible Social Security Number Disclosure	Informative
https://www.glesec.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fwww.glesec.com%2F	Possible Secret Key Found	Informative
https://login.microsoftonline.com:443/glesec.com/v2.0/.well-known/openid-configu ration	Microsoft Azure - Domain Tenant ID	Informative
https://www.glesec.com/	TLS/SSL certificate expired in less than 90 days	Low
https://www.glesec.com	WAF detected	Informative
https://www.glesec.com/.well-known/security.txt	Security.txt file is missing	Informative
https://www.glesec.com/events/category/skywatch/	Possible Social Security Number Disclosure	Informative
https://login.microsoftonline.com:443/glesec.com/v2.0/.well-known/openid-configu ration	Microsoft Azure - Domain Tenant ID	Informative
https://www.glesec.com/	TLS/SSL certificate expired in less than 90 days	Low
https://www.glesec.com/calendar/action{new_param0}	Subresource Integrity (SRI)	Low
https://www.glesec.com/calendar/action{new_param0}	Possible External IP Disclosure	Low
https://www.glesec.com/	No SPF record found	Low

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

url	vuln_name	severity
https://www.glesec.com/	HTTP Strict Transport Security (HSTS) not implemented	Low

MSS-EPCM

Devices Reporting Home

34

Top 5 Vulnerable Devices

Device	High_Severity	Medium_Severity	Low_Severity	Total_Severity
DC-02	14	14	1	29
DC-01	15	12	1	28
GMSA-LAB	8	16	3	27
USASYSTEMSWS02	8	17	1	26
WINDEV	7	15	4	26

Top 5 Alerts

Signature
Dangerous low level privilege granted: Network Access
Dangerous privilege granted: Log on as a Batch
Dangerous privilege granted: Log on as a Service
Computer is providing Network File Shares
Users who can access Locally to the Domain Controller.

Hosts by Version

Version	Hosts
1.22.0609.0	34

ASM-VP REPORT

GLESEC 07/26/2023

Top 10 Weaknesses

signature	severity	count	percent
Windows Defender Credential Guard disabled	medium	25	4%
TLS Recent Events	medium	25	4%
PowerShell should only allow signed policies to run	low	25	4%
Accessing Shares Anonymously	medium	25	4%
Windows Updates or WSUS are misconfigured	medium	24	4%
Suspicious Task Scheduler Event Deleted	high	23	4%
Dangerous privilege granted: Deny log on Locally	medium	23	4%
Dangerous privilege granted: Allow log on Locally	medium	23	4%
Autorun Programs List	medium	23	4%
Dangerous low level privilege granted: Network Access	high	21	3%

MSS-BRAND

Brand

Name	Id
Glesec	5

Cease and Desist Items

CurrentScore	PreviousScore	Domain
88.4	88.4	globalbankingandfinance.com
59.98	59.98	slintel.com
41.63	41.63	enterpriseflorida.com

Security Alert

Module	Url	Title	Type	Priority
Website	https://estrategiasecreta.cloud	estrategiasecreta.cloud	NewDomain	Low
Website	https://strugglesociety.cfd	strugglesociety.cfd	NewDomain	Low
Website	https://hablainglescomonativo.com	hablainglescomonativo.com	NewDomain	Low
Website	https://aprendendoinglescomagringa.fun	aprendendoinglescomagringa.fun	NewDomain	Low
Website	https://adultsinglescanada.com	adultsinglescanada.com	NewDomain	Low
Website	https://wagglescreations.com	wagglescreations.com	NewDomain	Low

LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

TLP:AMBER

ASM-VP REPORT

GLESEC 07/26/2023

Module	Url	Title	Type	Priority
Website	https://aestrategiasecreta.fun	aestrategiasecreta.fun	NewDomain	Low
Website	https://savinglacecharleston.com	savinglacecharleston.com	NewDomain	Low
Website	https://skyndirtylittlesecret.com	skyndirtylittlesecret.com	NewDomain	Low
Website	https://doubledtroublesecurityllc.com	doubledtroublesecurityllc.com	NewDomain	Low
Website	https://estrategiasecreta-nh.com	estrategiasecreta-nh.com	NewDomain	Low
Website	https://gicsecurityaudit.com	gicsecurityaudit.com	NewDomain	Low
Website	https://responsiblesecurity.com	responsiblesecurity.com	NewDomain	Low
Website	https://eaglesconnect.co.uk	eaglesconnect.co.uk	NewDomain	Low
Website	https://eaglescar.uk	eaglescar.uk	NewDomain	Low
Website	https://teenagesecrets.com	teenagesecrets.com	NewDomain	Low
Website	https://schoolagesecrets.com	schoolagesecrets.com	NewDomain	Low
Website	https://inglesconliliana.com	inglesconliliana.com	NewDomain	Low
Website	https://stgeorgesecurity-login.com	stgeorgesecurity-login.com	NewDomain	Low
Website	https://laughingleech.com	laughingleech.com	NewDomain	Low
Website	https://wagsnwigglesdc.com	wagsnwigglesdc.com	NewDomain	Low
Website	https://prestigesecured.com	prestigesecured.com	NewDomain	Low
Website	https://eaglesceneryhotel.com	eaglesceneryhotel.com	NewDomain	Low
Website	https://stjamesstoragesecurity.com	stjamesstoragesecurity.com	NewDomain	Low
Website	https://stgeorgesecretforweightloss.com	stgeorgesecretforweightloss.com	NewDomain	Low
Website	https://bigesecurity.com	bigesecurity.com	NewDomain	Low
Website	https://aprendeinglesconivan.com	aprendeinglesconivan.com	NewDomain	Low
Website	https://glazecreate.com	glazecreate.com	NewDomain	Low
Website	https://egliseconnect.com	egliseconnect.com	NewDomain	Low
Website	https://triangledecor.com	triangledecor.com	NewDomain	Low
Website	https://boylesecrets.com	boylesecrets.com	NewDomain	Low
Website	https://noblesecurityboxinsurance.com	noblesecurityboxinsurance.com	NewDomain	Low
Website	https://gleecopotamus.site	gleecopotamus.site	NewDomain	Low
Website	https://howlongisshinglescontagious.site	howlongisshinglescontagious.site	NewDomain	Low
Website	https://anglesccs.link	anglesccs.link	NewDomain	Low
Website	https://idyllicsinglesconnect.com	idyllicsinglesconnect.com	NewDomain	Low
Website	https://gleefulsinglesconnect.com	gleefulsinglesconnect.com	NewDomain	Low
Website	https://estrategiasecreta.website	estrategiasecreta.website	NewDomain	Low
Website	https://jinglesycanciones.com	jinglesycanciones.com	NewDomain	Low
Website	https://harveyslittlesecret.com	harveyslittlesecret.com	NewDomain	Low
Website	https://upliftingsinglesconnect.com	upliftingsinglesconnect.com	NewDomain	Low
Website	https://inglescomounnativo.com	inglescomounnativo.com	NewDomain	Low
Website	https://charmingsinglesconnecthere.com	charmingsinglesconnecthere.com	NewDomain	Low
Website	https://eaglesecuritywatch.com	eaglesecuritywatch.com	NewDomain	Low
Website	https://guardianangelsecurityinc.com	guardianangelsecurityinc.com	NewDomain	Low
Website	https://ingagesecurlty.com	ingagesecurlty.com	NewDomain	Low
Website	https://onepagesecurity.com	onepagesecurity.com	NewDomain	Low
Website	https://jumglescount.com	jumglescount.com	NewDomain	Low
Website	https://junglescoffee.com	junglescoffee.com	NewDomain	Low
Website	https://trianglescroll.shop	trianglescroll.shop	NewDomain	Low
Website	https://clubbeagleschile.com	clubbeagleschile.com	NewDomain	Low
Website	https://estrategiasecreta.xyz	estrategiasecreta.xyz	NewDomain	Low

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

TLP:AMBER

ASM-VP REPORT

GLESEC 07/26/2023

Module	Url	Title	Type	Priority
Website	https://gamblesecond.com	gamblesecond.com	NewDomain	Low
Website	https://castlesecuritytoronto.com	castlesecuritytoronto.com	NewDomain	Low
Website	https://singleschat.info	singleschat.info	NewDomain	Low
Website	https://eaglesecuirty.com	eaglesecuirty.com	NewDomain	Low
Website	https://stgeorgesecure-alert.com	stgeorgesecure-alert.com	NewDomain	Low
Website	https://voltagesecure.com	voltagesecure.com	NewDomain	Low
Website	https://triangleecomm.com	triangleecomm.com	NewDomain	Low
Website	https://junglescoutmall.com	junglescoutmall.com	NewDomain	Low
Website	https://15924swglazect.com	15924swglazect.com	NewDomain	Low
Website	https://blueaglesoccer.com	blueaglesoccer.com	NewDomain	Low
Website	https://estrategiasecretainfo.online	estrategiasecretainfo.online	NewDomain	Low
Website	https://onlinearbitragesecrets.com	onlinearbitragesecrets.com	NewDomain	Low
Website	https://lowvoltagesecuritysystems.com	lowvoltagesecuritysystems.com	NewDomain	Low
Website	https://glsecom.com	glsecom.com	NewDomain	Low
Website	https://gogglesclub.com	gogglesclub.com	NewDomain	Low
Website	https://castlesecuritytoronto.online	castlesecuritytoronto.online	NewDomain	Low
Website	https://junglesecret34.com	junglesecret34.com	NewDomain	Low
Website	https://httpcreativeedgesecuritysys.com	httpcreativeedgesecuritysys.com	NewDomain	Low
Website	https://chargesecur.com	chargesecur.com	NewDomain	Low
Website	https://englesconstruction.com	englesconstruction.com	NewDomain	Low
Website	https://knoxeaglesconcretecorp.com	knoxeaglesconcretecorp.com	NewDomain	Low
Website	https://georgiasecureliving.com	georgiasecureliving.com	NewDomain	Low
Website	https://estrategiasecret.com	estrategiasecret.com	NewDomain	Low
Website	https://pagesecond.shop	pagesecond.shop	NewDomain	Low
Website	https://tiangesec.top	tiangesec.top	NewDomain	Low
Website	https://estategiasecreta.online	estategiasecreta.online	NewDomain	Low
Website	https://xn--estratgiasecreta-gqb.site	estratégiasecreta.site (xn--estratgiasecreta-gqb.site)	NewDomain	Low
Website	https://beaglecachorro.shop	beaglecachorro.shop	NewDomain	Low
Website	https://eaglescleaningclt.com	eaglescleaningclt.com	NewDomain	Low
Website	https://strategiesicure.com	strategiesicure.com	NewDomain	Low
Website	https://portdouglasaccommodationatseatempleresort.com	portdouglasaccommodationatseatempleresort.com	NewDomain	Low
Website	https://raowhaslittlesecret.com	raowhaslittlesecret.com	NewDomain	Low
Website	https://inglescomagringa.cloud	inglescomagringa.cloud	NewDomain	Low
Website	https://eaglescout.app	eaglescout.app	NewDomain	Low
Website	https://yaglisac.online	yaglisac.online	NewDomain	Low
Website	https://yaglisacbakimi.online	yaglisacbakimi.online	NewDomain	Low
Website	https://yaglisac.site	yaglisac.site	NewDomain	Low
Website	https://yaglisacbakimi.site	yaglisacbakimi.site	NewDomain	Low
Website	https://saggesecranes.com	saggesecranes.com	NewDomain	Low
Website	https://bayridgesecuritiesgroup.com	bayridgesecuritiesgroup.com	NewDomain	Low
Website	https://inglescompaula.com	inglescompaula.com	NewDomain	Low
Website	https://theeaglescharlotte.com	theeaglescharlotte.com	NewDomain	Low
Website	https://aprendainglescompaula.com	aprendainglescompaula.com	NewDomain	Low
Website	https://theeaglescleveland.com	theeaglescleveland.com	NewDomain	Low
Website	https://losangelesecom.com	losangelesecom.com	NewDomain	Low

TLP:AMBER

ASM-VP REPORT

GLESEC 07/26/2023

Module	Url	Title	Type	Priority
Website	https://georgiasecuritypros.com	georgiasecuritypros.com	NewDomain	Low
Website	https://glazecolor.com	glazecolor.com	NewDomain	Low
Website	https://gleecl.space	gleecl.space	NewDomain	Low
Website	https://aestrategiasecreta.online	aestrategiasecreta.online	NewDomain	Low
Website	https://xn--estratgiasecreta-gqb.online	estratégiasecreta.online (xn--estratgiasecreta-gqb.online)	NewDomain	Low
Website	https://theterriblesecretof.space	theterriblesecretof.space	NewDomain	Low
Website	https://eagleecom7.com	eagleecom7.com	NewDomain	Low
Website	https://junglescoutmarket.com	junglescoutmarket.com	NewDomain	Low
Website	https://eagleescort.com	eagleescort.com	NewDomain	Low
Website	https://stgeorgesecurity-alert.com	stgeorgesecurity-alert.com	NewDomain	Low
Website	https://rdgesecu.cfd	rdgesecu.cfd	NewDomain	Low
Website	https://inglescomopedro.com	inglescomopedro.com	NewDomain	Low
Website	https://goooglescholar.com	goooglescholar.com	NewDomain	Low
Website	https://movillagesecondlanding.com	movillagesecondlanding.com	NewDomain	Low
Website	https://wingleecreative.com	wingleecreative.com	NewDomain	Low
Website	https://estrategiasecreta.shop	estrategiasecreta.shop	NewDomain	Low
Website	https://portdouglasaccommodationatseatempleresort.store	portdouglasaccommodationatseatempleresort.store	NewDomain	Low
Website	https://grandangleeco.link	grandangleeco.link	NewDomain	Low
Website	https://googlssec.top	googlssec.top	NewDomain	Low
Website	https://thebestselfstoragesecrets.com	thebestselfstoragesecrets.com	NewDomain	Low
Website	https://eaglesclimbing.com	eaglesclimbing.com	NewDomain	Low
Website	https://thesinglescruise.com	thesinglescruise.com	NewDomain	Low
Website	https://inglesacademico.com	inglesacademico.com	NewDomain	Low
Website	https://eaglesacramentoschool.com	eaglesacramentoschool.com	NewDomain	Low
Website	https://inglescontex.online	inglescontex.online	NewDomain	Low
Website	https://estrategiasecreta.store	estrategiasecreta.store	NewDomain	Low
Website	https://glazecfjl.sbs	glazecfjl.sbs	NewDomain	Low
Website	https://yaglisac.com	yaglisac.com	NewDomain	Low
Website	https://yaglisacbakimi.com	yaglisacbakimi.com	NewDomain	Low
Website	https://trunglexeco.com	trunglexeco.com	NewDomain	Low
Website	https://singleschatonline69.com	singleschatonline69.com	NewDomain	Low
Website	https://urbanglazecr.com	urbanglazecr.com	NewDomain	Low
Website	https://tapicesparamueblesec.com	tapicesparamueblesec.com	NewDomain	Low
Website	https://inglescomfoco.online	inglescomfoco.online	NewDomain	Low
Website	https://junglescape.world	junglescape.world	NewDomain	Low
Website	https://inglescomfoco.store	inglescomfoco.store	NewDomain	Low
Website	https://glosecret.top	glosecret.top	NewDomain	Low
Website	https://glosecret.shop	glosecret.shop	NewDomain	Low
Website	https://glosecret.store	glosecret.store	NewDomain	Low
Website	https://singlesocks.shop	singlesocks.shop	NewDomain	Low
Website	https://glescore.com	glescore.com	NewDomain	Low
Website	https://estrategiasecretanh.com	estrategiasecretanh.com	NewDomain	Low
Website	https://hoanggiasecurity.com	hoanggiasecurity.com	NewDomain	Low
Website	https://globalstrategicsecurityinc.com	globalstrategicsecurityinc.com	NewDomain	Low
Website	https://moattitlesecurity.com	moattitlesecurity.com	NewDomain	Low

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

TLP:AMBER

ASM-VP REPORT

GLESEC 07/26/2023

Module	Url	Title	Type	Priority
Website	https://pebblesecurity.com	pebblesecurity.com	NewDomain	Low
Website	https://anglescreen.live	anglescreen.live	NewDomain	Low
Website	https://estrategiasecretant.shop	estrategiasecretant.shop	NewDomain	Low
Website	https://viaggiesicurezza.com	viaggiesicurezza.com	NewDomain	Low
Website	https://estrategiasecretanh.site	estrategiasecretanh.site	NewDomain	Low
Website	https://hedgesecurities.com	hedgesecurities.com	NewDomain	Low
Website	https://www.trianglesecondaryschool.com	trianglesecondaryschool.com	NewDomain	Low
Website	https://www.acuanglesecurity.com	acuanglesecurity.com	NewDomain	Low
Website	http://www.imparaingleseconme.com	imparaingleseconme.com	NewDomain	Low
Website	http://www.googlesecurityproducts.com	googlesecurityproducts.com	NewDomain	Low
Website	http://glesec.net	glesec.net	RelevantContentAddition	Low
Website	https://www.simulationinformation.com	simulationinformation.com	RelevantContentAddition	Low
Website	https://aeroleads.com	aeroleads.com	RelevantContentAddition	Low
Website	https://pa.computrabajo.com	pa.computrabajo.com	RelevantContentAddition	Low
Website	https://www.apollo.io	apollo.io	RelevantContentAddition	Low
Website	http://members.hispanicchamberorlando.com	members.hispanicchamberorlando.com	RelevantContentAddition	Low
Website	https://www.northeaglesecurityservices.com	northeaglesecurityservices.com	NewDomain	Low
Website	https://agesecure.live	agesecure.live	NewDomain	Low
Website	https://gleecookers.com	gleecookers.com	NewDomain	Low
Website	https://eagleeconsultingllc.com	eagleeconsultingllc.com	NewDomain	Low
Website	https://inglescomclara.com	inglescomclara.com	NewDomain	Low
Website	https://vigilanteaglesecurity.com	vigilanteaglesecurity.com	NewDomain	Low
Website	https://beigesecurities.com	beigesecurities.com	NewDomain	Low
Website	https://gaugesecurity.com	gaugesecurity.com	NewDomain	Low
Website	https://hiddenstrugglescoaching.com	hiddenstrugglescoaching.com	NewDomain	Low

LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

Vulnerability

MSS-EPM

Total Patches Deployed

0

Total Failed Patch Deployments

0

Number of Machines Deployed To

0

MSS-BAS Email

Cymulate Score

10%

Simulation Summary

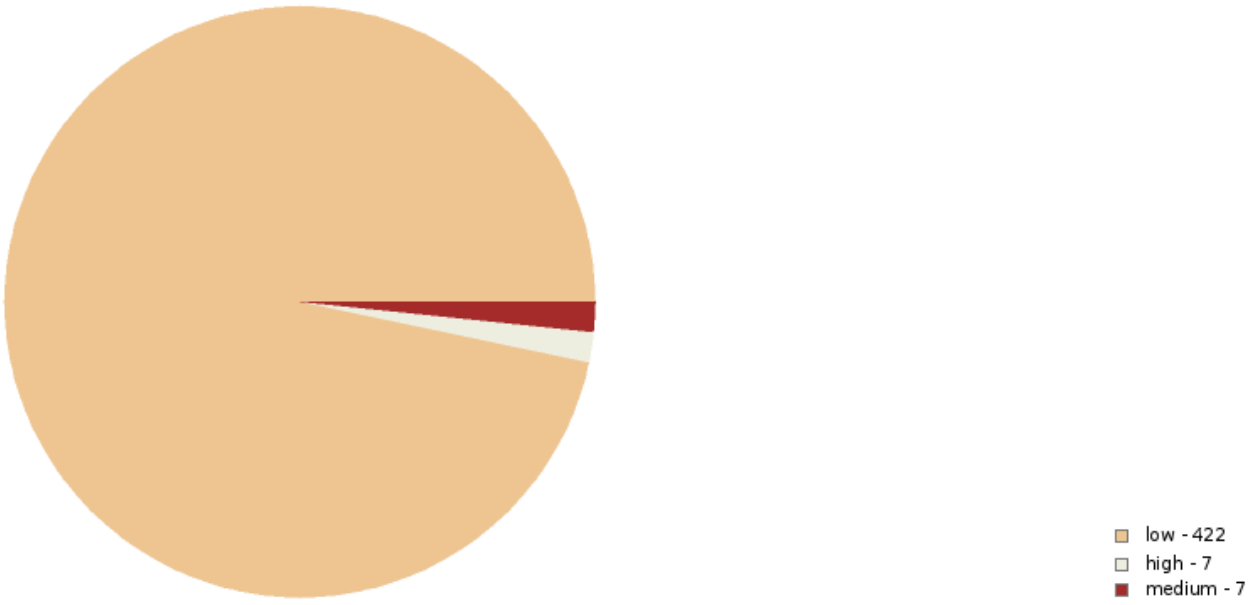
Penetrated : 436 / Total Tests: 4,000

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

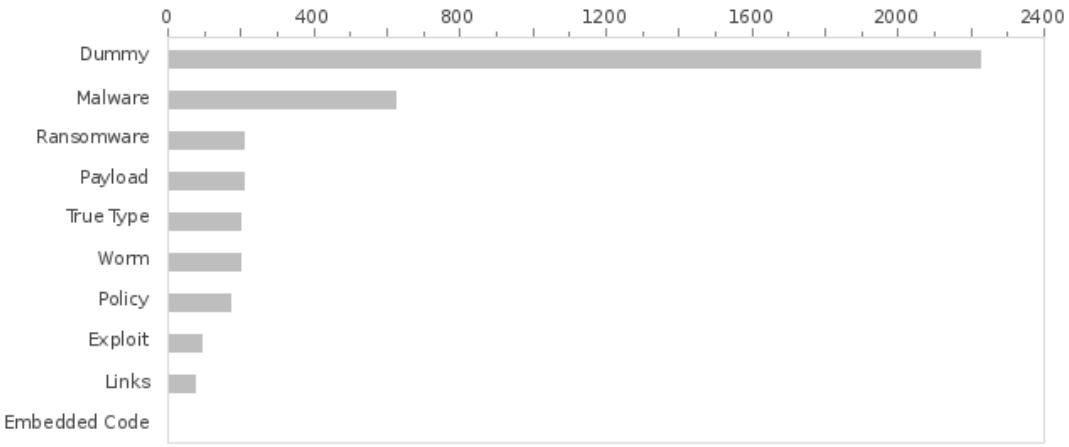
ASM-VP REPORT

GLESEC 07/26/2023

Penetrations by Severity



Emails Sent

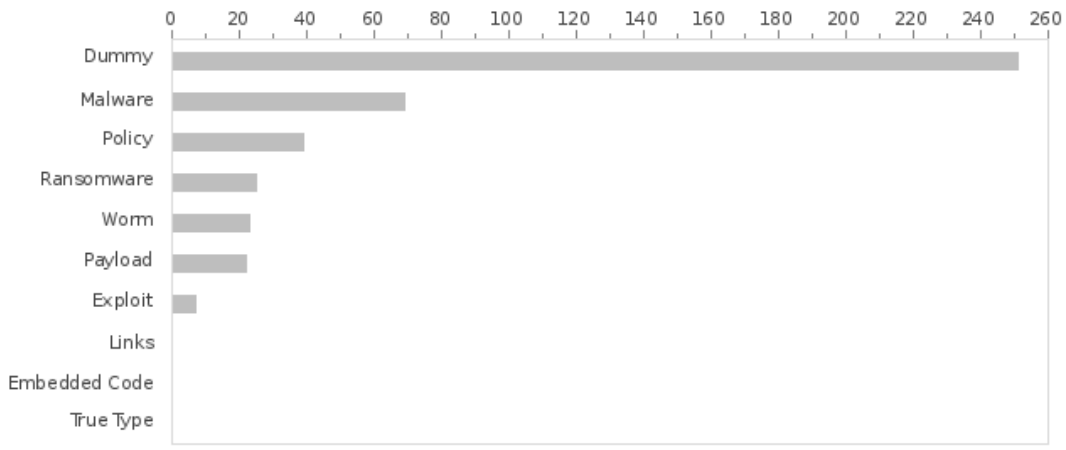


LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

ASM-VP REPORT

GLESEC 07/26/2023

Emails Penetrated



Percent Penetrated

11%

Simulations Sent/Penetrated

Category	Penetrated	Total
Dummy	251	2223
Malware	69	624
Ransomware	25	209
Payload	22	207
True Type	0	200
Worm	23	198
Policy	39	173
Exploit	7	91
Links	0	75
Embedded Code	0	0

MSS-BAS Web

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

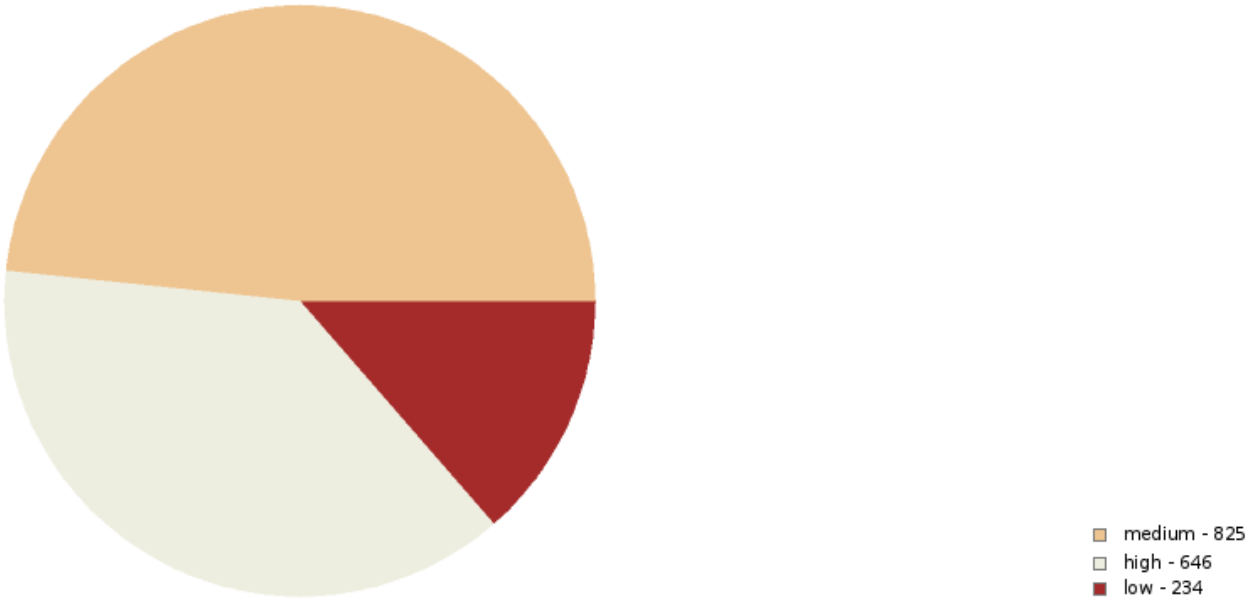
ASM-VP REPORT

GLESEC 07/26/2023

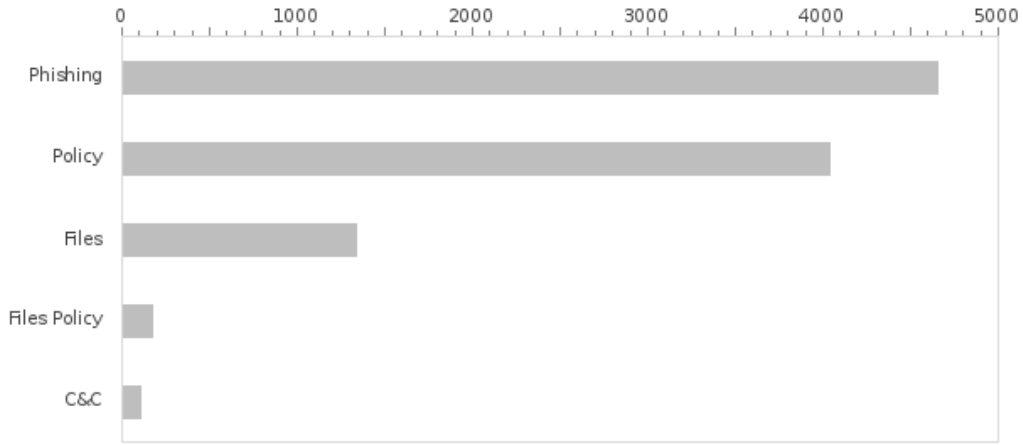
Simulation Summary

Penetrated : 2,483 / Total Tests: 10,299

Penetrations by Severity

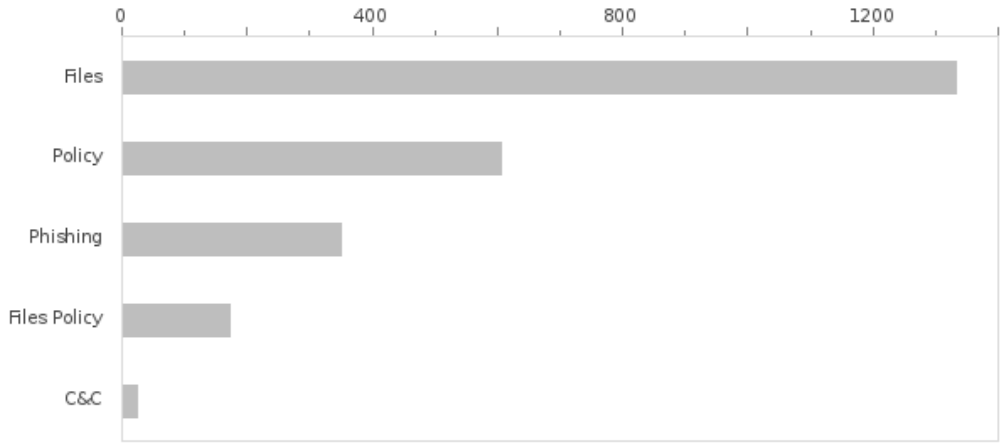


Browsing Sent



LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

Browsing Penetrated



Percent Penetrated

24%

Simulations Sent/Penetrated

Category	Penetrated	Total
Phishing	349	4650
Policy	606	4035
Files	1333	1338
Files Policy	172	174
C&C	23	102

MSS-BAS WAF

Cymulate Score

24%

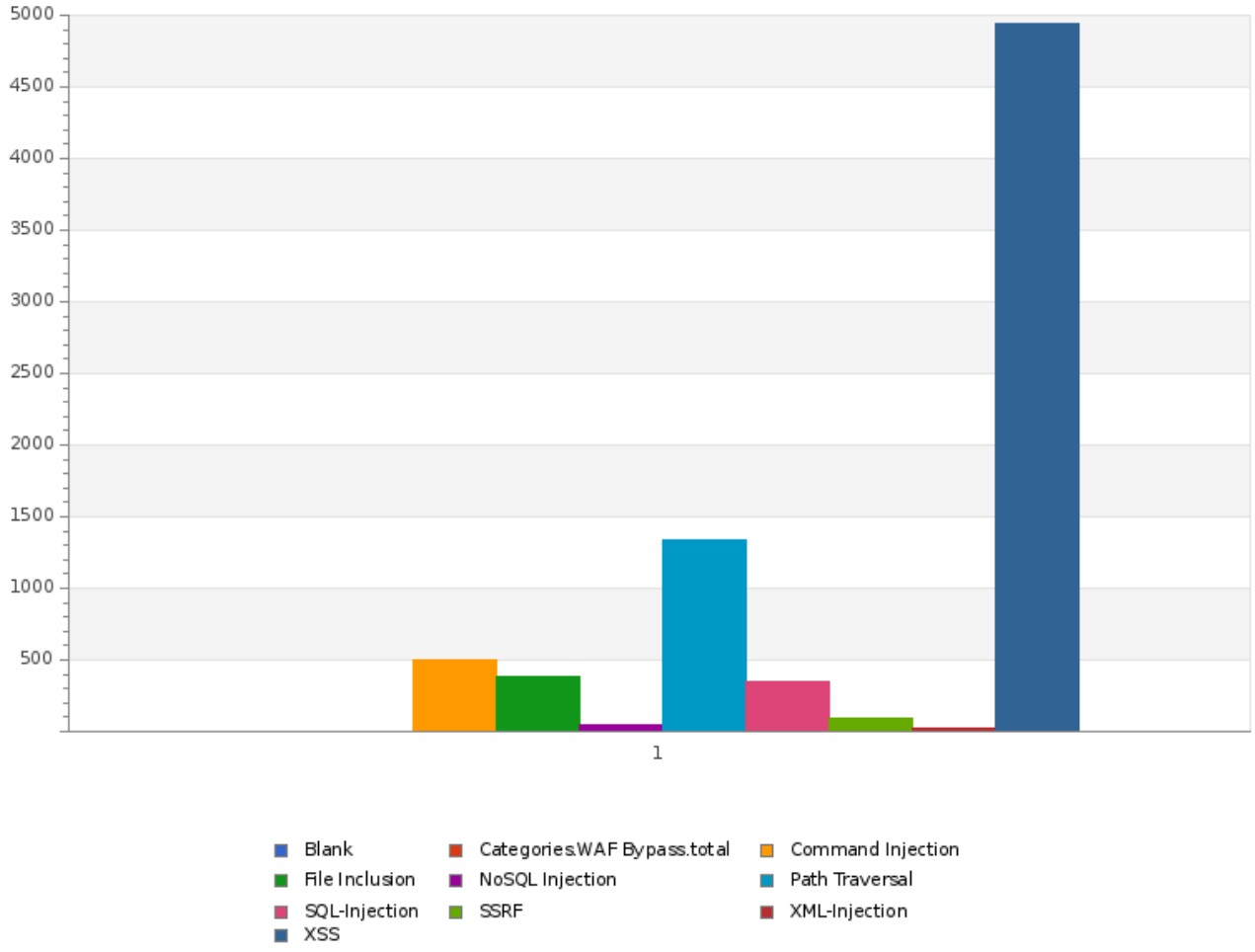
ASM-VP REPORT

GLESEC 07/26/2023

Simulation Summary

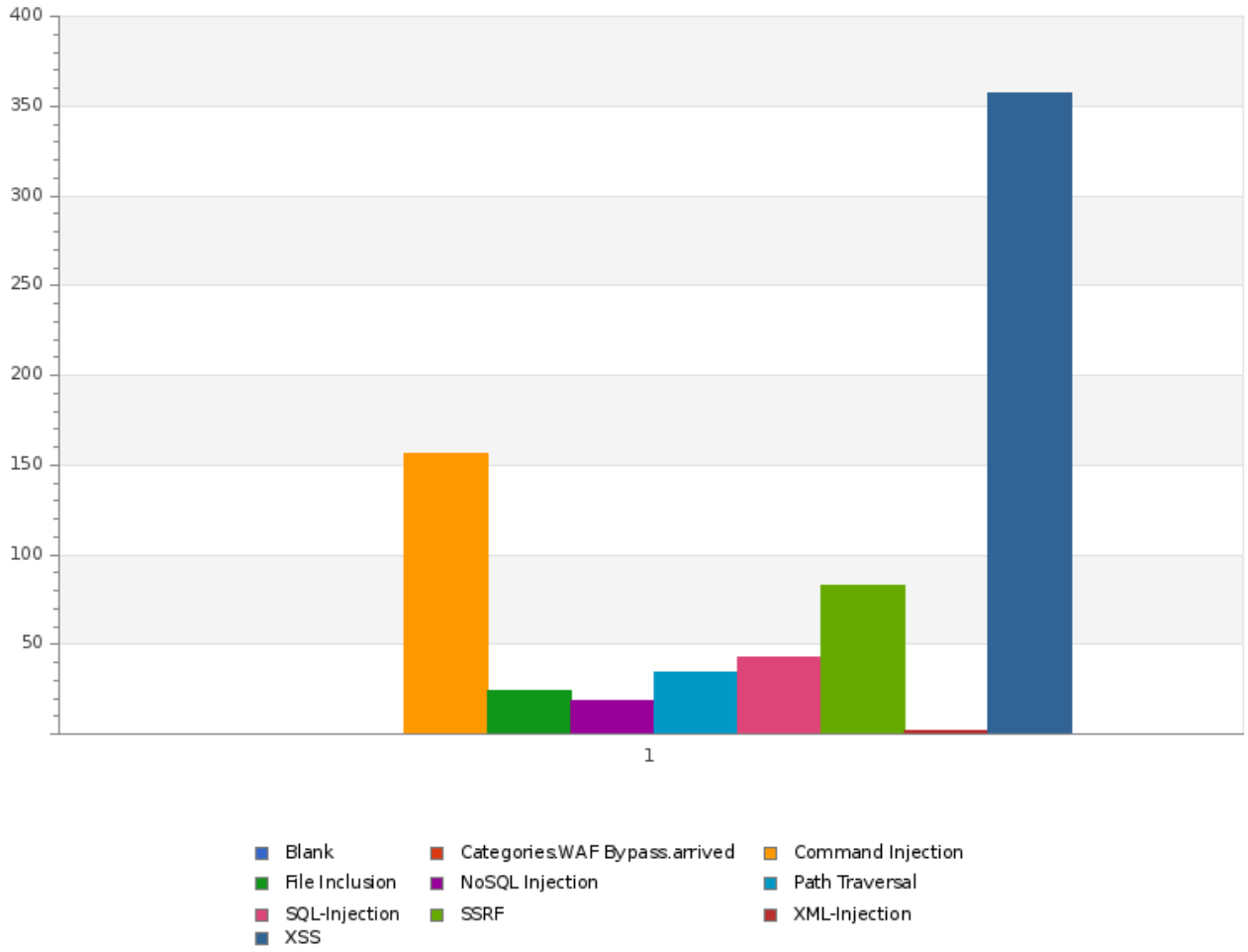
Penetrated : 380 / Total Tests: 7,670

WAF Sent



LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

WAF Penetrated



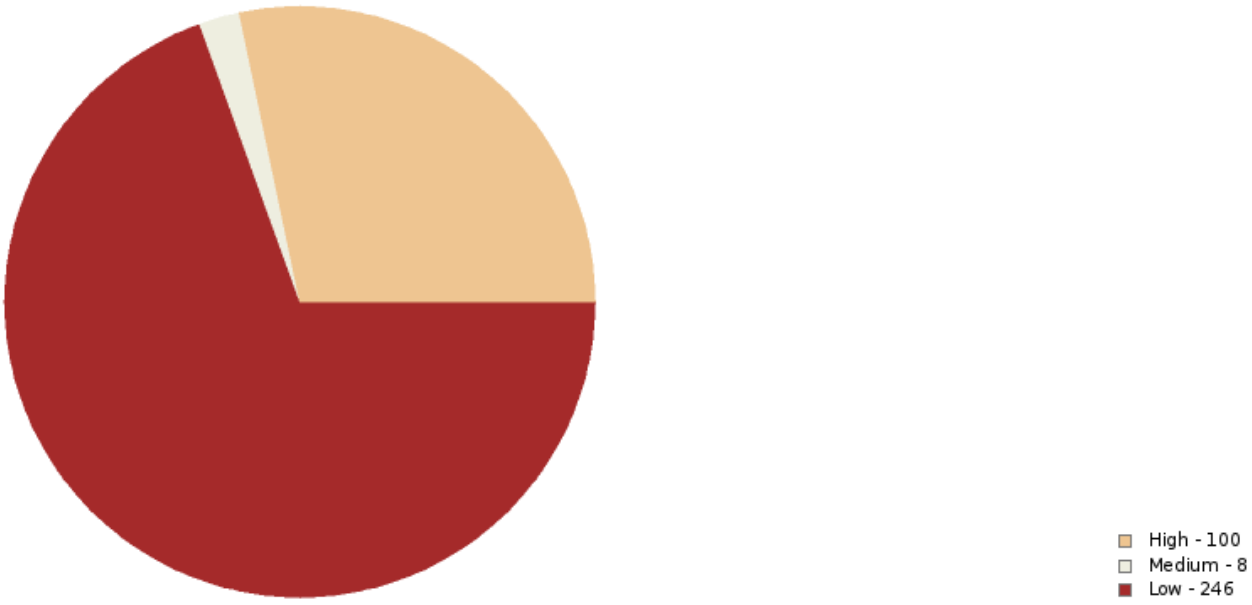
LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

TLP:AMBER

ASM-VP REPORT

GLESEC 07/26/2023

Penetrations by Severity



Percent Penetrated

9%

Simulations Sent/Penetrated

Command Injection	File Inclusion	NoSQL Injection	Path Traversal	SQL-Injection	SSRF	WAF Bypass	XML-Injection	XSS
502	384	41	1332	347	97	0	21	4946

MSS-BAS DLP

Cymulate Score

79%

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

TLP:AMBER

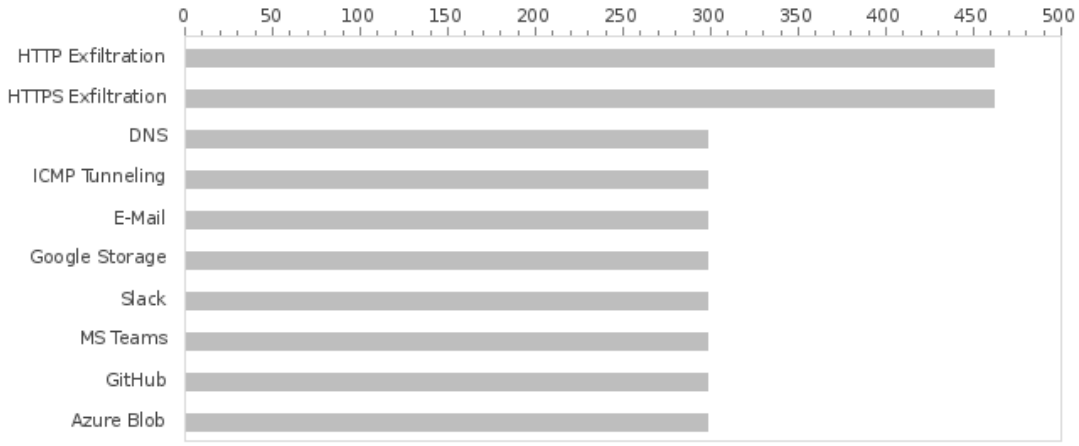
ASM-VP REPORT

GLESEC 07/26/2023

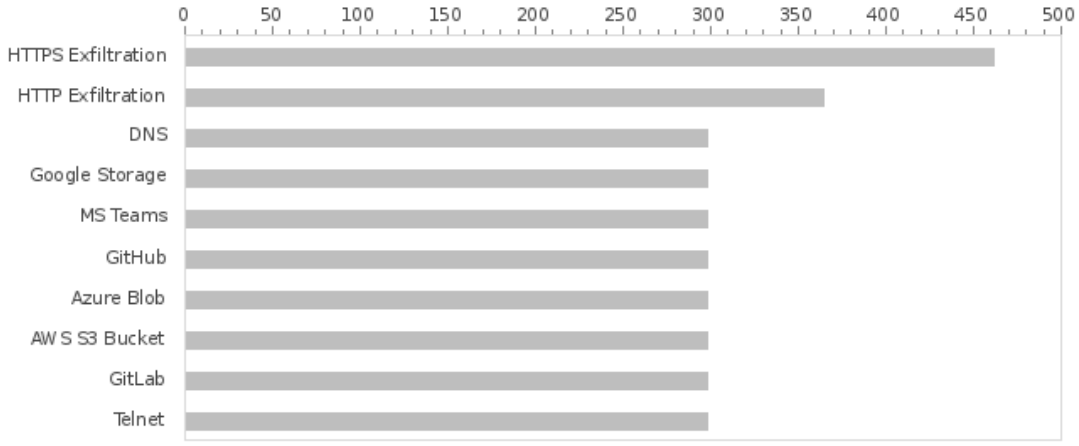
Simulation Summary

Penetrated : 4,403 / Total Tests: 5,427

Simulated Samples Sent



Simulated Samples Penetrated



Least and Most Vulnerable Categories

Least Vulnerable Classification	Most Vulnerable Classification	Least Vulnerable Phrase	Most Vulnerable Phrase
Medical	source code	Printscreen	AWS configuration

LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

Percent Penetrated

81%

Simulations Sent/Penetrated

Category	Penetrated	Total
HTTP Exfiltration	364	462
HTTPS Exfiltration	462	462
DNS	298	298
ICMP Tunneling	297	298
E-Mail	0	298
Google Storage	298	298
Slack	266	298
MS Teams	298	298
GitHub	298	298
Azure Blob	298	298
AWS S3 Bucket	298	298
GitLab	298	298
Telnet	298	298
Removable Device	0	265
Google Drive	265	265
One Drive	0	265
SFTP	234	265
Browser Http	33	33
Browser Https	33	33
DNS Tunneling	32	33
Open Ports	33	33
Gmail + Append	0	33

MSS-BAS LM

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

Lateral Movement Assessment Score

0%

Credentials Scraped

Databases Found

Endpoints Discovered

Local Admin Accounts Discovered

Endpoints Reached

Network Shares Discovered

Servers Discovered

Domain Admin Accounts Discovered

Webservers Discovered

Workstations Discovered

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

Security Validation

MSS-BAS Phishing

Cymulate Score

0%

Simulation Summary

Sent: 3, Opened: 2, Clicked: 2, Cred: 0

Clicked Links

output: 2<small style="color:#438864;">+2</small>

Credentials Harvested

output: 0<small style="color:#438864;">+0</small>

Opened Emails

output: 2<small style="color:#438864;">+2</small>

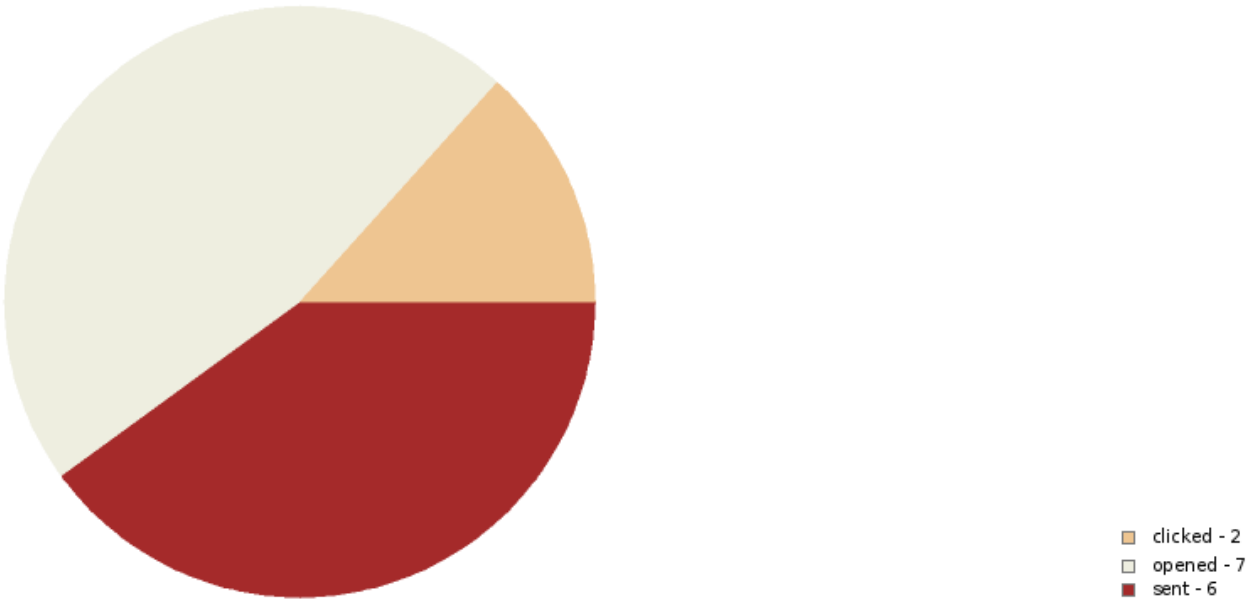
LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

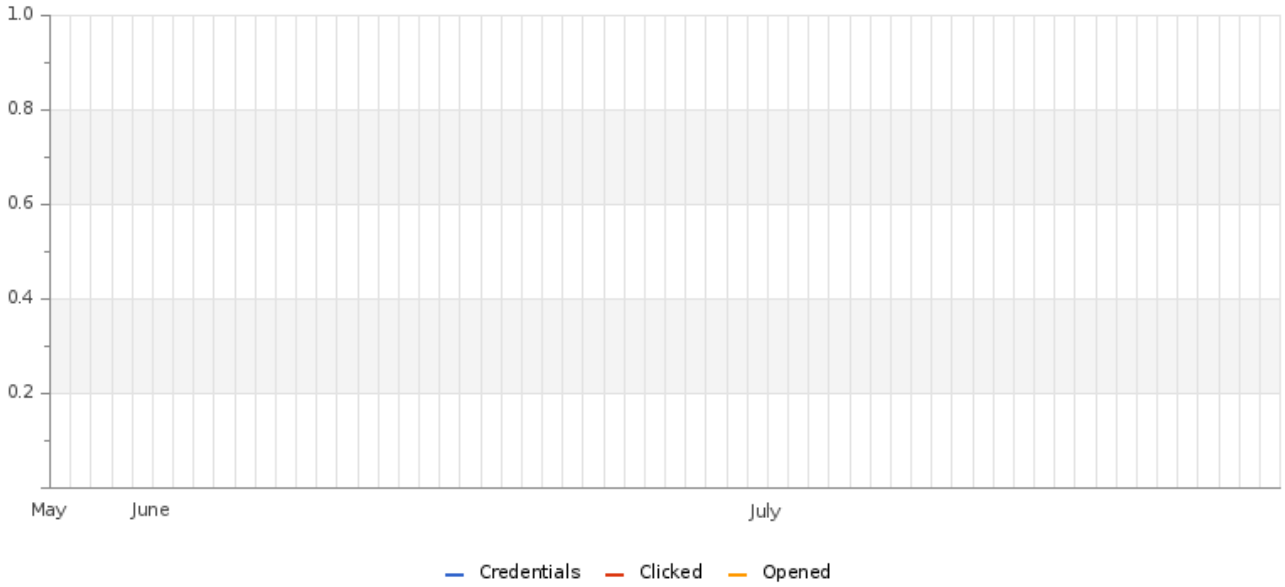
ASM-VP REPORT

GLESEC 07/26/2023

Phishing Sent



Phishing Penetrated



LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

TLP:AMBER

ASM-VP REPORT

GLESEC 07/26/2023

Simulations Sent/Penetrated

Category	Penetrated	Total
Dummy	251	2223
Malware	69	624
Ransomware	25	209
Payload	22	207
True Type	0	200
Worm	23	198
Policy	39	173
Exploit	7	91
Links	0	75
Embedded Code	0	0

MSS-BAS EDR

Simulation Summary

Penetrated : 0 / Sent : 0

Worm based code execution

penetrated : 0 / Total tests : 0

Percent Penetrated

%

MSS-BAS IMTHREAT

Cymulate Score

48%

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

TLP:AMBER

ASM-VP REPORT

GLESEC 07/26/2023

Percent Penetrated

37%

Simulation Summary

Penetrated: 634 / Total: 1,402

Immediate Threats Campaigns

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-07-26	India Cert Alert - Mallox Ransomware Targeting Unsecured MS SQL Servers	Mallboxbgjadhhiij6_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-07-26	India Cert Alert - Mallox Ransomware Targeting Unsecured MS SQL Servers	Mallboxbgjadhhiij11_edrPs1.ps1	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-07-26	India Cert Alert - Mallox Ransomware Targeting Unsecured MS SQL Servers	Mallboxbgjadhhiij8_edrPs1.ps1	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-07-26	India Cert Alert - Mallox Ransomware Targeting Unsecured MS SQL Servers	Mallboxbgjadhhiij14_edrBat.bat	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-07-26	India Cert Alert - Mallox Ransomware Targeting Unsecured MS SQL Servers	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ind ia_cert_alert_-_mallox_ransomware_targeting_unsecured_ms_sql_servers_a88804f4-9ba8-4e9a-89c8-0cf1c679ae06/Mallboxbgjadhhiij9_browsingPs1.ps1?X-Amz-Algorithm=AWS 4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230726%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230726T135059Z&X-Amz-Expires=600&X-Amz-Signature=8f214d46665f6179b81506eaaec3abbaeb6eeb895640af79dc75d6ec1d86f3de&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-26	India Cert Alert - Mallox Ransomware Targeting Unsecured MS SQL Servers	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ind ia_cert_alert_-_mallox_ransomware_targeting_unsecured_ms_sql_servers_a88804f4-9ba8-4e9a-89c8-0cf1c679ae06/Mallboxbgjadhhiij10_browsingPs1.ps1?X-Amz-Algorithm=AW S4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230726%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230726T135059Z&X-Amz-Expires=600&X-Amz-Signature=ce46755d961a872fc3d830dbde362b4776d7a54c3b079e634f88b2835f21ad48&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-26	India Cert Alert - Mallox Ransomware Targeting Unsecured MS SQL Servers	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ind ia_cert_alert_-_mallox_ransomware_targeting_unsecured_ms_sql_servers_a88804f4-9ba8-4e9a-89c8-0cf1c679ae06/Mallboxbgjadhhiij12_browsingPs1.ps1?X-Amz-Algorithm=AW S4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230726%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230726T135058Z&X-Amz-Expires=600&X-Amz-Signature=c707322074f48f164d5c5e5b2e2539529698caaceebfe3f907fcc5e2cbbf0d93&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-26	India Cert Alert - Mallox Ransomware Targeting Unsecured MS SQL Servers	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ind ia_cert_alert_-_mallox_ransomware_targeting_unsecured_ms_sql_servers_a88804f4-9ba8-4e9a-89c8-0cf1c679ae06/Mallboxbgjadhhiij13_browsingPs1.ps1?X-Amz-Algorithm=AW S4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230726%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230726T135053Z&X-Amz-Expires=600&X-Amz-Signature=ee7d2015350a7720bb86e4825b51456d708a8c4c4ff1727f016697a7e062d113&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-26	India Cert Alert - Mallox Ransomware Targeting Unsecured MS SQL Servers	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ind ia_cert_alert_-_mallox_ransomware_targeting_unsecured_ms_sql_servers_a88804f4-9ba8-4e9a-89c8-0cf1c679ae06/Mallboxbgjadhhiij15_browsingBat.bat?X-Amz-Algorithm=AW S4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230726%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230726T135052Z&X-Amz-Expires=600&X-Amz-Signature=af08cb46f5c648e8fa340ad671085d4ea16dd4005c71a820ebd0614fea92b145&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated

TLP:AMBER

ASM-VP REPORT

GLESEC 07/26/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-07-26	India Cert Alert - Mallox Ransomware Targeting Unsecured MS SQL Servers	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ind ia_cert_alert_-_mallox_ransomware_targeting_unsecured_ms_sql_servers_a88804f4-9b a8-4e9a-89c8-0cf1c679ae06/Mallboxbgjadhhiij1_browsingExe.exe?X-Amz-Algorithm=AWS 4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3 D5GWFTK3Q%2F20230726%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230726T135052Z &X-Amz-Expires=600&X-Amz-Signature=d7ebd57c87368b5583c0945bd25b7ed693ccf2f676d16 2f0035059776f1ba10f&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-26	India Cert Alert - Mallox Ransomware Targeting Unsecured MS SQL Servers	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ind ia_cert_alert_-_mallox_ransomware_targeting_unsecured_ms_sql_servers_a88804f4-9b a8-4e9a-89c8-0cf1c679ae06/Mallboxbgjadhhiij2_browsingExe.exe?X-Amz-Algorithm=AWS 4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3 D5GWFTK3Q%2F20230726%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230726T135051Z &X-Amz-Expires=600&X-Amz-Signature=d47ee61abe46dd834d09e73288f01e95aeb4400b3e6d6 dc0d34b82251de30f16&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-26	India Cert Alert - Mallox Ransomware Targeting Unsecured MS SQL Servers	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ind ia_cert_alert_-_mallox_ransomware_targeting_unsecured_ms_sql_servers_a88804f4-9b a8-4e9a-89c8-0cf1c679ae06/Mallboxbgjadhhiij3_browsingExe.exe?X-Amz-Algorithm=AWS 4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3 D5GWFTK3Q%2F20230726%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230726T135051Z &X-Amz-Expires=600&X-Amz-Signature=afe7626c5d171efbfdf81916630ce42a47326c560a034 77f3a59cfeddceb315d&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-26	India Cert Alert - Mallox Ransomware Targeting Unsecured MS SQL Servers	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ind ia_cert_alert_-_mallox_ransomware_targeting_unsecured_ms_sql_servers_a88804f4-9b a8-4e9a-89c8-0cf1c679ae06/Mallboxbgjadhhiij4_browsingExe.exe?X-Amz-Algorithm=AWS 4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3 D5GWFTK3Q%2F20230726%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230726T135051Z &X-Amz-Expires=600&X-Amz-Signature=e6de879a33f5489a0a54f4dd850b3732140747fef5715 ba52d2dfdebbbee4a3a&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-26	India Cert Alert - Mallox Ransomware Targeting Unsecured MS SQL Servers	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ind ia_cert_alert_-_mallox_ransomware_targeting_unsecured_ms_sql_servers_a88804f4-9b a8-4e9a-89c8-0cf1c679ae06/Mallboxbgjadhhiij5_browsingExe.exe?X-Amz-Algorithm=AWS 4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3 D5GWFTK3Q%2F20230726%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230726T135051Z &X-Amz-Expires=600&X-Amz-Signature=c9d0d70465bbf822168923cace5e63e605db1bc8162f1 c265352f93cf40fd255&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-26	India Cert Alert - Mallox Ransomware Targeting Unsecured MS SQL Servers	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ind ia_cert_alert_-_mallox_ransomware_targeting_unsecured_ms_sql_servers_a88804f4-9b a8-4e9a-89c8-0cf1c679ae06/Mallboxbgjadhhiij_browsing7Exe.exe?X-Amz-Algorithm=AWS 4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3 D5GWFTK3Q%2F20230726%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230726T135050Z &X-Amz-Expires=600&X-Amz-Signature=195e8fdf7a9bbb814bf5670cfca89ae3a12a83143a584 f22b93514328515d47c&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-26	First-ever Open-Source Software Supply Chain Attacks	Firsteverbgjacahebh51_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-07-26	First-ever Open-Source Software Supply Chain Attacks	Firsteverbgjacahebh52_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-07-26	First-ever Open-Source Software Supply Chain Attacks	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/fir st-ever_open-source_software_supply_chain_attacks_6df0d247-55bd-4848-a6e9-ebf2f8 cd6517/Firsteverbgjacahebh54_browsingElf.elf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X- Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F2023 0726%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230726T074811Z&X-Amz-Expires=6 00&X-Amz-Signature=84dcda76c8b6392d6dab737413b7fdc35bd153d63ef40132ebfbea918be83 3bf&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-26	First-ever Open-Source Software Supply Chain Attacks	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/fir st-ever_open-source_software_supply_chain_attacks_6df0d247-55bd-4848-a6e9-ebf2f8 cd6517/Firsteverbgjacahebh49_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X- Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F2023 0726%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230726T074808Z&X-Amz-Expires=6 00&X-Amz-Signature=5a87ea7e041b82f4cc8db31f9deb36a4ca09622edc95c8f68f865322b6a2d b7f&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-26	New Reptile Rootkit Malware Attacking Linux Systems Using Port Knocking	Newbgjadaaiej5_edrO.o	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-26	New Reptile Rootkit Malware Attacking Linux Systems Using Port Knocking	Newbgjadaaiej4_edrO.o	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-26	New Reptile Rootkit Malware Attacking Linux Systems Using Port Knocking	Newbgjadaaiej_edr7Elf.elf	Endpoint Security	GLESEC-AWS-CYMU	Blocked

TLP:AMBER

ASM-VP REPORT

GLESEC 07/26/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-07-26	India Cert Alert - Mallox Ransomware Targeting Unsecured MS SQL Servers	Mallboxbgjadhhiij_edr7Exe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-26	India Cert Alert - Mallox Ransomware Targeting Unsecured MS SQL Servers	Mallboxbgjadhhiij9_edrPs1.ps1	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-07-26	India Cert Alert - Mallox Ransomware Targeting Unsecured MS SQL Servers	Mallboxbgjadhhiij10_edrPs1.ps1	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-07-26	India Cert Alert - Mallox Ransomware Targeting Unsecured MS SQL Servers	Mallboxbgjadhhiij13_edrPs1.ps1	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-07-26	India Cert Alert - Mallox Ransomware Targeting Unsecured MS SQL Servers	Mallboxbgjadhhiij15_edrBat.bat	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-07-26	India Cert Alert - Mallox Ransomware Targeting Unsecured MS SQL Servers	Mallboxbgjadhhiij12_edrPs1.ps1	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-07-26	India Cert Alert - Mallox Ransomware Targeting Unsecured MS SQL Servers	Mallboxbgjadhhiij5_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-26	India Cert Alert - Mallox Ransomware Targeting Unsecured MS SQL Servers	Mallboxbgjadhhiij4_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-26	India Cert Alert - Mallox Ransomware Targeting Unsecured MS SQL Servers	Mallboxbgjadhhiij3_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-26	India Cert Alert - Mallox Ransomware Targeting Unsecured MS SQL Servers	Mallboxbgjadhhiij1_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-26	India Cert Alert - Mallox Ransomware Targeting Unsecured MS SQL Servers	Mallboxbgjadhhiij2_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-26	India Cert Alert - Mallox Ransomware Targeting Unsecured MS SQL Servers	hxxp://185.170.144.153	Web Gateway	GLESEC-AWS-CYMU	Offline/Removed
2023-07-26	India Cert Alert - Mallox Ransomware Targeting Unsecured MS SQL Servers	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ind ia_cert_alert_-_mallox_ransomware_targeting_unsecured_ms_sql_servers_a88804f4-9ba8-4e9a-89c8-0cf1c679ae06/Mallboxbgjadhhiij8_browsingPs1.ps1?X-Amz-Algorithm=AWS 4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230726%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230726T135059Z&X-Amz-Expires=600&X-Amz-Signature=5b9c04c8fb7e4b46c3f8040cde553dd7a7430e74a11925ba19df9ede9bf55770&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

TLP:AMBER

ASM-VP REPORT

GLESEC 07/26/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-07-26	India Cert Alert - Mallox Ransomware Targeting Unsecured MS SQL Servers	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ind ia_cert_alert_-_mallox_ransomware_targeting_unsecured_ms_sql_servers_a88804f4-9b a8-4e9a-89c8-0cf1c679ae06/Mallboxbgjadhhiij11_browsingPs1.ps1?X-Amz-Algorithm=AW S4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q 3D5GWFTK3Q%2F20230726%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230726T135059 Z&X-Amz-Expires=600&X-Amz-Signature=eedbb58010a7745cfd382053833ea75076117d028ddb 0588dad0eac2637bd781&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-26	India Cert Alert - Mallox Ransomware Targeting Unsecured MS SQL Servers	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ind ia_cert_alert_-_mallox_ransomware_targeting_unsecured_ms_sql_servers_a88804f4-9b a8-4e9a-89c8-0cf1c679ae06/Mallboxbgjadhhiij14_browsingBat.bat?X-Amz-Algorithm=AW S4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q 3D5GWFTK3Q%2F20230726%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230726T135052 Z&X-Amz-Expires=600&X-Amz-Signature=b382601102cf631af029b72dba585fbc406e72f9bf97 bb700e027f052b32f29c&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-26	India Cert Alert - Mallox Ransomware Targeting Unsecured MS SQL Servers	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ind ia_cert_alert_-_mallox_ransomware_targeting_unsecured_ms_sql_servers_a88804f4-9b a8-4e9a-89c8-0cf1c679ae06/Mallboxbgjadhhiij6_browsingExe.exe?X-Amz-Algorithm=AWS 4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3 D5GWFTK3Q%2F20230726%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230726T135050Z &X-Amz-Expires=600&X-Amz-Signature=60b63c398b1dedf27cf477d4625a10fcc0b8551b2b229 7951cb402d4385077b5&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-26	First-ever Open-Source Software Supply Chain Attacks	Firsteverbgjacahebh49_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-07-26	First-ever Open-Source Software Supply Chain Attacks	Firsteverbgjacahebh54_edrElf.elf	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-07-26	First-ever Open-Source Software Supply Chain Attacks	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/fir st-ever_open-source_software_supply_chain_attacks_6df0d247-55bd-4848-a6e9-ebf2f8 cd6517/Firsteverbgjacahebh52_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X- Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F2023 0726%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230726T074810Z&X-Amz-Expires=6 00&X-Amz-Signature=013cb7af488766f6f16a9866b76aebacd1cfb98163eb06b93f4c8b253723a 4a5&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-26	First-ever Open-Source Software Supply Chain Attacks	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/fir st-ever_open-source_software_supply_chain_attacks_6df0d247-55bd-4848-a6e9-ebf2f8 cd6517/Firsteverbgjacahebh51_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X- Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F2023 0726%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230726T074809Z&X-Amz-Expires=6 00&X-Amz-Signature=f324ac05c108d37a0f8bd51cbe9fa9eece971e1df8bc0a6fe1d6fc804ba2d 2e4&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-26	New Reptile Rootkit Malware Attacking Linux Systems Using Port Knocking	Newbgjadaaiej1_edrSh.sh	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-07-26	New Reptile Rootkit Malware Attacking Linux Systems Using Port Knocking	Newbgjadaaiej6_edrElf.elf	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-07-26	New Reptile Rootkit Malware Attacking Linux Systems Using Port Knocking	Newbgjadaaiej2_edrO.o	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-07-26	New Reptile Rootkit Malware Attacking Linux Systems Using Port Knocking	Newbgjadaaiej3_edrO.o	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-26	New Reptile Rootkit Malware Attacking Linux Systems Using Port Knocking	Newbgjadaaiej8_edrO.o	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-26	New Reptile Rootkit Malware Attacking Linux Systems Using Port Knocking	Newbgjadaaiej9_edrElf.elf	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-10	Operation Brainleeches Targets Microsoft 365 Users	hxxp://137.184.153.238	Web Gateway	GLESEC-AWS-CYMU	Offline/Removed
2023-07-10	TeamTNT Targets Cloud Native Environments	Teamtntbgiigjfdih1_edrElf.elf	Endpoint Security	GLESEC-AWS-CYMU	Blocked

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

TLP:AMBER

GLESEC
COMPLETELY PERCEPTI

ASM-VP REPORT

GLESEC 07/26/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-07-10	TeamTNT Targets Cloud Native Environments	Teamtntbgiigjfdih2_edrElf.elf	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-09	US Cert Alert - (AA23-187A) Increased Truebot Activity Infects U.S. And Canada Networks	Truebotbgiiijfbga9_edrDll.dll	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-09	US Cert Alert - (AA23-187A) Increased Truebot Activity Infects U.S. And Canada Networks	Truebotbgiiijfbga5_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-09	US Cert Alert - (AA23-187A) Increased Truebot Activity Infects U.S. And Canada Networks	Truebotbgiiijfbga2_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-09	US Cert Alert - (AA23-187A) Increased Truebot Activity Infects U.S. And Canada Networks	Truebotbgiiijfbga6_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-09	US Cert Alert - (AA23-187A) Increased Truebot Activity Infects U.S. And Canada Networks	Truebotbgiiijfbga8_edrDll.dll	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-09	US Cert Alert - (AA23-187A) Increased Truebot Activity Infects U.S. And Canada Networks	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/us_ cert_alert_-_%28aa23-187a%29_increased_truebot_activity_infects_u.s.and_canada_networks_c18bd470-6c4d-4289-a966-659944d071c9/Truebotbgiiijfbga_browsing7Dll.dll? X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230709T102857Z&X-Amz-Expires=600&X-Amz-Signature=a861c735e16d14975de60f04079cfedd120df22da39be10aeb7ef22d2e6a7e25&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-09	US Cert Alert - (AA23-187A) Increased Truebot Activity Infects U.S. And Canada Networks	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/us_ cert_alert_-_%28aa23-187a%29_increased_truebot_activity_infects_u.s.and_canada_networks_c18bd470-6c4d-4289-a966-659944d071c9/Truebotbgiiijfbga4_browsingExe.exe? X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230709T102857Z&X-Amz-Expires=600&X-Amz-Signature=585540d8a3f63b4c48f5152cc5f202b9e9acadfa722883c9000ae937e64341c1&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-09	US Cert Alert - (AA23-187A) Increased Truebot Activity Infects U.S. And Canada Networks	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/us_ cert_alert_-_%28aa23-187a%29_increased_truebot_activity_infects_u.s.and_canada_networks_c18bd470-6c4d-4289-a966-659944d071c9/Truebotbgiiijfbga3_browsingExe.exe? X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230709T102851Z&X-Amz-Expires=600&X-Amz-Signature=af0dad1edf9fb34012c9555844d9daf0295a9be84f500917309c68005360dfaa&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-09	US Cert Alert - (AA23-187A) Increased Truebot Activity Infects U.S. And Canada Networks	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/us_ cert_alert_-_%28aa23-187a%29_increased_truebot_activity_infects_u.s.and_canada_networks_c18bd470-6c4d-4289-a966-659944d071c9/Truebotbgiiijfbga1_browsingExe.exe? X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230709T102849Z&X-Amz-Expires=600&X-Amz-Signature=47cc9d86a858c932b942fa0820850c889179ef034b2da15b5e86a67c85884c71&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-09	Buddyransome	Buddyransombgiiiijacb1_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-09	Buddyransome	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/buddyransome_8cb491e4-5136-4deb-8e19-2027964f5bd2/Buddyransombgiiiijacb2_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230709T080250Z&X-Amz-Expires=600&X-Amz-Signature=15c43ee106f916105fa0ddeb9fb146ec74822f43192393b636363bc7c69ceb87&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-09	Threat Profile UNC3944	Threatbgiigjfhhb80_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-07-09	Threat Profile UNC3944	Threatbgiigjfhhb82_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-07-09	Threat Profile UNC3944	Threatbgiigjfhhb_edr79Exe.exe	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-07-09	Threat Profile UNC3944	Threatbgiigjfhhb83_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-07-09	Threat Profile UNC3944	Threatbgiigjfhhb_edr72Exe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked

TLP:AMBER

ASM-VP REPORT

GLESEC 07/26/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-07-09	Threat Profile UNC3944	Threatbgiigjfhhb_edr73Exe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-09	Threat Profile UNC3944	Threatbgiigjfhhb_edr75Exe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-09	Threat Profile UNC3944	Threatbgiigjfhhb_edr77Exe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-09	Threat Profile UNC3944	Threatbgiigjfhhb_edr76Exe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-09	Threat Profile UNC3944	Threatbgiigjfhhb84_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-09	Threat Profile UNC3944	Threatbgiigjfhhb85_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-26	New Reptile Rootkit Malware Attacking Linux Systems Using Port Knocking	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/new_reptile_rootkit_malware_attacking_linux_systems_using_port_knocking_c90e131d-0bd0-4024-978d-6ccdbb54f8c0/Newbgjadaaiej9_browsingElf.elf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230726%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230726T074212Z&X-Amz-Expires=600&X-Amz-Signature=bf07898b8462fdaf9301e60923a3945af9f93b6d758ead4daea04a7b2e11c6bb&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-26	New Reptile Rootkit Malware Attacking Linux Systems Using Port Knocking	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/new_reptile_rootkit_malware_attacking_linux_systems_using_port_knocking_c90e131d-0bd0-4024-978d-6ccdbb54f8c0/Newbgjadaaiej8_browsingO.o?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230726%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230726T074212Z&X-Amz-Expires=600&X-Amz-Signature=6073e547f453a191dbd15c57beaffcb20da2e1d1fe398f2f6141f799fd96f19f&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-26	New Reptile Rootkit Malware Attacking Linux Systems Using Port Knocking	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/new_reptile_rootkit_malware_attacking_linux_systems_using_port_knocking_c90e131d-0bd0-4024-978d-6ccdbb54f8c0/Newbgjadaaiej6_browsingElf.elf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230726%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230726T074211Z&X-Amz-Expires=600&X-Amz-Signature=e2b15982164484263b51fa5383fb1e15924bed2ad3d0bc1711e724660f2cb0e1&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-26	New Reptile Rootkit Malware Attacking Linux Systems Using Port Knocking	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/new_reptile_rootkit_malware_attacking_linux_systems_using_port_knocking_c90e131d-0bd0-4024-978d-6ccdbb54f8c0/Newbgjadaaiej3_browsingO.o?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230726%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230726T074210Z&X-Amz-Expires=600&X-Amz-Signature=a4282ae99df7e13cbe31654c7ff288d9b456f637cc094a37ceff596fdd3be981&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-26	New Reptile Rootkit Malware Attacking Linux Systems Using Port Knocking	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/new_reptile_rootkit_malware_attacking_linux_systems_using_port_knocking_c90e131d-0bd0-4024-978d-6ccdbb54f8c0/Newbgjadaaiej2_browsingO.o?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230726%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230726T074210Z&X-Amz-Expires=600&X-Amz-Signature=5a1adfe701fb9132032584d2cdaa4b816396cf1df118335541cc389e92790807&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-26	New Reptile Rootkit Malware Attacking Linux Systems Using Port Knocking	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/new_reptile_rootkit_malware_attacking_linux_systems_using_port_knocking_c90e131d-0bd0-4024-978d-6ccdbb54f8c0/Newbgjadaaiej1_browsingSh.sh?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230726%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230726T074209Z&X-Amz-Expires=600&X-Amz-Signature=4f216df07a30cc20fcfb6a626a862fe31b1367e6ba23798e0ca6aeceb20b5c33&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-25	Ransomware Spotlight Play	Ransomwarebgjacdgace1_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-25	Ransomware Spotlight Play	Ransomwarebgjacdgace12_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-07-25	Ransomware Spotlight Play	Ransomwarebgjacdgace5_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-25	Ransomware Spotlight Play	Ransomwarebgjacdgace3_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-25	Ransomware Spotlight Play	Ransomwarebgjacdgace14_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-25	Ransomware Spotlight Play	Ransomwarebgjacdgace11_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-25	Ransomware Spotlight Play	Ransomwarebgjacdgace9_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-25	Ransomware Spotlight Play	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ransomware_spotlight_play_9c7a6699-8793-486d-b28c-2b289d802cf8/Ransomwarebgjacdgace10_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230725%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230725T060143Z&X-Amz-Expires=600&X-Amz-Signature=c65c4b28d3181075efdbd65ec4ebf39d706a88d7e2980023d6364e5038665b52&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

TLP:AMBER

ASM-VP REPORT

GLESEC 07/26/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-07-25	Ransomware Spotlight Play	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ransomware_spotlight_play_9c7a6699-8793-486d-b28c-2b289d802cf8/Ransomwarebgjacdgace8_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230725%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230725T060143Z&X-Amz-Expires=600&X-Amz-Signature=7e0d6aee490fb5d510de340a463f3f7480ff4eee287870e95c8932d84737c0c9&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-25	Ransomware Spotlight Play	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ransomware_spotlight_play_9c7a6699-8793-486d-b28c-2b289d802cf8/Ransomwarebgjacdgace_browsing7Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230725%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230725T060142Z&X-Amz-Expires=600&X-Amz-Signature=5384abd0698fc166d3893417f154db117b3286c9797c67c957783b2abfb5279a&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-25	Ransomware Spotlight Play	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ransomware_spotlight_play_9c7a6699-8793-486d-b28c-2b289d802cf8/Ransomwarebgjacdgace4_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230725%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230725T060142Z&X-Amz-Expires=600&X-Amz-Signature=c06737dd02fe37b73bdd95af6591e65d36702f4063692a6b6cc2cb3fbc132813&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-25	Ransomware Spotlight Play	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ransomware_spotlight_play_9c7a6699-8793-486d-b28c-2b289d802cf8/Ransomwarebgjacdgace2_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230725%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230725T060141Z&X-Amz-Expires=600&X-Amz-Signature=c2729538ed01927970211635c64d087fec0fa381609f6745a8c208790a7726a7&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-24	Ursnif campaign in Italy	Ursnifbgijhigahi1_edrDll.dll	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-24	Ursnif campaign in Italy	Ursnifbgijhigahi4_edrPs1.ps1	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-07-23	Manipulated Caiman: The Sophisticated Snare of Mexico's Banking Predator	Manipulatedcaimanbgjabaaibd5_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-07-23	Manipulated Caiman: The Sophisticated Snare of Mexico's Banking Predator	Manipulatedcaimanbgjabaaibd13_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-23	Manipulated Caiman: The Sophisticated Snare of Mexico's Banking Predator	Manipulatedcaimanbgjabaaibd6_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-23	Manipulated Caiman: The Sophisticated Snare of Mexico's Banking Predator	Manipulatedcaimanbgjabaaibd9_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-23	Manipulated Caiman: The Sophisticated Snare of Mexico's Banking Predator	Manipulatedcaimanbgjabaaibd4_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-23	Manipulated Caiman: The Sophisticated Snare of Mexico's Banking Predator	Manipulatedcaimanbgjabaaibd10_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-23	Manipulated Caiman: The Sophisticated Snare of Mexico's Banking Predator	Manipulatedcaimanbgjabaaibd2_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-23	Manipulated Caiman: The Sophisticated Snare of Mexico's Banking Predator	Manipulatedcaimanbgjabaaibd1_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-23	Manipulated Caiman: The Sophisticated Snare of Mexico's Banking Predator	hxxp://45.153.240.94	Web Gateway	GLESEC-AWS-CYMU	Offline/Removed

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

TLP:AMBER

ASM-VP REPORT

GLESEC 07/26/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-07-23	Manipulated Caiman: The Sophisticated Snare of Mexico's Banking Predator	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/manipulated_caiman%3A_the_sophisticated_snare_of_mexico%27s_banking_predator_4b58497a-83ae-4fdd-bb38-8219794cb25b/Manipulatedcaimanbgjabaaibd3_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230723%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230723T085406Z&X-Amz-Expires=600&X-Amz-Signature=2008727be9309510379e9efc022eedcf980516b08dd86473088524b93dfb3e62&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-23	Manipulated Caiman: The Sophisticated Snare of Mexico's Banking Predator	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/manipulated_caiman%3A_the_sophisticated_snare_of_mexico%27s_banking_predator_4b58497a-83ae-4fdd-bb38-8219794cb25b/Manipulatedcaimanbgjabaaibdbrowsing7Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230723%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230723T085359Z&X-Amz-Expires=600&X-Amz-Signature=b13c284a469780ba9f938fb53735769852b2c7dab27f4bf46168824de967bfba&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-23	Manipulated Caiman: The Sophisticated Snare of Mexico's Banking Predator	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/manipulated_caiman%3A_the_sophisticated_snare_of_mexico%27s_banking_predator_4b58497a-83ae-4fdd-bb38-8219794cb25b/ManipulatedcaimanbgjabaaibdbrowsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230723%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230723T085359Z&X-Amz-Expires=600&X-Amz-Signature=5b5b762d1a3b11794b8c7124abc9245eeb0b5947a4626ddfc95114cfc65cb469&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-23	Manipulated Caiman: The Sophisticated Snare of Mexico's Banking Predator	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/manipulated_caiman%3A_the_sophisticated_snare_of_mexico%27s_banking_predator_4b58497a-83ae-4fdd-bb38-8219794cb25b/Manipulatedcaimanbgjabaaibd11_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230723%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230723T085357Z&X-Amz-Expires=600&X-Amz-Signature=866c7e541ffe1cda68209e7c257f1882803321466ca8dcce8a6e92eb9b9d9dff&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-23	Manipulated Caiman: The Sophisticated Snare of Mexico's Banking Predator	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/manipulated_caiman%3A_the_sophisticated_snare_of_mexico%27s_banking_predator_4b58497a-83ae-4fdd-bb38-8219794cb25b/Manipulatedcaimanbgjabaaibd12_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230723%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230723T085357Z&X-Amz-Expires=600&X-Amz-Signature=5eba9d614905538eca4e2d39a90526a97d04ea0c5751b7a9a42b08cca53f9680&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-23	Manipulated Caiman: The Sophisticated Snare of Mexico's Banking Predator	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/manipulated_caiman%3A_the_sophisticated_snare_of_mexico%27s_banking_predator_4b58497a-83ae-4fdd-bb38-8219794cb25b/Manipulatedcaimanbgjabaaibd14_browsingJs.js?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230723%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230723T085357Z&X-Amz-Expires=600&X-Amz-Signature=f0b009487e52d60a57db7f93a1e837812b7f9cd60a02f41d30ae508b0a617fd7&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-23	Manipulated Caiman: The Sophisticated Snare of Mexico's Banking Predator	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/manipulated_caiman%3A_the_sophisticated_snare_of_mexico%27s_banking_predator_4b58497a-83ae-4fdd-bb38-8219794cb25b/Manipulatedcaimanbgjabaaibd15_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230723%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230723T085356Z&X-Amz-Expires=600&X-Amz-Signature=fa645429f8b7c9facdfae2a729a5bd988ee962362a3a59a970b8b81272a71b54&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-23	A Look Into Space Pirates Unconventional Techniques Attack Vectors And Tools	Abgijibigeg22_edrDll.dll	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-07-23	A Look Into Space Pirates Unconventional Techniques Attack Vectors And Tools	Abgijibigeg62_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-07-23	A Look Into Space Pirates Unconventional Techniques Attack Vectors And Tools	Abgijibigeg65_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-07-23	A Look Into Space Pirates Unconventional Techniques Attack Vectors And Tools	Abgijibigeg30_edrDll.dll	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-07-23	A Look Into Space Pirates Unconventional Techniques Attack Vectors And Tools	Abgijibigeg6_edr7Exe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked

LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

TLP:AMBER

ASM-VP REPORT

GLESEC 07/26/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-07-23	A Look Into Space Pirates Unconventional Techniques Attack Vectors And Tools	Abgijibigeg28_edrDll.dll	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-23	A Look Into Space Pirates Unconventional Techniques Attack Vectors And Tools	Abgijibigeg24_edrDll.dll	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-23	A Look Into Space Pirates Unconventional Techniques Attack Vectors And Tools	hxxps://beachdrivingfun.com	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-23	A Look Into Space Pirates Unconventional Techniques Attack Vectors And Tools	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/a_look_into_space_pirates_unconventional_techniques_attack_vectors_and_tools_995867 c2-733c-4527-bde5-5c324ac95e6d/Abgijibigeg66_browsingExe.exe?X-Amz-Algorithm=AWS 4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230723%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230723T064226Z&X-Amz-Expires=600&X-Amz-Signature=e808593898b84b1fbfab2acd436caa1b0e89dfffd9ba0d42547adada9f4f732a&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-23	A Look Into Space Pirates Unconventional Techniques Attack Vectors And Tools	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/a_look_into_space_pirates_unconventional_techniques_attack_vectors_and_tools_995867 c2-733c-4527-bde5-5c324ac95e6d/Abgijibigeg64_browsingExe.exe?X-Amz-Algorithm=AWS 4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230723%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230723T064226Z&X-Amz-Expires=600&X-Amz-Signature=5ed58addcb7c1155119cbea9208f4b185775e27cb9f7875d04c6df2689eb1217&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-23	A Look Into Space Pirates Unconventional Techniques Attack Vectors And Tools	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/a_look_into_space_pirates_unconventional_techniques_attack_vectors_and_tools_995867 c2-733c-4527-bde5-5c324ac95e6d/Abgijibigeg63_browsingExe.exe?X-Amz-Algorithm=AWS 4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230723%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230723T064220Z&X-Amz-Expires=600&X-Amz-Signature=cd86b0802b7dbb66e5892c193c17292999a20ae6d93e1273ac974a1a413e1c62&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-23	A Look Into Space Pirates Unconventional Techniques Attack Vectors And Tools	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/a_look_into_space_pirates_unconventional_techniques_attack_vectors_and_tools_995867 c2-733c-4527-bde5-5c324ac95e6d/Abgijibigeg58_browsingExe.exe?X-Amz-Algorithm=AWS 4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230723%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230723T064219Z&X-Amz-Expires=600&X-Amz-Signature=8b1b9da6b236f1127c980b47a5dad92366e5977d97da523ac06d901130bfbfc8&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-23	A Look Into Space Pirates Unconventional Techniques Attack Vectors And Tools	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/a_look_into_space_pirates_unconventional_techniques_attack_vectors_and_tools_995867 c2-733c-4527-bde5-5c324ac95e6d/Abgijibigeg23_browsingDll.dll?X-Amz-Algorithm=AWS 4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230723%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230723T064219Z&X-Amz-Expires=600&X-Amz-Signature=09cf60a1d7accaaaa86f8ea2bf60a22a87e89fbe11e25f3bfc81de4f509b07db&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-23	A Look Into Space Pirates Unconventional Techniques Attack Vectors And Tools	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/a_look_into_space_pirates_unconventional_techniques_attack_vectors_and_tools_995867 c2-733c-4527-bde5-5c324ac95e6d/Abgijibigeg21_browsingDll.dll?X-Amz-Algorithm=AWS 4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230723%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230723T064218Z&X-Amz-Expires=600&X-Amz-Signature=d6deaee3c92fbfcdd1b747c501062de3c44cda74b8babe24a73a52e40acd0830&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-23	A Look Into Space Pirates Unconventional Techniques Attack Vectors And Tools	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/a_look_into_space_pirates_unconventional_techniques_attack_vectors_and_tools_995867 c2-733c-4527-bde5-5c324ac95e6d/Abgijibigeg18_browsingDll.dll?X-Amz-Algorithm=AWS 4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230723%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230723T064217Z&X-Amz-Expires=600&X-Amz-Signature=1f94b22c4ba1ada48ea78cb2a0497415b1b645d87cb9a2f1dc8d625c487bffaf&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-23	Threat Actor Launches ScarLeteel 2.00	Threatbgijdaabfc3_edrSh.sh	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-23	Threat Actor Launches ScarLeteel 2.00	hxxp://175.102.182.6	Web Gateway	GLESEC-AWS-CYMU	Offline/Removed
2023-07-23	Threat Actor Launches ScarLeteel 2.00	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/threat_actor_launches_scarleteel_2.0_5c3a31c4-d75d-4f35-8a4e-ab9dc96ff553/Threatbgijdaabfc4_browsingSh.sh?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230723%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230723T063744Z&X-Amz-Expires=600&X-Amz-Signature=f6ab82190373ffab54ad4aa0fd0a42921b8e7084bb578ac5a1f631778191415c&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

TLP:AMBER

ASM-VP REPORT

GLESEC 07/26/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-07-23	Threat Actor Launches ScarLeteel 2.00	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/threat_actor_launches_scarleteel_2.0_5c3a31c4-d75d-4f35-8a4e-ab9dc96ff553/Threatbgijdaabfc2_browsingSh.sh?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230723%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230723T063743Z&X-Amz-Expires=600&X-Amz-Signature=76010bc2052a657d9fd1cc55262a6ff2d3990ed7503813b677a02f01ce6a85fe&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-20	The Turla APT Group Uses Multiple Malware Families To Exfiltrate Data (CERT-UA6981)	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/the_turla_apt_group_uses_multiple_malware_families_to_exfiltrate_data_%28cert-ua6981%29_a81930dd-7462-451c-a175-656d5b0b5612/Thebgijibifhf1_browsingDll.dll?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230720%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230720T053643Z&X-Amz-Expires=600&X-Amz-Signature=8b85946aaf7399888177777e6ac93c75f215e68bbe8edf73ec411e0c55218d08&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-20	DDoS Botnet Targets Zyxel Vulnerability (CVE-2023-28771)	Ddosbgijibiigd_edr77Elf.elf	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-20	DDoS Botnet Targets Zyxel Vulnerability (CVE-2023-28771)	Ddosbgijibiigd_edr79Elf.elf	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-20	DDoS Botnet Targets Zyxel Vulnerability (CVE-2023-28771)	Ddosbgijibiigd83_edrElf.elf	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-20	DDoS Botnet Targets Zyxel Vulnerability (CVE-2023-28771)	Ddosbgijibiigd82_edrElf.elf	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-20	DDoS Botnet Targets Zyxel Vulnerability (CVE-2023-28771)	Ddosbgijibiigd81_edrElf.elf	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-20	DDoS Botnet Targets Zyxel Vulnerability (CVE-2023-28771)	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ddos_botnet_targets_zyxel_vulnerability_%28cve-2023-28771%29_726e7b63-4627-4776-a657-7c9d9a38820c/Ddosbgijibiigd86_browsingElf.elf?X-Amz-Algorithm=AWS4-HMAC-SHA256 &X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230720%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230720T053347Z&X-Amz-Expires=600&X-Amz-Signature=f151fe84d4bf7829344b546e9fc7b0b99c72766775f99e8416f231e4b7e4d5e5&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-20	DDoS Botnet Targets Zyxel Vulnerability (CVE-2023-28771)	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ddos_botnet_targets_zyxel_vulnerability_%28cve-2023-28771%29_726e7b63-4627-4776-a657-7c9d9a38820c/Ddosbgijibiigd84_browsingElf.elf?X-Amz-Algorithm=AWS4-HMAC-SHA256 &X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230720%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230720T053347Z&X-Amz-Expires=600&X-Amz-Signature=2f8ef825f6047b38629daba935cfc24a829955e5fa93155b55c33fc2c099790e&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-20	DDoS Botnet Targets Zyxel Vulnerability (CVE-2023-28771)	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ddos_botnet_targets_zyxel_vulnerability_%28cve-2023-28771%29_726e7b63-4627-4776-a657-7c9d9a38820c/Ddosbgijibiigd80_browsingElf.elf?X-Amz-Algorithm=AWS4-HMAC-SHA256 &X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230720%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230720T053346Z&X-Amz-Expires=600&X-Amz-Signature=5b5fb32af087f5a230d52e7b3d16509a402b71628c82b4d8ae413635d63313de&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-20	DDoS Botnet Targets Zyxel Vulnerability (CVE-2023-28771)	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ddos_botnet_targets_zyxel_vulnerability_%28cve-2023-28771%29_726e7b63-4627-4776-a657-7c9d9a38820c/Ddosbgijibiigd_browsing78Elf.elf?X-Amz-Algorithm=AWS4-HMAC-SHA256 &X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230720%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230720T053345Z&X-Amz-Expires=600&X-Amz-Signature=e5a20a8c9cd096f855d4247661bfd6c541bea1fce98acfeed64dac98877290dd&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-19	FIN8 Uses Revamped Sardonic Backdoor to Deliver Noberus Ransomware	Fin8bgijhbhgec9_edrDll.dll	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-07-19	FIN8 Uses Revamped Sardonic Backdoor to Deliver Noberus Ransomware	Fin8bgijhbhgec15_edrDll.dll	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-07-19	FIN8 Uses Revamped Sardonic Backdoor to Deliver Noberus Ransomware	Fin8bgijhbhgec19_edrDll.dll	Endpoint Security	GLESEC-AWS-CYMU	Penetrated

TLP:AMBER

GLESEC
COMPLETELY PERCEPTI

ASM-VP REPORT

GLESEC 07/26/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-07-19	FIN8 Uses Revamped Sardonic Backdoor to Deliver Noberus Ransomware	Fin8bgijhbhgec10_edrDll.dll	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-07-19	FIN8 Uses Revamped Sardonic Backdoor to Deliver Noberus Ransomware	Fin8bgijhbhgec12_edrDll.dll	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-19	Google Firebase Hosting Abused To Deliver Sorillus RAT	Googlebgijhdccbi10_edrHtml.html	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-07-19	Google Firebase Hosting Abused To Deliver Sorillus RAT	Googlebgijhdccbi_edr7Html.html	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-07-19	Google Firebase Hosting Abused To Deliver Sorillus RAT	Googlebgijhdccbi6_edrHtml.html	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-07-19	FIN8 Uses Revamped Sardonic Backdoor to Deliver Noberus Ransomware	hxxp://37.10.71.215	Web Gateway	GLESEC-AWS-CYMU	Offline/Removed
2023-07-19	FIN8 Uses Revamped Sardonic Backdoor to Deliver Noberus Ransomware	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/fin8_uses_revamped_sardonic_backdoor_to_deliver_noberus_ransomware_df7ab7db-17fe-4d78-9d45-04631de9cab9/Fin8bgijhbhgec14_browsingPs1.ps1?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230719%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230719T074903Z&X-Amz-Expires=600&X-Amz-Signature=2a0e9e0b6439ea859c048ffebf402983d159d266e181195819c6da5b6d7bd7f7&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-19	FIN8 Uses Revamped Sardonic Backdoor to Deliver Noberus Ransomware	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/fin8_uses_revamped_sardonic_backdoor_to_deliver_noberus_ransomware_df7ab7db-17fe-4d78-9d45-04631de9cab9/Fin8bgijhbhgec4_browsingPs1.ps1?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230719%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230719T074901Z&X-Amz-Expires=600&X-Amz-Signature=33c9c4242e4577bdcf60fc07146cf7e71bdae75b4afb730609203b34f4a46208&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-19	Google Firebase Hosting Abused To Deliver Sorillus RAT	hxxp://185.196.220.62	Web Gateway	GLESEC-AWS-CYMU	Offline/Removed
2023-07-19	Google Firebase Hosting Abused To Deliver Sorillus RAT	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/google_firebase_hosting_abused_to_deliver_sorillus_rat_cc09fcb8-0060-4086-b1d8-29d1619ef79f/Googlebgijhdccbi9_browsingHtml.html?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230719%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230719T074807Z&X-Amz-Expires=600&X-Amz-Signature=37fa006ca689f1304b91a9b3e717c08e85ffae36f5a9a85c889409602e9f22ec&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-19	Google Firebase Hosting Abused To Deliver Sorillus RAT	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/google_firebase_hosting_abused_to_deliver_sorillus_rat_cc09fcb8-0060-4086-b1d8-29d1619ef79f/Googlebgijhdccbi8_browsingHtml.html?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230719%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230719T074807Z&X-Amz-Expires=600&X-Amz-Signature=4705343b5a1b3bd81fd970b16f993730f4a999a7445bb01a989ea0a7e8010530&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-19	Google Firebase Hosting Abused To Deliver Sorillus RAT	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/google_firebase_hosting_abused_to_deliver_sorillus_rat_cc09fcb8-0060-4086-b1d8-29d1619ef79f/Googlebgijhdccbi5_browsingHtml.html?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230719%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230719T074806Z&X-Amz-Expires=600&X-Amz-Signature=13a6d72822d89b3f20cc8ccfe9a3abd936a6388fa57546c2106d22248c10361b&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-19	Google Firebase Hosting Abused To Deliver Sorillus RAT	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/google_firebase_hosting_abused_to_deliver_sorillus_rat_cc09fcb8-0060-4086-b1d8-29d1619ef79f/Googlebgijhdccbi4_browsingZip.zip?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230719%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230719T074805Z&X-Amz-Expires=600&X-Amz-Signature=ae61014a67d598ed5274a5677bfa7064ba9d06ab8ff951ad9b2488b03769cade&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-18	Infamous Meduza Stealer	Infamousbgijcbdjad21_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-07-18	Infamous Meduza Stealer	Infamousbgijcbdjad20_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked

LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

TLP:AMBER

ASM-VP REPORT

GLESEC 07/26/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-07-18	Infamous Meduza Stealer	Infamousbgijcbdjad18_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-18	Infamous Meduza Stealer	Infamousbgijcbdjad19_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-18	Infamous Meduza Stealer	Infamousbgijcbdjad15_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-18	Infamous Meduza Stealer	Infamousbgijcbdjad12_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-18	Infamous Meduza Stealer	hxxp://79.137.203.37	Web Gateway	GLESEC-AWS-CYMU	Offline/Removed
2023-07-18	Infamous Meduza Stealer	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/infamous_meduza_stealer_21000adb-78d3-4a28-94c3-8427f297ac31/Infamousbgijcbdjad1_browsing7Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230718%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230718T065233Z&X-Amz-Expires=600&X-Amz-Signature=1253dec47ec1d2fef27ce69a1637939dd32bf4ed6c8a1e7af02993dc3e9474df&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-18	Infamous Meduza Stealer	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/infamous_meduza_stealer_21000adb-78d3-4a28-94c3-8427f297ac31/Infamousbgijcbdjad13_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230718%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230718T065227Z&X-Amz-Expires=600&X-Amz-Signature=7ec92f2bf9fba5c20e9b9173770cb4a42c83ca5e6d3cebb3889358dda085d1f7&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-18	Infamous Meduza Stealer	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/infamous_meduza_stealer_21000adb-78d3-4a28-94c3-8427f297ac31/Infamousbgijcbdjad11_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230718%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230718T065226Z&X-Amz-Expires=600&X-Amz-Signature=0b1a9e95a355ac9fa3c94d64a38a4bd28e752d87855a02419eb81f48a1de1b7a&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-18	Infamous Meduza Stealer	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/infamous_meduza_stealer_21000adb-78d3-4a28-94c3-8427f297ac31/Infamousbgijcbdjad16_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230718%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230718T065226Z&X-Amz-Expires=600&X-Amz-Signature=7dbe788a76b32f8f2986d8bcc5a2161ca925c9161390dcbf14c7e0a290b89991&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-18	Infamous Meduza Stealer	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/infamous_meduza_stealer_21000adb-78d3-4a28-94c3-8427f297ac31/Infamousbgijcbdjad14_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230718%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230718T065225Z&X-Amz-Expires=600&X-Amz-Signature=aa91b6e983466b1b101f24109b04cdca26ee457d54e7035509119bba675599fe&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-18	APT36 Delivers Crimson RAT Using Pilgrimage Security Briefing Lure	Apt36bgijdaafca_edr79Exe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-18	APT36 Delivers Crimson RAT Using Pilgrimage Security Briefing Lure	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/apt36_delivers_crimson_rat_using_pilgrimage_security_briefing_lure_d3803684-14d2-4b40-97f4-11d6c9cba750/Apt36bgijdaafca_browsing77Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230718%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230718T055527Z&X-Amz-Expires=600&X-Amz-Signature=7452f821563247da22bbeb53221989250c0ef99232bb984dfcf810c0fa45c711&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Blocked
2023-07-18	APT36 Delivers Crimson RAT Using Pilgrimage Security Briefing Lure	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/apt36_delivers_crimson_rat_using_pilgrimage_security_briefing_lure_d3803684-14d2-4b40-97f4-11d6c9cba750/Apt36bgijdaafca80_browsingDocx.docx?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230718%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230718T055526Z&X-Amz-Expires=600&X-Amz-Signature=ce5f66c2efc809f1dda6bdaeba461d04f7e5ab8312daae6142703b9ff65fe8e8&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-18	APT36 Delivers Crimson RAT Using Pilgrimage Security Briefing Lure	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/apt36_delivers_crimson_rat_using_pilgrimage_security_briefing_lure_d3803684-14d2-4b40-97f4-11d6c9cba750/Apt36bgijdaafca81_browsingZip.zip?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230718%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230718T055526Z&X-Amz-Expires=600&X-Amz-Signature=5ab689992644a523967b620bedb3e82f04149e3c2826589f93eb3d16ecf1e8e6&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-16	Cloudy With a Chance of Credentials | AWS-Targeting Cred Stealer Expands to Azure GCP	Cloudybgijdhcafh1_edrSh.sh	Endpoint Security	GLESEC-AWS-CYMU	Penetrated

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

TLP:AMBER

ASM-VP REPORT

GLESEC 07/26/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-07-16	Cloudy With a Chance of Credentials | AWS-Targeting Cred Stealer Expands to Azure GCP	Cloudybgijdhcafh3_edrSh.sh	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-07-16	Cloudy With a Chance of Credentials | AWS-Targeting Cred Stealer Expands to Azure GCP	Cloudybgijdhcafh6_edrSh.sh	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-07-16	Cloudy With a Chance of Credentials | AWS-Targeting Cred Stealer Expands to Azure GCP	Cloudybgijdhcafh16_edrSh.sh	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-07-16	Cloudy With a Chance of Credentials | AWS-Targeting Cred Stealer Expands to Azure GCP	Cloudybgijdhcafh8_edrSh.sh	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-07-16	Cloudy With a Chance of Credentials | AWS-Targeting Cred Stealer Expands to Azure GCP	Cloudybgijdhcafh11_edrSh.sh	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-07-16	Cloudy With a Chance of Credentials | AWS-Targeting Cred Stealer Expands to Azure GCP	Cloudybgijdhcafh21_edrSh.sh	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-07-16	Cloudy With a Chance of Credentials | AWS-Targeting Cred Stealer Expands to Azure GCP	Cloudybgijdhcafh20_edrSh.sh	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-07-16	Cloudy With a Chance of Credentials | AWS-Targeting Cred Stealer Expands to Azure GCP	Cloudybgijdhcafh9_edrSh.sh	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-07-16	Cloudy With a Chance of Credentials | AWS-Targeting Cred Stealer Expands to Azure GCP	Cloudybgijdhcafh18_edrSh.sh	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-07-16	Cloudy With a Chance of Credentials | AWS-Targeting Cred Stealer Expands to Azure GCP	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/cloudy_with_a_chance_of_credentials_%7C_aws-targeting_cred_stealer_expands_to_azure_gcp_3206978e-9740-4736-8720-3e2241f499a6/Cloudybgijdhcafh15_browsingSh.sh?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230716%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230716T045959Z&X-Amz-Expires=600&X-Amz-Signature=27b90d2ca170cde695956a7197f500c3d781bd6a082a99defba1f743c57ae57f&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-16	Cloudy With a Chance of Credentials | AWS-Targeting Cred Stealer Expands to Azure GCP	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/cloudy_with_a_chance_of_credentials_%7C_aws-targeting_cred_stealer_expands_to_azure_gcp_3206978e-9740-4736-8720-3e2241f499a6/Cloudybgijdhcafh14_browsingSh.sh?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230716%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230716T045959Z&X-Amz-Expires=600&X-Amz-Signature=711a3c0a98bd4ffcabe94772923efcc825272cc84cba527c887c8a61c2ab01c0&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

TLP:AMBER

ASM-VP REPORT

GLESEC 07/26/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-07-16	Cloudy With a Chance of Credentials | AWS-Targeting Cred Stealer Expands to Azure GCP	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/cloudy_with_a_chance_of_credentials_%7C_aws-targeting_cred_stealer_expands_to_azure_gcp_3206978e-9740-4736-8720-3e2241f499a6/Cloudybgijdhcafh10_browsingSh.sh?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230716%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230716T045959Z&X-Amz-Expires=600&X-Amz-Signature=a00c2750af89dddbe3f4efc53e37ac51a66c6a4acc5f92db04af56d789ba453b&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-16	Cloudy With a Chance of Credentials | AWS-Targeting Cred Stealer Expands to Azure GCP	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/cloudy_with_a_chance_of_credentials_%7C_aws-targeting_cred_stealer_expands_to_azure_gcp_3206978e-9740-4736-8720-3e2241f499a6/Cloudybgijdhcafh_browsing7Sh.sh?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230716%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230716T045958Z&X-Amz-Expires=600&X-Amz-Signature=80d3a8be78cb51035273b5649ff0d09cff047ae4a64786ee0067b2b91dbd1ac0&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-16	Cloudy With a Chance of Credentials | AWS-Targeting Cred Stealer Expands to Azure GCP	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/cloudy_with_a_chance_of_credentials_%7C_aws-targeting_cred_stealer_expands_to_azure_gcp_3206978e-9740-4736-8720-3e2241f499a6/Cloudybgijdhcafh5_browsingElf.elf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230716%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230716T045957Z&X-Amz-Expires=600&X-Amz-Signature=72465ba93bef3e9436d0fac81f94776227aed5ba997e5a843411d8cf5f36f0c6&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-13	Attackers Exploit (CVE-2023-36884) Unpatched Windows Zero-Day Vulnerability	Attackersbgijcceegh1_edrDocx.docx	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-13	Attackers Exploit (CVE-2023-36884) Unpatched Windows Zero-Day Vulnerability	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/attackers_exploit_unpatched_windows_zero-day_vulnerability_40d6eeaa-f493-4fe6-929d-ac7ddc09b8b1/Attackersbgijcceegh4_browsingLnk.lnk?X-Amz-Algorithm=AWS4-HMAC-SHA2 56&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230713%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230713T053150Z&X-Amz-Expires=600&X-Amz-Signature=620c36f0276322ce8b0f28a3c393ad69b0955edf1c8f03892918a26ff126c462&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-12	Underground Team Ransomware Demands Millions	Undergroundbgijafbfig39_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-12	Underground Team Ransomware Demands Millions	hxxp://undgrddapc4reaunnrdrmnagvdelqfvmgycuvilgwb5uxm25sxawaoqd.onion/	Web Gateway	GLESEC-AWS-CYMU	Offline/Removed
2023-07-11	Unleashing WhiteSnake Stealer	Unleashingbgijafbdca1_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-11	Unleashing WhiteSnake Stealer	Unleashingbgijafbdca2_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-11	Threat Trend Report On Kimsuky	Threatbgijafbfgb38_edrChm.chm	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-07-10	Operation Brainleeches Targets Microsoft 365 Users	Operationbgiihibied11_edrJs.js	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-07-09	Threat Profile UNC3944	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/threat_profile_unc3944_f7ba8a64-eecc-477f-a86e-0cbdccc2a0c9/Threatbgiigjfhhb81_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230709T060403Z&X-Amz-Expires=600&X-Amz-Signature=51c89997039516b1ef4e46c507a41dc96fc9977b6de5422b39c878e08d8b75e5&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-09	Threat Profile UNC3944	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/threat_profile_unc3944_f7ba8a64-eecc-477f-a86e-0cbdccc2a0c9/Threatbgiigjfhhb_browsing78Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230709T060402Z&X-Amz-Expires=600&X-Amz-Signature=d65d9b9ee86bcf0d385a724db68c61a9a7600cbf692861cc97c978634b23dd34&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-09	Threat Profile UNC3944	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/threat_profile_unc3944_f7ba8a64-eecc-477f-a86e-0cbdccc2a0c9/Threatbgiigjfhhb_browsing74Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230709T060400Z&X-Amz-Expires=600&X-Amz-Signature=a4d1ba25bfcad8929d171c92f4ab1ebda755151a1ab25ce086e919b8b0fe4308&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated

TLP:AMBER

GLESEC
COMPLETELY PERCEPTI

ASM-VP REPORT

GLESEC 07/26/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-07-09	Threat Profile UNC3944	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/threat_profile_unc3944_f7ba8a64-eecc-477f-a86e-0cbdccc2a0c9/Threatbgiigjfhhb_browsing71Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230709T060359Z&X-Amz-Expires=600&X-Amz-Signature=46edce813d31907f553cff6ea8b66f9b8b8263e75936ec3df2e561861f548ba2&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-09	Threat Profile UNC3944	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/threat_profile_unc3944_f7ba8a64-eecc-477f-a86e-0cbdccc2a0c9/Threatbgiigjfhhb_browsi ng70Elf.elf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLO AD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230709%2Feu-west-1%2Fs3%2Faws4_requ est&X-Amz-Date=20230709T060357Z&X-Amz-Expires=600&X-Amz-Signature=fd5d66208fff5440be1313d55ca2f32d059888741148bce6ba3b00938b3c60a8&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-09	Threat Profile UNC3944	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/threat_profile_unc3944_f7ba8a64-eecc-477f-a86e-0cbdccc2a0c9/Threatbgiigjfhhb66_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230709T060356Z&X-Amz-Expires=600&X-Amz-Signature=7cad70acf6449f90bcda4ede5da888d28a2aba774c549a2e982fb8ff4f235c1e&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-06	PhonyC2 Framework Used By MuddyWater	Phonyc2bgiigaijja10_edrJs.js	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-07-06	PhonyC2 Framework Used By MuddyWater	Phonyc2bgiigaijja9_edrJs.js	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-07-06	PhonyC2 Framework Used By MuddyWater	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/phonyc2_framework_used_by_muddywater_055285f0-d830-4652-b2b3-c438a424a18e/Phonyc2bgiigaijja5_browsingPs1.ps1?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230706%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230706T050232Z&X-Amz-Expires=600&X-Amz-Signature=21fdf95a3a68735c186a8380b69dcf60646d37fd6b92e08c911a287886820e5c&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
N/A	The suspected Maha grass organization uses the WarHawk backdoor variant Spyder to spy on many countries	Thebgiifccegi20_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-05	The suspected Maha grass organization uses the WarHawk backdoor variant Spyder to spy on many countries	Thebgiifccegi9_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-05	The suspected Maha grass organization uses the WarHawk backdoor variant Spyder to spy on many countries	Thebgiifccegi19_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-05	The suspected Maha grass organization uses the WarHawk backdoor variant Spyder to spy on many countries	Thebgiifccegi13_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-05	The suspected Maha grass organization uses the WarHawk backdoor variant Spyder to spy on many countries	Thebgiifccegi1_edr7Exe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-05	The suspected Maha grass organization uses the WarHawk backdoor variant Spyder to spy on many countries	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/the_suspected_maha_grass_organization_uses_the_warhawk_backdoor_variant_spyder_to_spy_on_many_countries_b12092f9-cbef-4912-87fe-16158033afbc/Thebgiifccegi21_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230705%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230705T050504Z&X-Amz-Expires=600&X-Amz-Signature=3a2f2aeff053add056d381eb0acf347ecb544ee8feb5e8100f6b9628abe8a7d7&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

TLP:AMBER

ASM-VP REPORT

GLESEC 07/26/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-07-05	The suspected Maha grass organization uses the WarHawk backdoor variant Spyder to spy on many countries	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/the_suspected_maha_grass_organization_uses_the_warhawk_backdoor_variant_spyder_to_spy_on_many_countries_b12092f9-cbef-4912-87fe-16158033afbc/Thebgiifccegi18_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230705%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230705T050503Z&X-Amz-Expires=600&X-Amz-Signature=bc1e28aa774276d48a3d4b7041f8b34e783080896224a5e6ffe749bd9b171308&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-05	The suspected Maha grass organization uses the WarHawk backdoor variant Spyder to spy on many countries	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/the_suspected_maha_grass_organization_uses_the_warhawk_backdoor_variant_spyder_to_spy_on_many_countries_b12092f9-cbef-4912-87fe-16158033afbc/Thebgiifccegi14_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230705%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230705T050502Z&X-Amz-Expires=600&X-Amz-Signature=edb62af340c3e2994c9b0650c847b0e1c5903ccb2859bf18b99b8815145fc4c0&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-05	The suspected Maha grass organization uses the WarHawk backdoor variant Spyder to spy on many countries	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/the_suspected_maha_grass_organization_uses_the_warhawk_backdoor_variant_spyder_to_spy_on_many_countries_b12092f9-cbef-4912-87fe-16158033afbc/Thebgiifccegi10_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230705%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230705T050502Z&X-Amz-Expires=600&X-Amz-Signature=07dc3ef3320415a35e8b2ecb62dacf07cbccecbdd6adf7e8bd3d83782e90b352&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-04	The DPRK strikes using a new variant of RUSTBUCKET	Thebgiiecjcjg122_edrMacho.macho	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-04	The DPRK strikes using a new variant of RUSTBUCKET	Thebgiiecjcjg126_edrMacho.macho	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-04	The DPRK strikes using a new variant of RUSTBUCKET	Thebgiiecjcjg125_edrMacho.macho	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-04	The DPRK strikes using a new variant of RUSTBUCKET	Thebgiiecjcjg131_edrMacho.macho	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-04	The DPRK strikes using a new variant of RUSTBUCKET	hxxp://companydeck.online	Web Gateway	GLESEC-AWS-CYMU	Offline/Removed
2023-07-04	The DPRK strikes using a new variant of RUSTBUCKET	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/the_dprk_strikes_using_a_new_variant_of_rustbucket_5ef1bf2d-e849-470a-b237-647c9e112e12/Thebgiiecjcjg132_browsingMacho.macho?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230704%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230704T061302Z&X-Amz-Expires=600& X-Amz-Signature=18d4f3396080200e8bca71bf630c8af523128453cc77ccd60652d152d1dc87b1 &X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-04	The DPRK strikes using a new variant of RUSTBUCKET	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/the_dprk_strikes_using_a_new_variant_of_rustbucket_5ef1bf2d-e849-470a-b237-647c9e112e12/Thebgiiecjcjg129_browsingMacho.macho?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230704%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230704T061301Z&X-Amz-Expires=600& X-Amz-Signature=f6d67714f370efd417ccd58d8b695b344f086c55ebecece4478db90658477e39 &X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-04	The DPRK strikes using a new variant of RUSTBUCKET	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/the_dprk_strikes_using_a_new_variant_of_rustbucket_5ef1bf2d-e849-470a-b237-647c9e112e12/Thebgiiecjcjg12_browsing7Macho.macho?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230704%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230704T061300Z&X-Amz-Expires=600& X-Amz-Signature=d33e7735b74e5366a62c22a236e589a06b1f193f95eb3e126e07714d38f366ef &X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-03	Word Document with an Online Attached Template	Matryoshkabgiididgjd2_edrRtf.rtf	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-03	Word Document with an Online Attached Template	Matryoshkabgiididgjd3_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-07-03	Word Document with an Online Attached Template	Matryoshkabgiididgjd1_edrDocx.docx	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-03	New Qakbot (Qbot) activity	Qbotbgiidicbbd3_edrZip.zip	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-07-03	New Qakbot (Qbot) activity	hxxps://brotherocean.com	Web Gateway	GLESEC-AWS-CYMU	Offline/Removed

TLP:AMBER

GLESEC
COMPLETELY PERCEPTI

ASM-VP REPORT

GLESEC 07/26/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-07-03	New Qakbot (Qbot) activity	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/new_qakbot_%28qbot%29_activity_f5a2f41e-fc87-429d-b4af-e3e89d8c012f/Qbotbgiidicbbd2_browsingJs.js?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230703%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230703T111503Z&X-Amz-Expires=600&X-Amz-Signature=b4ff14e6db055d385639bbdc51b4df5068bc300bfdb92fa3f2f2ed37a4471704&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-03	New Qakbot (Qbot) activity	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/new_qakbot_%28qbot%29_activity_f5a2f41e-fc87-429d-b4af-e3e89d8c012f/Qbotbgiidicbbd1_browsingDll.dll?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230703%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230703T111502Z&X-Amz-Expires=600&X-Amz-Signature=6936c420156ae27cb8e961bb73ccd5e0257e26d67040bf1a3b45f64b7928a35f&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-03	Mirai Campaign Leveraging Multiple IoT Exploits	Miraibgihfhcccf1_edrElf.elf	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-03	Mirai Campaign Leveraging Multiple IoT Exploits	Miraibgihfhcccf9_edrElf.elf	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-03	Mirai Campaign Leveraging Multiple IoT Exploits	Miraibgihfhcccf13_edrElf.elf	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-03	Mirai Campaign Leveraging Multiple IoT Exploits	Miraibgihfhcccf10_edrElf.elf	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-03	Mirai Campaign Leveraging Multiple IoT Exploits	Miraibgihfhcccf4_edrElf.elf	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-03	Mirai Campaign Leveraging Multiple IoT Exploits	Miraibgihfhcccf8_edrElf.elf	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-03	Mirai Campaign Leveraging Multiple IoT Exploits	Miraibgihfhcccf11_edrElf.elf	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-03	Mirai Campaign Leveraging Multiple IoT Exploits	hxxp://185.225.74.251/sparc	Web Gateway	GLESEC-AWS-CYMU	Blocked
2023-07-03	Mirai Campaign Leveraging Multiple IoT Exploits	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/miraai_campaign_leveraging_multiple_iot_exploits_29e3fabb-a46e-42e6-9931-6276108ef13d/Miraibgihfhcccf12_browsingElf.elf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230703%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230703T083511Z&X-Amz-Expires=600&X-Amz-Signature=72ba4c7b4641fd56570170be364251f62f646719eaad4fec652ae302cdffa515&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-03	Mirai Campaign Leveraging Multiple IoT Exploits	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/miraai_campaign_leveraging_multiple_iot_exploits_29e3fabb-a46e-42e6-9931-6276108ef13d/Miraibgihfhcccf_browsing7Elf.elf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230703%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230703T083510Z&X-Amz-Expires=600&X-Amz-Signature=4c2c9dc18373a9b042fb63990bbdfdc8da10b0501231aeb6e8384f6c0624dcfb&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-03	Mirai Campaign Leveraging Multiple IoT Exploits	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/miraai_campaign_leveraging_multiple_iot_exploits_29e3fabb-a46e-42e6-9931-6276108ef13d/Miraibgihfhcccf6_browsingElf.elf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230703%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230703T083509Z&X-Amz-Expires=600&X-Amz-Signature=4a2491b47083ff2292e2e714a6a7df43f4e5cd7eca7ceea3031c40d9db702db1&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-03	Mirai Campaign Leveraging Multiple IoT Exploits	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/miraai_campaign_leveraging_multiple_iot_exploits_29e3fabb-a46e-42e6-9931-6276108ef13d/Miraibgihfhcccf5_browsingElf.elf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230703%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230703T083509Z&X-Amz-Expires=600&X-Amz-Signature=edeb28be80513d1265ab88b5e50ee9116768023008afab79459c534c36773d9c&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-03	Mirai Campaign Leveraging Multiple IoT Exploits	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/miraai_campaign_leveraging_multiple_iot_exploits_29e3fabb-a46e-42e6-9931-6276108ef13d/Miraibgihfhcccf3_browsingElf.elf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230703%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230703T083509Z&X-Amz-Expires=600&X-Amz-Signature=89d02ae39e39613067b16fe7949fb0f3d9b7b979d90ed947c15386b6cf2aa81c&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated

TLP:AMBER

GLESEC
COMPLETELY PERCEPTI

ASM-VP REPORT

GLESEC 07/26/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-07-03	Mirai Campaign Leveraging Multiple IoT Exploits	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/mirai_campaign_leveraging_multiple_iot_exploits_29e3fabb-a46e-42e6-9931-6276108ef13d/Miraibgihfhcccf2_browsingElf.elf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Conten t-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230703%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230703T083508Z&X-Amz-Expires=600&X-Amz-Signature=d6126e6ed98a8c2c751072ecafcd7d359343e17695518f06e32ce07aafa1bb4a&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-02	Gh0stBins RAT Analysis	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/gh0stbins_rat_analysis_c3247a6f-a237-42c1-b6a7-bc7b5a1e890a/Gh0stbinsbgihjbhhhb4_browsingDll.dll?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230702%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230702T053252Z&X-Amz-Expires=600&X-Amz-Signature=2deaf24a780964768507bcb5b7132f83d4c69f996b2b082a8bcc8aa25ebbe29d&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-02	Gh0stBins RAT Analysis	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/gh0stbins_rat_analysis_c3247a6f-a237-42c1-b6a7-bc7b5a1e890a/Gh0stbinsbgihjbhhhb3_browsingDll.dll?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230702%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230702T053252Z&X-Amz-Expires=600&X-Amz-Signature=a5274706d953f9938d47659d83c57c51f822bd3337f40ac955e3e5c29b4d343b&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-02	Gh0stBins RAT Analysis	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/gh0stbins_rat_analysis_c3247a6f-a237-42c1-b6a7-bc7b5a1e890a/Gh0stbinsbgihjbhhhb1_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230702%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230702T053250Z&X-Amz-Expires=600&X-Amz-Signature=3c1a2391be74ac54df1c6e44055bccf1e5c9419c02490f308cb4328395b0b01f&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-06-29	8Base Ransomware - A Heavy Hitting Player	Eightbasebgiiacggfh3_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-06-29	8Base Ransomware - A Heavy Hitting Player	Eightbasebgiiacggfh2_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-06-29	8Base Ransomware - A Heavy Hitting Player	Eightbasebgiiacggfh1_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-06-29	8Base Ransomware - A Heavy Hitting Player	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/8base_ransomware_-_a_heavy_hitting_player_a5893f49-67e5-45ef-a151-6ce0c11c6ff8/Eightbasebgiiacggfh4_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230629%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230629T082224Z&X-Amz-Expires=600&X-Amz-Signature=113b50c86c956d5b19105986404c80801e6a137d9c07abf650626058ffffc208&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Blocked
2023-06-29	Tracing The Footsteps Of Red Wolf	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/tracing_the_footsteps_of_red_wolf_4c0c8a2b-4185-4f42-9746-029b05056114/Tracingbgiiaaecbg3_browsingDll.dll?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230629%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230629T060209Z&X-Amz-Expires=600&X-Amz-Signature=0bfb162a9097a95dc463de7bf8c1b34fd826d807de14e69d95761b47c9f40a7a&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-06-29	Tracing The Footsteps Of Red Wolf	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/tracing_the_footsteps_of_red_wolf_4c0c8a2b-4185-4f42-9746-029b05056114/Tracingbgiiaaecbg2_browsingLnk.lnk?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230629%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230629T060209Z&X-Amz-Expires=600&X-Amz-Signature=b34a9cb0f97e3666ec03376a33301fd684762f5db3e2b32a3b8de3e4dfa6bb42&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-06-29	Tracing The Footsteps Of Red Wolf	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/tracing_the_footsteps_of_red_wolf_4c0c8a2b-4185-4f42-9746-029b05056114/Tracingbgiiaaecbg1_browsingIso.iso?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230629%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230629T060208Z&X-Amz-Expires=600&X-Amz-Signature=c618f855b1c0a5d63b573563b28ea6ff3db96a5cd67362aecec3b2c431016264&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-06-28	Wagner Ransomware Cyber Recruitment	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/wagner_ransomware_cyber_recruitment_8554ca68-cbf7-4a40-9e5c-35fa77b13e87/Wagnerbgihjbhidd5_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230628%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230628T064353Z&X-Amz-Expires=600&X-Amz-Signature=ddb79c0ccc58ca818ee01d24dc007622003d35ca13797b2ea024faf97ec43750&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
N/A	Python-Based Loader Masquerading As OneDrive Utilities To Drop Multiple RATs	Python_basedbgihfhchhc1_edr72Js.js	Endpoint Security	GLESEC-AWS-CYMU	Blocked

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

TLP:AMBER

ASM-VP REPORT

GLESEC 07/26/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
N/A	Python-Based Loader Masquerading As OneDrive Utilities To Drop Multiple RATs	Python_basedbgihfhchhc1_edr73Lnk.lnk	Endpoint Security	GLESEC-AWS-CYMU	Blocked
N/A	Python-Based Loader Masquerading As OneDrive Utilities To Drop Multiple RATs	Python_basedbgihfhchhc1_edr76Lnk.lnk	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-06-27	Python-Based Loader Masquerading As OneDrive Utilities To Drop Multiple RATs	Python_basedbgihfhchhc166_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-06-27	Python-Based Loader Masquerading As OneDrive Utilities To Drop Multiple RATs	Python_basedbgihfhchhc16_edr7Dll.dll	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-06-27	Python-Based Loader Masquerading As OneDrive Utilities To Drop Multiple RATs	Python_basedbgihfhchhc1_edr70Exe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-06-27	Python-Based Loader Masquerading As OneDrive Utilities To Drop Multiple RATs	Python_basedbgihfhchhc169_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-06-27	Python-Based Loader Masquerading As OneDrive Utilities To Drop Multiple RATs	hxxp://134.19.179.147	Web Gateway	GLESEC-AWS-CYMU	Offline/Removed
2023-06-27	Python-Based Loader Masquerading As OneDrive Utilities To Drop Multiple RATs	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/pyt hon-based_loader_masquerading_as_onedrive_utilities_to_drop_multiple_rats_b625cc 6d-f13a-4148-828e-c3925f11db4c/Python_basedbgihfhchhc1_browsing78Exe.exe?X-Amz-A lgorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential =AKIAJPJC2Q3D5GWFTK3Q%2F20230627%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=2023 0627T044701Z&X-Amz-Expires=600&X-Amz-Signature=2c027a7b6e37d698d83fb4a695ed6b8ec 434c965ccd2e518c05509ab9f8dd25c&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-06-27	Python-Based Loader Masquerading As OneDrive Utilities To Drop Multiple RATs	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/pyt hon-based_loader_masquerading_as_onedrive_utilities_to_drop_multiple_rats_b625cc 6d-f13a-4148-828e-c3925f11db4c/Python_basedbgihfhchhc168_browsingPs1.ps1?X-Amz-A lgorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential =AKIAJPJC2Q3D5GWFTK3Q%2F20230627%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=2023 0627T044700Z&X-Amz-Expires=600&X-Amz-Signature=d7b76f4b5ca6020e7fe5582ff6c1821d0 c56433ea69bc5bd9a48aeb0000f6b65&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-06-26	Operation Magalenha - Long-Running Campaign Pursues Portuguese Credentials and PII	Magalenhabgihgjegca94_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-06-26	Operation Magalenha - Long-Running Campaign Pursues Portuguese Credentials and PII	Magalenhabgihgjegca9_edr7Exe.exe	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-06-26	Operation Magalenha - Long-Running Campaign Pursues Portuguese Credentials and PII	Magalenhabgihgjegca104_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

TLP:AMBER

GLESEC
COMPLETELY PERCEPTI

ASM-VP REPORT

GLESEC 07/26/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-06-26	Operation Magalenha - Long-Running Campaign Pursues Portuguese Credentials and PII	Magalenhabgihgjegca98_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-06-26	Operation Magalenha - Long-Running Campaign Pursues Portuguese Credentials and PII	Magalenhabgihgjegca101_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-06-26	Operation Magalenha - Long-Running Campaign Pursues Portuguese Credentials and PII	Magalenhabgihgjegca99_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
N/A	Operation Magalenha - Long-Running Campaign Pursues Portuguese Credentials and PII	Magalenhabgihgjegca100_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-06-26	Operation Magalenha - Long-Running Campaign Pursues Portuguese Credentials and PII	Magalenhabgihgjegca92_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-06-26	Operation Magalenha - Long-Running Campaign Pursues Portuguese Credentials and PII	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/operation_magalenha_-_long-running_campaign_pursues_portuguese_credentials_and_pii_39302ab3-8137-4c47-8629-bc09e763c579/Magalenhabgihgjegca90_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230626%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230626T125622Z&X-Amz-Expires=600&X-Amz-Signature=5e4401063d89f8ab37796f43511f71d68c2a3312e1ac7469881bd66e7cd4b67e&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-06-26	Operation Magalenha - Long-Running Campaign Pursues Portuguese Credentials and PII	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/operation_magalenha_-_long-running_campaign_pursues_portuguese_credentials_and_pii_39302ab3-8137-4c47-8629-bc09e763c579/Magalenhabgihgjegca91_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230626%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230626T125616Z&X-Amz-Expires=600&X-Amz-Signature=af50a5e8e32b9f893e32a715f3a756e94819cbefaf06660dee683d3162f8891e&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-06-26	Operation Magalenha - Long-Running Campaign Pursues Portuguese Credentials and PII	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/operation_magalenha_-_long-running_campaign_pursues_portuguese_credentials_and_pii_39302ab3-8137-4c47-8629-bc09e763c579/Magalenhabgihgjegca93_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230626%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230626T125613Z&X-Amz-Expires=600&X-Amz-Signature=60895b0abd94a5dd6c74bf5db2232fea6074c135fd02320bc17d14d3b24a0e83&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-06-26	Operation Magalenha - Long-Running Campaign Pursues Portuguese Credentials and PII	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/operation_magalenha_-_long-running_campaign_pursues_portuguese_credentials_and_pii_39302ab3-8137-4c47-8629-bc09e763c579/Magalenhabgihgjegca102_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230626%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230626T125547Z&X-Amz-Expires=600&X-Amz-Signature=6c75eb573a14d63c71a5e7b989586a22d00888d8ce31e8ae2bd50898d993ebca&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-06-26	Operation Magalenha - Long-Running Campaign Pursues Portuguese Credentials and PII	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/operation_magalenha_-_long-running_campaign_pursues_portuguese_credentials_and_pii_39302ab3-8137-4c47-8629-bc09e763c579/Magalenhabgihgjegca103_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230626%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230626T125541Z&X-Amz-Expires=600&X-Amz-Signature=40c7ae40a36acb07f4b283fe54ed260c2b6699f23cbe0ad7350d57b088ca1ae3&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

TLP:AMBER

GLESEC
COMPLETELY PERCEPTI

ASM-VP REPORT

GLESEC 07/26/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-06-26	Operation Magalenha - Long-Running Campaign Pursues Portuguese Credentials and PII	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/operation_magalenha_-_long-running_campaign_pursues_portuguese_credentials_and_pii_39302ab3-8137-4c47-8629-bc09e763c579/Magalenhabgihgjegca105_browsingExe.exe?X-Am z-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230626%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230626T125534Z&X-Amz-Expires=600&X-Amz-Signature=2e7d52210605739dbd2ab62dbb8afa96150f246b32fc74b6289084e9b7c518c0&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-06-26	Operation Magalenha - Long-Running Campaign Pursues Portuguese Credentials and PII	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/operation_magalenha_-_long-running_campaign_pursues_portuguese_credentials_and_pii_39302ab3-8137-4c47-8629-bc09e763c579/Magalenhabgihgjegca10_browsing7Exe.exe?X-Am z-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230626%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230626T125528Z&X-Amz-Expires=600&X-Amz-Signature=c2a04f7ac1f7bcd97f733674edfbe1db1686056a78d4acec0d18dc16eff78333&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-06-26	Crysis And Venus Ransomware Installed Via RDP	Crysisbgihfhcije188_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-06-26	Crysis And Venus Ransomware Installed Via RDP	Crysisbgihfhcije180_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-06-26	Crysis And Venus Ransomware Installed Via RDP	Crysisbgihfhcije184_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-06-26	Crysis And Venus Ransomware Installed Via RDP	Crysisbgihfhcije182_edrDll.dll	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-06-26	Crysis And Venus Ransomware Installed Via RDP	Crysisbgihfhcije181_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-06-26	Crysis And Venus Ransomware Installed Via RDP	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/crysis_and_venus_ransomware_installed_via_rdp_f8741241-ed45-4a8f-8e68-09566cd32555/Crysisbgihfhcije194_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230626%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230626T062942Z&X-Amz-Expires=600&X-Amz-Signature=bf75f5946cd81a8ab9a186a06497e344fab05f627bf1c1b449d0aba8bb8aecf6&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-06-26	Crysis And Venus Ransomware Installed Via RDP	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/crysis_and_venus_ransomware_installed_via_rdp_f8741241-ed45-4a8f-8e68-09566cd32555/Crysisbgihfhcije190_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230626%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230626T062942Z&X-Amz-Expires=600&X-Amz-Signature=088d19c2d389d9650e3a28c3765522bca05bc3c0bcbc7da69e9d61dbb734bb3e&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-06-26	Crysis And Venus Ransomware Installed Via RDP	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/crysis_and_venus_ransomware_installed_via_rdp_f8741241-ed45-4a8f-8e68-09566cd32555/Crysisbgihfhcije186_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230626%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230626T062941Z&X-Amz-Expires=600&X-Amz-Signature=2b290d2690c3b3ad67bb88ab43b27450236b55f6b0b34c8afe9827739a261ace&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-06-26	Crysis And Venus Ransomware Installed Via RDP	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/crysis_and_venus_ransomware_installed_via_rdp_f8741241-ed45-4a8f-8e68-09566cd32555/Crysisbgihfhcije185_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230626%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230626T062941Z&X-Amz-Expires=600&X-Amz-Signature=61d7844fd3ce85225e86d9a985d6abb16b64881d0af4c2a09c9f53bc793bfb98&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-06-26	Crysis And Venus Ransomware Installed Via RDP	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/crysis_and_venus_ransomware_installed_via_rdp_f8741241-ed45-4a8f-8e68-09566cd32555/Crysisbgihfhcije183_browsingDll.dll?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230626%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230626T062940Z&X-Amz-Expires=600&X-Amz-Signature=dd4abc0b7a50967752853ee8804d926768c828197a88e72da7b0dbadb682d05a&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-06-26	Crysis And Venus Ransomware Installed Via RDP	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/crysis_and_venus_ransomware_installed_via_rdp_f8741241-ed45-4a8f-8e68-09566cd32555/Crysisbgihfhcije1_browsing79Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230626%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230626T062938Z&X-Amz-Expires=600&X-Amz-Signature=2babccf17a563d948f368224413e1051f14eaa58ab7461a458fdf3779e13c63f&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-10	Operation Brainleeches Targets Microsoft 365 Users	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/operation_brainleeches_targets_microsoft_365_users_acac1185-0d7f-47a2-8dfc-ddea7a245502/Operationbgiihibied11_browsingJs.js?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz- Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230710 %2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230710T102356Z&X-Amz-Expires=600&X -Amz-Signature=0a156c394f8f0ef81b203f1fe80df1391bec763157c7da173b73b4ff8776afcd& X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

TLP:AMBER

GLESEC
COMPLETELY PERCEPTI

ASM-VP REPORT

GLESEC 07/26/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-07-10	TeamTNT Targets Cloud Native Environments	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/teamtnt_targets_cloud_native_environments_b865aebc-e863-4bd8-b32b-3f6ee3bd2645/Teamtntbgiigjfdih2_browsingElf.elf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230710%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230710T072454Z&X-Amz-Expires=600&X-Amz-Signature=85da2ae0c729b7cad4cfb2dbf16d01926d1f81a6066fc9333c3eed651c8719e9&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-10	TeamTNT Targets Cloud Native Environments	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/teamtnt_targets_cloud_native_environments_b865aebc-e863-4bd8-b32b-3f6ee3bd2645/Teamtntbgiigjfdih1_browsingElf.elf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230710%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230710T072453Z&X-Amz-Expires=600&X-Amz-Signature=28c8462295d7bf4ed55ff3bf4484bce303f3f0ce90c087ff47fe87e635ff8428&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-09	US Cert Alert - (AA23-187A) Increased Truebot Activity Infects U.S. And Canada Networks	Truebotbgiiijfbga1_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-07-09	US Cert Alert - (AA23-187A) Increased Truebot Activity Infects U.S. And Canada Networks	Truebotbgiiijfbga3_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-09	US Cert Alert - (AA23-187A) Increased Truebot Activity Infects U.S. And Canada Networks	Truebotbgiiijfbga4_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-09	US Cert Alert - (AA23-187A) Increased Truebot Activity Infects U.S. And Canada Networks	Truebotbgiiijfbga_edr7Dll.dll	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-09	US Cert Alert - (AA23-187A) Increased Truebot Activity Infects U.S. And Canada Networks	hxxp://45.227.253.102	Web Gateway	GLESEC-AWS-CYMU	Offline/Removed
2023-07-09	US Cert Alert - (AA23-187A) Increased Truebot Activity Infects U.S. And Canada Networks	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/us_ cert_alert_-_%28aa23-187a%29_increased_truebot_activity_infects_u.s.and_canada_networks_c18bd470-6c4d-4289-a966-659944d071c9/Truebotbgiiijfbga9_browsingDll.dll? X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230709T102858Z&X-Amz-Expires=600&X-Amz-Signature=4456b0ff5fbf574668f831c229514705b724fe1bef779ddb1194b9413c68ef49&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-09	US Cert Alert - (AA23-187A) Increased Truebot Activity Infects U.S. And Canada Networks	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/us_ cert_alert_-_%28aa23-187a%29_increased_truebot_activity_infects_u.s.and_canada_networks_c18bd470-6c4d-4289-a966-659944d071c9/Truebotbgiiijfbga8_browsingDll.dll? X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230709T102857Z&X-Amz-Expires=600&X-Amz-Signature=b6814e25ff1bf83285e08e5fb51ebbb4584f11852855146e59d943d243ad1d97&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-09	US Cert Alert - (AA23-187A) Increased Truebot Activity Infects U.S. And Canada Networks	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/us_ cert_alert_-_%28aa23-187a%29_increased_truebot_activity_infects_u.s.and_canada_networks_c18bd470-6c4d-4289-a966-659944d071c9/Truebotbgiiijfbga6_browsingExe.exe? X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230709T102857Z&X-Amz-Expires=600&X-Amz-Signature=e0f33ab10835f2c67a2b3d469629c843f0953e004f1e7fec78ae02140ebc4c24&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-09	US Cert Alert - (AA23-187A) Increased Truebot Activity Infects U.S. And Canada Networks	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/us_ cert_alert_-_%28aa23-187a%29_increased_truebot_activity_infects_u.s.and_canada_networks_c18bd470-6c4d-4289-a966-659944d071c9/Truebotbgiiijfbga5_browsingExe.exe? X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230709T102856Z&X-Amz-Expires=600&X-Amz-Signature=899d50d3a181f6bfcc0ef167ed32c7a0b6fc4cf843204d444c1e3639d73a0b5d&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-09	US Cert Alert - (AA23-187A) Increased Truebot Activity Infects U.S. And Canada Networks	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/us_ cert_alert_-_%28aa23-187a%29_increased_truebot_activity_infects_u.s.and_canada_networks_c18bd470-6c4d-4289-a966-659944d071c9/Truebotbgiiijfbga2_browsingExe.exe? X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230709T102850Z&X-Amz-Expires=600&X-Amz-Signature=6f3544d37de557faf85779a3131095c3e0fdb26cafd64a40044d4dcdf1fc172a&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-09	Buddyransome	Buddyransombgiiiijacb2_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

TLP:AMBER

ASM-VP REPORT

GLESEC 07/26/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-07-09	Buddyransome	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/buddyransome_8cb491e4-5136-4deb-8e19-2027964f5bd2/Buddyransombgiiiijacb1_browsingEx e.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-A mz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230709%2Feu-west-1%2Fs3%2Faws4_request&X- Amz-Date=20230709T080250Z&X-Amz-Expires=600&X-Amz-Signature=0ac1bd8f044640e0e3c8d676f556174fd2bfe957a07d7cf6dd5f0013517b2db5&X-Amz-SignedHeaders=host&x-id=GetOb ject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-09	Threat Profile UNC3944	Threatbgiigjfhhb66_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-09	Threat Profile UNC3944	Threatbgiigjfhhb_edr71Exe.exe	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-07-09	Threat Profile UNC3944	Threatbgiigjfhhb_edr70Elf.elf	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-09	Threat Profile UNC3944	Threatbgiigjfhhb_edr74Exe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-09	Threat Profile UNC3944	Threatbgiigjfhhb81_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-09	Threat Profile UNC3944	Threatbgiigjfhhb_edr78Exe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-09	Threat Profile UNC3944	hxxp://149.28.110.16	Web Gateway	GLESEC-AWS-CYMU	Offline/Removed
2023-07-26	New Reptile Rootkit Malware Attacking Linux Systems Using Port Knocking	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/new_reptile_rootkit_malware_attacking_linux_systems_using_port_knocking_c90e131d-0bd0-4024-978d-6ccdbb54f8c0/Newbgjadaaiej_browsing7Elf.elf?X-Amz-Algorithm=AWS4-HM AC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GW FTK3Q%2F20230726%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230726T074212Z&X-Amz-Expires=600&X-Amz-Signature=b94c8c0368ed936f9e1dae7a14357d8e5b6b1c437e66807f523514635ea11715&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-26	New Reptile Rootkit Malware Attacking Linux Systems Using Port Knocking	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/new_reptile_rootkit_malware_attacking_linux_systems_using_port_knocking_c90e131d-0bd0-4024-978d-6ccdbb54f8c0/Newbgjadaaiej5_browsingO.o?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230726%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230726T074211Z&X-Amz-Expires=600&X-Amz-Signature=9071c6bdc3555c0429f9a1495710def159cb8d5e2d35a0f1ee26b93e60808f2e&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-26	New Reptile Rootkit Malware Attacking Linux Systems Using Port Knocking	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/new_reptile_rootkit_malware_attacking_linux_systems_using_port_knocking_c90e131d-0bd0-4024-978d-6ccdbb54f8c0/Newbgjadaaiej4_browsingO.o?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230726%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230726T074211Z&X-Amz-Expires=600&X-Amz-Signature=9c8ffa895abfaefe6c992bcfcd2aaee2e46b5d7a7dd598fa7a933d137d434157&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-25	Ransomware Spotlight Play	Ransomwarebgjacdgace2_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-07-25	Ransomware Spotlight Play	Ransomwarebgjacdgace8_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-07-25	Ransomware Spotlight Play	Ransomwarebgjacdgace_edr7Exe.exe	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-07-25	Ransomware Spotlight Play	Ransomwarebgjacdgace4_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-25	Ransomware Spotlight Play	Ransomwarebgjacdgace10_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-25	Ransomware Spotlight Play	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ransomware_spotlight_play_9c7a6699-8793-486d-b28c-2b289d802cf8/Ransomwarebgjacdgace14_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNE D-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230725%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230725T060149Z&X-Amz-Expires=600&X-Amz-Signature=0c596ff1dad491faecc5111d0abf5681f592511259e4db49b268a6b68e612043&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-25	Ransomware Spotlight Play	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ransomware_spotlight_play_9c7a6699-8793-486d-b28c-2b289d802cf8/Ransomwarebgjacdgace12_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNE D-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230725%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230725T060149Z&X-Amz-Expires=600&X-Amz-Signature=0c491ec91a254b34895b93244cec1f0deb5aa206c6041ef263e432518af74c0c&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-25	Ransomware Spotlight Play	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ransomware_spotlight_play_9c7a6699-8793-486d-b28c-2b289d802cf8/Ransomwarebgjacdgace11_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNE D-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230725%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230725T060143Z&X-Amz-Expires=600&X-Amz-Signature=f2c4c0be4962e97bd278ad3a04abb55f22098371ed9949dbcb8c8c7b683649b1&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

TLP:AMBER

ASM-VP REPORT

GLESEC 07/26/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-07-25	Ransomware Spotlight Play	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ransomware_spotlight_play_9c7a6699-8793-486d-b28c-2b289d802cf8/Ransomwarebgjacdgace9_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230725%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230725T060143Z&X-Amz-Expires=600&X-Amz-Signature=e0d62adec34c41ebbfd3b7a0c8fb0087c941015ea66cd7d720edb14d4ef04d99&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-25	Ransomware Spotlight Play	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ransomware_spotlight_play_9c7a6699-8793-486d-b28c-2b289d802cf8/Ransomwarebgjacdgace5_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230725%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230725T060142Z&X-Amz-Expires=600&X-Amz-Signature=d8dbb7f3c6302caff7914eef19e0c18c30a45bdb02b4d9603ac7e34a824f7029&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-25	Ransomware Spotlight Play	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ransomware_spotlight_play_9c7a6699-8793-486d-b28c-2b289d802cf8/Ransomwarebgjacdgace3_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230725%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230725T060141Z&X-Amz-Expires=600&X-Amz-Signature=c87cca4b4796e2909cf071cf42e1a6c4f2164176b5314dab094323d4d13bf4bd&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-25	Ransomware Spotlight Play	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ransomware_spotlight_play_9c7a6699-8793-486d-b28c-2b289d802cf8/Ransomwarebgjacdgace1_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230725%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230725T060140Z&X-Amz-Expires=600&X-Amz-Signature=888029155be514ee1e73a067bdbcceddc8626968474ce675eb9f7ae99958d6b7&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-24	Ursnif campaign in Italy	hxxp://109.105.198.129/pictures/...	Web Gateway	GLESEC-AWS-CYMU	Offline/Removed
2023-07-24	Ursnif campaign in Italy	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ursnif_campaign_in_italy_dcb21441-3f3a-4596-a36a-f8929756993e/Ursnifbgijhigahi4_browsingPs1.ps1?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230724%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230724T065516Z&X-Amz-Expires=600&X-Amz-Signature=89167b3edec621b9aaf54425e3d5f786d377eeab3a54b046883d777de935402b&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-24	Ursnif campaign in Italy	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ursnif_campaign_in_italy_dcb21441-3f3a-4596-a36a-f8929756993e/Ursnifbgijhigahi1_bro wsingDll.dll?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYL OAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230724%2Feu-west-1%2Fs3%2Faws4_req uest&X-Amz-Date=20230724T065515Z&X-Amz-Expires=600&X-Amz-Signature=aae77aa7817b4830dd0bca1aaf8244d24dae592b849a492df3b5c380db9e7b8e&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-23	Manipulated Caiman: The Sophisticated Snare of Mexico's Banking Predator	Manipulatedcaimanbgjabaaibd15_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-23	Manipulated Caiman: The Sophisticated Snare of Mexico's Banking Predator	Manipulatedcaimanbgjabaaibd14_edrJs.js	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-23	Manipulated Caiman: The Sophisticated Snare of Mexico's Banking Predator	Manipulatedcaimanbgjabaaibd12_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-23	Manipulated Caiman: The Sophisticated Snare of Mexico's Banking Predator	Manipulatedcaimanbgjabaaibd11_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-23	Manipulated Caiman: The Sophisticated Snare of Mexico's Banking Predator	Manipulatedcaimanbgjabaaibd8_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-23	Manipulated Caiman: The Sophisticated Snare of Mexico's Banking Predator	Manipulatedcaimanbgjabaaibd3_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-23	Manipulated Caiman: The Sophisticated Snare of Mexico's Banking Predator	Manipulatedcaimanbgjabaaibd_edr7Exe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked

TLP:AMBER

ASM-VP REPORT

GLESEC 07/26/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-07-23	Manipulated Caiman: The Sophisticated Snare of Mexico's Banking Predator	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/manipulated_caiman%3A_the_sophisticated_snare_of_mexico%27s_banking_predator_4b58497a-83ae-4fdd-bb38-8219794cb25b/Manipulatedcaimanbgjabaaibd1_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230723%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230723T085406Z&X-Amz-Expires=600&X-Amz-Signature=c577f378133468b6fb163dbb3683459e6b61455036bed2698a5044a8756b1655&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-23	Manipulated Caiman: The Sophisticated Snare of Mexico's Banking Predator	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/manipulated_caiman%3A_the_sophisticated_snare_of_mexico%27s_banking_predator_4b58497a-83ae-4fdd-bb38-8219794cb25b/Manipulatedcaimanbgjabaaibd2_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230723%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230723T085406Z&X-Amz-Expires=600&X-Amz-Signature=b39762c8935098e220a3cc647b78edf6c3b31ab64c2efcf5f588fae3fc66fd17&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-23	Manipulated Caiman: The Sophisticated Snare of Mexico's Banking Predator	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/manipulated_caiman%3A_the_sophisticated_snare_of_mexico%27s_banking_predator_4b58497a-83ae-4fdd-bb38-8219794cb25b/Manipulatedcaimanbgjabaaibd4_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230723%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230723T085405Z&X-Amz-Expires=600&X-Amz-Signature=685eec5fb7737969b86b20548bbbe65e17d951322a7b144ccf389418828e3bae&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-23	Manipulated Caiman: The Sophisticated Snare of Mexico's Banking Predator	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/manipulated_caiman%3A_the_sophisticated_snare_of_mexico%27s_banking_predator_4b58497a-83ae-4fdd-bb38-8219794cb25b/Manipulatedcaimanbgjabaaibd5_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230723%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230723T085405Z&X-Amz-Expires=600&X-Amz-Signature=17a2b111fb07c7c1f417bab02e09240a1a88ef147a35c92ef1f8f39b56dcf4c6&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-23	Manipulated Caiman: The Sophisticated Snare of Mexico's Banking Predator	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/manipulated_caiman%3A_the_sophisticated_snare_of_mexico%27s_banking_predator_4b58497a-83ae-4fdd-bb38-8219794cb25b/Manipulatedcaimanbgjabaaibd6_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230723%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230723T085359Z&X-Amz-Expires=600&X-Amz-Signature=65509abf3a035a8025b78c7cbe3695ba4f0d55f36a4a0628f6b5d4cd5d88b6d3&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-23	Manipulated Caiman: The Sophisticated Snare of Mexico's Banking Predator	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/manipulated_caiman%3A_the_sophisticated_snare_of_mexico%27s_banking_predator_4b58497a-83ae-4fdd-bb38-8219794cb25b/Manipulatedcaimanbgjabaaibd9_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230723%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230723T085358Z&X-Amz-Expires=600&X-Amz-Signature=36dcaeb961a47f9404578553ab3fa7e49d9444145c3945f2d0e54f6a1c847695&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-23	Manipulated Caiman: The Sophisticated Snare of Mexico's Banking Predator	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/manipulated_caiman%3A_the_sophisticated_snare_of_mexico%27s_banking_predator_4b58497a-83ae-4fdd-bb38-8219794cb25b/Manipulatedcaimanbgjabaaibd10_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230723%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230723T085358Z&X-Amz-Expires=600&X-Amz-Signature=79caf697c8cdef3e9a6f7fbd0e71cf745ff50cf0b534c8279699adfcdf24cbc8&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-23	Manipulated Caiman: The Sophisticated Snare of Mexico's Banking Predator	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/manipulated_caiman%3A_the_sophisticated_snare_of_mexico%27s_banking_predator_4b58497a-83ae-4fdd-bb38-8219794cb25b/Manipulatedcaimanbgjabaaibd13_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230723%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230723T085357Z&X-Amz-Expires=600&X-Amz-Signature=b6ae26f5934cdec71c60ceae5dd41f10b41d52f1690a7011b7c512a076bd7061&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-23	A Look Into Space Pirates Unconventional Techniques Attack Vectors And Tools	Abgijibigeg18_edrDll.dll	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-23	A Look Into Space Pirates Unconventional Techniques Attack Vectors And Tools	Abgijibigeg21_edrDll.dll	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-07-23	A Look Into Space Pirates Unconventional Techniques Attack Vectors And Tools	Abgijibigeg63_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-07-23	A Look Into Space Pirates Unconventional Techniques Attack Vectors And Tools	Abgijibigeg66_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Penetrated

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

TLP:AMBER

GLESEC
COMPLETELY PERCEPTI

ASM-VP REPORT

GLESEC 07/26/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-07-23	A Look Into Space Pirates Unconventional Techniques Attack Vectors And Tools	Abgijibigeg64_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-07-23	A Look Into Space Pirates Unconventional Techniques Attack Vectors And Tools	Abgijibigeg58_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-07-23	A Look Into Space Pirates Unconventional Techniques Attack Vectors And Tools	Abgijibigeg23_edrDll.dll	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-23	A Look Into Space Pirates Unconventional Techniques Attack Vectors And Tools	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/a_look_into_space_pirates_unconventional_techniques_attack_vectors_and_tools_995867 c2-733c-4527-bde5-5c324ac95e6d/Abgijibigeg6_browsing7Exe.exe?X-Amz-Algorithm=AWS 4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230723%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230723T064227Z&X-Amz-Expires=600&X-Amz-Signature=16d474b66e92668f9410a657b4277a9012b0a1a81310bb9df46bd09907ed53e0&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-23	A Look Into Space Pirates Unconventional Techniques Attack Vectors And Tools	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/a_look_into_space_pirates_unconventional_techniques_attack_vectors_and_tools_995867 c2-733c-4527-bde5-5c324ac95e6d/Abgijibigeg65_browsingExe.exe?X-Amz-Algorithm=AWS 4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230723%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230723T064226Z&X-Amz-Expires=600&X-Amz-Signature=a0e3dba13cba653553bfc14e3d3794547286271efc22f587c4ba837ec5ee5289&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-23	A Look Into Space Pirates Unconventional Techniques Attack Vectors And Tools	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/a_look_into_space_pirates_unconventional_techniques_attack_vectors_and_tools_995867 c2-733c-4527-bde5-5c324ac95e6d/Abgijibigeg62_browsingExe.exe?X-Amz-Algorithm=AWS 4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230723%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230723T064220Z&X-Amz-Expires=600&X-Amz-Signature=554da1d5ee54059c34884591eb12454b68e91ce08391ca36294d79b79ad14f15&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-23	A Look Into Space Pirates Unconventional Techniques Attack Vectors And Tools	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/a_look_into_space_pirates_unconventional_techniques_attack_vectors_and_tools_995867 c2-733c-4527-bde5-5c324ac95e6d/Abgijibigeg30_browsingDll.dll?X-Amz-Algorithm=AWS 4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230723%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230723T064219Z&X-Amz-Expires=600&X-Amz-Signature=da6c83d84b597a7d206aac6fec9ec3ed2ef29ab9f6bf65b18e6aeaf63e13b34c&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-23	A Look Into Space Pirates Unconventional Techniques Attack Vectors And Tools	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/a_look_into_space_pirates_unconventional_techniques_attack_vectors_and_tools_995867 c2-733c-4527-bde5-5c324ac95e6d/Abgijibigeg28_browsingDll.dll?X-Amz-Algorithm=AWS 4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230723%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230723T064219Z&X-Amz-Expires=600&X-Amz-Signature=df2276df0867cad04cb4aeb8f588b9931937e6a513280c5610239b66da981927&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-23	A Look Into Space Pirates Unconventional Techniques Attack Vectors And Tools	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/a_look_into_space_pirates_unconventional_techniques_attack_vectors_and_tools_995867 c2-733c-4527-bde5-5c324ac95e6d/Abgijibigeg24_browsingDll.dll?X-Amz-Algorithm=AWS 4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230723%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230723T064219Z&X-Amz-Expires=600&X-Amz-Signature=d17b4694ca841d140b65e127be8ea13deede83036e26ab83c9680a36044716ee&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-23	A Look Into Space Pirates Unconventional Techniques Attack Vectors And Tools	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/a_look_into_space_pirates_unconventional_techniques_attack_vectors_and_tools_995867 c2-733c-4527-bde5-5c324ac95e6d/Abgijibigeg22_browsingDll.dll?X-Amz-Algorithm=AWS 4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230723%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230723T064218Z&X-Amz-Expires=600&X-Amz-Signature=ae5d88156858b6a76d937a7a49dda981de6ea1d01bc38017ba7eec186fb25c0a&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-23	Threat Actor Launches ScarLeteel 2.00	Threatbgijdaabfc2_edrSh.sh	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-07-23	Threat Actor Launches ScarLeteel 2.00	Threatbgijdaabfc4_edrSh.sh	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-23	Threat Actor Launches ScarLeteel 2.00	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/threat_actor_launches_scarleteel_2.0_5c3a31c4-d75d-4f35-8a4e-ab9dc96ff553/Threatbgijdaabfc3_browsingSh.sh?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230723%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230723T063743Z&X-Amz-Expires=600&X-Amz-Signature=bb41cda5e09c36e6ee1bfca20acc0d1512fe1ab24d482806aaa4d78e4b8c7bf1&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

TLP:AMBER

GLESEC
COMPLETELY PERCEPTI

ASM-VP REPORT

GLESEC 07/26/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-07-20	The Turla APT Group Uses Multiple Malware Families To Exfiltrate Data (CERT-UA6981)	Thebgijibifhf1_edrDll.dll	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-07-20	The Turla APT Group Uses Multiple Malware Families To Exfiltrate Data (CERT-UA6981)	hxxps://mail.kzp.bg/outlook/api/logoff.aspx	Web Gateway	GLESEC-AWS-CYMU	Offline/Removed
2023-07-20	DDoS Botnet Targets Zyxel Vulnerability (CVE-2023-28771)	Ddosbgijibiigd_edr78Elf.elf	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-20	DDoS Botnet Targets Zyxel Vulnerability (CVE-2023-28771)	Ddosbgijibiigd84_edrElf.elf	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-20	DDoS Botnet Targets Zyxel Vulnerability (CVE-2023-28771)	Ddosbgijibiigd86_edrElf.elf	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-20	DDoS Botnet Targets Zyxel Vulnerability (CVE-2023-28771)	Ddosbgijibiigd80_edrElf.elf	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-20	DDoS Botnet Targets Zyxel Vulnerability (CVE-2023-28771)	hxxp://109.207.200.44	Web Gateway	GLESEC-AWS-CYMU	Offline/Removed
2023-07-20	DDoS Botnet Targets Zyxel Vulnerability (CVE-2023-28771)	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ddos_botnet_targets_zyxel_vulnerability_%28cve-2023-28771%29_726e7b63-4627-4776-a657-7c9d9a38820c/Ddosbgijibiigd83_browsingElf.elf?X-Amz-Algorithm=AWS4-HMAC-SHA256 &X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230720%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230720T053347Z&X-Amz-Expires=600&X-Amz-Signature=1a48739a76b35237b4ceabd48138cbf84859bcafde684a1784c1f6e8b7951ead&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-20	DDoS Botnet Targets Zyxel Vulnerability (CVE-2023-28771)	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ddos_botnet_targets_zyxel_vulnerability_%28cve-2023-28771%29_726e7b63-4627-4776-a657-7c9d9a38820c/Ddosbgijibiigd82_browsingElf.elf?X-Amz-Algorithm=AWS4-HMAC-SHA256 &X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230720%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230720T053346Z&X-Amz-Expires=600&X-Amz-Signature=9e811f4deb4ff91a1ce6fca8ed29ea0fe2f9c84e17d244e94fad9f27a1ea2979&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-20	DDoS Botnet Targets Zyxel Vulnerability (CVE-2023-28771)	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ddos_botnet_targets_zyxel_vulnerability_%28cve-2023-28771%29_726e7b63-4627-4776-a657-7c9d9a38820c/Ddosbgijibiigd81_browsingElf.elf?X-Amz-Algorithm=AWS4-HMAC-SHA256 &X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230720%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230720T053346Z&X-Amz-Expires=600&X-Amz-Signature=f6626099e299a0fbc6ae7f16bd3dcb8a86272bbf91baadad87c881614650d566&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-20	DDoS Botnet Targets Zyxel Vulnerability (CVE-2023-28771)	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ddos_botnet_targets_zyxel_vulnerability_%28cve-2023-28771%29_726e7b63-4627-4776-a657-7c9d9a38820c/Ddosbgijibiigd_browsing79Elf.elf?X-Amz-Algorithm=AWS4-HMAC-SHA256 &X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230720%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230720T053346Z&X-Amz-Expires=600&X-Amz-Signature=bc1d87de07bb2e371e47d8c1ddca43b00881f311568010de7fd4f9ca49db3281&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-20	DDoS Botnet Targets Zyxel Vulnerability (CVE-2023-28771)	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ddos_botnet_targets_zyxel_vulnerability_%28cve-2023-28771%29_726e7b63-4627-4776-a657-7c9d9a38820c/Ddosbgijibiigd_browsing77Elf.elf?X-Amz-Algorithm=AWS4-HMAC-SHA256 &X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230720%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230720T053344Z&X-Amz-Expires=600&X-Amz-Signature=f954f8ae4cd0805511bf5863f49a7acbb2b766d06c5fd5e04517263508962764&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-19	FIN8 Uses Revamped Sardonic Backdoor to Deliver Noberus Ransomware	Fin8bgijhbhgec4_edrPs1.ps1	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-07-19	FIN8 Uses Revamped Sardonic Backdoor to Deliver Noberus Ransomware	Fin8bgijhbhgec14_edrPs1.ps1	Endpoint Security	GLESEC-AWS-CYMU	Blocked

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

TLP:AMBER

GLESEC
COMPLETELY PERCEPTI

ASM-VP REPORT

GLESEC 07/26/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-07-19	Google Firebase Hosting Abused To Deliver Sorillus RAT	Googlebgijhdccbi4_edrZip.zip	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-19	Google Firebase Hosting Abused To Deliver Sorillus RAT	Googlebgijhdccbi5_edrHtml.html	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-07-19	Google Firebase Hosting Abused To Deliver Sorillus RAT	Googlebgijhdccbi8_edrHtml.html	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-07-19	Google Firebase Hosting Abused To Deliver Sorillus RAT	Googlebgijhdccbi9_edrHtml.html	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-07-19	FIN8 Uses Revamped Sardonic Backdoor to Deliver Noberus Ransomware	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/fin8_uses_revamped_sardonic_backdoor_to_deliver_noberus_ransomware_df7ab7db-17fe-4d78-9d45-04631de9cab9/Fin8bgijhbhgec19_browsingDll.dll?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230719%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230719T074903Z&X-Amz-Expires=600&X-Amz-Signature=74f0af56e9d6fd588736326e1e04e872e77a78589bea90c64443946c93566ad8&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-19	FIN8 Uses Revamped Sardonic Backdoor to Deliver Noberus Ransomware	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/fin8_uses_revamped_sardonic_backdoor_to_deliver_noberus_ransomware_df7ab7db-17fe-4d78-9d45-04631de9cab9/Fin8bgijhbhgec15_browsingDll.dll?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230719%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230719T074903Z&X-Amz-Expires=600&X-Amz-Signature=1d2161dd9cc700610535ae3759a3c584484696677272bc2e12b5d7566d9d9014&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-19	FIN8 Uses Revamped Sardonic Backdoor to Deliver Noberus Ransomware	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/fin8_uses_revamped_sardonic_backdoor_to_deliver_noberus_ransomware_df7ab7db-17fe-4d78-9d45-04631de9cab9/Fin8bgijhbhgec12_browsingDll.dll?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230719%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230719T074902Z&X-Amz-Expires=600&X-Amz-Signature=93bc0a3581cc2fe205ba5dfe09aab34a34ad943591e9705cbaf73cf90c90765c&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-19	FIN8 Uses Revamped Sardonic Backdoor to Deliver Noberus Ransomware	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/fin8_uses_revamped_sardonic_backdoor_to_deliver_noberus_ransomware_df7ab7db-17fe-4d78-9d45-04631de9cab9/Fin8bgijhbhgec10_browsingDll.dll?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230719%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230719T074902Z&X-Amz-Expires=600&X-Amz-Signature=4c7518b6400b0a555390693a4f613f8ae3faf41023ffa6900139c8ee02cd8cdc&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-19	FIN8 Uses Revamped Sardonic Backdoor to Deliver Noberus Ransomware	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/fin8_uses_revamped_sardonic_backdoor_to_deliver_noberus_ransomware_df7ab7db-17fe-4d78-9d45-04631de9cab9/Fin8bgijhbhgec9_browsingDll.dll?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230719%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230719T074902Z&X-Amz-Expires=600&X-Amz-Signature=3eb294f115581ae30212b1134e6aeef333902f8ffb7c46ff35272483c1b312dc&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-19	Google Firebase Hosting Abused To Deliver Sorillus RAT	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/google_firebase_hosting_abused_to_deliver_sorillus_rat_cc09fcb8-0060-4086-b1d8-29d1619ef79f/Googlebgijhdccbi10_browsingHtml.html?X-Amz-Algorithm=AWS4-HMAC-SHA256&X -Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230719%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230719T074807Z&X-Amz-Expires=600&X-Amz-Signature=484ea6ef0c56cc282418d4d6160a3be45a67342b809420c12c932ba5ed0aa2e5&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-19	Google Firebase Hosting Abused To Deliver Sorillus RAT	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/google_firebase_hosting_abused_to_deliver_sorillus_rat_cc09fcb8-0060-4086-b1d8-29d1619ef79f/Googlebgijhdccbi_browsing7Html.html?X-Amz-Algorithm=AWS4-HMAC-SHA256&X- Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230719%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230719T074807Z&X-Amz-Expires=600&X-Amz-Signature=4723b77175d5fa564966e9cd5435510cffeade966ff9e7283ffc5ae3eccc1bc3&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-19	Google Firebase Hosting Abused To Deliver Sorillus RAT	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/google_firebase_hosting_abused_to_deliver_sorillus_rat_cc09fcb8-0060-4086-b1d8-29d1619ef79f/Googlebgijhdccbi6_browsingHtml.html?X-Amz-Algorithm=AWS4-HMAC-SHA256&X- Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230719%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230719T074807Z&X-Amz-Expires=600&X-Amz-Signature=2638e8f28dd9daa7cc6491eddfa1040475d91a0e9a0e65fe4bcd1c32a49e1f2c&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-18	Infamous Meduza Stealer	Infamousbgijcbdjad11_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-18	Infamous Meduza Stealer	Infamousbgijcbdjad14_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-18	Infamous Meduza Stealer	Infamousbgijcbdjad13_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-18	Infamous Meduza Stealer	Infamousbgijcbdjad1_edr7Exe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked

TLP:AMBER

ASM-VP REPORT

GLESEC 07/26/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-07-18	Infamous Meduza Stealer	Infamousbgijcbdjad16_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-18	Infamous Meduza Stealer	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/infamous_meduza_stealer_21000adb-78d3-4a28-94c3-8427f297ac31/Infamousbgijcbdjad21_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230718%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230718T065227Z&X-Amz-Expires=600&X-Amz-Signature=c39134ec9f22b344c6af9f3b30f643b789a80fb7b5c6eeab8f1e2ccf1ffdc58f&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-18	Infamous Meduza Stealer	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/infamous_meduza_stealer_21000adb-78d3-4a28-94c3-8427f297ac31/Infamousbgijcbdjad20_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230718%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230718T065227Z&X-Amz-Expires=600&X-Amz-Signature=ccc45430ea251aabadb90210dc9cfe1f8287ea4711dd95cf3bc2830b5b67c055&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-18	Infamous Meduza Stealer	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/infamous_meduza_stealer_21000adb-78d3-4a28-94c3-8427f297ac31/Infamousbgijcbdjad12_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230718%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230718T065226Z&X-Amz-Expires=600&X-Amz-Signature=17aa170fa36b0f41bda9841f86e1a509725423aed5ce41009436769c2409ee4e&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-18	Infamous Meduza Stealer	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/infamous_meduza_stealer_21000adb-78d3-4a28-94c3-8427f297ac31/Infamousbgijcbdjad15_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230718%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230718T065225Z&X-Amz-Expires=600&X-Amz-Signature=c8b21045d8279034dd289e7c284ab8b922a6e8ff0485aaf25fcd6907471dc105&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-18	Infamous Meduza Stealer	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/infamous_meduza_stealer_21000adb-78d3-4a28-94c3-8427f297ac31/Infamousbgijcbdjad18_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230718%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230718T065225Z&X-Amz-Expires=600&X-Amz-Signature=c0b55513c32010af6790ca00da4c48129a252576568ca1397cecfd37ef4bc82b&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-18	Infamous Meduza Stealer	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/infamous_meduza_stealer_21000adb-78d3-4a28-94c3-8427f297ac31/Infamousbgijcbdjad19_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230718%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230718T065224Z&X-Amz-Expires=600&X-Amz-Signature=b5bf2590462ba96c23a20c609bfc3f10b07d8a9aefab9ad60fc326cd5323aaa7&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-18	APT36 Delivers Crimson RAT Using Pilgrimage Security Briefing Lure	Apt36bgijdaafca_edr77Exe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-18	APT36 Delivers Crimson RAT Using Pilgrimage Security Briefing Lure	Apt36bgijdaafca80_edrDocx.docx	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-18	APT36 Delivers Crimson RAT Using Pilgrimage Security Briefing Lure	Apt36bgijdaafca81_edrZip.zip	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-18	APT36 Delivers Crimson RAT Using Pilgrimage Security Briefing Lure	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/apt36_delivers_crimson_rat_using_pilgrimage_security_briefing_lure_d3803684-14d2-4b40-97f4-11d6c9cba750/Apt36bgijdaafca_browsing79Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230718%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230718T055524Z&X-Amz-Expires=600&X-Amz-Signature=a177955abc54f91c7ecd25be870c2e7c97edaa765bb576bd8d5ea779ba449511&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Blocked
2023-07-16	Cloudy With a Chance of Credentials | AWS-Targeting Cred Stealer Expands to Azure GCP	Cloudybgijdhcafh_edr7Sh.sh	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-07-16	Cloudy With a Chance of Credentials | AWS-Targeting Cred Stealer Expands to Azure GCP	Cloudybgijdhcafh5_edrElf.elf	Endpoint Security	GLESEC-AWS-CYMU	Blocked

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

TLP:AMBER

GLESEC
COMPLETELY PERCEPTI

ASM-VP REPORT

GLESEC 07/26/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-07-16	Cloudy With a Chance of Credentials | AWS-Targeting Cred Stealer Expands to Azure GCP	Cloudybgijdhcafh14_edrSh.sh	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-07-16	Cloudy With a Chance of Credentials | AWS-Targeting Cred Stealer Expands to Azure GCP	Cloudybgijdhcafh15_edrSh.sh	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-07-16	Cloudy With a Chance of Credentials | AWS-Targeting Cred Stealer Expands to Azure GCP	Cloudybgijdhcafh10_edrSh.sh	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-07-16	Cloudy With a Chance of Credentials | AWS-Targeting Cred Stealer Expands to Azure GCP	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/cloudy_with_a_chance_of_credentials_%7C_aws-targeting_cred_stealer_expands_to_azure_gcp_3206978e-9740-4736-8720-3e2241f499a6/Cloudybgijdhcafh21_browsingSh.sh?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230716%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230716T050000Z&X-Amz-Expires=600&X-Amz-Signature=8d4ce381eae1f45e6e5a3a681180ff1c63af3443c84659d683051cb9007edc2d&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-16	Cloudy With a Chance of Credentials | AWS-Targeting Cred Stealer Expands to Azure GCP	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/cloudy_with_a_chance_of_credentials_%7C_aws-targeting_cred_stealer_expands_to_azure_gcp_3206978e-9740-4736-8720-3e2241f499a6/Cloudybgijdhcafh20_browsingSh.sh?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230716%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230716T050000Z&X-Amz-Expires=600&X-Amz-Signature=f2b23e7aeb93590937a0beccb2f6b2090815b3a5db7e2c58b963e10976d0e57a&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-16	Cloudy With a Chance of Credentials | AWS-Targeting Cred Stealer Expands to Azure GCP	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/cloudy_with_a_chance_of_credentials_%7C_aws-targeting_cred_stealer_expands_to_azure_gcp_3206978e-9740-4736-8720-3e2241f499a6/Cloudybgijdhcafh18_browsingSh.sh?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230716%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230716T050000Z&X-Amz-Expires=600&X-Amz-Signature=a57f526505b3ba20b80940248f10c26b144c19536f4901972185f434a28d5e24&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-16	Cloudy With a Chance of Credentials | AWS-Targeting Cred Stealer Expands to Azure GCP	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/cloudy_with_a_chance_of_credentials_%7C_aws-targeting_cred_stealer_expands_to_azure_gcp_3206978e-9740-4736-8720-3e2241f499a6/Cloudybgijdhcafh16_browsingSh.sh?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230716%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230716T050000Z&X-Amz-Expires=600&X-Amz-Signature=1e1f6500cbeb8c0d61760ea1502272a7ca7b4e3721d6bdf5f4a9144579066b03&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-16	Cloudy With a Chance of Credentials | AWS-Targeting Cred Stealer Expands to Azure GCP	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/cloudy_with_a_chance_of_credentials_%7C_aws-targeting_cred_stealer_expands_to_azure_gcp_3206978e-9740-4736-8720-3e2241f499a6/Cloudybgijdhcafh11_browsingSh.sh?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230716%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230716T045959Z&X-Amz-Expires=600&X-Amz-Signature=61d9af19b73252384b6683394364382927dbacc18b832bd0e6c5b8335fa5de0&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-16	Cloudy With a Chance of Credentials | AWS-Targeting Cred Stealer Expands to Azure GCP	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/cloudy_with_a_chance_of_credentials_%7C_aws-targeting_cred_stealer_expands_to_azure_gcp_3206978e-9740-4736-8720-3e2241f499a6/Cloudybgijdhcafh9_browsingSh.sh?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230716%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230716T045958Z&X-Amz-Expires=600&X-Amz-Signature=f86ade1f5486cd9334b1a0a15b7cc8bd9edc5c22a5c249ffb40a70d3391bdb92&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-16	Cloudy With a Chance of Credentials | AWS-Targeting Cred Stealer Expands to Azure GCP	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/cloudy_with_a_chance_of_credentials_%7C_aws-targeting_cred_stealer_expands_to_azure_gcp_3206978e-9740-4736-8720-3e2241f499a6/Cloudybgijdhcafh8_browsingSh.sh?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230716%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230716T045958Z&X-Amz-Expires=600&X-Amz-Signature=8838ecdf44e4c180fff947d0232acf7d3171930e4c13abe25d5cc1b742c0d9d1&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-16	Cloudy With a Chance of Credentials | AWS-Targeting Cred Stealer Expands to Azure GCP	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/cloudy_with_a_chance_of_credentials_%7C_aws-targeting_cred_stealer_expands_to_azure_gcp_3206978e-9740-4736-8720-3e2241f499a6/Cloudybgijdhcafh6_browsingSh.sh?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230716%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230716T045958Z&X-Amz-Expires=600&X-Amz-Signature=f265043d055f861cae773ed6af8f82d07513f01acd27aa25362aab6d07341bf6&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated

TLP:AMBER

GLESEC
COMPLETELY PERCEPTI

ASM-VP REPORT

GLESEC 07/26/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-07-16	Cloudy With a Chance of Credentials | AWS-Targeting Cred Stealer Expands to Azure GCP	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/cloudy_with_a_chance_of_credentials_%7C_aws-targeting_cred_stealer_expands_to_azure_gcp_3206978e-9740-4736-8720-3e2241f499a6/Cloudybgijdhcafh3_browsingSh.sh?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230716%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230716T045957Z&X-Amz-Expires=600&X-Amz-Signature=6cce28562de750d42bb988addc90e9587d73cefb990020667ddb60cc3307626b&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-16	Cloudy With a Chance of Credentials | AWS-Targeting Cred Stealer Expands to Azure GCP	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/cloudy_with_a_chance_of_credentials_%7C_aws-targeting_cred_stealer_expands_to_azure_gcp_3206978e-9740-4736-8720-3e2241f499a6/Cloudybgijdhcafh1_browsingSh.sh?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230716%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230716T045957Z&X-Amz-Expires=600&X-Amz-Signature=3142c009b0d374fa5ebe299c93da296d4e1ddbc0c669b1ddce1aee8a702c0b20&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-13	Attackers Exploit (CVE-2023-36884) Unpatched Windows Zero-Day Vulnerability	Attackersbgijcceegh4_edrLnk.lnk	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-07-13	Attackers Exploit (CVE-2023-36884) Unpatched Windows Zero-Day Vulnerability	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/attackers_exploit_unpatched_windows_zero-day_vulnerability_40d6eeaa-f493-4fe6-929d-ac7ddc09b8b1/Attackersbgijcceegh1_browsingDocx.docx?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230713%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230713T053149Z&X-Amz-Expires=600&X-Amz-Signature=c7fc6f4830fa5da681f27b5589f4a173933e5995d00fd748af54346da8f8ff22&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-12	Underground Team Ransomware Demands Millions	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/underground_team_ransomware_demands_millions_c68c3697-ffa1-48cf-bfaa-b932e24ac09f/Undergroundbgijafbfig39_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230712%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230712T053040Z&X-Amz-Expires=600&X-Amz-Signature=c8cbe798c0582103af4dc5544eb9a1574fb80e36cd8acade77d84fb2b267dd3b&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-11	Unleashing WhiteSnake Stealer	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/unleashing_whitesnake_stealer_087f2f0a-b8cc-45d8-aa36-a6a01b9297a7/Unleashingbgijafbdca2_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230711%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230711T100624Z&X-Amz-Expires=600&X-Amz-Signature=53df5b97eea23e8d561d457af55f1e76313e2722154b380e375b3233cd5afbd4&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-11	Unleashing WhiteSnake Stealer	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/unleashing_whitesnake_stealer_087f2f0a-b8cc-45d8-aa36-a6a01b9297a7/Unleashingbgijafbdca1_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230711%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230711T100623Z&X-Amz-Expires=600&X-Amz-Signature=6a08fb2f2874841f2bab6982ca5115dd4e5fd10f870e1fde273caa13165b0988&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-11	Threat Trend Report On Kimsuky	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/threat_trend_report_on_kimsuky_1cf690bf-821f-48ed-8c03-cb291a519d85/Threatbgijafbfgb38_browsingChm.chm?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230711%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230711T051257Z&X-Amz-Expires=600&X-Amz-Signature=b87484f665d292db61613afe011d9435e32679ab9d79dadf4fafc1e46cf19e82&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-09	Threat Profile UNC3944	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/threat_profile_unc3944_f7ba8a64-eecc-477f-a86e-0cbdccc2a0c9/Threatbgiigjfhhb85_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230709T060404Z&X-Amz-Expires=600&X-Amz-Signature=d419f1db4f287cf3dcb7f843f00d484e887ac622ef93b6d16b412c39f7b48ba4&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-09	Threat Profile UNC3944	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/threat_profile_unc3944_f7ba8a64-eecc-477f-a86e-0cbdccc2a0c9/Threatbgiigjfhhb84_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230709T060404Z&X-Amz-Expires=600&X-Amz-Signature=240bf4f84a028ec564e77f7b2d5590739da7872e24559c59f8fd7f9ee3a7713a&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-09	Threat Profile UNC3944	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/threat_profile_unc3944_f7ba8a64-eecc-477f-a86e-0cbdccc2a0c9/Threatbgiigjfhhb83_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230709T060403Z&X-Amz-Expires=600&X-Amz-Signature=7ab22eb603dfa19560d87d2aae2764c98327279a7ba0bdfeaf65dc655f0de301&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-09	Threat Profile UNC3944	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/threat_profile_unc3944_f7ba8a64-eecc-477f-a86e-0cbdccc2a0c9/Threatbgiigjfhhb82_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230709T060403Z&X-Amz-Expires=600&X-Amz-Signature=bf2bcd27baad065bbd7648b02b68de8d8898853420afe55d0b8f7584c997bfe0&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

TLP:AMBER

ASM-VP REPORT

GLESEC 07/26/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-07-09	Threat Profile UNC3944	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/threat_profile_unc3944_f7ba8a64-eecc-477f-a86e-0cbdccc2a0c9/ThreatbgiigjfhhbBrowsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230709T060403Z&X-Amz-Expires=600&X-Amz-Signature=a3c1603d13ee6da4e6b4bcc8e52a8a973a83a14332607eb58cb2363d79c59c9e&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-09	Threat Profile UNC3944	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/threat_profile_unc3944_f7ba8a64-eecc-477f-a86e-0cbdccc2a0c9/ThreatbgiigjfhhbBrowsing79Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230709T060402Z&X-Amz-Expires=600&X-Amz-Signature=04d8005bcce0c34bd63fd9c7a947bcc86b76d3584450b477f10f34976ab4dd79&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-09	Threat Profile UNC3944	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/threat_profile_unc3944_f7ba8a64-eecc-477f-a86e-0cbdccc2a0c9/ThreatbgiigjfhhbBrowsing77Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230709T060401Z&X-Amz-Expires=600&X-Amz-Signature=61ca301dc840884642fdcbbbf4abc263d8e8bd273c196ad54e01495a0e376bc0&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-09	Threat Profile UNC3944	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/threat_profile_unc3944_f7ba8a64-eecc-477f-a86e-0cbdccc2a0c9/ThreatbgiigjfhhbBrowsing76Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230709T060401Z&X-Amz-Expires=600&X-Amz-Signature=d3987aea71aa2a37ac73a9b7aa6701dd20058f56fbc7a52131ad708c09433fbe&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-09	Threat Profile UNC3944	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/threat_profile_unc3944_f7ba8a64-eecc-477f-a86e-0cbdccc2a0c9/ThreatbgiigjfhhbBrowsing75Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230709T060400Z&X-Amz-Expires=600&X-Amz-Signature=b8d1185b8573ee1c9f5b65a1df97999c32250a91d39444a510dc1064b04cb147&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-09	Threat Profile UNC3944	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/threat_profile_unc3944_f7ba8a64-eecc-477f-a86e-0cbdccc2a0c9/ThreatbgiigjfhhbBrowsing73Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230709T060400Z&X-Amz-Expires=600&X-Amz-Signature=5115b7b57c97caefc83c65a96f38f555a1b9114bd1df438836877a1f829631bd&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-09	Threat Profile UNC3944	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/threat_profile_unc3944_f7ba8a64-eecc-477f-a86e-0cbdccc2a0c9/ThreatbgiigjfhhbBrowsing72Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230709T060400Z&X-Amz-Expires=600&X-Amz-Signature=5f968a280fef66addeac8f3e64c5ec5d60a240a7ed667d8635663270c8e3b3fe&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-06	PhonyC2 Framework Used By MuddyWater	Phonyc2bgiigaijja5_edrPs1.ps1	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-07-06	PhonyC2 Framework Used By MuddyWater	hxxp://164.132.237.79	Web Gateway	GLESEC-AWS-CYMU	Offline/Removed
2023-07-06	PhonyC2 Framework Used By MuddyWater	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/phonyc2_framework_used_by_muddywater_055285f0-d830-4652-b2b3-c438a424a18e/Phonyc2bgiigaijja10_browsingJs.js?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230706%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230706T050232Z&X-Amz-Expires=600&X-Amz-Signature=1809f9e2cb57d1fb084bceb800c59435d06d3fa6699214923adf5424b82a8118&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-06	PhonyC2 Framework Used By MuddyWater	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/phonyc2_framework_used_by_muddywater_055285f0-d830-4652-b2b3-c438a424a18e/Phonyc2bgiigaijja9_browsingJs.js?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230706%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230706T050232Z&X-Amz-Expires=600&X-Amz-Signature=7c746f69a23068c58228de91ecccd4144422b6a7c70fb76cdd90538967de4e90&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
N/A	The suspected Maha grass organization uses the WarHawk backdoor variant Spyder to spy on many countries	Thebgiifccegi21_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

TLP:AMBER

ASM-VP REPORT

GLESEC 07/26/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
N/A	The suspected Maha grass organization uses the WarHawk backdoor variant Spyder to spy on many countries	Thebgiifccegi14_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-05	The suspected Maha grass organization uses the WarHawk backdoor variant Spyder to spy on many countries	Thebgiifccegi18_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-05	The suspected Maha grass organization uses the WarHawk backdoor variant Spyder to spy on many countries	Thebgiifccegi10_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-05	The suspected Maha grass organization uses the WarHawk backdoor variant Spyder to spy on many countries	hxxp://192.169.7.142	Web Gateway	GLESEC-AWS-CYMU	Offline/Removed
2023-07-05	The suspected Maha grass organization uses the WarHawk backdoor variant Spyder to spy on many countries	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/the_suspected_maha_grass_organization_uses_the_warhawk_backdoor_variant_spyder_to_spy_on_many_countries_b12092f9-cbef-4912-87fe-16158033afbc/Thebgiifccegi20_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230705%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230705T050503Z&X-Amz-Expires=600&X-Amz-Signature=b1e1ab2e159d5b31dbb4f309624c84328629268967fee6b10bb887d8d34e2ee6&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-05	The suspected Maha grass organization uses the WarHawk backdoor variant Spyder to spy on many countries	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/the_suspected_maha_grass_organization_uses_the_warhawk_backdoor_variant_spyder_to_spy_on_many_countries_b12092f9-cbef-4912-87fe-16158033afbc/Thebgiifccegi19_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230705%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230705T050503Z&X-Amz-Expires=600&X-Amz-Signature=7677e41e48bde0625b6428970b672fc833fbf984e088d4ca74ecbdbb8492ad93&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-05	The suspected Maha grass organization uses the WarHawk backdoor variant Spyder to spy on many countries	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/the_suspected_maha_grass_organization_uses_the_warhawk_backdoor_variant_spyder_to_spy_on_many_countries_b12092f9-cbef-4912-87fe-16158033afbc/Thebgiifccegi1_browsing7Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230705%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230705T050503Z&X-Amz-Expires=600&X-Amz-Signature=f9a24c2a2c268b875f14f539a10b9cb82cca5813343f97a0350a02b254f339f4&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-05	The suspected Maha grass organization uses the WarHawk backdoor variant Spyder to spy on many countries	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/the_suspected_maha_grass_organization_uses_the_warhawk_backdoor_variant_spyder_to_spy_on_many_countries_b12092f9-cbef-4912-87fe-16158033afbc/Thebgiifccegi13_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230705%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230705T050502Z&X-Amz-Expires=600&X-Amz-Signature=6436ed4460b786d3fb7c387bb5d7ccc263e312921e614d470163f99b014e2629&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-05	The suspected Maha grass organization uses the WarHawk backdoor variant Spyder to spy on many countries	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/the_suspected_maha_grass_organization_uses_the_warhawk_backdoor_variant_spyder_to_spy_on_many_countries_b12092f9-cbef-4912-87fe-16158033afbc/Thebgiifccegi9_browsin gExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD& X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230705%2Feu-west-1%2Fs3%2Faws4_request &X-Amz-Date=20230705T050501Z&X-Amz-Expires=600&X-Amz-Signature=4f6752acce685add0400e15f342f729db1786819470291edb8689a0163ed561d&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-04	The DPRK strikes using a new variant of RUSTBUCKET	Thebgiiecjcjg12_edr7Macho.macho	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-04	The DPRK strikes using a new variant of RUSTBUCKET	Thebgiiecjcjg132_edrMacho.macho	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-04	The DPRK strikes using a new variant of RUSTBUCKET	Thebgiiecjcjg129_edrMacho.macho	Endpoint Security	GLESEC-AWS-CYMU	Blocked

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

TLP:AMBER

ASM-VP REPORT

GLESEC 07/26/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-07-04	The DPRK strikes using a new variant of RUSTBUCKET	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/the_dprk_strikes_using_a_new_variant_of_rustbucket_5ef1bf2d-e849-470a-b237-647c9e112e12/Thebgiiecjcjg131_browsingMacho.macho?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230704%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230704T061302Z&X-Amz-Expires=600&X-Amz-Signature=de0141f38b13d33e5cce3af1d1144768303bac972b3b527390f6eeeb9b6005ec &X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-04	The DPRK strikes using a new variant of RUSTBUCKET	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/the_dprk_strikes_using_a_new_variant_of_rustbucket_5ef1bf2d-e849-470a-b237-647c9e112e12/Thebgiiecjcjg126_browsingMacho.macho?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230704%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230704T061300Z&X-Amz-Expires=600&X-Amz-Signature=7e20bfa25055746c21c9965eafd98b21eb0bb76492c3462425a5d41bfb80cc10 &X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-04	The DPRK strikes using a new variant of RUSTBUCKET	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/the_dprk_strikes_using_a_new_variant_of_rustbucket_5ef1bf2d-e849-470a-b237-647c9e112e12/Thebgiiecjcjg125_browsingMacho.macho?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230704%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230704T061259Z&X-Amz-Expires=600&X-Amz-Signature=fe0f7a9a77bf9714700f032293a4f2cf498aaeb54dd6d06c3eea8893303ee1e2 &X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-04	The DPRK strikes using a new variant of RUSTBUCKET	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/the_dprk_strikes_using_a_new_variant_of_rustbucket_5ef1bf2d-e849-470a-b237-647c9e112e12/Thebgiiecjcjg122_browsingMacho.macho?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230704%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230704T061257Z&X-Amz-Expires=600&X-Amz-Signature=2ad09aac098ec7d61093b3e979e4f188772a0007cf879291ccf604b76d65fc44 &X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-03	Word Document with an Online Attached Template	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/word_document_with_an_online_attached_template_10c61f38-086a-4f78-980a-6d2253adcd93/Matryoshkabgiididgjd3_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Co ntent-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230703%2 Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230703T113604Z&X-Amz-Expires=600&X-A mz-Signature=93890d6822fc3d0cc22f5c2a2dd8ad6b2bd1ec8b5d5741fb930c27114a086f7c&X- Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-03	Word Document with an Online Attached Template	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/word_document_with_an_online_attached_template_10c61f38-086a-4f78-980a-6d2253adcd93/Matryoshkabgiididgjd1_browsingDocx.docx?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230703%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230703T113604Z&X-Amz-Expires=600&X -Amz-Signature=418cb4ac674054d84d2609597119093905a329a78851377553d1ff194c5f7d66& X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-03	Word Document with an Online Attached Template	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/word_document_with_an_online_attached_template_10c61f38-086a-4f78-980a-6d2253adcd93/Matryoshkabgiididgjd2_browsingRtf.rtf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Co ntent-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230703%2 Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230703T113603Z&X-Amz-Expires=600&X-A mz-Signature=0db91b5ea14aa5bbbb480adc56bcddd3991fc6468f9e86d974575036db83a399&X- Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-03	New Qakbot (Qbot) activity	Qbotbgiidicbbd1_edrDll.dll	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-03	New Qakbot (Qbot) activity	Qbotbgiidicbbd2_edrJs.js	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-07-03	New Qakbot (Qbot) activity	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/new_qakbot_%28qbot%29_activity_f5a2f41e-fc87-429d-b4af-e3e89d8c012f/Qbotbgiidicbbd3_browsingZip.zip?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230703%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230703T111503Z&X-Amz-Expires=600&X-Amz-Signature=f9be98830319f00386be9250148eff8e7c04b29c88914560e147e13590889b9a&X-Amz-SignedHeaders=host &x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-03	Mirai Campaign Leveraging Multiple IoT Exploits	Miraibgihfhcccf2_edrElf.elf	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-03	Mirai Campaign Leveraging Multiple IoT Exploits	Miraibgihfhcccf3_edrElf.elf	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-03	Mirai Campaign Leveraging Multiple IoT Exploits	Miraibgihfhcccf6_edrElf.elf	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-03	Mirai Campaign Leveraging Multiple IoT Exploits	Miraibgihfhcccf_edr7Elf.elf	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-03	Mirai Campaign Leveraging Multiple IoT Exploits	Miraibgihfhcccf5_edrElf.elf	Endpoint Security	GLESEC-AWS-CYMU	Blocked

TLP:AMBER

ASM-VP REPORT

GLESEC 07/26/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-07-03	Mirai Campaign Leveraging Multiple IoT Exploits	Miraibgihfhcccf12_edrElf.elf	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-03	Mirai Campaign Leveraging Multiple IoT Exploits	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/mir ai_campaign_leveraging_multiple_iot_exploits_29e3fabb-a46e-42e6-9931-6276108ef13 d/Miraibgihfhcccf13_browsingElf.elf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Conte nt-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230703%2Feu - west-1%2Fs3%2Faws4_request&X-Amz-Date=20230703T083511Z&X-Amz-Expires=600&X-Amz-Signature=af73c6f39c5061619c31bca7af6e19c1e5acc64c362d36fe6bd27c648e32ac6f&X-Amz - SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-03	Mirai Campaign Leveraging Multiple IoT Exploits	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/mir ai_campaign_leveraging_multiple_iot_exploits_29e3fabb-a46e-42e6-9931-6276108ef13 d/Miraibgihfhcccf11_browsingElf.elf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Conte nt-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230703%2Feu - west-1%2Fs3%2Faws4_request&X-Amz-Date=20230703T083511Z&X-Amz-Expires=600&X-Amz-Signature=57386a5b249827c8a6eccb9d4d498efb6109f3ccca8f69762e0471137ba9d56b&X-Amz - SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-03	Mirai Campaign Leveraging Multiple IoT Exploits	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/mir ai_campaign_leveraging_multiple_iot_exploits_29e3fabb-a46e-42e6-9931-6276108ef13 d/Miraibgihfhcccf10_browsingElf.elf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Conte nt-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230703%2Feu - west-1%2Fs3%2Faws4_request&X-Amz-Date=20230703T083510Z&X-Amz-Expires=600&X-Amz-Signature=ac527e12aeb4c8076c509d36ddf4a8bce2d08cae78309fa08e9a9ff762300da3&X-Amz - SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-03	Mirai Campaign Leveraging Multiple IoT Exploits	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/mir ai_campaign_leveraging_multiple_iot_exploits_29e3fabb-a46e-42e6-9931-6276108ef13 d/Miraibgihfhcccf9_browsingElf.elf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Conten t-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230703%2Feu- west-1%2Fs3%2Faws4_request&X-Amz-Date=20230703T083510Z&X-Amz-Expires=600&X-Amz-Signature=94e85ff0f2d254b3999fcb38b87b153e4b952944edbfe7496cab4e883d8d02c2&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-03	Mirai Campaign Leveraging Multiple IoT Exploits	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/mir ai_campaign_leveraging_multiple_iot_exploits_29e3fabb-a46e-42e6-9931-6276108ef13 d/Miraibgihfhcccf8_browsingElf.elf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Conten t-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230703%2Feu- west-1%2Fs3%2Faws4_request&X-Amz-Date=20230703T083510Z&X-Amz-Expires=600&X-Amz-Signature=96b678c438e50bd8dc4401f8f377d1c8a7ffdad9af9c5cab265bcd832ac4b047&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-03	Mirai Campaign Leveraging Multiple IoT Exploits	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/mir ai_campaign_leveraging_multiple_iot_exploits_29e3fabb-a46e-42e6-9931-6276108ef13 d/Miraibgihfhcccf4_browsingElf.elf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Conten t-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230703%2Feu- west-1%2Fs3%2Faws4_request&X-Amz-Date=20230703T083509Z&X-Amz-Expires=600&X-Amz-Signature=f7b4fec1057883a3cdb22fc3e42e8382181460a7b0f798fc983230196242b1e2&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-03	Mirai Campaign Leveraging Multiple IoT Exploits	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/mir ai_campaign_leveraging_multiple_iot_exploits_29e3fabb-a46e-42e6-9931-6276108ef13 d/Miraibgihfhcccf1_browsingElf.elf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Conten t-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230703%2Feu- west-1%2Fs3%2Faws4_request&X-Amz-Date=20230703T083508Z&X-Amz-Expires=600&X-Amz-Signature=600ea0407ba1efdeb3813df1be60b0f0e7134bd01abdf7021e65d85a2c750e65&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-07-02	Gh0stBins RAT Analysis	Gh0stbinsbgihjbhhhb1_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-07-02	Gh0stBins RAT Analysis	Gh0stbinsbgihjbhhhb4_edrDll.dll	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-07-02	Gh0stBins RAT Analysis	Gh0stbinsbgihjbhhhb3_edrDll.dll	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-07-02	Gh0stBins RAT Analysis	hxxp://193.134.208.217	Web Gateway	GLESEC-AWS-CYMU	Offline/Removed
2023-06-29	8Base Ransomware - A Heavy Hitting Player	Eightbasebgiiacggfh4_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-06-29	8Base Ransomware - A Heavy Hitting Player	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/8ba se_ransomware_-_a_heavy_hitting_player_a5893f49-67e5-45ef-a151-6ce0c11c6ff8/Eigh tbasebgiiacggfh1_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230629%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230629T082226Z&X-Amz-Expires=600&X-Amz-Signature=9dcec3e8b59e83d537cb77d276cabdb59e70c877512dbdccddcd88865be25a21&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-06-29	8Base Ransomware - A Heavy Hitting Player	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/8ba se_ransomware_-_a_heavy_hitting_player_a5893f49-67e5-45ef-a151-6ce0c11c6ff8/Eigh tbasebgiiacggfh2_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230629%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230629T082226Z&X-Amz-Expires=600&X-Amz-Signature=1539886949054fb088bdc7236d34969c0333665df892d2fdfb46b6718e32d596&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated

TLP:AMBER

GLESEC
COMPLETELY PERCEPTI

ASM-VP REPORT

GLESEC 07/26/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-06-29	8Base Ransomware - A Heavy Hitting Player	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/8base_ransomware_-_a_heavy_hitting_player_a5893f49-67e5-45ef-a151-6ce0c11c6ff8/Eightbasebgiiacggfh3_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230629%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230629T082225Z&X-Amz-Expires=600&X-Amz-Signature=37e2b0cbdff87897ad8a16a7bc545c73b64e52d95db0fa7fa52037492abd5a2c&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-06-29	Tracing The Footsteps Of Red Wolf	Tracingbgiiaaecbg1_edrIso.iso	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-06-29	Tracing The Footsteps Of Red Wolf	Tracingbgiiaaecbg2_edrLnk.lnk	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-06-29	Tracing The Footsteps Of Red Wolf	Tracingbgiiaaecbg3_edrDll.dll	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-06-28	Wagner Ransomware Cyber Recruitment	Wagnerbgihjbhidd5_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
N/A	Python-Based Loader Masquerading As OneDrive Utilities To Drop Multiple RATs	Python_basedbgihfhchhc1_edr78Exe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
N/A	Python-Based Loader Masquerading As OneDrive Utilities To Drop Multiple RATs	Python_basedbgihfhchhc168_edrPs1.ps1	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-06-27	Python-Based Loader Masquerading As OneDrive Utilities To Drop Multiple RATs	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/python-based_loader_masquerading_as_onedrive_utilities_to_drop_multiple_rats_b625cc6d-f13a-4148-828e-c3925f11db4c/Python_basedbgihfhchhc1_browsing76Lnk.lnk?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230627%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230627T044701Z&X-Amz-Expires=600&X-Amz-Signature=d5417faf42aba722fa19a1d8c5f4bd369740a416398951d76068b718d9adfa8e&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-06-27	Python-Based Loader Masquerading As OneDrive Utilities To Drop Multiple RATs	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/python-based_loader_masquerading_as_onedrive_utilities_to_drop_multiple_rats_b625cc6d-f13a-4148-828e-c3925f11db4c/Python_basedbgihfhchhc1_browsing73Lnk.lnk?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230627%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230627T044701Z&X-Amz-Expires=600&X-Amz-Signature=de3a2f7fc5faad14bc9ef149e315b7012d435831d219b1d1700df2802c0205fe&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-06-27	Python-Based Loader Masquerading As OneDrive Utilities To Drop Multiple RATs	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/python-based_loader_masquerading_as_onedrive_utilities_to_drop_multiple_rats_b625cc6d-f13a-4148-828e-c3925f11db4c/Python_basedbgihfhchhc1_browsing72Js.js?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230627%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230627T044701Z&X-Amz-Expires=600&X-Amz-Signature=91dccd9ae85658788521ec518766e690c0ff01b7deea94233c57a94a8192f394&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-06-27	Python-Based Loader Masquerading As OneDrive Utilities To Drop Multiple RATs	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/python-based_loader_masquerading_as_onedrive_utilities_to_drop_multiple_rats_b625cc6d-f13a-4148-828e-c3925f11db4c/Python_basedbgihfhchhc1_browsing70Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230627%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230627T044700Z&X-Amz-Expires=600&X-Amz-Signature=a3b1450457a79de363c06facb0dd2dd008ffbfb428e9dbbe968386e2932e8927&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-06-27	Python-Based Loader Masquerading As OneDrive Utilities To Drop Multiple RATs	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/python-based_loader_masquerading_as_onedrive_utilities_to_drop_multiple_rats_b625cc6d-f13a-4148-828e-c3925f11db4c/Python_basedbgihfhchhc169_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230627%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230627T044700Z&X-Amz-Expires=600&X-Amz-Signature=5e17ffdf84279e9a53476ba585785f9c659efc748e67cfb38bdd0ad25b26f2ce&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-06-27	Python-Based Loader Masquerading As OneDrive Utilities To Drop Multiple RATs	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/python-based_loader_masquerading_as_onedrive_utilities_to_drop_multiple_rats_b625cc6d-f13a-4148-828e-c3925f11db4c/Python_basedbgihfhchhc16_browsing7Dll.dll?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230627%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230627T044659Z&X-Amz-Expires=600&X-Amz-Signature=e304773de30555762b20ebaada799e2545337b472167dea1bd84a199043e9f0c&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-06-27	Python-Based Loader Masquerading As OneDrive Utilities To Drop Multiple RATs	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/python-based_loader_masquerading_as_onedrive_utilities_to_drop_multiple_rats_b625cc6d-f13a-4148-828e-c3925f11db4c/Python_basedbgihfhchhc166_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230627%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230627T044658Z&X-Amz-Expires=600&X-Amz-Signature=32f82904ea9e63126639c99a041c4dabe7e59ae199e262ffebe3d253cc3430e2&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated

TLP:AMBER

ASM-VP REPORT

GLESEC 07/26/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-06-26	Operation Magalenha - Long-Running Campaign Pursues Portuguese Credentials and PII	Magalenhabgihgjegca10_edr7Exe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-06-26	Operation Magalenha - Long-Running Campaign Pursues Portuguese Credentials and PII	Magalenhabgihgjegca91_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-06-26	Operation Magalenha - Long-Running Campaign Pursues Portuguese Credentials and PII	Magalenhabgihgjegca90_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-06-26	Operation Magalenha - Long-Running Campaign Pursues Portuguese Credentials and PII	Magalenhabgihgjegca93_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-06-26	Operation Magalenha - Long-Running Campaign Pursues Portuguese Credentials and PII	Magalenhabgihgjegca103_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-06-26	Operation Magalenha - Long-Running Campaign Pursues Portuguese Credentials and PII	Magalenhabgihgjegca105_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-06-26	Operation Magalenha - Long-Running Campaign Pursues Portuguese Credentials and PII	Magalenhabgihgjegca102_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-06-26	Operation Magalenha - Long-Running Campaign Pursues Portuguese Credentials and PII	hxxp://94.228.121.36	Web Gateway	GLESEC-AWS-CYMU	Offline/Removed
2023-06-26	Operation Magalenha - Long-Running Campaign Pursues Portuguese Credentials and PII	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/operation_magalenha_-_long-running_campaign_pursues_portuguese_credentials_and_pii_39302ab3-8137-4c47-8629-bc09e763c579/Magalenhabgihgjegca92_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230626%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230626T125615Z&X-Amz-Expires=600&X-Amz-Signature=236de58e7d999080350e0252d90c2f602e5813c6f3ad704cb6febb33709f4d5d&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-06-26	Operation Magalenha - Long-Running Campaign Pursues Portuguese Credentials and PII	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/operation_magalenha_-_long-running_campaign_pursues_portuguese_credentials_and_pii_39302ab3-8137-4c47-8629-bc09e763c579/Magalenhabgihgjegca94_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230626%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230626T125610Z&X-Amz-Expires=600&X-Amz-Signature=aeabc617ce499627c0605a0ca00837101e07179c426c6e51725ad1e982085837&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

TLP:AMBER

GLESEC
COMPLETELY PERCEPTI

ASM-VP REPORT

GLESEC 07/26/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-06-26	Operation Magalenha - Long-Running Campaign Pursues Portuguese Credentials and PII	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/operation_magalenha_-_long-running_campaign_pursues_portuguese_credentials_and_pii_39302ab3-8137-4c47-8629-bc09e763c579/Magalenhabgihgjegca9_browsing7Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230626%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230626T125607Z&X-Amz-Expires=600&X-Amz-Signature=09a96305704814250e8085b2a1f2c1205963b944aef518e1991a9aa3141c2c82&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-06-26	Operation Magalenha - Long-Running Campaign Pursues Portuguese Credentials and PII	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/operation_magalenha_-_long-running_campaign_pursues_portuguese_credentials_and_pii_39302ab3-8137-4c47-8629-bc09e763c579/Magalenhabgihgjegca98_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230626%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230626T125604Z&X-Amz-Expires=600&X-Amz-Signature=36577fc61c0f3be74a010dca59485d72acc1dc759bd3ddab390edf17a5898a5d&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-06-26	Operation Magalenha - Long-Running Campaign Pursues Portuguese Credentials and PII	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/operation_magalenha_-_long-running_campaign_pursues_portuguese_credentials_and_pii_39302ab3-8137-4c47-8629-bc09e763c579/Magalenhabgihgjegca99_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230626%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230626T125602Z&X-Amz-Expires=600&X-Amz-Signature=9e70afb8a47c396bb9b02a4346cd363e2060f097c897550d2610bc9e4ecf866c&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-06-26	Operation Magalenha - Long-Running Campaign Pursues Portuguese Credentials and PII	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/operation_magalenha_-_long-running_campaign_pursues_portuguese_credentials_and_pii_39302ab3-8137-4c47-8629-bc09e763c579/Magalenhabgihgjegca100_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230626%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230626T125552Z&X-Amz-Expires=600&X-Amz-Signature=16a6e1392003d6b1ebf949f1c751f54cd7ca0712eea019670622717dea0b8d1a&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-06-26	Operation Magalenha - Long-Running Campaign Pursues Portuguese Credentials and PII	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/operation_magalenha_-_long-running_campaign_pursues_portuguese_credentials_and_pii_39302ab3-8137-4c47-8629-bc09e763c579/Magalenhabgihgjegca101_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230626%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230626T125548Z&X-Amz-Expires=600&X-Amz-Signature=3599a5d8922c0719890c5f13b7fe1e98c3aff317515f03e06b99218bff9ea350&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-06-26	Operation Magalenha - Long-Running Campaign Pursues Portuguese Credentials and PII	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/operation_magalenha_-_long-running_campaign_pursues_portuguese_credentials_and_pii_39302ab3-8137-4c47-8629-bc09e763c579/Magalenhabgihgjegca104_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230626%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230626T125536Z&X-Amz-Expires=600&X-Amz-Signature=b3fbeda09c39700521b2f271a46c9cf9ef263f5cae6cd8f5601b75f643bd10dc&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-06-26	Crysis And Venus Ransomware Installed Via RDP	Crysisbgihfhcije1_edr79Exe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-06-26	Crysis And Venus Ransomware Installed Via RDP	Crysisbgihfhcije186_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-06-26	Crysis And Venus Ransomware Installed Via RDP	Crysisbgihfhcije190_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Penetrated
2023-06-26	Crysis And Venus Ransomware Installed Via RDP	Crysisbgihfhcije194_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-06-26	Crysis And Venus Ransomware Installed Via RDP	Crysisbgihfhcije185_edrExe.exe	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-06-26	Crysis And Venus Ransomware Installed Via RDP	Crysisbgihfhcije183_edrDll.dll	Endpoint Security	GLESEC-AWS-CYMU	Blocked
2023-06-26	Crysis And Venus Ransomware Installed Via RDP	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/crysis_and_venus_ransomware_installed_via_rdp_f8741241-ed45-4a8f-8e68-09566cd32555/Crysisbgihfhcije188_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230626%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230626T062941Z&X-Amz-Expires=600&X-Amz-Signature=464084f9dc64149ca6d5244fcb4346739794e62beb99125541bc41aa4939ee6c&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-06-26	Crysis And Venus Ransomware Installed Via RDP	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/crysis_and_venus_ransomware_installed_via_rdp_f8741241-ed45-4a8f-8e68-09566cd32555/Crysisbgihfhcije184_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230626%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230626T062940Z&X-Amz-Expires=600&X-Amz-Signature=8481002ae5a3b92aa603c1255ebdb4658949324b52837e498caec0a61d509971&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

ASM-VP REPORT

GLESEC 07/26/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-06-26	Crysis And Venus Ransomware Installed Via RDP	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/crysis_and_venus_ransomware_installed_via_rdp_f8741241-ed45-4a8f-8e68-09566cd32555/Crysisbgihfhcije182_browsingDll.dll?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230626%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230626T062940Z&X-Amz-Expires=600&X-Amz-Signature=79ffd8fea176a129fe7773c2686dbf9765ab3f5dad94cdb3d5231da2968c4e77&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-06-26	Crysis And Venus Ransomware Installed Via RDP	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/crysis_and_venus_ransomware_installed_via_rdp_f8741241-ed45-4a8f-8e68-09566cd32555/Crysisbgihfhcije181_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230626%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230626T062939Z&X-Amz-Expires=600&X-Amz-Signature=ebe0c10066d76bcadde0cea2ec71926e0a5a425a5e9cd7c84832f92171b26bb6&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated
2023-06-26	Crysis And Venus Ransomware Installed Via RDP	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/crysis_and_venus_ransomware_installed_via_rdp_f8741241-ed45-4a8f-8e68-09566cd32555/Crysisbgihfhcije180_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230626%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230626T062939Z&X-Amz-Expires=600&X-Amz-Signature=7c02131526e68a067c811c0a4e0f0afc295120cf2344ffd00b86b5199b1a2f12&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	GLESEC-AWS-CYMU	Penetrated

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

Threats

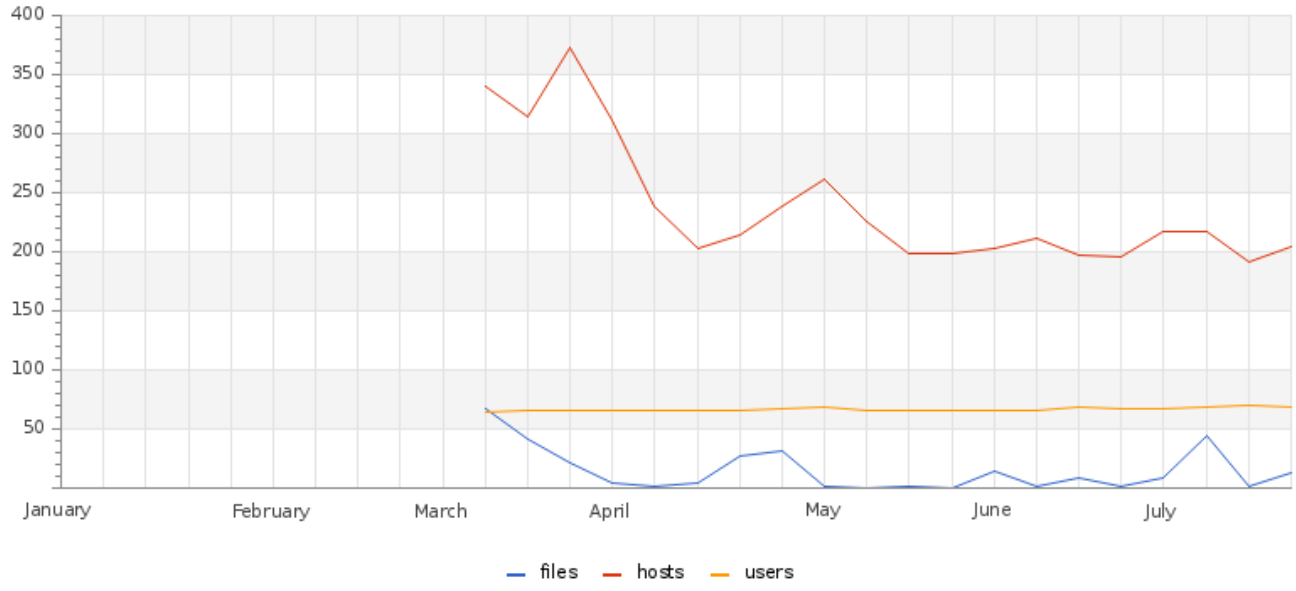
MSS-UTM

MSS-EDR

Average Threat - User Defined

85

Threat Score

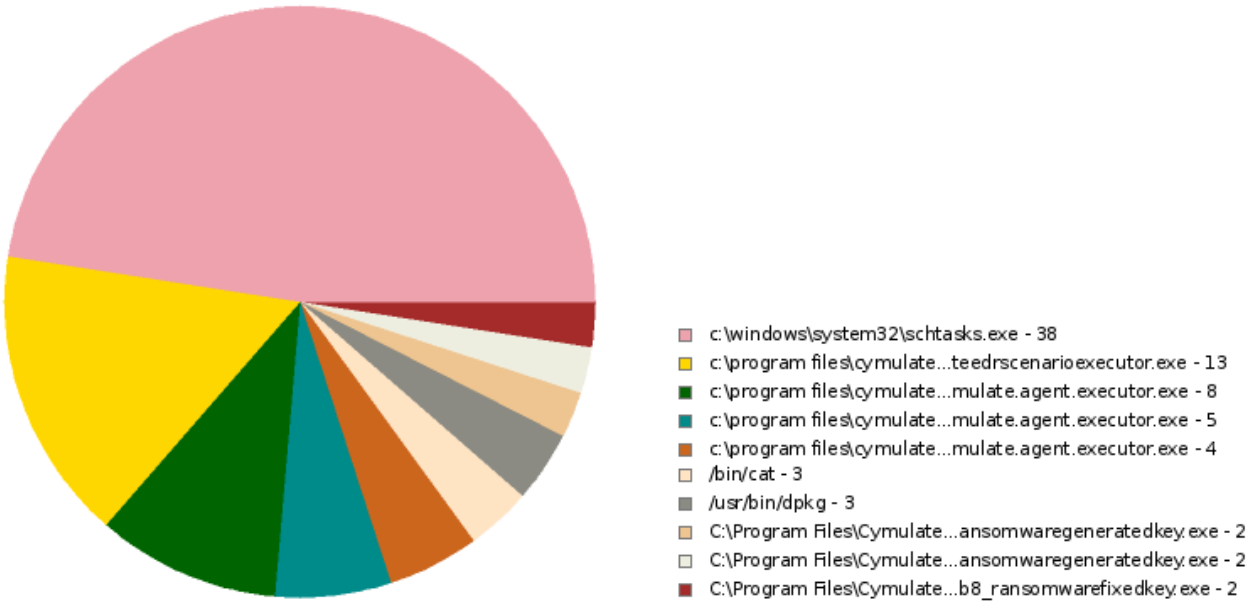


LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

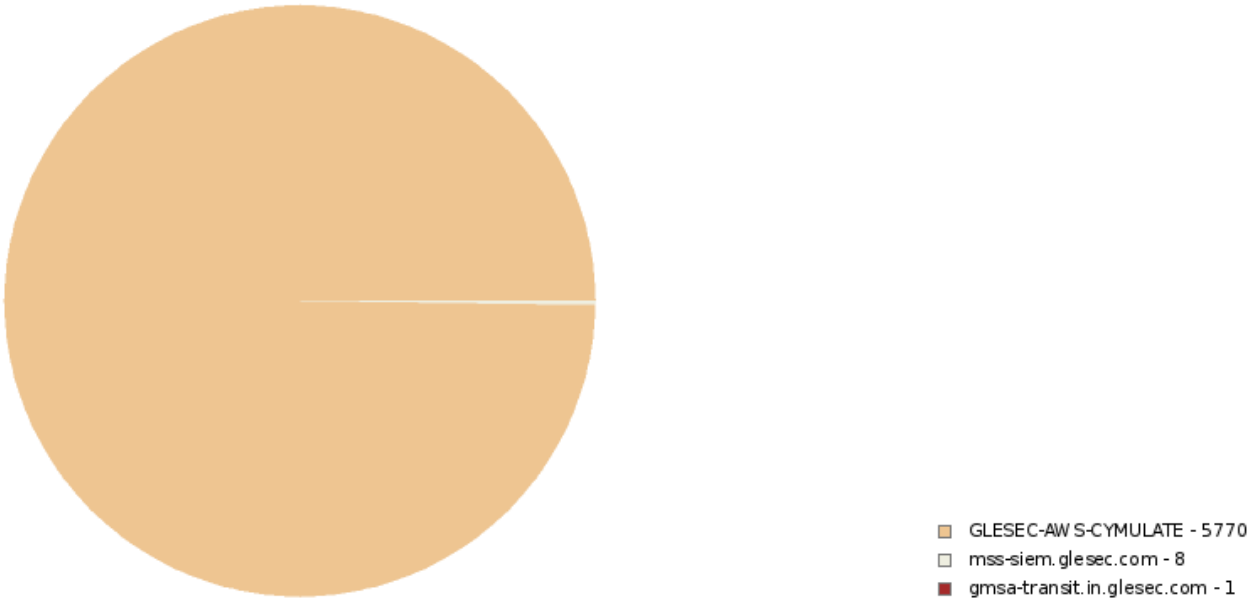
ASM-VP REPORT

GLESEC 07/26/2023

Events by File Path - User Defined



Events by Host Name - User Defined



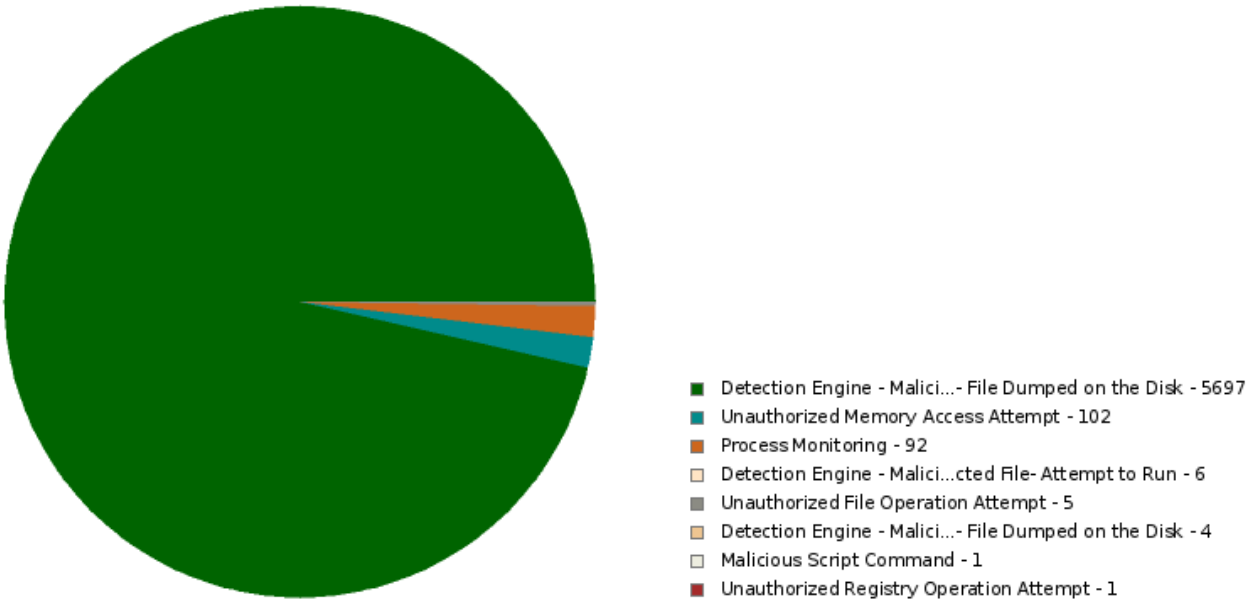
LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

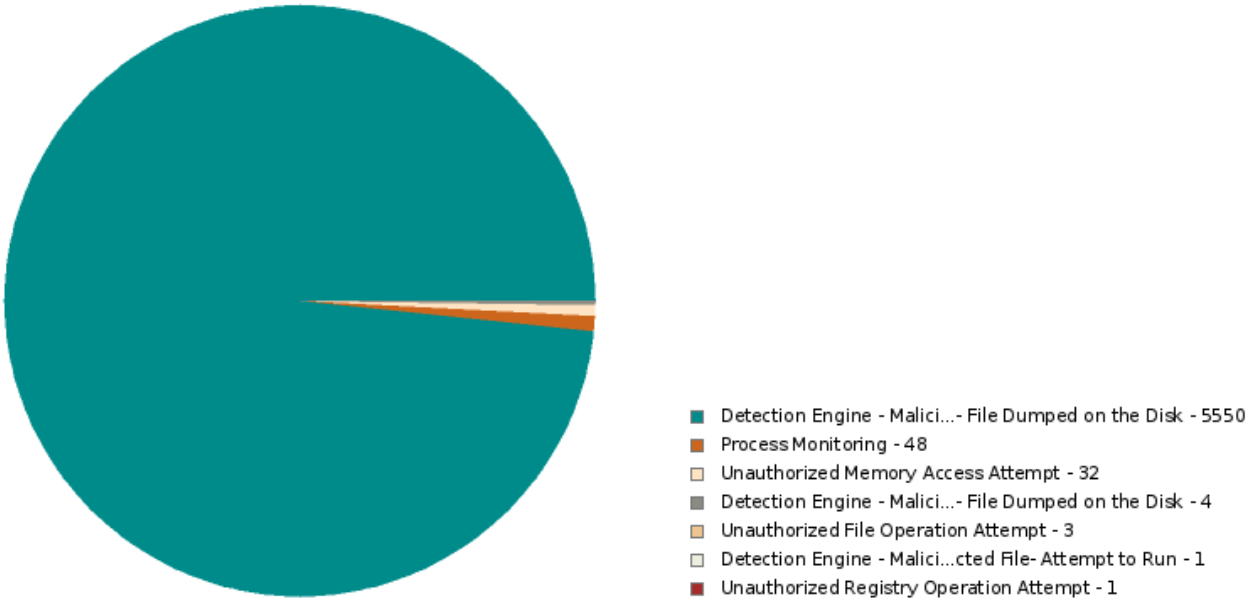
ASM-VP REPORT

GLESEC 07/26/2023

Events by Event Name - User Defined



High Severity Events by Event Name - User Defined



LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

Brute Force Detection by Ratio - User Defined

Host \ User Name	Ratio (Bad : Good)	Probability
veeam_server\administrator	51 : 97	0.53
dc-01\luis.montenegro	1 : 164	0.01
mss-epm\administrator	1 : 94	0.01
dc-02\luis.montenegro	1 : 194	0.01
dc-01\deyka.atencio	1 : 301	0.00

High Severity Events

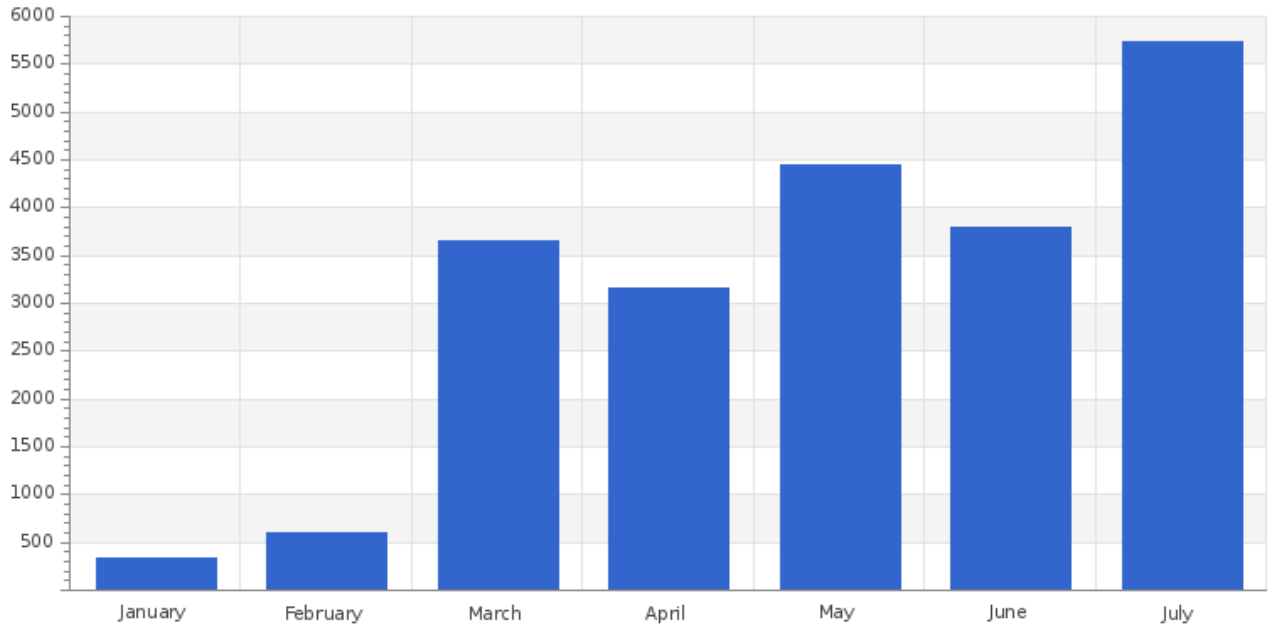
Host	File Path	Severity	count
GLESEC-AWS-CYMULATE	c:\windows\system32\control.exe	4	1
GLESEC-AWS-CYMULATE	c:\windows\system32\mshta.exe	4	1
GLESEC-AWS-CYMULATE	c:\windows\system32\regsvr32.exe	4	1
GLESEC-AWS-CYMULATE	c:\windows\system32\rundll32.exe	4	2
GLESEC-AWS-CYMULATE	c:\windows\system32\schtasks.exe	4	38
GLESEC-AWS-CYMULATE	c:\windows\system32\services.exe	4	1
GLESEC-AWS-CYMULATE	c:\windows\system32\windowspowershell\v1.0\powershell.exe	4	1
gmsa-transit.in.glesec.com	/usr/bin/bash	4	1
mss-siem.glesec.com	/bin/bash	4	1
mss-siem.glesec.com	/bin/cat	4	3

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

ASM-VP REPORT

GLESEC 07/26/2023

Events



Total Hosts - User Defined

36

High Severity Events by File Path - User Defined

File Path	Severity	Event Count
C:\ProgramData\Cymulate\AV\6495c7e63811b9709777c95f\Bluenoroffsbgiejbhacj19_edrP df.pdf	5	1
C:\ProgramData\Cymulate\AV\6495c7e63811b9709777c95f\Bluenoroffsbgiejbhacj8_edrPd f.pdf	5	1
C:\ProgramData\Cymulate\AV\64a2881cd85bfc6f44cb5ddd\Miraibgihfhcccf10_edrElf.elf	5	1
C:\ProgramData\Cymulate\AV\64a2b287d85bfc6f44cbe670\Matryoshkabgiididgjd2_edrRtf .rtf	5	1
C:\ProgramData\Cymulate\AV\64ad82e669f3b7083dbb86a9\Bluenoroffbgiecegcij14_edrPd f.pdf	5	1
C:\ProgramData\Cymulate\AV\64ad82e669f3b7083dbb86a9\Multiplebgieceghea45_edrUnkn .unkn	5	1
C:\ProgramData\Cymulate\AV\64ad82e669f3b7083dbb86a9\Multiplebgieceghea49_edrUnkn .unkn	5	1
C:\ProgramData\Cymulate\AV\64ad82e669f3b7083dbb86a9\Multiplebgieceghea4_edr7Unkn .unkn	5	1
C:\ProgramData\Cymulate\AV\64ad82e669f3b7083dbb86a9\Multiplebgieceghea52_edrUnkn .unkn	5	1
C:\ProgramData\Cymulate\AV\64ad82e669f3b7083dbb86a9\Sample100Html.html	5	1

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

High Severity Events by Host Name - User Defined

Host	Severity	Event Count
GLESEC-AWS-CYMULATE	5	922
GLESEC-AWS-CYMULATE	4	4701
mss-siem.glesec.com	4	6
gmsa-transit.in.glesec.com	4	1

MSS-DDOS

Total Attacks over 24 hours

0

Critical Attacks over 24 hours

0

MSS-WAF

Block Events

0

Applications

0

MSS-DLP

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

Total Users - Last 30 days

0

MSS-BOT

Bot Hits

145456

Signatures

695

Transactions

145408

Impacted Paths

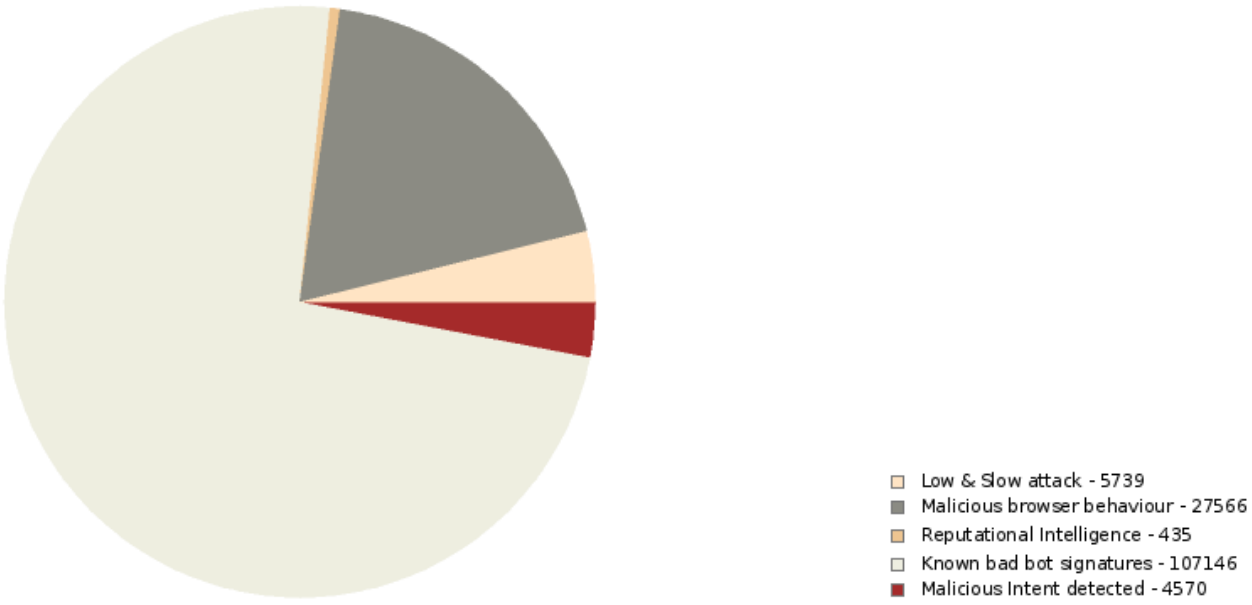
56777

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

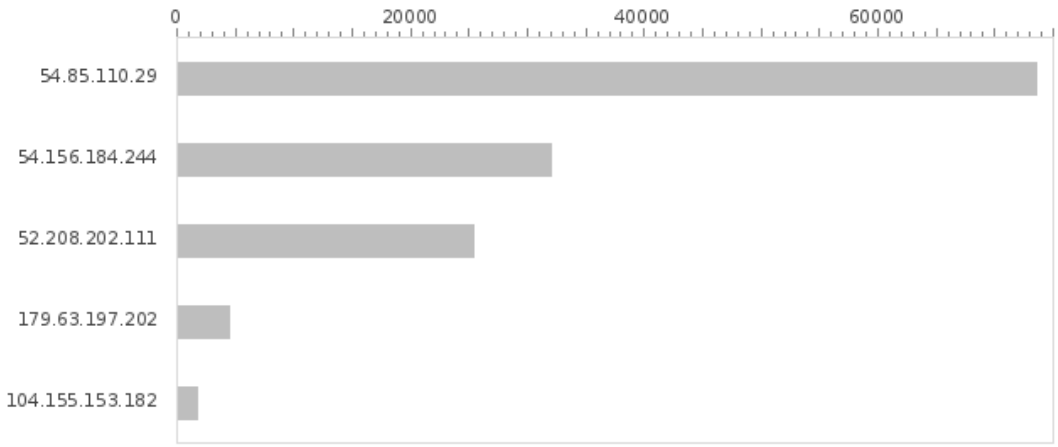
ASM-VP REPORT

GLESEC 07/26/2023

Bot Classification



Top Bad Bot IPs

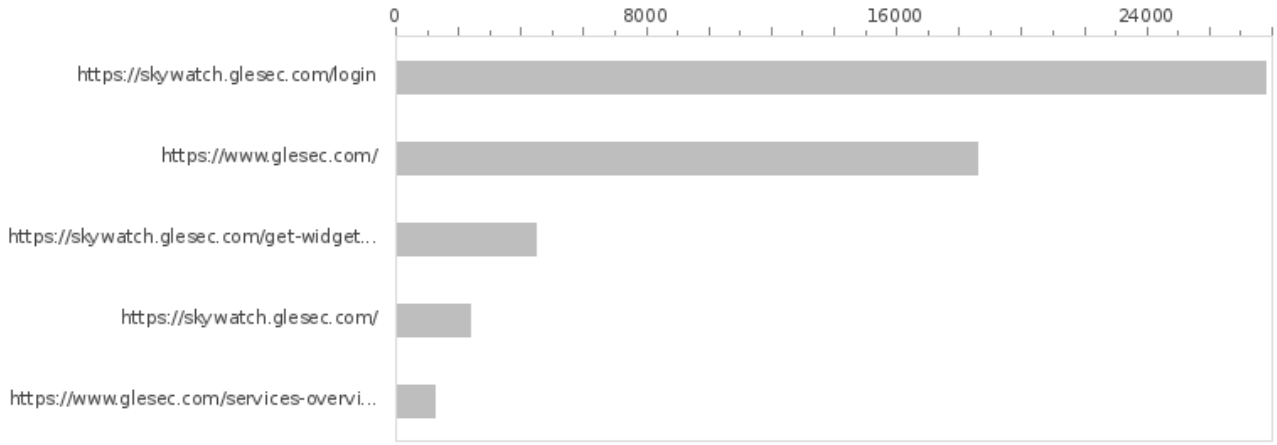


LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

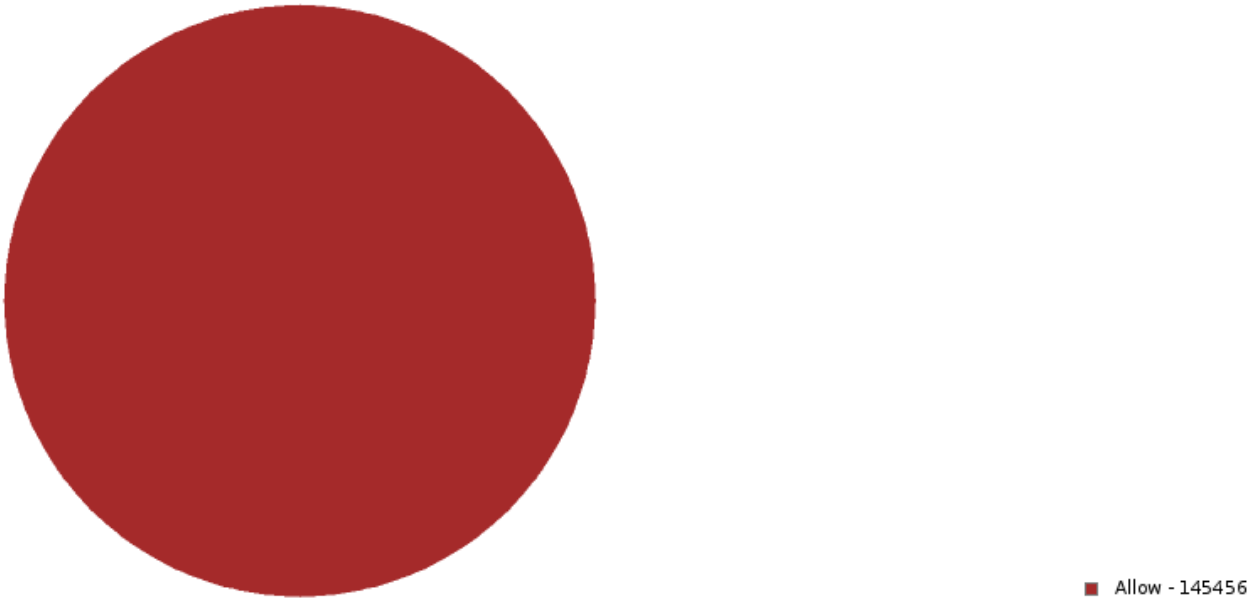
ASM-VP REPORT

GLESEC 07/26/2023

Top Impacted Paths



Bot Action

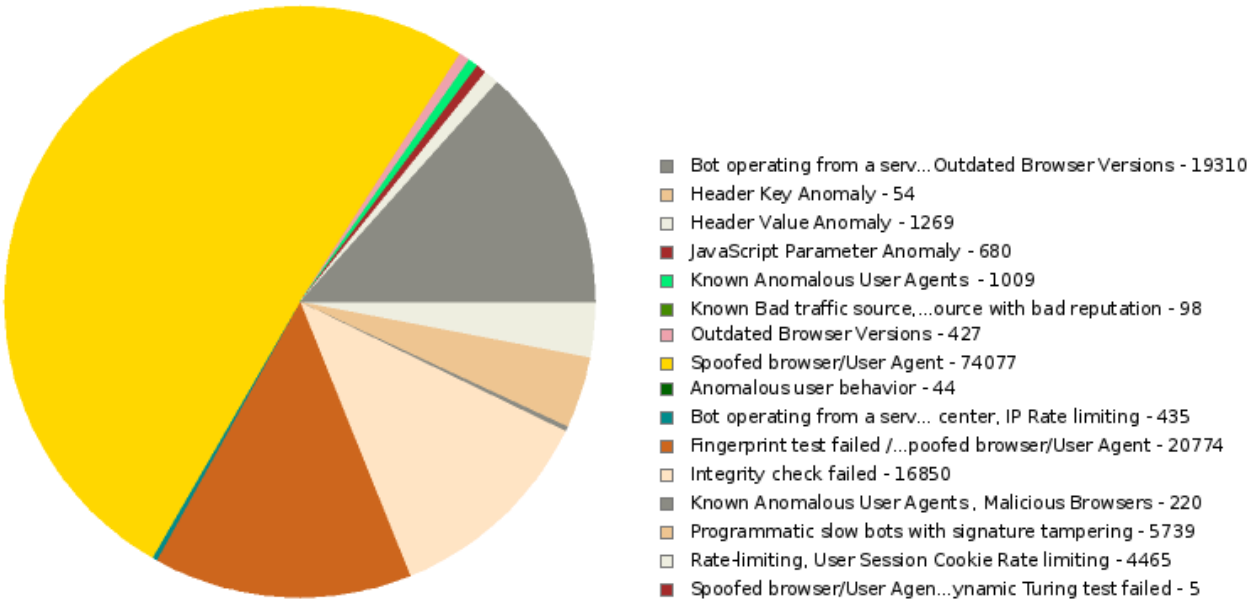


LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

ASM-VP REPORT

GLESEC 07/26/2023

Bot Violation



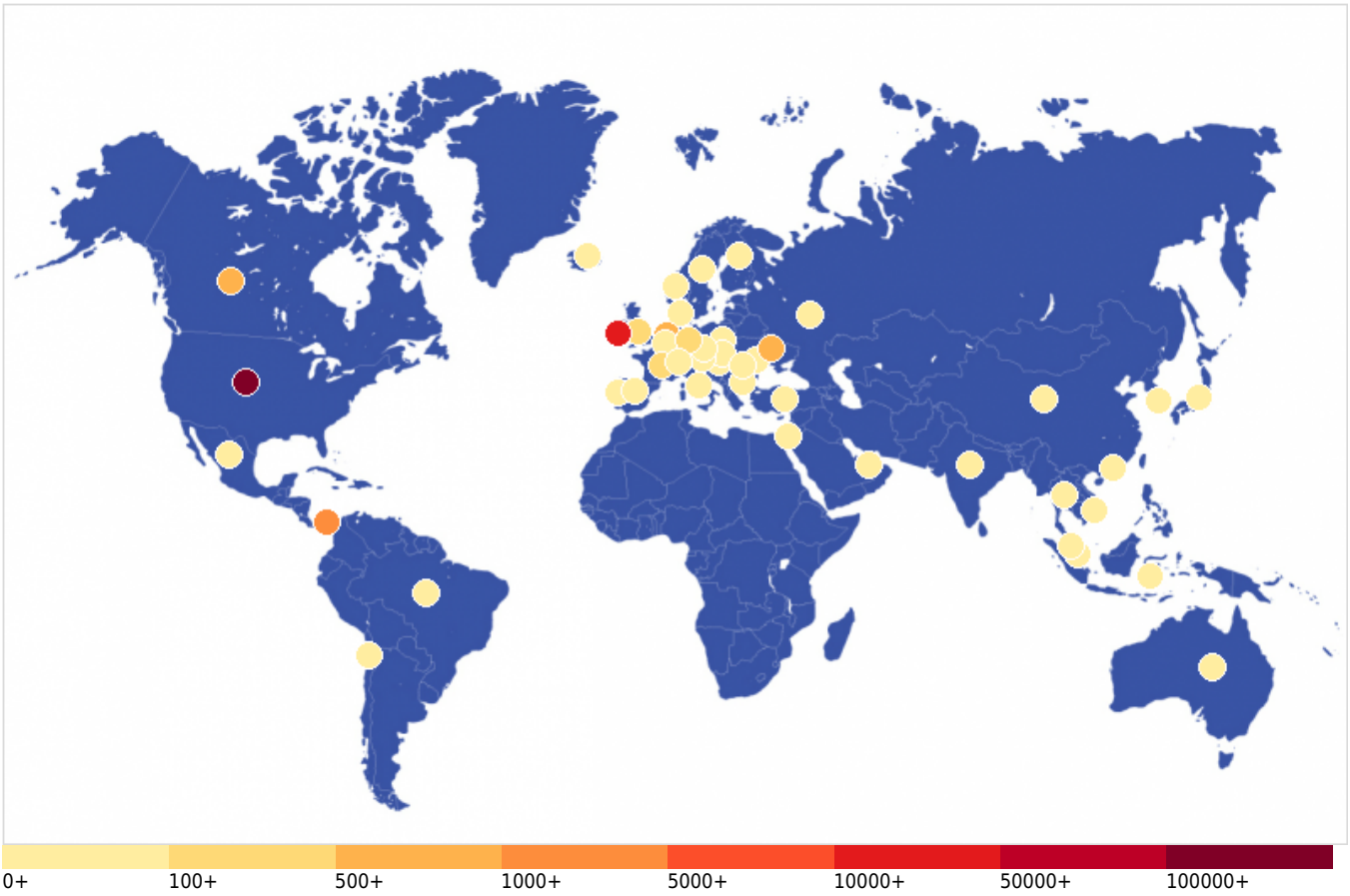
Bot Activity Map

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

TLP:AMBER

ASM-VP REPORT

GLESEC 07/26/2023



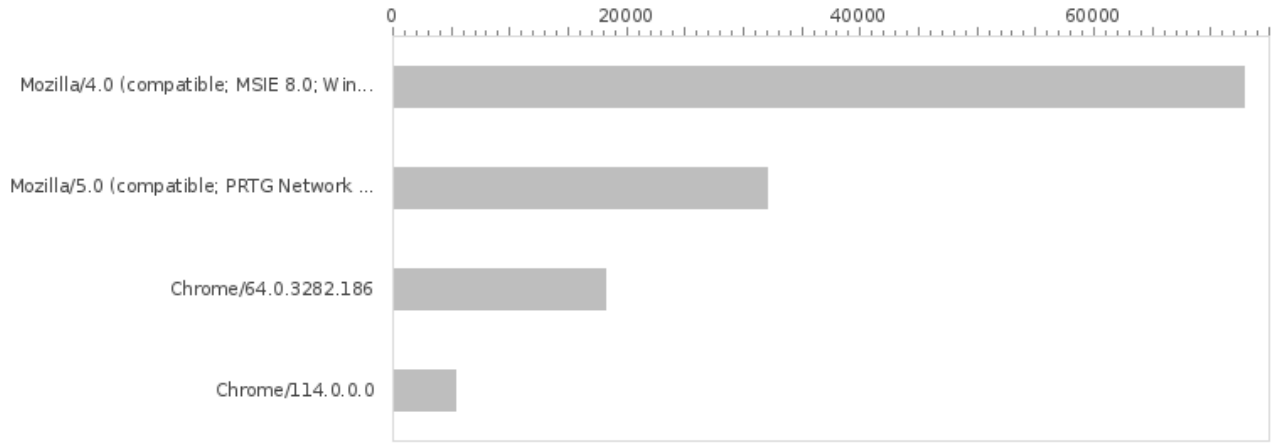
Australia - 13
Brazil - 6
Canada - 545
Denmark - 18
Finland - 18
Hungary - 5
Iceland - 1
Indonesia - 5
Israel - 2
Japan - 4
Luxembourg - 38
Moldova - 4
Netherlands - 589
Norway - 6
Panama - 4465
Poland - 65
Portugal - 3
Singapore - 52
Slovakia - 1
Sweden - 13
Turkey - 8
United Kingdom - 154
Vietnam - 2
Austria - 5
Belgium - 19
Bulgaria - 2
Chile - 1
China - 29
Czechia - 4
France - 124
Germany - 348
Hong Kong - 21
India - 60
Ireland - 25381
Italy - 30
Malaysia - 3
Mexico - 5
Romania - 13
Russia - 57
South Korea - 9
Spain - 31
Switzerland - 1
Thailand - 5
Ukraine - 553
United Arab Emirates - 7
United States - 112731

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

ASM-VP REPORT

GLESEC 07/26/2023

Top User Agents



Peak Times By Bot Classification

Peak Time	Category	Count
30/06/2023 0:00:00 AM	Malicious Intent detected	725
05/07/2023 7:00:00 AM	Known bad bot signatures	16871
30/06/2023 7:00:00 AM	Low & Slow attack	742
10/07/2023 11:00:00 AM	Reputational Intelligence	258
10/07/2023 14:00:00 PM	Malicious browser behaviour	6138

LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

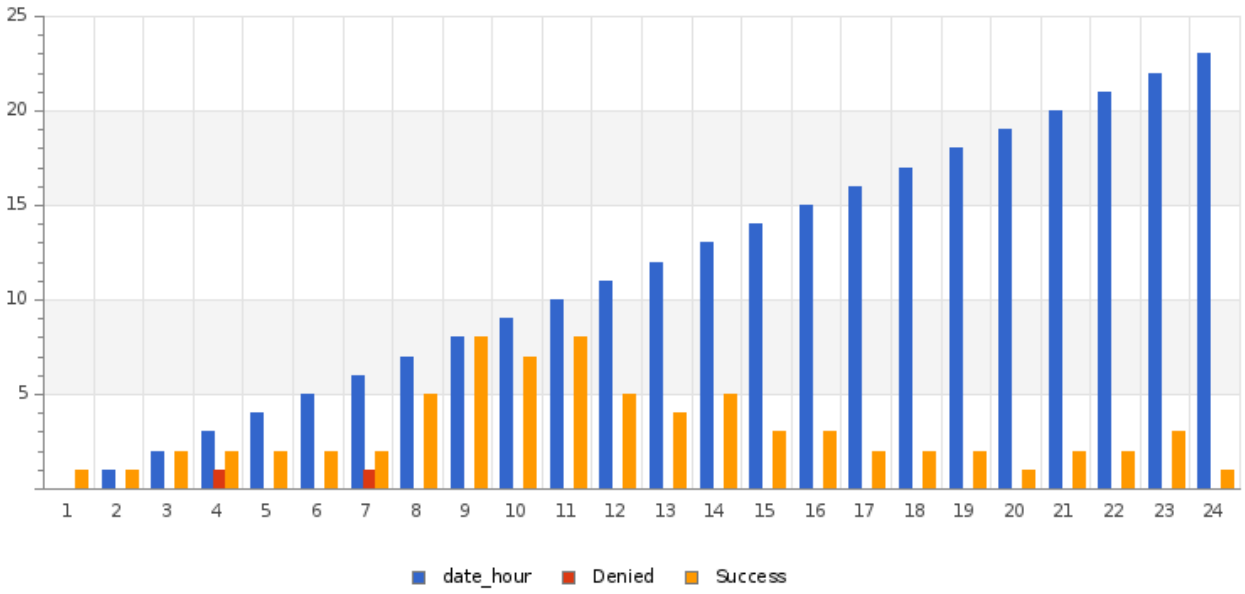
Trusted Access

MSS-TAS

Total Users *

32

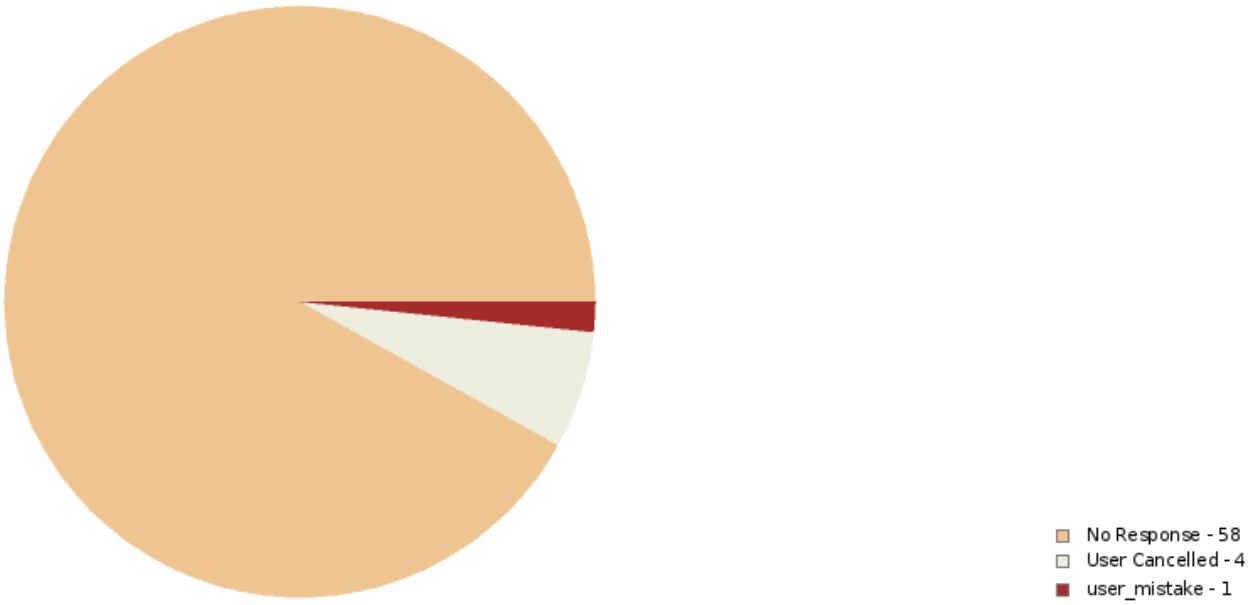
Average Authentications by Hour of the Day



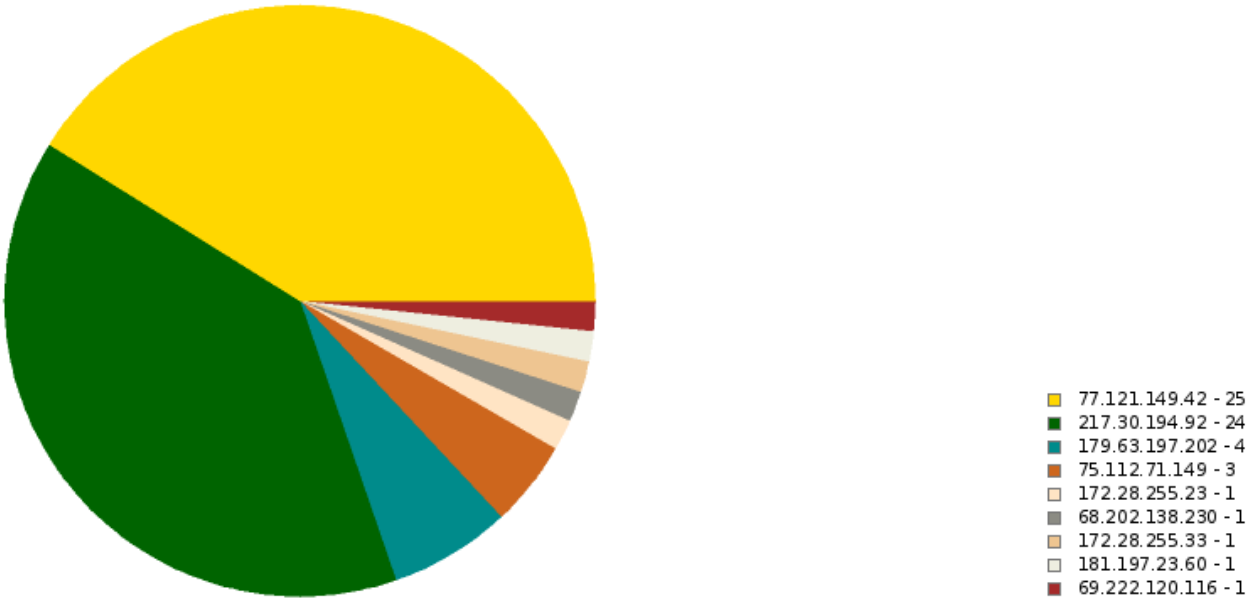
ASM-VP REPORT

GLESEC 07/26/2023

Top of Failed Authentications *



Top Authentications Failed by IPs *



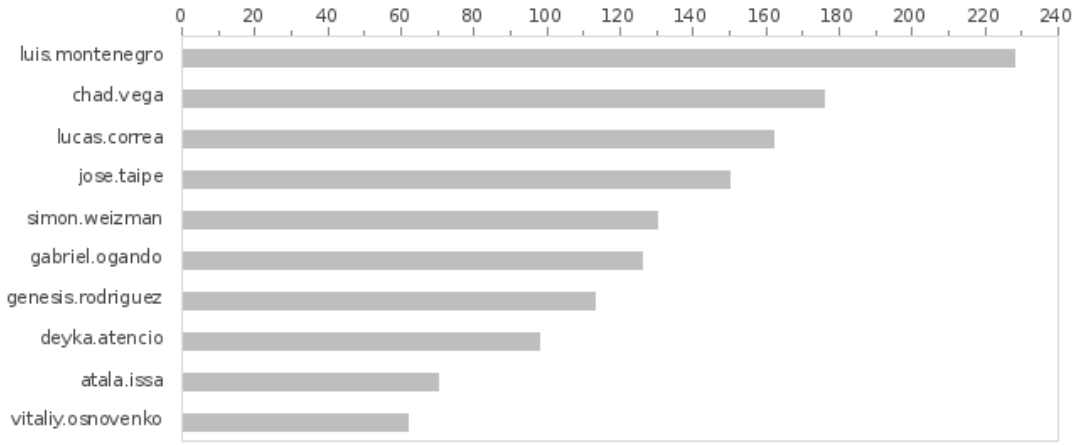
LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

ASM-VP REPORT

GLESEC 07/26/2023

Top Authenticated Users *



Most Active Applications *

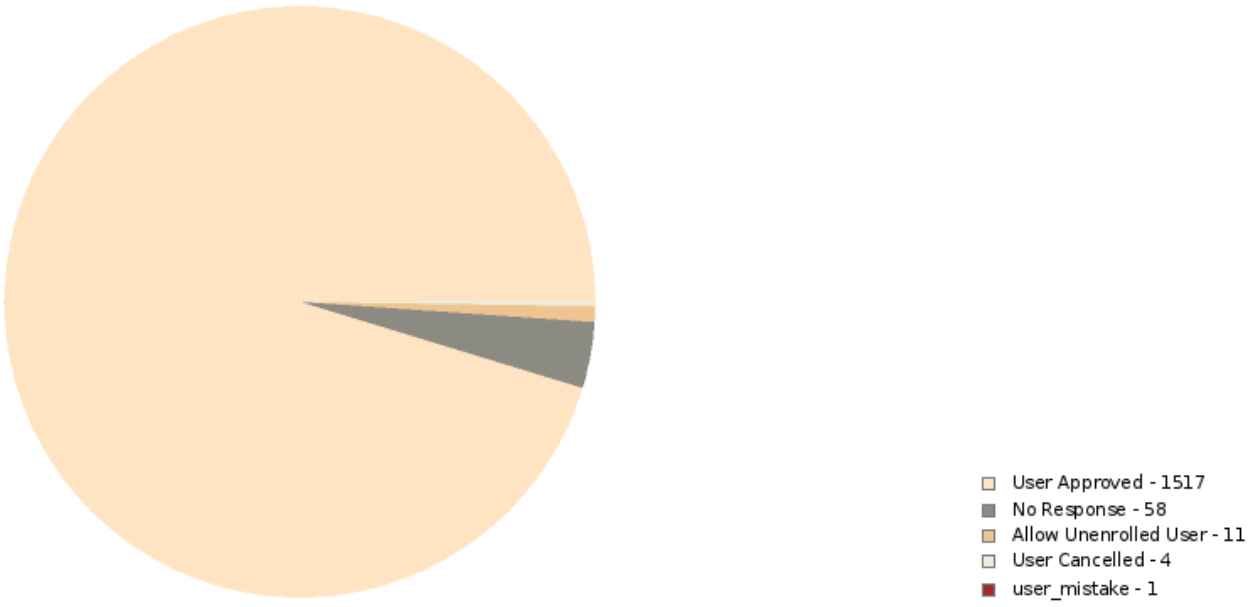
app	Denied	Success	Total
GLESEC Workstation Logon	3	355	358
Splunk	23	246	269
Cymulate	6	262	268
GLESEC INTRANET	21	168	189
Palo Alto GlobalProtect 2	4	167	171
Palo Alto GlobalProtect 1	2	134	136
Skywatch	3	68	71
Glesec Server Logon	1	53	54
Radware Cloud WAF	0	40	40
Zabbix	0	21	21
Panorama	0	7	7
GMP	0	4	4
Skywatch DEV	0	4	4

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

ASM-VP REPORT

GLESEC 07/26/2023

Authentication Status in the Last 24 Hours *



Users with failed authentications *

user	Time	src_ip
josh.goldberg	Wed Jul 26 8:14:14 2,023 EDT	69.222.120.116
luis.montenegro	Fri Jul 21 13:18:40 2,023 EDT	179.63.197.202
illya.sukhanov	Wed Jul 19 8:19:08 2,023 EDT	217.30.194.92
atala.issa	Fri Jul 14 10:58:18 2,023 EDT	75.112.71.149
illya.sukhanov	Mon Jul 10 10:10:47 2,023 EDT	77.121.149.42
illya.sukhanov	Mon Jul 10 10:12:03 2,023 EDT	77.121.149.42
illya.sukhanov	Mon Jul 10 10:19:03 2,023 EDT	77.121.149.42
illya.sukhanov	Mon Jul 10 10:20:05 2,023 EDT	77.121.149.42
illya.sukhanov	Mon Jul 10 10:21:28 2,023 EDT	77.121.149.42
illya.sukhanov	Mon Jul 10 10:42:00 2,023 EDT	77.121.149.42
illya.sukhanov	Tue Jul 11 3:26:35 2,023 EDT	77.121.149.42
illya.sukhanov	Tue Jul 11 3:27:37 2,023 EDT	77.121.149.42
illya.sukhanov	Tue Jul 11 3:35:32 2,023 EDT	217.30.194.92
illya.sukhanov	Fri Jul 7 2:57:17 2,023 EDT	217.30.194.92
illya.sukhanov3	Fri Jul 7 4:02:50 2,023 EDT	217.30.194.92
illya.sukhanov3	Fri Jul 7 4:02:52 2,023 EDT	217.30.194.92

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

ASM-VP REPORT

GLESEC 07/26/2023

user	Time	src_ip
illya.sukhanov3	Fri Jul 7 4:02:54 2,023 EDT	217.30.194.92
illya.sukhanov3	Fri Jul 7 4:05:10 2,023 EDT	217.30.194.92
illya.sukhanov3	Fri Jul 7 4:05:13 2,023 EDT	217.30.194.92
illya.sukhanov3	Fri Jul 7 4:05:15 2,023 EDT	217.30.194.92
illya.sukhanov	Fri Jul 7 4:29:38 2,023 EDT	77.121.149.42
jose.taipe	Fri Jul 7 6:11:35 2,023 EDT	179.63.197.202
vitalii.loievskyi	Mon Jul 3 11:24:10 2,023 EDT	77.121.149.42
vitalii.loievskyi	Mon Jul 3 11:24:26 2,023 EDT	77.121.149.42
illya.sukhanov3	Fri Jun 30 8:14:31 2,023 EDT	77.121.149.42
illya.sukhanov3	Fri Jun 30 8:21:15 2,023 EDT	77.121.149.42
luis.montenegro	Mon Jun 26 6:41:49 2,023 EDT	179.63.197.202
vitalii.loievskyi	Tue Jun 27 3:29:18 2,023 EDT	77.121.149.42
illya.sukhanov	Tue Jun 27 3:55:30 2,023 EDT	77.121.149.42
chad.vega	Fri Jul 21 11:49:42 2,023 EDT	75.112.71.149
chad.vega	Wed Jul 19 10:17:13 2,023 EDT	75.112.71.149
illya.sukhanov	Wed Jul 19 6:32:02 2,023 EDT	217.30.194.92
deyka.atencio	Sun Jul 16 13:47:52 2,023 EDT	181.197.23.60
illya.sukhanov	Mon Jul 10 5:33:09 2,023 EDT	217.30.194.92
illya.sukhanov	Mon Jul 10 5:34:12 2,023 EDT	217.30.194.92
vitaliy.osnovenko	Wed Jul 12 10:58:36 2,023 EDT	217.30.194.92
luis.montenegro	Tue Jul 4 21:28:49 2,023 EDT	0.0.0.0
luis.montenegro	Tue Jul 4 16:55:27 2,023 EDT	0.0.0.0
simon.weizman	Tue Jul 4 15:47:01 2,023 EDT	172.28.255.23
vitalii.loievskyi	Fri Jul 7 10:04:05 2,023 EDT	77.121.149.42
illya.sukhanov3	Fri Jun 30 9:12:22 2,023 EDT	217.30.194.92
illya.sukhanov3	Fri Jun 30 9:12:23 2,023 EDT	217.30.194.92
illya.sukhanov3	Fri Jun 30 9:12:25 2,023 EDT	217.30.194.92
illya.sukhanov3	Fri Jun 30 9:19:50 2,023 EDT	217.30.194.92
illya.sukhanov3	Fri Jun 30 9:19:52 2,023 EDT	217.30.194.92
illya.sukhanov3	Fri Jun 30 9:19:55 2,023 EDT	217.30.194.92
illya.sukhanov	Tue Jun 27 7:58:49 2,023 EDT	77.121.149.42
sergio.heker	Tue Jul 25 11:05:50 2,023 EDT	68.202.138.230
illya.sukhanov3	Fri Jul 14 3:15:57 2,023 EDT	77.121.149.42
illya.sukhanov3	Fri Jul 14 3:31:48 2,023 EDT	217.30.194.92
illya.sukhanov3	Fri Jul 14 3:31:49 2,023 EDT	217.30.194.92

LATAM HQ +507 836-5355
US HQ +1 (321) 430-0500

user	Time	src_ip
illya.sukhanov3	Fri Jul 14 3:31:51 2,023 EDT	217.30.194.92
illya.sukhanov	Mon Jul 10 9:45:53 2,023 EDT	77.121.149.42
illya.sukhanov	Mon Jul 10 9:48:47 2,023 EDT	77.121.149.42
illya.sukhanov	Mon Jul 10 9:50:01 2,023 EDT	77.121.149.42
lucas.correa	Wed Jul 5 10:58:03 2,023 EDT	172.28.255.33
illya.sukhanov3	Mon Jul 3 6:18:38 2,023 EDT	77.121.149.42
illya.sukhanov3	Mon Jul 3 6:19:48 2,023 EDT	77.121.149.42
genesis.rodriguez	Mon Jul 3 0:07:26 2,023 EDT	179.63.197.202
illya.sukhanov	Fri Jun 30 6:08:28 2,023 EDT	217.30.194.92
illya.sukhanov	Fri Jun 30 6:09:29 2,023 EDT	217.30.194.92
vitalii.loievskyi	Thu Jun 29 2:54:52 2,023 EDT	77.121.149.42
illya.sukhanov	Wed Jun 28 10:07:22 2,023 EDT	77.121.149.42

Authentications left as No response by Users *

Username	IP Address	Time
sergio.heker	68.202.138.230	Tue Jul 25 11:05:50 2,023 EDT
chad.vega	75.112.71.149	Wed Jul 19 10:17:13 2,023 EDT
illya.sukhanov	217.30.194.92	Wed Jul 19 6:32:02 2,023 EDT
deyka.atencio	181.197.23.60	Sun Jul 16 13:47:52 2,023 EDT
illya.sukhanov	217.30.194.92	Mon Jul 10 5:33:09 2,023 EDT
illya.sukhanov	217.30.194.92	Mon Jul 10 5:34:12 2,023 EDT
luis.montenegro	0.0.0.0	Tue Jul 4 21:28:49 2,023 EDT
luis.montenegro	0.0.0.0	Tue Jul 4 16:55:27 2,023 EDT
simon.weizman	172.28.255.23	Tue Jul 4 15:47:01 2,023 EDT
vitalii.loievskyi	77.121.149.42	Fri Jul 7 10:04:05 2,023 EDT
illya.sukhanov3	217.30.194.92	Fri Jun 30 9:12:22 2,023 EDT
illya.sukhanov3	217.30.194.92	Fri Jun 30 9:12:23 2,023 EDT
illya.sukhanov3	217.30.194.92	Fri Jun 30 9:12:25 2,023 EDT
illya.sukhanov3	217.30.194.92	Fri Jun 30 9:19:50 2,023 EDT
illya.sukhanov3	217.30.194.92	Fri Jun 30 9:19:52 2,023 EDT
illya.sukhanov3	217.30.194.92	Fri Jun 30 9:19:55 2,023 EDT
illya.sukhanov	77.121.149.42	Tue Jun 27 7:58:49 2,023 EDT
illya.sukhanov3	77.121.149.42	Fri Jul 14 3:15:57 2,023 EDT
illya.sukhanov3	217.30.194.92	Fri Jul 14 3:31:48 2,023 EDT

ASM-VP REPORT

GLESEC 07/26/2023

Username	IP Address	Time
illya.sukhanov3	217.30.194.92	Fri Jul 14 3:31:49 2,023 EDT
illya.sukhanov3	217.30.194.92	Fri Jul 14 3:31:51 2,023 EDT
illya.sukhanov	77.121.149.42	Mon Jul 10 9:45:53 2,023 EDT
illya.sukhanov	77.121.149.42	Mon Jul 10 9:48:47 2,023 EDT
illya.sukhanov	77.121.149.42	Mon Jul 10 9:50:01 2,023 EDT
illya.sukhanov3	77.121.149.42	Mon Jul 3 6:18:38 2,023 EDT
illya.sukhanov3	77.121.149.42	Mon Jul 3 6:19:48 2,023 EDT
genesis.rodriguez	179.63.197.202	Mon Jul 3 0:07:26 2,023 EDT
illya.sukhanov	217.30.194.92	Fri Jun 30 6:08:28 2,023 EDT
illya.sukhanov	217.30.194.92	Fri Jun 30 6:09:29 2,023 EDT
illya.sukhanov	77.121.149.42	Wed Jun 28 10:07:22 2,023 EDT
josh.goldberg	69.222.120.116	Wed Jul 26 8:14:14 2,023 EDT
luis.montenegro	179.63.197.202	Fri Jul 21 13:18:40 2,023 EDT
illya.sukhanov	217.30.194.92	Wed Jul 19 8:19:08 2,023 EDT
atala.issa	75.112.71.149	Fri Jul 14 10:58:18 2,023 EDT
illya.sukhanov	77.121.149.42	Mon Jul 10 10:10:47 2,023 EDT
illya.sukhanov	77.121.149.42	Mon Jul 10 10:12:03 2,023 EDT
illya.sukhanov	77.121.149.42	Mon Jul 10 10:19:03 2,023 EDT
illya.sukhanov	77.121.149.42	Mon Jul 10 10:20:05 2,023 EDT
illya.sukhanov	77.121.149.42	Mon Jul 10 10:21:28 2,023 EDT
illya.sukhanov	77.121.149.42	Mon Jul 10 10:42:00 2,023 EDT
illya.sukhanov	77.121.149.42	Tue Jul 11 3:26:35 2,023 EDT
illya.sukhanov	77.121.149.42	Tue Jul 11 3:27:37 2,023 EDT
illya.sukhanov	217.30.194.92	Tue Jul 11 3:35:32 2,023 EDT
illya.sukhanov	217.30.194.92	Fri Jul 7 2:57:17 2,023 EDT
illya.sukhanov3	217.30.194.92	Fri Jul 7 4:02:50 2,023 EDT
illya.sukhanov3	217.30.194.92	Fri Jul 7 4:02:52 2,023 EDT
illya.sukhanov3	217.30.194.92	Fri Jul 7 4:02:54 2,023 EDT
illya.sukhanov3	217.30.194.92	Fri Jul 7 4:05:10 2,023 EDT
illya.sukhanov3	217.30.194.92	Fri Jul 7 4:05:13 2,023 EDT
illya.sukhanov3	217.30.194.92	Fri Jul 7 4:05:15 2,023 EDT
illya.sukhanov	77.121.149.42	Fri Jul 7 4:29:38 2,023 EDT
jose.taipe	179.63.197.202	Fri Jul 7 6:11:35 2,023 EDT
vitalii.loievskyi	77.121.149.42	Mon Jul 3 11:24:10 2,023 EDT
vitalii.loievskyi	77.121.149.42	Mon Jul 3 11:24:26 2,023 EDT

Username	IP Address	Time
illya.sukhanov3	77.121.149.42	Fri Jun 30 8:14:31 2,023 EDT
illya.sukhanov3	77.121.149.42	Fri Jun 30 8:21:15 2,023 EDT
luis.montenegro	179.63.197.202	Mon Jun 26 6:41:49 2,023 EDT
illya.sukhanov	77.121.149.42	Tue Jun 27 3:55:30 2,023 EDT

Call timed out by Users *

Username	Time	IP Address
chad.vega	Wed Jul 19 10:17:13 2,023 EDT	75.112.71.149
illya.sukhanov	Wed Jul 19 6:32:02 2,023 EDT	217.30.194.92
deyka.atencio	Sun Jul 16 13:47:52 2,023 EDT	181.197.23.60
illya.sukhanov	Mon Jul 10 5:33:09 2,023 EDT	217.30.194.92
illya.sukhanov	Mon Jul 10 5:34:12 2,023 EDT	217.30.194.92
luis.montenegro	Tue Jul 4 21:28:49 2,023 EDT	0.0.0.0
luis.montenegro	Tue Jul 4 16:55:27 2,023 EDT	0.0.0.0
simon.weizman	Tue Jul 4 15:47:01 2,023 EDT	172.28.255.23
vitalii.loievskyi	Fri Jul 7 10:04:05 2,023 EDT	77.121.149.42
illya.sukhanov3	Fri Jun 30 9:12:22 2,023 EDT	217.30.194.92
illya.sukhanov3	Fri Jun 30 9:12:23 2,023 EDT	217.30.194.92
illya.sukhanov3	Fri Jun 30 9:12:25 2,023 EDT	217.30.194.92
illya.sukhanov3	Fri Jun 30 9:19:50 2,023 EDT	217.30.194.92
illya.sukhanov3	Fri Jun 30 9:19:52 2,023 EDT	217.30.194.92
illya.sukhanov3	Fri Jun 30 9:19:55 2,023 EDT	217.30.194.92
illya.sukhanov	Tue Jun 27 7:58:49 2,023 EDT	77.121.149.42
sergio.heker	Tue Jul 25 11:05:50 2,023 EDT	68.202.138.230
illya.sukhanov3	Fri Jul 14 3:15:57 2,023 EDT	77.121.149.42
illya.sukhanov3	Fri Jul 14 3:31:48 2,023 EDT	217.30.194.92
illya.sukhanov3	Fri Jul 14 3:31:49 2,023 EDT	217.30.194.92
illya.sukhanov3	Fri Jul 14 3:31:51 2,023 EDT	217.30.194.92
illya.sukhanov	Mon Jul 10 9:45:53 2,023 EDT	77.121.149.42
illya.sukhanov	Mon Jul 10 9:48:47 2,023 EDT	77.121.149.42
illya.sukhanov	Mon Jul 10 9:50:01 2,023 EDT	77.121.149.42
illya.sukhanov3	Mon Jul 3 6:18:38 2,023 EDT	77.121.149.42
illya.sukhanov3	Mon Jul 3 6:19:48 2,023 EDT	77.121.149.42
genesis.rodriguez	Mon Jul 3 0:07:26 2,023 EDT	179.63.197.202

ASM-VP REPORT

GLESEC 07/26/2023

Username	Time	IP Address
illya.sukhanov	Fri Jun 30 6:08:28 2,023 EDT	217.30.194.92
illya.sukhanov	Fri Jun 30 6:09:29 2,023 EDT	217.30.194.92
illya.sukhanov	Wed Jun 28 10:07:22 2,023 EDT	77.121.149.42
josh.goldberg	Wed Jul 26 8:14:14 2,023 EDT	69.222.120.116
luis.montenegro	Fri Jul 21 13:18:40 2,023 EDT	179.63.197.202
illya.sukhanov	Wed Jul 19 8:19:08 2,023 EDT	217.30.194.92
atala.issa	Fri Jul 14 10:58:18 2,023 EDT	75.112.71.149
illya.sukhanov	Mon Jul 10 10:10:47 2,023 EDT	77.121.149.42
illya.sukhanov	Mon Jul 10 10:12:03 2,023 EDT	77.121.149.42
illya.sukhanov	Mon Jul 10 10:19:03 2,023 EDT	77.121.149.42
illya.sukhanov	Mon Jul 10 10:20:05 2,023 EDT	77.121.149.42
illya.sukhanov	Mon Jul 10 10:21:28 2,023 EDT	77.121.149.42
illya.sukhanov	Mon Jul 10 10:42:00 2,023 EDT	77.121.149.42
illya.sukhanov	Tue Jul 11 3:26:35 2,023 EDT	77.121.149.42
illya.sukhanov	Tue Jul 11 3:27:37 2,023 EDT	77.121.149.42
illya.sukhanov	Tue Jul 11 3:35:32 2,023 EDT	217.30.194.92
illya.sukhanov	Fri Jul 7 2:57:17 2,023 EDT	217.30.194.92
illya.sukhanov3	Fri Jul 7 4:02:50 2,023 EDT	217.30.194.92
illya.sukhanov3	Fri Jul 7 4:02:52 2,023 EDT	217.30.194.92
illya.sukhanov3	Fri Jul 7 4:02:54 2,023 EDT	217.30.194.92
illya.sukhanov3	Fri Jul 7 4:05:10 2,023 EDT	217.30.194.92
illya.sukhanov3	Fri Jul 7 4:05:13 2,023 EDT	217.30.194.92
illya.sukhanov3	Fri Jul 7 4:05:15 2,023 EDT	217.30.194.92
illya.sukhanov	Fri Jul 7 4:29:38 2,023 EDT	77.121.149.42
jose.taipe	Fri Jul 7 6:11:35 2,023 EDT	179.63.197.202
vitalii.loievskyi	Mon Jul 3 11:24:10 2,023 EDT	77.121.149.42
vitalii.loievskyi	Mon Jul 3 11:24:26 2,023 EDT	77.121.149.42
illya.sukhanov3	Fri Jun 30 8:14:31 2,023 EDT	77.121.149.42
illya.sukhanov3	Fri Jun 30 8:21:15 2,023 EDT	77.121.149.42
luis.montenegro	Mon Jun 26 6:41:49 2,023 EDT	179.63.197.202
illya.sukhanov	Tue Jun 27 3:55:30 2,023 EDT	77.121.149.42

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

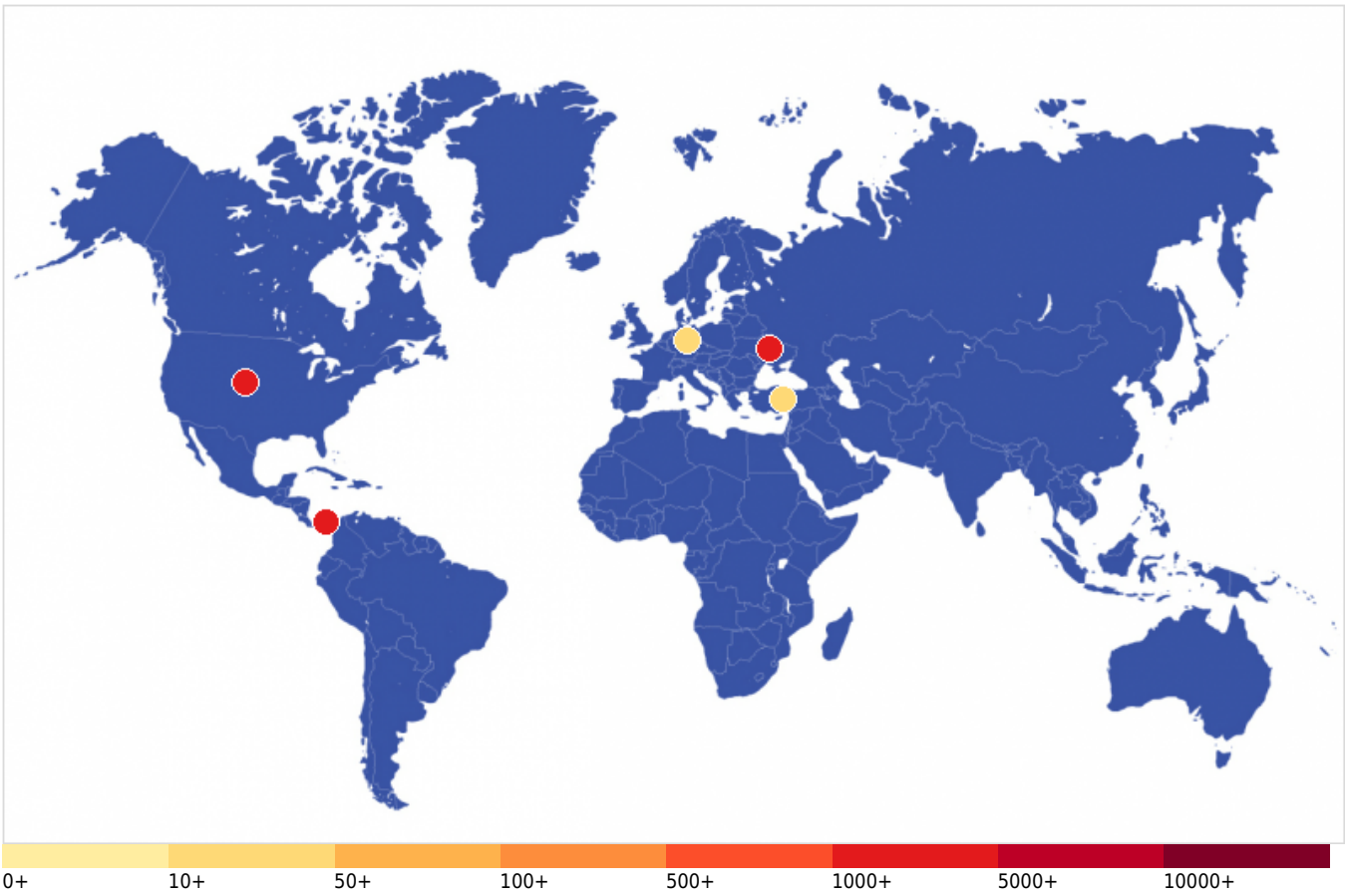
ASM-VP REPORT

GLESEC 07/26/2023

Authentications Cancelled by the Users *

Username	Time	IP Address
chad.vega	Fri Jul 21 11:49:42 2,023 EDT	75.112.71.149
vitaliy.osnovenko	Wed Jul 12 10:58:36 2,023 EDT	217.30.194.92
vitalii.loievskyi	Tue Jun 27 3:29:18 2,023 EDT	77.121.149.42
vitalii.loievskyi	Thu Jun 29 2:54:52 2,023 EDT	77.121.149.42

Most Successful Authenticated Countries *

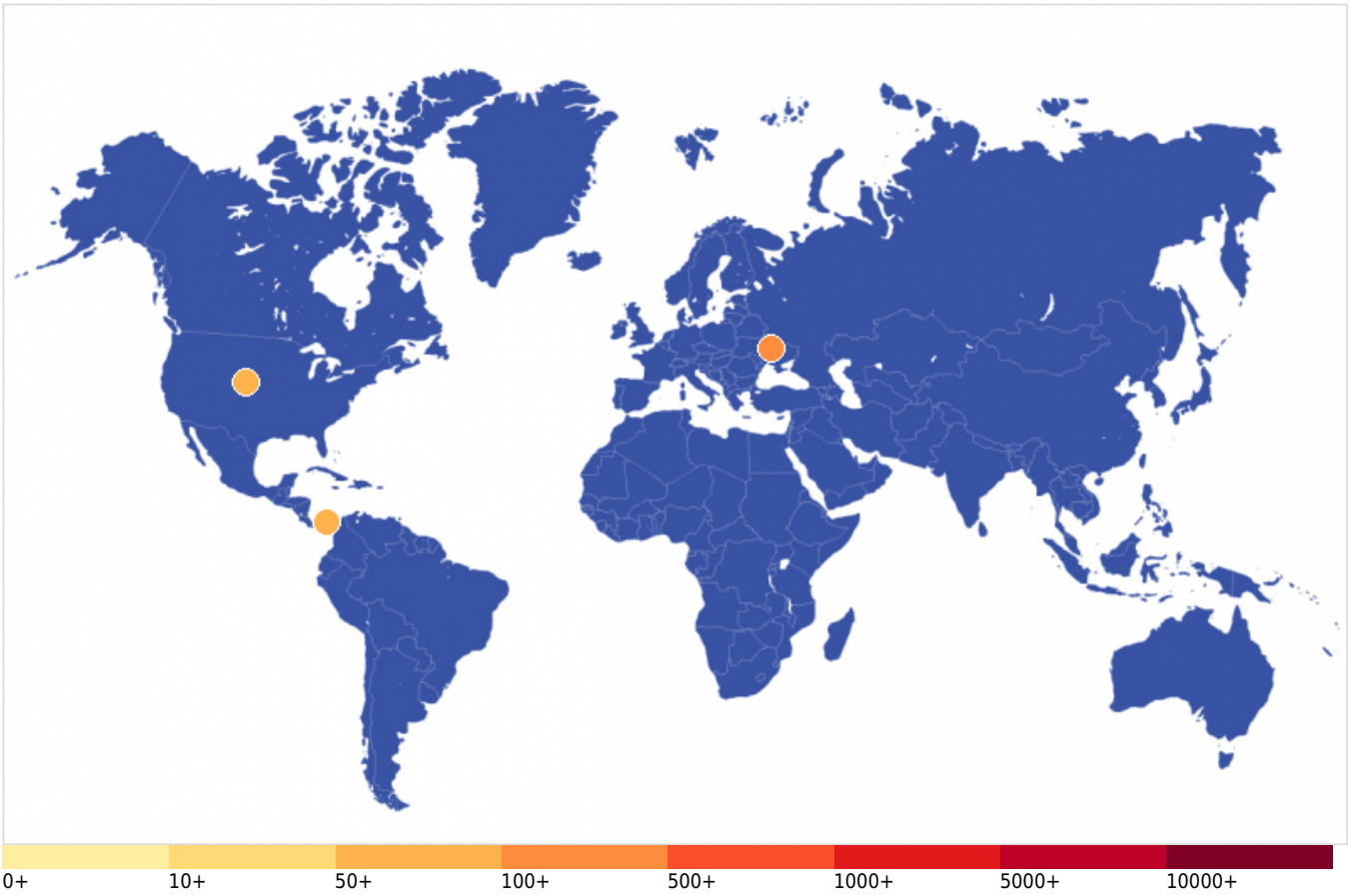


Countries with Most Failed Authentications *

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

ASM-VP REPORT

GLESEC 07/26/2023

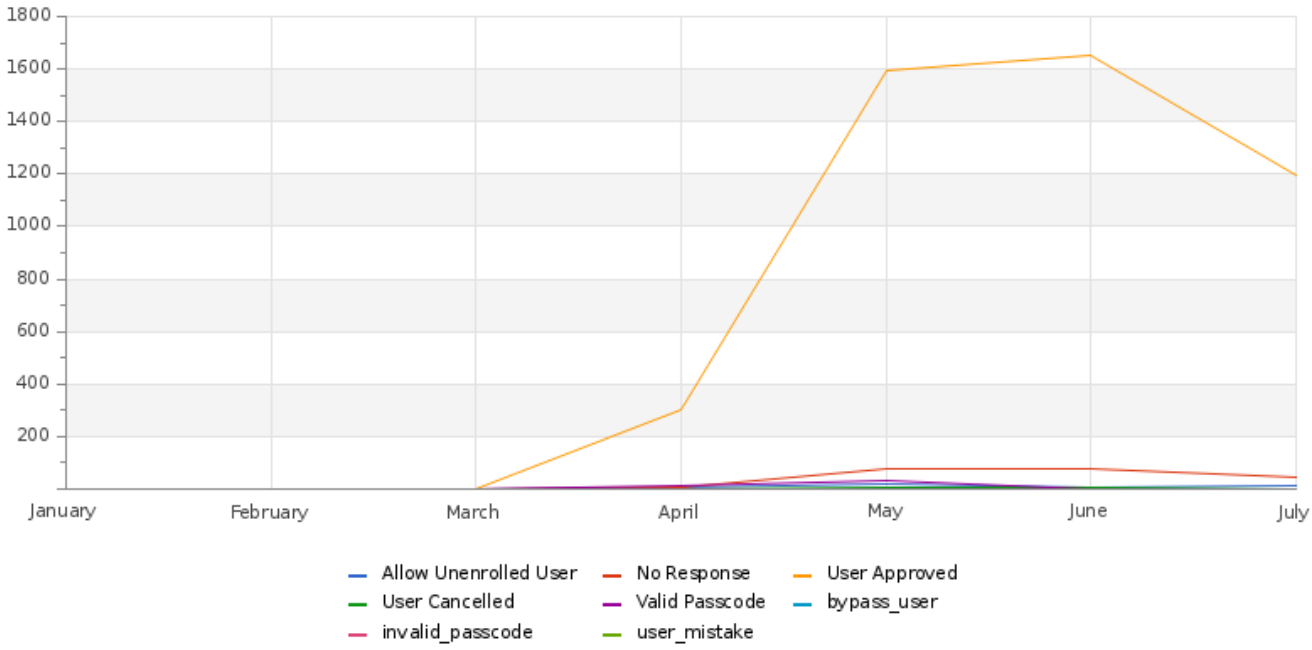


LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

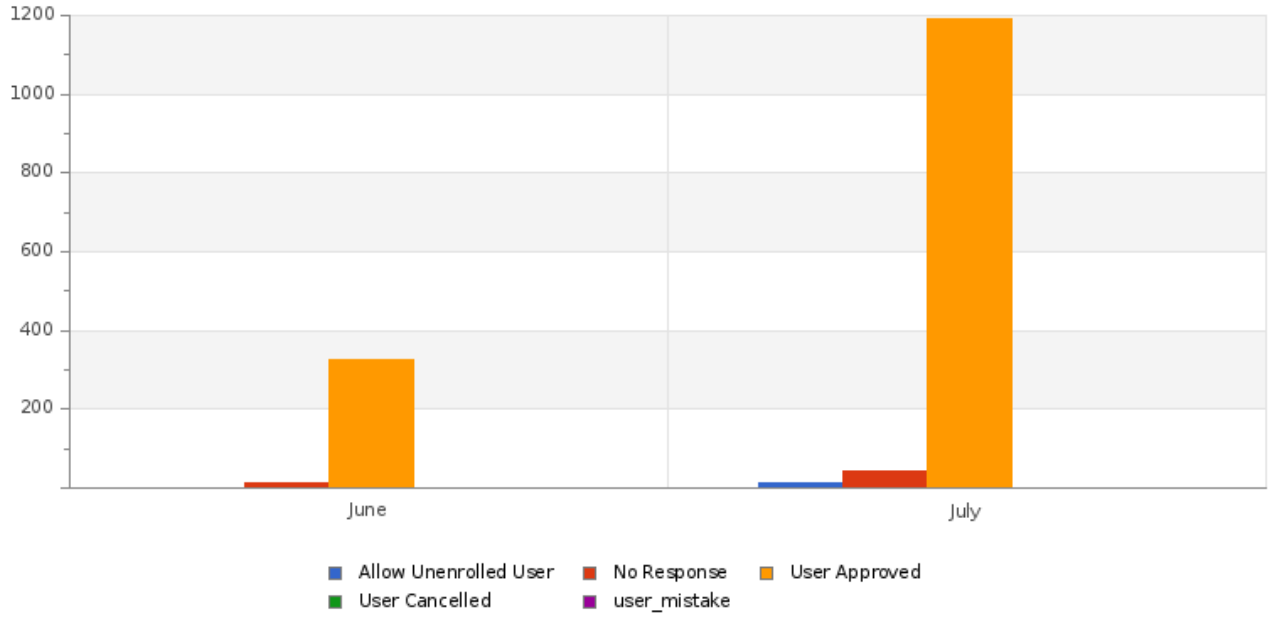
ASM-VP REPORT

GLESEC 07/26/2023

Trusted Access In Last 6 Months



Successful and Failed Authentications *

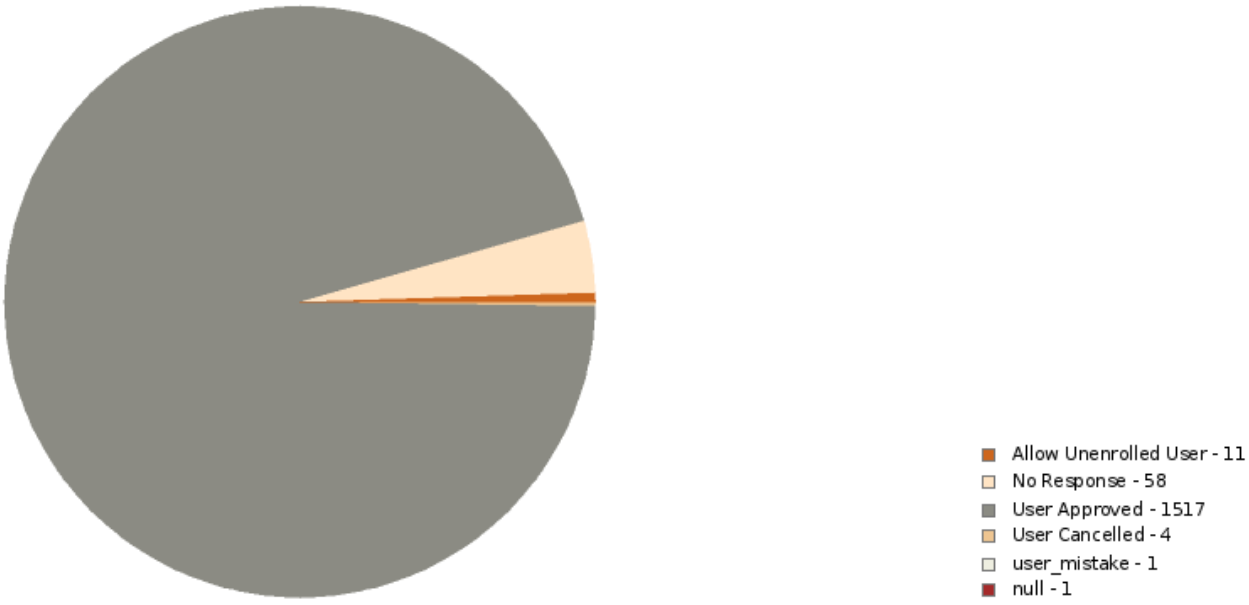


LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

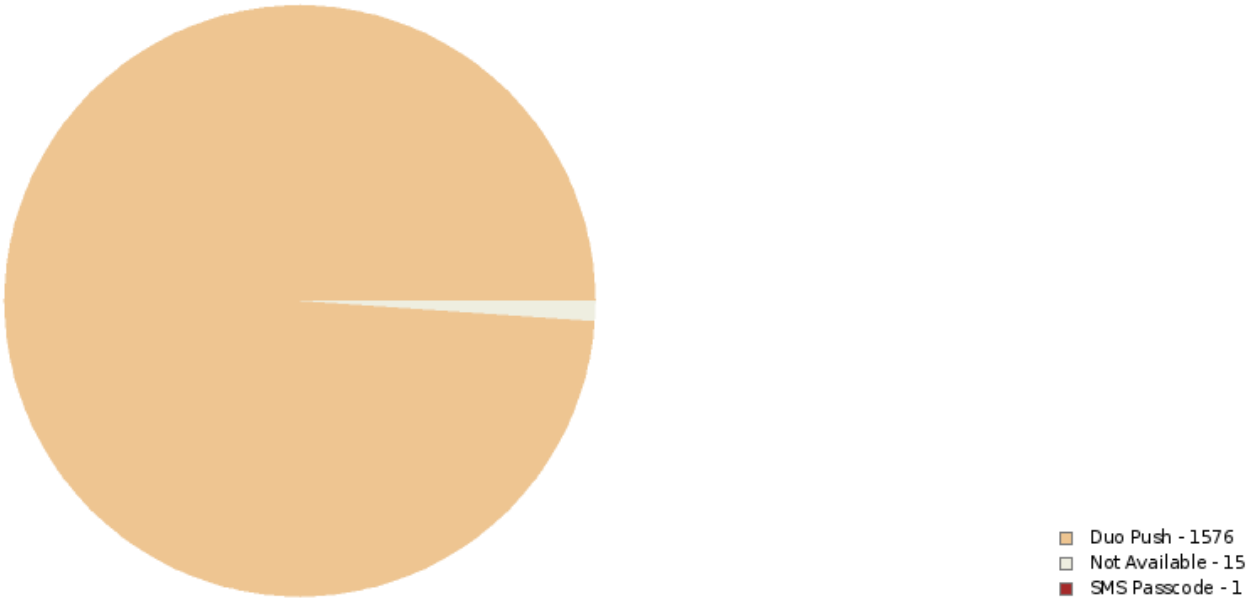
ASM-VP REPORT

GLESEC 07/26/2023

Successful Authentications *



Successful Authentications by Factor *

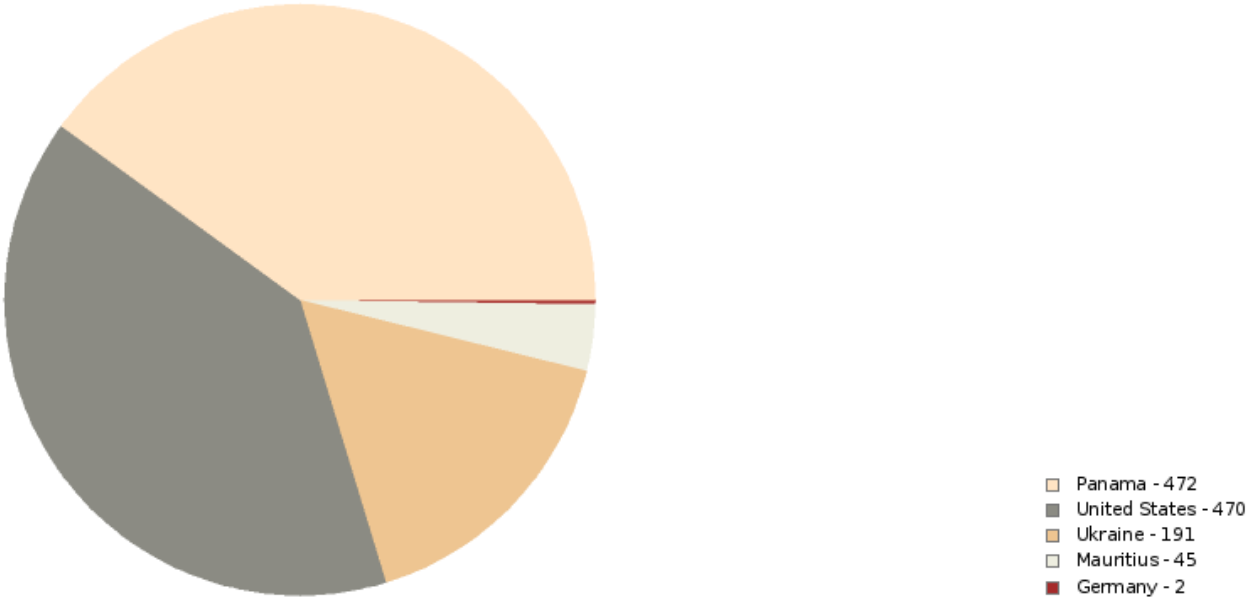


LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

ASM-VP REPORT

GLESEC 07/26/2023

Authentication Per Country *



MSS-USB

Top Actions

action	count
file_create	8
file_move	8
file_delete	2
logout	2

Top Locations - Cities

City	Country	Count
Orlando	US	37

LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

ASM-VP REPORT

GLESEC 07/26/2023

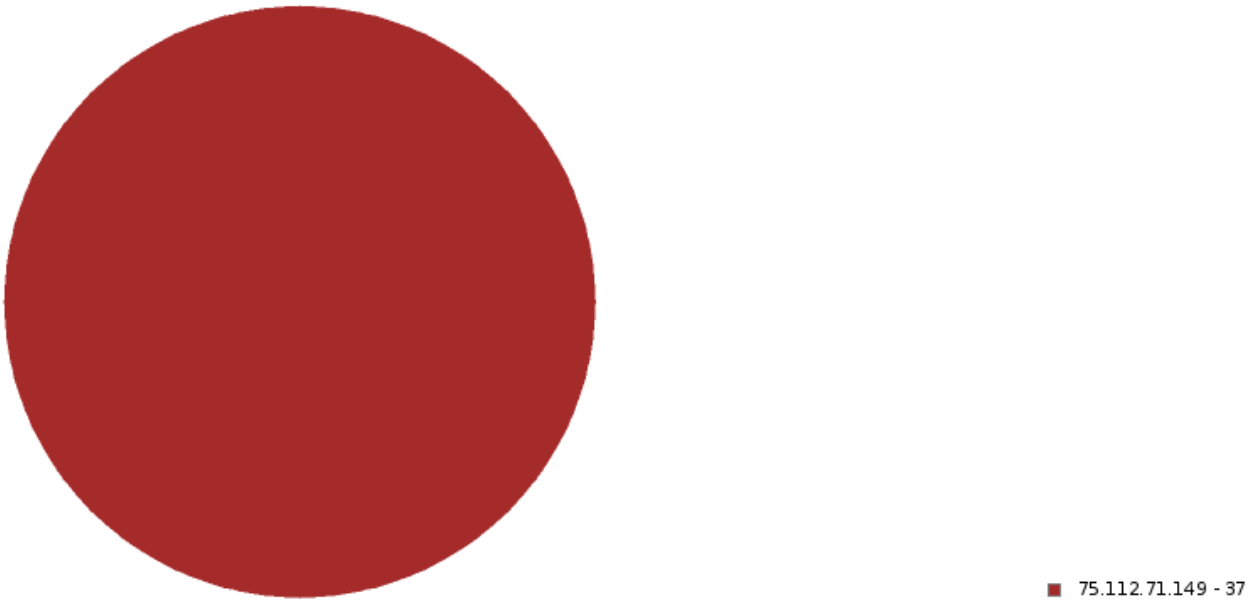
IP Addresses - List

IP Address	Count
75.112.71.149	37

Drives used in Last 30 days

Serial	Drive Model	User	Computer	City	Country	IP
2C27D7349F00B260B00055B4	SafeStick Managed	in.glesec.com/GLESEC/Users/Orlando/Lucas Correa	USASYSTEMSWS03	Orlando	US	75.112.71.149

IP Addresses - Top 10



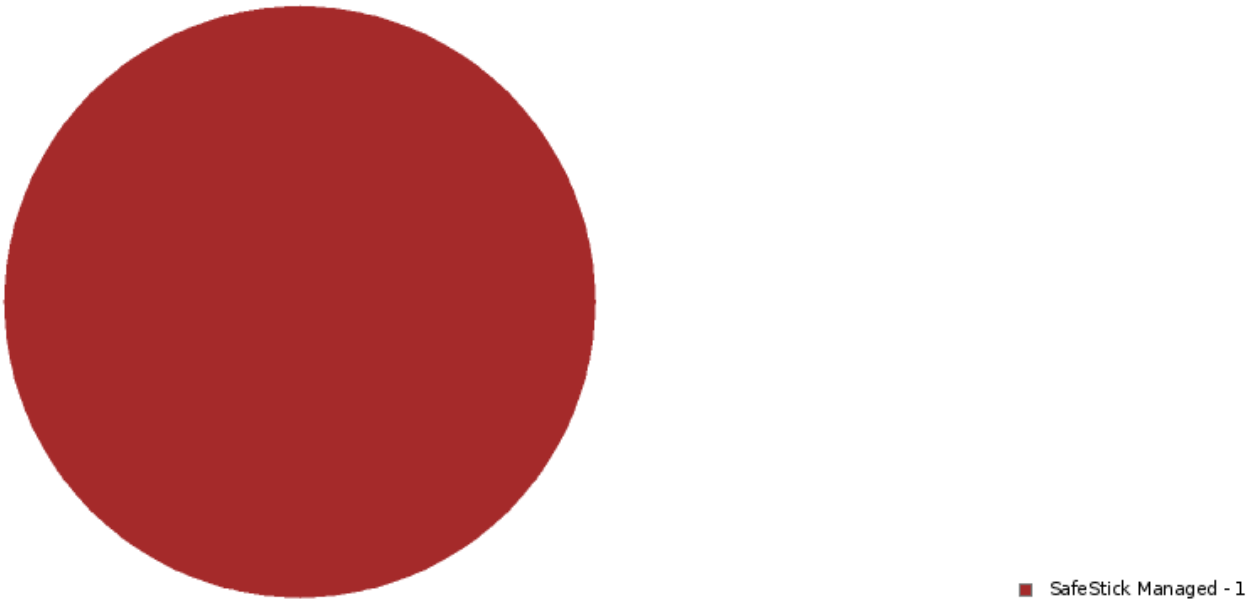
LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

TLP:AMBER

ASM-VP REPORT

GLESEC 07/26/2023

Drive Inventory - Model Count



Drive Inventory

Drive Model	Serial	User	Location
SafeStick Managed	2C27D7349F00B260B00055B4	in.glesec.com/GLESEC/Users/Orlando/Lucas Correa	Orlando, US

TLP:AMBER = Limited disclosure, restricted to participants' organizations. Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.**

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

TLP:AMBER

ASM-VP REPORT

HOW CAN WE HELP?

Contact us today for more information on
our services and security solutions.

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500