TLP:AMBER

ASM-VP REPORT

GOAA

July 26, 2024

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

22%

Discovered Hosts

43

Vulnerable Hosts

32

Executive Summary Vulnerability Severity Distribution

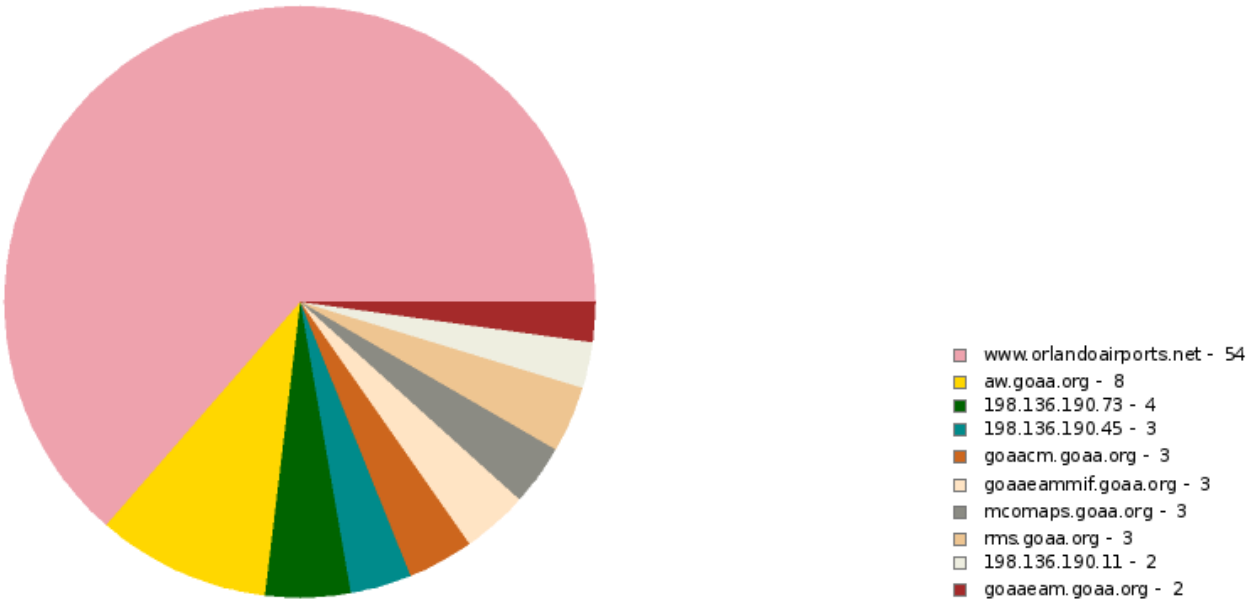
Scanner	Critical	High	Medium	Low	Total
GOAA	0	0	53	8	61
Domain Scan: www.orlandoairports.net	34	0	3	17	54

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

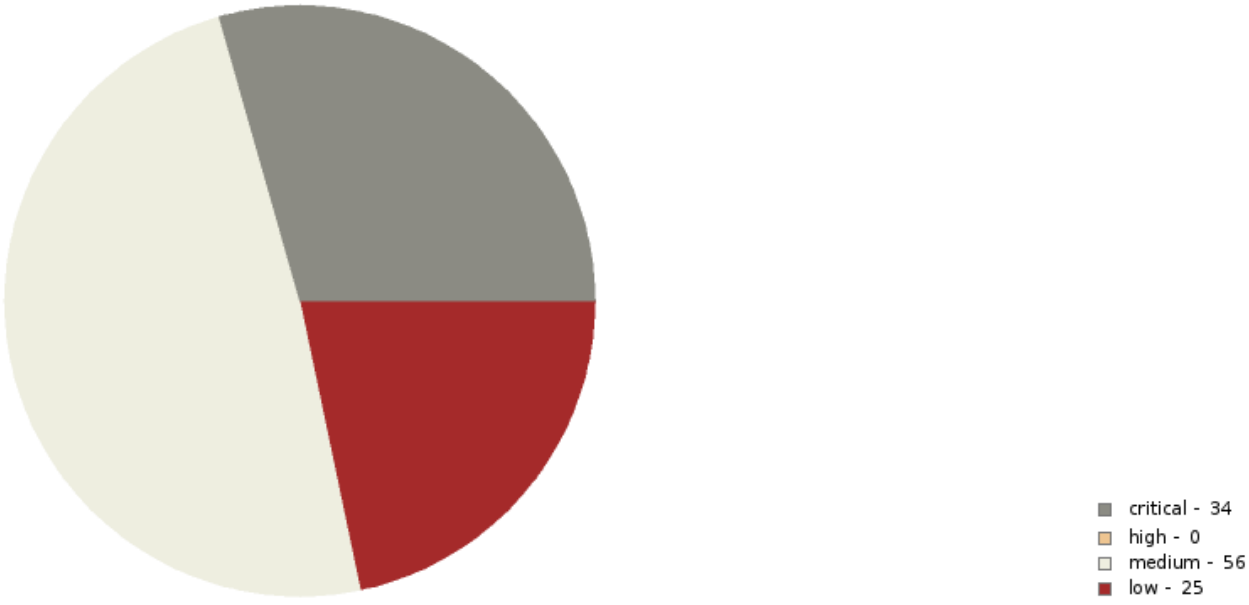
ASM-VP REPORT

GOAA 07/26/2024

Most Vulnerable Host *



Vulnerability Distribution



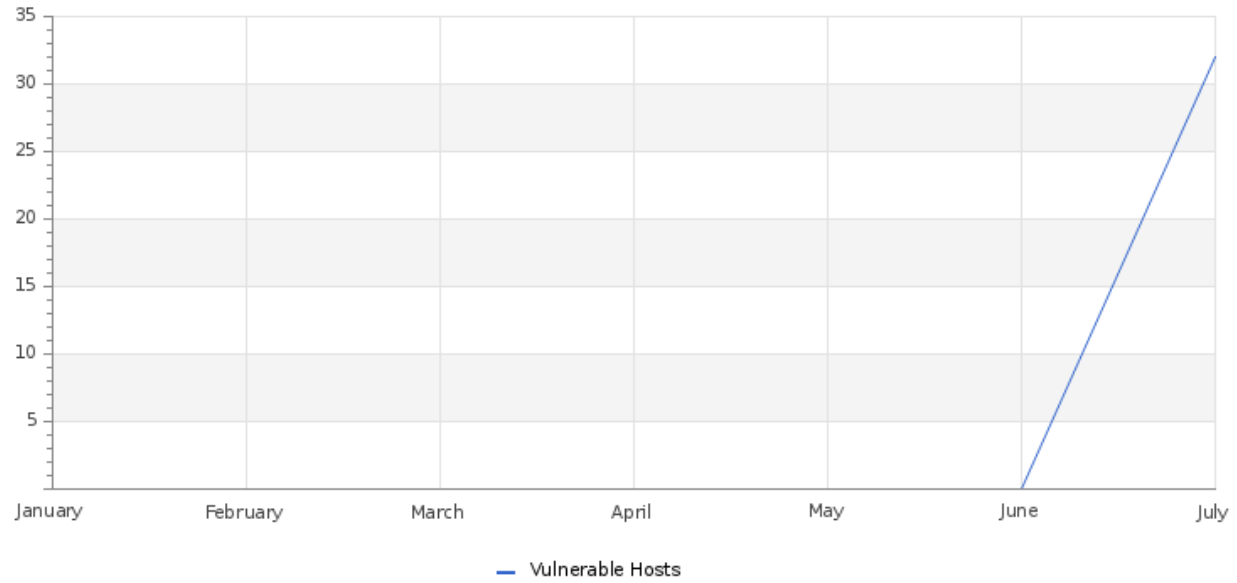
LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

Top 10 Most Common Vulnerabilities

Vulnerability
Web cache poisoning
HSTS Missing From HTTPS Server (RFC 6,797)
TLS Version 1.10 Deprecated Protocol
Open redirection (DOM-based)
SSL Certificate Cannot Be Trusted
ICMP Timestamp Request Remote Date Disclosure
SSL Medium Strength Cipher Suites Supported (SWEET32)
Client-side HTTP parameter pollution (reflected)
F5 BIG-IP Cookie Remote Information Disclosure
TLS Version 1.00 Protocol Detection

History

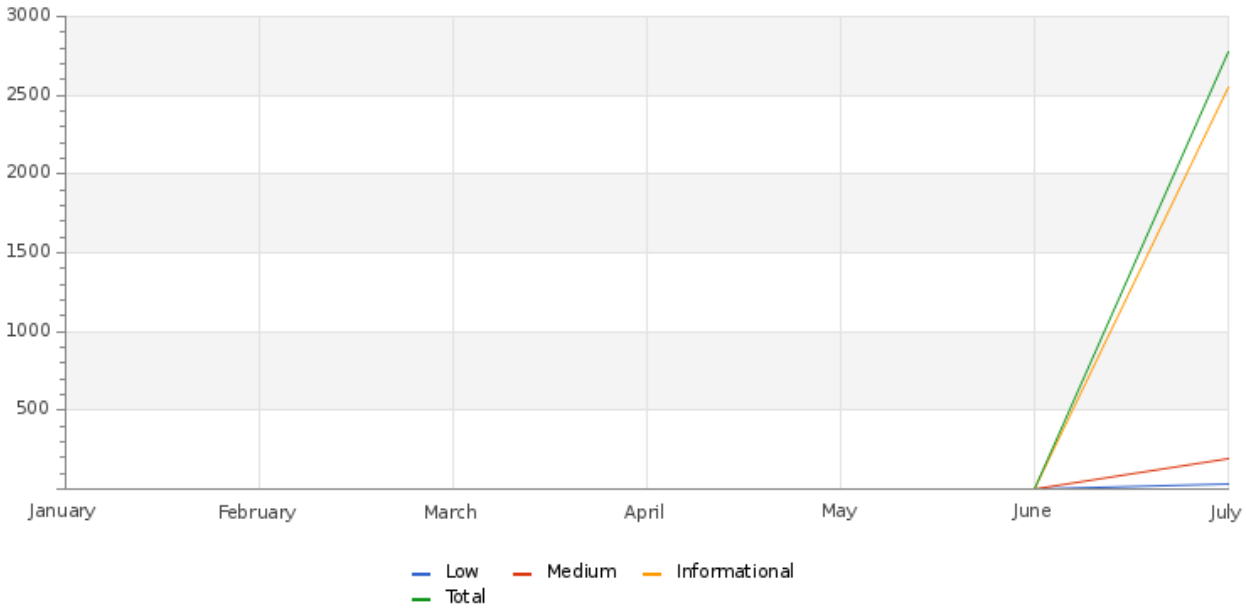
Vulnerable Host History



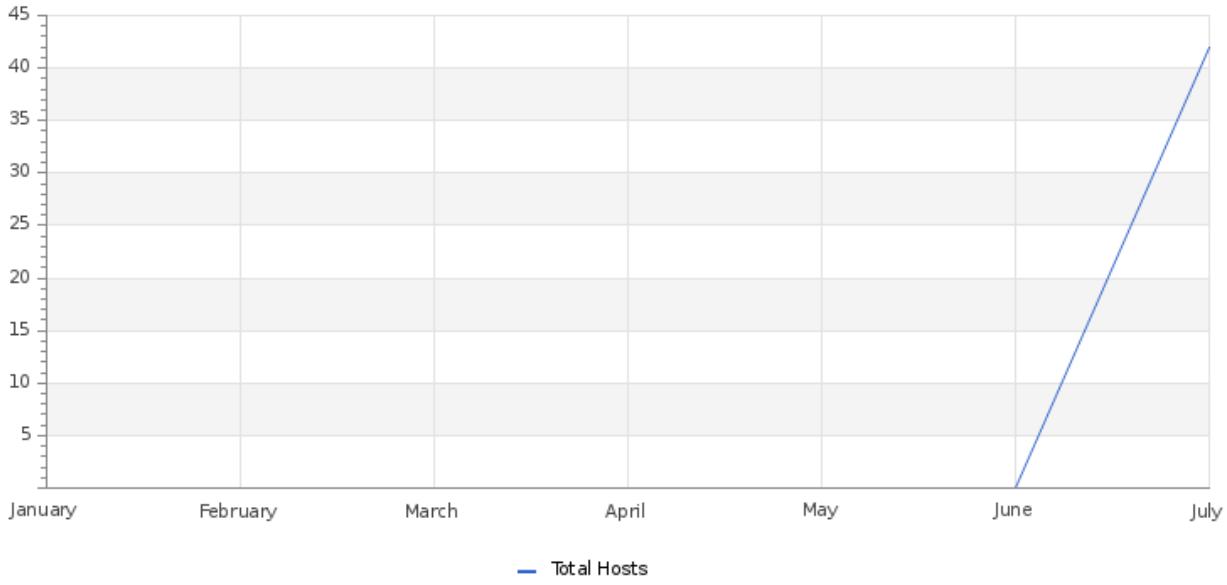
ASM-VP REPORT

GOAA 07/26/2024

Vulnerability Severity History



Discovered Host History



Open Port Monitoring

Open Ports

ip	hostname	port	status	protocol	service
198.136.190.25	owa.goaa.org	80	open	tcp	www
198.136.190.25	owa.goaa.org	443	open	tcp	www
198.136.190.144	dns.goaa.org	53	open	tcp	dns
198.136.190.45		80	open	tcp	www
198.136.190.45		443	open	tcp	www
198.136.190.124	mcomaps.goaa.org	443	open	tcp	www
198.136.190.244		80	open	tcp	www
198.136.190.244		443	open	tcp	www
198.136.190.145	dns2.goaa.org	53	open	tcp	dns
198.136.190.11		80	open	tcp	www
198.136.190.11		443	open	tcp	www
198.136.190.71	aw.goaa.org	443	open	tcp	www
198.136.190.71	aw.goaa.org	2020	open	tcp	http_proxy
198.136.190.71	aw.goaa.org	8443	open	tcp	No Service Detected
198.136.190.50	ipro.goaa.org	443	open	tcp	www
198.136.190.47	goaarmswsd.goaa.org	443	open	tcp	www
198.136.190.52		443	open	tcp	www
198.136.190.10	goaaeamtest.testgoaa.org	443	open	tcp	www
198.136.190.7	tportal.goaa.org	443	open	tcp	www
198.136.190.54	mcomobile.goaa.org	443	open	tcp	www
198.136.190.48	rms.goaa.org	443	open	tcp	www
198.136.190.31	mcomapstest.testgoaa.org	443	open	tcp	www
198.136.190.19	goaanet.goaa.org	443	open	tcp	www
198.136.190.15	mcotaxidispatch.goaa.org	443	open	tcp	www
198.136.190.53	mcomobiletest.testgoaa.org	443	open	tcp	www
198.136.190.42	pwa.goaa.org	443	open	tcp	www
198.136.190.35	goaaeammif.goaa.org	443	open	tcp	www
198.136.190.39	goaaeam.goaa.org	443	open	tcp	www
198.136.190.73		443	open	tcp	www
198.136.190.73		8443	open	tcp	www
198.136.190.20	bcws.goaa.aero	443	open	tcp	www

ip	hostname	port	status	protocol	service
198.136.190.20	bcws.goaa.aero	8443	open	tcp	www
198.136.190.37		443	open	tcp	www
198.136.190.44	goaacm.goaa.org	443	open	tcp	www

Penetration Tab

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

Vulnerability

MSS-BAS Email

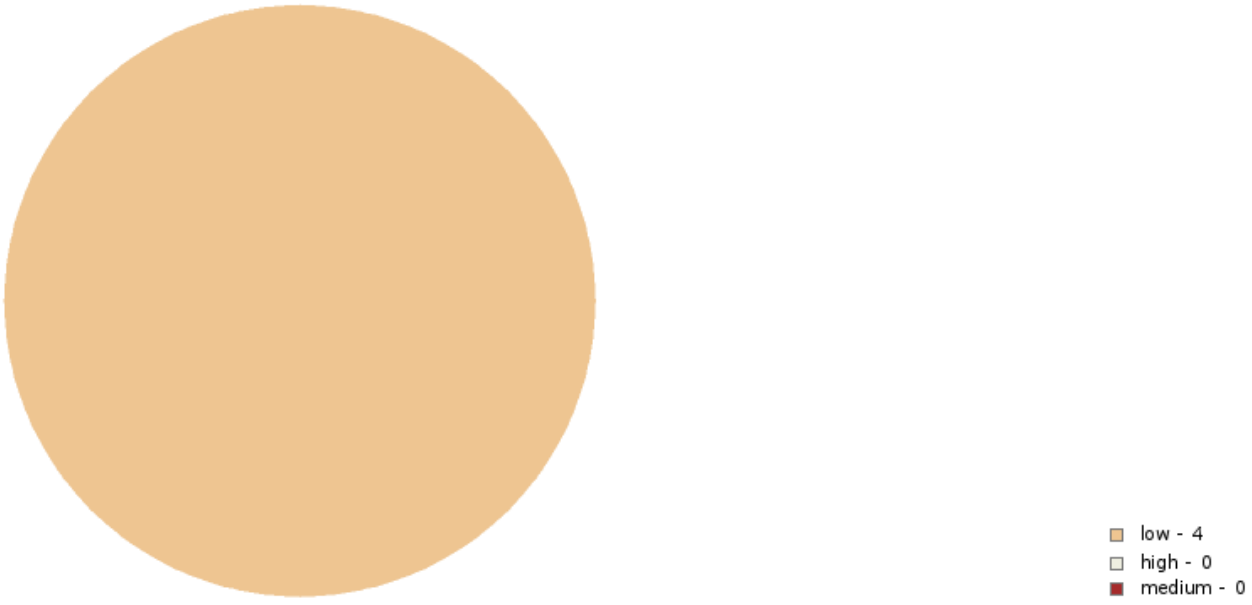
Cymulate Score

4%

Simulation Summary

Penetrated : 4 / Total Tests: 51

Penetrations by Severity

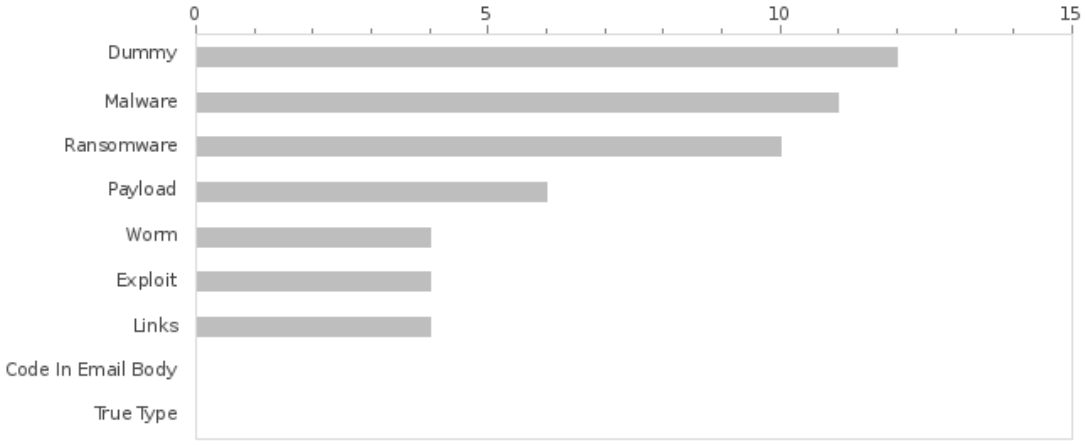


LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

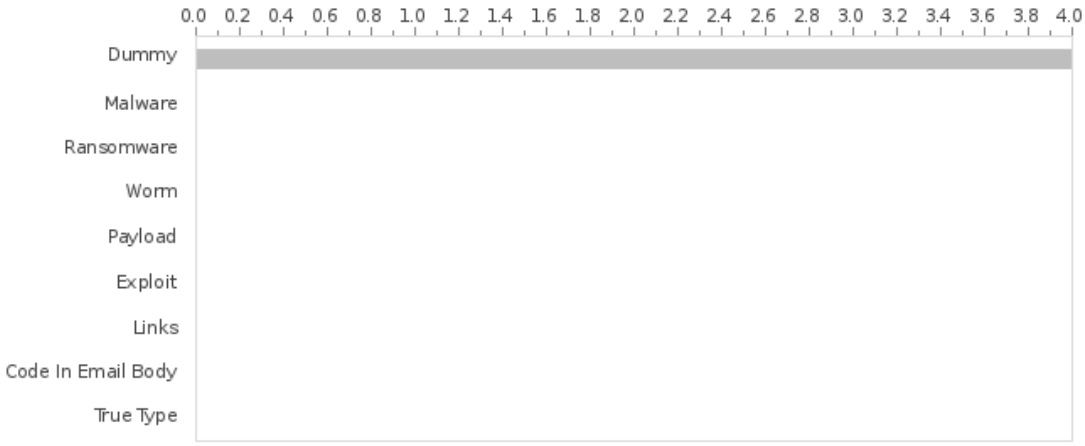
ASM-VP REPORT

GOAA 07/26/2024

Emails Sent



Emails Penetrated



Percent Penetrated

8%

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

ASM-VP REPORT

GOAA 07/26/2024

Simulations Sent/Penetrated

Category	Penetrated	Total
Dummy	4	12
Malware	0	11
Ransomware	0	10
Payload	0	6
Worm	0	4
Exploit	0	4
Links	0	4
Code In Email Body	0	0
True Type	0	0

MSS-BAS Web

Cymulate Score

37%

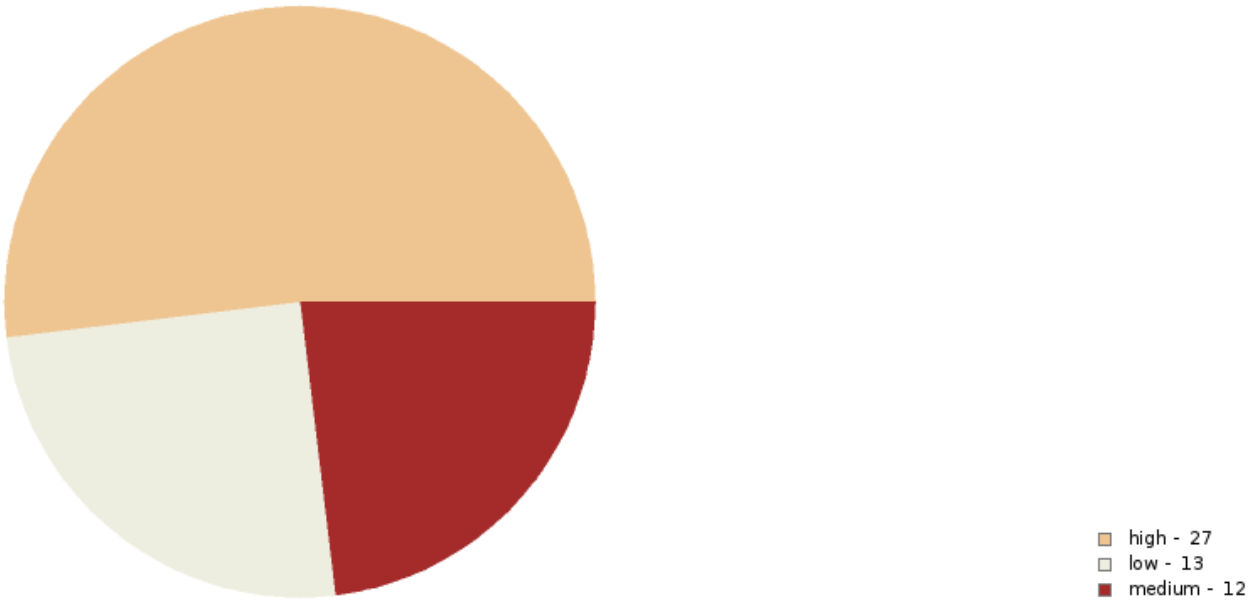
Simulation Summary

Penetrated : 52 / Total Tests: 92

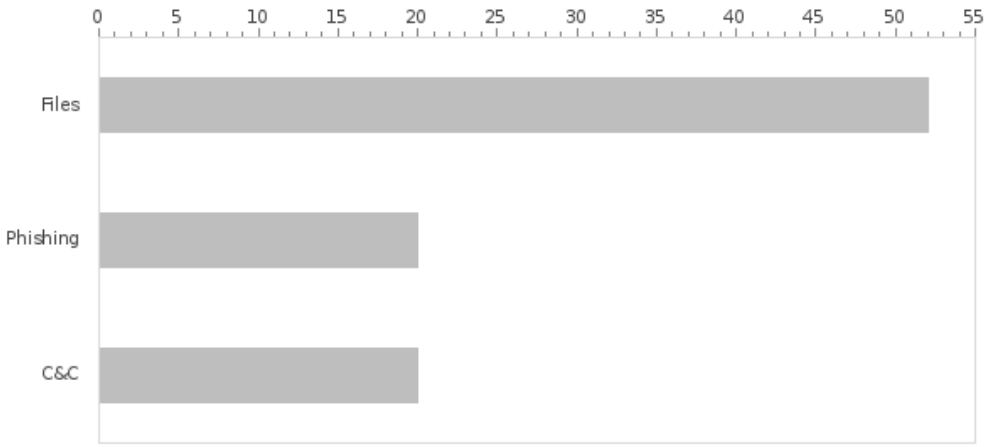
ASM-VP REPORT

GOAA 07/26/2024

Penetrations by Severity



Browsing Sent



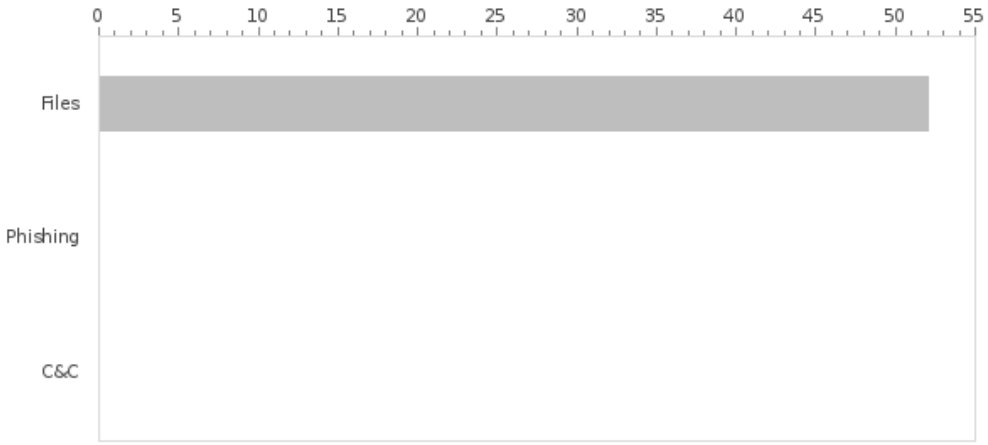
LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

TLP:AMBER

ASM-VP REPORT

GOAA 07/26/2024

Browsing Penetrated



Percent Penetrated

57%

Simulations Sent/Penetrated

Category	Penetrated	Total
Files	52	52
Phishing	0	20
C&C	0	20

LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

Security Validation

MSS-BAS EDR

cymulate score

13%

Simulation Summary

Penetrated : 0 / Sent : 27

Ransomware based code execution

Penetrated : 0 / Total Tests: 27

Malware based execution

Not detected : 0 / Total: 0

Trojan based code execution

penetrated : 0 / Total tests : 0

Ransomware Scenarios blocked

100%

Malware Signatures blocked

100%

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

ASM-VP REPORT

GOAA 07/26/2024

Trojan Scenarios blocked

100%

Worm based code execution

penetrated : 0 / Total tests : 0

Worm Scenarios blocked

100%

Percent Penetrated

0%

Simulations Sent/Penetrated

Category	Penetrated	Total
Ransomware	0	27
Worm	0	0
Trojan	0	0
Antivirus	0	0

MSS-BAS IMTHREAT

Cymulate Score

41%

Percent Penetrated

41%

TLP:AMBER

ASM-VP REPORT

GOAA 07/26/2024

Simulation Summary

Penetrated: 227 / Total: 558

Immediate Threats Campaigns

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2024-07-22	HotPage Story of a signed vulnerable ad-injecting driver	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/hotpage_story_of_a_signed_vulnerable_ad-injecting_driver_2068524e-376a-4591-aa66-b649b6e769d7/453821429c83c661164fbaf121f5c8fac849fbdec0d6_browsing760b8e46b668b5d86885XxX1Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240722%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240722T115110Z&X-Amz-Expires=600&X-Amz-Signature=7aaa7224fee2f73890784ab9aed56f79b6d051fb99ee99801d3f1d1752492948&X-Amz-SignedHeaders=host& x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-22	Cert IL Alert - Phishing Campaign Following CrowdStrike Glitch	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/phishing_campaign_following_crowdstrike_glitch_0174b26d-922f-44c0-b845-9da3b286a856/4491901eff338ab52c85a_browsing77a3fbd3ce80fda738046ee3b7da7be468da5b331a3XxX2Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240722%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240722T110409Z&X-Amz-Expires=600&X-Amz-Signature=66582220ec81e405f26e740d9536a6b8abe272661020bc112d68b3332acd0661&X-Amz-SignedHeaders=host&x-id=GetOb ject	Web Gateway	IT55	Penetrated
2024-07-22	Cert IL Alert - Phishing Campaign Following CrowdStrike Glitch	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/phishing_campaign_following_crowdstrike_glitch_0174b26d-922f-44c0-b845-9da3b286a856/96dec6e0_browsing7229201a02f538310815c695cf6147c548ff1c6a0def2fe38f3dcbc8XxX1Zi p.zip?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-A mz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240722%2Feu-west-1%2Fs3%2Faws4_request&X- Amz-Date=20240722T110404Z&X-Amz-Expires=600&X-Amz-Signature=bd0e1beecbbe7bdc09bc4120d27c923e63bd1cf122b22bb263b170498ac8fc5c&X-Amz-SignedHeaders=host&x-id=GetOb ject	Web Gateway	IT55	Penetrated
2024-07-22	Likely eCrime Actor Uses Filenames Capitalizing on 19 July 2,024 Falcon Sensor Content Issues in Operation Targeting LATAM-Based CrowdStrike Customers	c44506fe6e1ede5a104008_edr755abf5b6ace51f1a84ad656a2dccc7f2c39c0eca2XxX1Zip.zip	Endpoint Security	IT55	Prevented
2024-07-22	Likely eCrime Actor Uses Filenames Capitalizing on 19 July 2,024 Falcon Sensor Content Issues in Operation Targeting LATAM-Based CrowdStrike Customers	931,308cfe_edr733376e19d6cd2401e27f8b2945cec0b9c696aebe7029ea76d45bf6XxX9Unkn.unkn	Endpoint Security	IT55	Prevented
2024-07-22	Likely eCrime Actor Uses Filenames Capitalizing on 19 July 2,024 Falcon Sensor Content Issues in Operation Targeting LATAM-Based CrowdStrike Customers	hxxp://213.5.130.58	Web Gateway	IT55	Offline/Removed
2024-07-22	Likely eCrime Actor Uses Filenames Capitalizing on 19 July 2,024 Falcon Sensor Content Issues in Operation Targeting LATAM-Based CrowdStrike Customers	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/likely_ecrime_actor_uses_filenames_capitalizing_on_19_july_2024_falcon_sensor_content_issues_in_operation_targeting_latam-based_crowdstrike_customers_816acce3-f9fd -4b09-8d86-d0aaf3edc2e5/d6d5ff8e9dc6d2b195a6_browsing715280c2f1ba471048a7ce68d256040672b801fda0eaXxX13Dll.dll?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240722%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240722T083712Z&X-Amz-Expires=600&X-Amz-Signature=a38ceaddc31b664cac1f33876abaa90a5409066a7a46dc56b85862a98db62d53&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated

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

TLP:AMBER

ASM-VP REPORT

GOAA 07/26/2024

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
N/A	Likely eCrime Actor Uses Filenames Capitalizing on 19 July 2,024 Falcon Sensor Content Issues in Operation Targeting LATAM-Based CrowdStrike Customers	c44506fe6e1ede5a104008_mail755abf5b6ace51f1a84ad656a2dccc7f2c39c0eca2XxX1Zip.zip	Email Gateway	skywatch@goaa.org	Prevented
2024-07-21	CVE-2024-38112 Void Banshee Targets Windows Users Through Zombie Internet Explorer in Zero-Day Attacks	b3_edr71fbdce6935039218d4b4272db3521881c9cec48ef82dec1e9e0188a32d3adXxX10Url.url	Endpoint Security	IT55	Prevented
2024-07-21	CVE-2024-38112 Void Banshee Targets Windows Users Through Zombie Internet Explorer in Zero-Day Attacks	hxxp://185.172.128.95	Web Gateway	IT55	Offline/Removed
2024-07-22	HotPage Story of a signed vulnerable ad-injecting driver	453,821,429c83c661164fbaf121f5c8fac849fbdec0d6_edr760b8e46b668b5d86885XxX1Exe.exe	Endpoint Security	IT55	Prevented
2024-07-22	Cert IL Alert - Phishing Campaign Following CrowdStrike Glitch	96dec6e0_edr7229201a02f538310815c695cf6147c548ff1c6a0def2fe38f3dcbc8XxX1Zip.zip	Endpoint Security	IT55	Prevented
2024-07-22	Cert IL Alert - Phishing Campaign Following CrowdStrike Glitch	4,491,901eff338ab52c85a_edr77a3fbd3ce80fda738046ee3b7da7be468da5b331a3XxX2Exe.exe	Endpoint Security	IT55	Prevented
2024-07-22	Cert IL Alert - Phishing Campaign Following CrowdStrike Glitch	hxxp://fix-crowdstrike-apocalypse.com	Web Gateway	IT55	Offline/Removed
N/A	Cert IL Alert - Phishing Campaign Following CrowdStrike Glitch	96dec6e0_mail7229201a02f538310815c695cf6147c548ff1c6a0def2fe38f3dcbc8XxX1Zip.zip	Email Gateway	skywatch@goaa.org	Prevented
2024-07-22	Likely eCrime Actor Uses Filenames Capitalizing on 19 July 2,024 Falcon Sensor Content Issues in Operation Targeting LATAM-Based CrowdStrike Customers	d6d5ff8e9dc6d2b195a6_edr715280c2f1ba471048a7ce68d256040672b801fda0eaXxX13Dll.dll	Endpoint Security	IT55	Prevented
2024-07-22	Likely eCrime Actor Uses Filenames Capitalizing on 19 July 2,024 Falcon Sensor Content Issues in Operation Targeting LATAM-Based CrowdStrike Customers	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/likely_ecrime_actor_uses_filenames_capitalizing_on_19_july_2024_falcon_sensor_content_issues_in_operation_targeting_latam-based_crowdstrike_customers_816acce3-f9fd-4b09-8d86-d0aaf3edc2e5/931308cfe_browsing733376e19d6cd2401e27f8b2945cec0b9c696aebe7029ea76d45bf6XxX9Unkn.unkn?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240722%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240722T083711Z&X-Amz-Expires=600&X-Amz-Signature=d9525bae0c67104d02fd6b4869798a69c504f92db5514ed3e4660b2845d0dc02&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated

TLP:AMBER

ASM-VP REPORT

GOAA 07/26/2024

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2024-07-22	Likely eCrime Actor Uses Filenames Capitalizing on 19 July 2,024 Falcon Sensor Content Issues in Operation Targeting LATAM-Based CrowdStrike Customers	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/likely_ecrime_actor_uses_filenames_capitalizing_on_19_july_2024_falcon_sensor_content_issues_in_operation_targeting_latam-based_crowdstrike_customers_816acce3-f9fd -4b09-8d86-d0aaf3edc2e5/c44506fe6e1ede5a104008_browsing755abf5b6ace51f1a84ad656a2dccc7f2c39c0eca2XxX1Zip.zip?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240722%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240722T083708Z&X-Amz-Expires=600&X-Amz-Signature=fea7d681796c5c731c99006f2b7eba8802e810d66d847be172e5877e18c33c41&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-21	CVE-2024-38112 Void Banshee Targets Windows Users Through Zombie Internet Explorer in Zero-Day Attacks	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/cve-2024-38112_void_banshee_targets_windows_users_through_zombie_internet_explorer_ in_zero-day_attacks_8b908601-f45f-4776-a202-eaebcf7b453e/b3_browsing71fbdce6935039218d4b4272db3521881c9cec48ef82dec1e9e0188a32d3adXxX10Url.url?X-Amz-Algorithm=A WS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240721%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240721T073538Z&X-Amz-Expires=600&X-Amz-Signature=6e2097956c30277e3f8003172225ef4c2c47e1764b2aabc7466b1d0bbeee0cad&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-21	APT41 Adds New Malware To Compromise Entities Across Multiple Sectors	c6a3a1ea84251aed908_edr702a1f2a565496d583239c5f467f5dcd0cfc5bfb1a6dbXxX52Dll.dll	Endpoint Security	IT55	Prevented
2024-07-21	APT41 Adds New Malware To Compromise Entities Across Multiple Sectors	b0890685b25c6_edr736827573e9536b2bf8c42dbaf36760fc947d461efdb6309aecXxX54Dll.dll	Endpoint Security	IT55	Penetrated
2024-07-21	APT41 Adds New Malware To Compromise Entities Across Multiple Sectors	6b3_edr7e0e0b0586769bc7b32ae3e0bc2f29e8ad2a1d3de07d50bb3e5489e2dd136XxX72Dll.dll	Endpoint Security	IT55	Penetrated
2024-07-25	UAC-0063 attacks research institutions in Ukraine HATVIBE CHERRYSPY CVE-2024-23692	93,322be0_edr785556e627d2b09832c18e39c115e6a6fbff64b1e590e1ddcf8f6a43XxX5Doc.doc	Endpoint Security	IT55	Prevented
2024-07-25	UAC-0063 attacks research institutions in Ukraine HATVIBE CHERRYSPY CVE-2024-23692	f4ada2b858c84da8b53c08ce45_edr79f8b5b5df25e0d0f17ee0b48e10c87c338d23XxX9Docx.doc x	Endpoint Security	IT55	Prevented
2024-07-25	UAC-0063 attacks research institutions in Ukraine HATVIBE CHERRYSPY CVE-2024-23692	332d9db35daa83c5ad226b9bf50e992_edr713bc6a69c9ecd52a1223b81e992bc725XxX19Hta.hta	Endpoint Security	IT55	Prevented
2024-07-25	UAC-0063 attacks research institutions in Ukraine HATVIBE CHERRYSPY CVE-2024-23692	hxxp://trust-certificate.net/tmp/379.zip	Web Gateway	IT55	Offline/Removed
2024-07-25	UAC-0063 attacks research institutions in Ukraine HATVIBE CHERRYSPY CVE-2024-23692	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/uac-0063_attacks_research_institutions_in_ukraine_hatvibe_cherryspy_cve-2024-23692_8b5a1493-32bc-456b-91be-a15124f48c76/e6daa00e095948acfc1_browsing76d71c5bf667a0403e5259653ea5ac8950aee13180ae0XxX8Docx.docx?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240725%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240725T055944Z&X-Amz-Expires=600&X-Amz-Signature=59ab7b80032dd8c5596fefe7f3360d48c156f44f49aaf21c6356fa8ed1369c fc&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-25	UAC-0063 attacks research institutions in Ukraine HATVIBE CHERRYSPY CVE-2024-23692	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/uac-0063_attacks_research_institutions_in_ukraine_hatvibe_cherryspy_cve-2024-23692_8b5a1493-32bc-456b-91be-a15124f48c76/bcdbe035001af9d2cc1_browsing73e975fa0b13b133e613b7d9b6e90df86672f9057e19bXxX7Docx.docx?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-A mz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240725%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240725T055944Z&X-Amz-Expires=600&X-Amz-Signature=b3a6998cb555ee2a1bc8ef2cb1dfb7eb018fdcae39af4585dde1f278988d3c da&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated

TLP:AMBER

GLESEC
COMPLETELY PERCEPTI

ASM-VP REPORT

GOAA 07/26/2024

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
N/A	UAC-0063 attacks research institutions in Ukraine HATVIBE CHERRYSPY CVE-2024-23692	f4ada2b858c84da8b53c08ce45_mail79f8b5b5df25e0d0f17ee0b48e10c87c338d23XxX9Docx.do cx	Email Gateway	skywatch@goaa.org	Prevented
2024-07-24	Daggerfly Espionage Group Makes Major Update to Toolset	3,894a8b82338_edr791764524fddac786a2c5025cad37175877959a06c372b96ef05XxX4Elf.elf	Endpoint Security	IT55	Prevented
2024-07-24	Daggerfly Espionage Group Makes Major Update to Toolset	eff1c0_edr78895bbb76502f1bbad12be6aa23914a4d208859d848d5f087da8e35e0XxX5Macho.ma cho	Endpoint Security	IT55	Prevented
2024-07-24	Daggerfly Espionage Group Makes Major Update to Toolset	fce66c26deff6a5b_edr7320842bc5fa8fe12db991efe6e3edc9c63ffaa3cc5b8cedXxX7Macho.ma cho	Endpoint Security	IT55	Prevented
2024-07-24	Daggerfly Espionage Group Makes Major Update to Toolset	4c3b9a568d8911a2a256fdc2ebe9ff5911a6b2b63c_edr7784da08a4daf692e93c1aXxX8Elf.elf	Endpoint Security	IT55	Prevented
2024-07-24	Daggerfly Espionage Group Makes Major Update to Toolset	5c52e41090cdd13e0bfa_edr7ec11c283f5051347ba02c9868b4fddfd9c3fc452191XxX11Dll.dll	Endpoint Security	IT55	Prevented
2024-07-24	Daggerfly Espionage Group Makes Major Update to Toolset	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/daggerfly_espionage_group_makes_major_update_to_toolset_ffdc9c71-da33-4c2c-b4de-c684b12dcded/ef9aebcd9022080189af8aa2fb0b6594c3dfdc862340f_browsing79c17fb248e51fc9929XxX34Elf.elf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240724%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240724T062924Z&X-Amz-Expires=600&X-Amz-Signature=474723e45672c492cba267fc588c6ac13cb74bb18ee67ba5ae5af855388d3f65&X-Amz-SignedHeaders=host& x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-24	Daggerfly Espionage Group Makes Major Update to Toolset	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/daggerfly_espionage_group_makes_major_update_to_toolset_ffdc9c71-da33-4c2c-b4de-c684b12dcded/dad13b0a9f5fde_browsing7bcdda3e5afa10e7d83af0ff39288b9f11a725850b1e6f6313XxX33Macho.macho?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240724%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240724T062923Z&X-Amz-Expires=600&X-Amz-Signature=fe2428dc2e9755d0410c9bd685068b610cef4e0482281e6efcb6162e5bc05107&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-24	Daggerfly Espionage Group Makes Major Update to Toolset	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/daggerfly_espionage_group_makes_major_update_to_toolset_ffdc9c71-da33-4c2c-b4de-c684b12dcded/d8a49e688f214553a_browsing7525be96cadddec224db19bae3771d14083a2c4c45f28ebXxX32Macho.macho?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240724%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240724T062923Z&X-Amz-Expires=600&X-Amz-Signature=8cd4cb47667d7b571e09e28e6abad8707dc00cd068acfbb2b4ba3247d36e0b63&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-24	Daggerfly Espionage Group Makes Major Update to Toolset	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/daggerfly_espionage_group_makes_major_update_to_toolset_ffdc9c71-da33-4c2c-b4de-c684b12dcded/5_browsing70cd76bf49cf52e0cb347a68bdcf0590b2eaece134e1b1eba7e8d66261bdbe6XxX28Macho.macho?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240724%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240724T062922Z&X-Amz-Expires=600&X-Amz-Signature=8eae117d34343aa56e487738e3af612ae2ff4ac268e49b213590f61f6a288b08&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-24	Daggerfly Espionage Group Makes Major Update to Toolset	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/daggerfly_espionage_group_makes_major_update_to_toolset_ffdc9c71-da33-4c2c-b4de-c684b12dcded/568_browsing7b32cdd5c4d1b3e928ee0792f6ec43817883721f9b86ec8066c5ec2791595XxX27Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240724%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240724T062922Z&X-Amz-Expires=600&X-Amz-Signature=21c9c23a3334966588089ee362ea990856b1a7117b4b58a9d6b57a0349d73a89&X-Amz-SignedHeaders=host& x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-24	Daggerfly Espionage Group Makes Major Update to Toolset	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/daggerfly_espionage_group_makes_major_update_to_toolset_ffdc9c71-da33-4c2c-b4de-c684b12dcded/490_browsing79ea789e75736f8f8fad804da4a99db52cbaca21e1d2b6d6e1ea4db56faadXxX25Dll.dll?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240724%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240724T062921Z&X-Amz-Expires=600&X-Amz-Signature=fc6a4b763205a98ac655587c631e974108bb0e6e8017617c6a1b36a020cc3aa1&X-Amz-SignedHeaders=host& x-id=GetObject	Web Gateway	IT55	Penetrated

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

TLP:AMBER

GLESEC
COMPLETELY PERCEPTI

ASM-VP REPORT

GOAA 07/26/2024

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2024-07-24	Daggerfly Espionage Group Makes Major Update to Toolset	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/daggerfly_espionage_group_makes_major_update_to_toolset_ffdc9c71-da33-4c2c-b4de-c684b12dcded/1f5e4d2f_browsing71478518fe76b0efbb75609d3fb6cab06d1b021d6aa30db424f84a5eXxX22Macho.macho?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240724%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240724T062915Z&X-Amz-Expires=600&X-Amz-Signature=d837b20fe4265b7e8b74d1ed9ba426b81a4a47d42a8ef4d6aa690fa69089f52e&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-24	Daggerfly Espionage Group Makes Major Update to Toolset	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/daggerfly_espionage_group_makes_major_update_to_toolset_ffdc9c71-da33-4c2c-b4de-c684b12dcded/003_browsing764fd74bf13cff9bf1ddd870cbf593b23e2b584ba4465114023870ea6fbefXxX20Macho.macho?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240724%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240724T062914Z&X-Amz-Expires=600&X-Amz-Signature=5273b6797dfa97b9959725864423eab13716686ef5f3df444ea5dc286dad584e&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-24	Daggerfly Espionage Group Makes Major Update to Toolset	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/daggerfly_espionage_group_makes_major_update_to_toolset_ffdc9c71-da33-4c2c-b4de-c684b12dcded/0cabb6_browsing780b804d4ee285b0ddb00b02468f91b218bd2db2e2310c90471f7f8e74XxX10Elf.elf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240724%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240724T062913Z&X-Amz-Expires=600&X-Amz-Signature=ecc41d89ec4ed6cfa8d994c489474c9d1797f84680d03a3a8160699c22ba2fa7&X-Amz-SignedHeaders=host& x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-24	Daggerfly Espionage Group Makes Major Update to Toolset	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/daggerfly_espionage_group_makes_major_update_to_toolset_ffdc9c71-da33-4c2c-b4de-c684b12dcded/3a6605266184d96_browsing7ab4643af2c73dafb8b7724d21c7aa69e58d78b84ebc06612XxX9Elf.elf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240724%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240724T062912Z&X-Amz-Expires=600&X-Amz-Signature=0779fd8001965bcf434860b058188ce90035977bb54faa298439da437b72045a&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-24	Daggerfly Espionage Group Makes Major Update to Toolset	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/daggerfly_espionage_group_makes_major_update_to_toolset_ffdc9c71-da33-4c2c-b4de-c684b12dcded/65441ea5a_browsing7c0d08c1467e9154312ac9d3fdd3ca9188b4234b5944b767d135074XxX6Elf.elf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240724%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240724T062910Z&X-Amz-Expires=600&X-Amz-Signature=ed759937732196f931cbcd931f304a810593018942a16680e239eee2bca27f2b&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-23	Cert IL Alert - More MuddyWater IOCs	7,858,932c69d15fdca6f11c4_edr7169fa99cc5ac83617e28383795baad3f0a400e17XxX16Fpx.fpx	Endpoint Security	IT55	Penetrated
2024-07-23	Cert IL Alert - More MuddyWater IOCs	73c6_edr77dd3b264e7eb80e26e78ac9df1dba30915b5ce3b1bc1c83db52b9c6b30eXxX3Exe.exe	Endpoint Security	IT55	Prevented
2024-07-23	Cert IL Alert - More MuddyWater IOCs	b8_edr703744744555ad841f922995cef5dbca11da22565195d05529f5f9095fbfcaXxX11Exe.exe	Endpoint Security	IT55	Prevented
2024-07-23	Cert IL Alert - More MuddyWater IOCs	942_edr78fa01900fdbfb58d2e373895c045c69c01915edc5349cd6f3e5b7130c472XxX9Exe.exe	Endpoint Security	IT55	Prevented
2024-07-23	Cert IL Alert - More MuddyWater IOCs	3dab_edr72090588941a1f80ead3e4784fbabe526309e4cf6fa5bb23fbec69aaa2fXxX15Zip.zip	Endpoint Security	IT55	Prevented
2024-07-23	Cert IL Alert - More MuddyWater IOCs	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/cert_il_alert_-_more_muddywater_iocs__5485318d-3c54-4170-b8bf-dbcb42f24f32/99024abd1f43992698fe6d3b6fa9_browsing79c7f061ca73cc01d738440339a8bca199b5XxX13Zip.zip?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240723%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240723T103543Z&X-Amz-Expires=600&X-Amz-Signature=52e23764b37045eab00f7a484fcdfe9a18a5734dd6826693a68efc0b7e753a05&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-23	Cert IL Alert - More MuddyWater IOCs	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/cert_il_alert_-_more_muddywater_iocs__5485318d-3c54-4170-b8bf-dbcb42f24f32/8340185bcdda0ec2eb51cfabe4e3b164_browsing7a8477c31af7a56d2f1dd3ca0de99b9aXxX12Zip.zip?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240723%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240723T103543Z&X-Amz-Expires=600&X-Amz-Signature=4c5c224420622f874812f3f3be6ddec0fed56eb0699b89c7bb1626521d3c8128&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-23	Cert IL Alert - More MuddyWater IOCs	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/cert_il_alert_-_more_muddywater_iocs__5485318d-3c54-4170-b8bf-dbcb42f24f32/c884531_browsing78f5f6aaab0cab2e126b0db27b25a5cfe6905914cc430f6f100b7675cXxX10Zip.zip?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240723%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240723T103537Z&X-Amz-Expires=600&X-Amz-Signature=24fa228b03ef52b49646fe34495d84f9450b3bfaa11da4caafb369ffd434dc82&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated

LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

TLP:AMBER

GLESEC
COMPLETELY PERCEPTI

ASM-VP REPORT

GOAA 07/26/2024

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2024-07-23	Cert IL Alert - More MuddyWater IOCs	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/cer t_il_alert_-_more_muddywater_iocs__5485318d-3c54-4170-b8bf-dbcb42f24f32/c80c8dd_browsing7be3ccf18e327355b880afb5a24d5a0596939458fb13319e05c4d43e9XxX8Zip.zip?X-A mz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240723%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240723T103536Z&X-Amz-Expires=600&X-Amz-Signature=9ad7d8979d8cd82a0c2eb6900185e24668b310d2af276a9283650ffa25e37c93&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-23	Cert IL Alert - More MuddyWater IOCs	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/cer t_il_alert_-_more_muddywater_iocs__5485318d-3c54-4170-b8bf-dbcb42f24f32/3a5f_browsing7d40e51ddecfa6f081d11f8768383b32f6e65d1860d7afe4336f009614d5XxX7Pdf.pdf?X-A mz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240723%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240723T103536Z&X-Amz-Expires=600&X-Amz-Signature=227d6b1b764742b4d644ac415fb33029faa67d68cf3d4819c228d1dff165c851&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-23	Cert IL Alert - More MuddyWater IOCs	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/cer t_il_alert_-_more_muddywater_iocs__5485318d-3c54-4170-b8bf-dbcb42f24f32/960d4c9e_browsing79e751be6cad470e4f8e1d3a2b11f76f47597df8619ae41c96ba5809XxX6Exe.exe?X-A mz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240723%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240723T103536Z&X-Amz-Expires=600&X-Amz-Signature=ab68a90d0c998fbe2a87dc0cd2fbb6368642f9eae393401d2d7bdcc51ac93371&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-23	Cert IL Alert - More MuddyWater IOCs	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/cer t_il_alert_-_more_muddywater_iocs__5485318d-3c54-4170-b8bf-dbcb42f24f32/424a9c85f9_browsing7aa1aece9480bd658266c366a60ff1d62c31b87ddc15a1913c10e4XxX5Zip.zip?X-A mz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240723%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240723T103535Z&X-Amz-Expires=600&X-Amz-Signature=4a11a10076b4269df647f328413cc8a4d5b9a847ee355b1b029f5786d6c7f011&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-23	Cert IL Alert - More MuddyWater IOCs	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/cer t_il_alert_-_more_muddywater_iocs__5485318d-3c54-4170-b8bf-dbcb42f24f32/bf0b1c094_browsing73f05ea4d14640ae14dd4af5cd14f67067041bca45fb12abc3e28b3XxX4Zip.zip?X-A mz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240723%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240723T103535Z&X-Amz-Expires=600&X-Amz-Signature=842fa58628c32b2fdac3a6fd766eb3a0437b50be6052b12447e9d0836149b664&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-23	Cert IL Alert - More MuddyWater IOCs	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/cer t_il_alert_-_more_muddywater_iocs__5485318d-3c54-4170-b8bf-dbcb42f24f32/4064e4bb9a425494804_browsing7858301f2b75e276a878321b0cc02710e1738b42548caXxX2Zip.zip?X-A mz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240723%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240723T103534Z&X-Amz-Expires=600&X-Amz-Signature=26e04b73d2393493d0588f77163d35fe84e92c5e68eabe48508ca7d1ede42a4e&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
N/A	Cert IL Alert - More MuddyWater IOCs	3dab_mail72090588941a1f80ead3e4784fbabe526309e4cf6fa5bb23fbec69aaa2fXxX15Zip.zip	Email Gateway	skywatch@goaa.org	Prevented
2024-07-23	Cert IL Alert - More MuddyWater IOCs	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/cer t_il_alert_-_more_muddywater_iocs__5485318d-3c54-4170-b8bf-dbcb42f24f32/3fe2_browsing71ce6fb0bf62c1165187f71976199a98ba2b1e1ea33f3e53d9e500a3c6d2XxX1Pdf.pdf?X-A mz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240723%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240723T103533Z&X-Amz-Expires=600&X-Amz-Signature=00b3d3416620a3cf95a49c329cd20d980db2f3711b64899c5623bb1346abc8ae&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-23	WhiteSnake Stealer Delivered In A Multi-Stage Phishing Campaign	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/whitesnake_stealer_delivered_in_a_multi-stage_phishing_campaign_80382e8a-c593-48f7-b207-2a47b7fcc0be/c234ce22d4e0a606ba5af02_browsing7d6af8b42ee5c2497f7399d7ea682237ce12ada76XxX3Bat.bat?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240723%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240723T052300Z&X-Amz-Expires=600&X-Amz-Signature=4e63ccde112be3e4de797dfaf6559ce59fd6426f0b663aef515c7718639bcb1d&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-25	UAC-0063 attacks research institutions in Ukraine HATVIBE CHERRYSPY CVE-2024-23692	e6daa00e095948acfc1_edr76d71c5bf667a0403e5259653ea5ac8950aee13180ae0XxX8Docx.doc x	Endpoint Security	IT55	Prevented
2024-07-25	UAC-0063 attacks research institutions in Ukraine HATVIBE CHERRYSPY CVE-2024-23692	bcdbe035001af9d2cc1_edr73e975fa0b13b133e613b7d9b6e90df86672f9057e19bXxX7Docx.doc x	Endpoint Security	IT55	Prevented
2024-07-25	UAC-0063 attacks research institutions in Ukraine HATVIBE CHERRYSPY CVE-2024-23692	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/uac-0063_attacks_research_institutions_in_ukraine_hatvibe_cherryspy_cve-2024-23692_8b5a1493-32bc-456b-91be-a15124f48c76/332d9db35daa83c5ad226b9bf50e992_browsing713bc6a69c9ecd52a1223b81e992bc725XxX19Hta.hta?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240725%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240725T055948Z&X-Amz-Expires=600 &X-Amz-Signature=eff4df4661a96368125f2101e450a755a9dc391b5436c199749a2c9f9cf29d0 5&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated

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

ASM-VP REPORT

GOAA 07/26/2024

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2024-07-25	UAC-0063 attacks research institutions in Ukraine HATVIBE CHERRYSPY CVE-2024-23692	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/uac-0063_attacks_research_institutions_in_ukraine_hatvibe_cherryspy_cve-2024-23692_8b5a1493-32bc-456b-91be-a15124f48c76/f4ada2b858c84da8b53c08ce45_browsing79f8b5b5df25e0d0f17ee0b48e10c87c338d23XxX9Docx.docx?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-A mz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240725%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240725T055947Z&X-Amz-Expires=600&X-Amz-Signature=a26a65516601f963d15c936ebf8a313213a5f364e5256dafba78b9eaa4370dae&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
N/A	UAC-0063 attacks research institutions in Ukraine HATVIBE CHERRYSPY CVE-2024-23692	bcdbe035001af9d2cc1_mail73e975fa0b13b133e613b7d9b6e90df86672f9057e19bXxX7Docx.do cx	Email Gateway	skywatch@goaa.org	Prevented
N/A	UAC-0063 attacks research institutions in Ukraine HATVIBE CHERRYSPY CVE-2024-23692	e6daa00e095948acfc1_mail76d71c5bf667a0403e5259653ea5ac8950aee13180ae0XxX8Docx.do cx	Email Gateway	skywatch@goaa.org	Prevented
2024-07-25	UAC-0063 attacks research institutions in Ukraine HATVIBE CHERRYSPY CVE-2024-23692	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/uac-0063_attacks_research_institutions_in_ukraine_hatvibe_cherryspy_cve-2024-23692_8b5a1493-32bc-456b-91be-a15124f48c76/93322be0_browsing785556e627d2b09832c18e39c115e6a6fbff64b1e590e1ddcf8f6a43XxX5Doc.doc?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz -Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240725%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240725T055943Z&X-Amz-Expires=600& X-Amz-Signature=9273ee4b018629da4d270ac332a2b408f257cdf853708859000adbbb60e87d3d &X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-24	Daggerfly Espionage Group Makes Major Update to Toolset	65,441ea5a_edr7c0d08c1467e9154312ac9d3fdd3ca9188b4234b5944b767d135074XxX6Elf.elf	Endpoint Security	IT55	Prevented
2024-07-24	Daggerfly Espionage Group Makes Major Update to Toolset	3a6605266184d96_edr7ab4643af2c73dafb8b7724d21c7aa69e58d78b84ebc06612XxX9Elf.elf	Endpoint Security	IT55	Prevented
2024-07-24	Daggerfly Espionage Group Makes Major Update to Toolset	568_edr7b32cdd5c4d1b3e928ee0792f6ec43817883721f9b86ec8066c5ec2791595XxX27Exe.exe	Endpoint Security	IT55	Prevented
2024-07-24	Daggerfly Espionage Group Makes Major Update to Toolset	0cabb6_edr780b804d4ee285b0ddb00b02468f91b218bd2db2e2310c90471f7f8e74XxX10Elf.elf	Endpoint Security	IT55	Prevented
2024-07-24	Daggerfly Espionage Group Makes Major Update to Toolset	490_edr79ea789e75736f8f8fad804da4a99db52cbaca21e1d2b6d6e1ea4db56faadXxX25Dll.dll	Endpoint Security	IT55	Prevented
2024-07-24	Daggerfly Espionage Group Makes Major Update to Toolset	ef9aebcd9022080189af8aa2fb0b6594c3dfdc862340f_edr79c17fb248e51fc9929XxX34Elf.elf	Endpoint Security	IT55	Prevented
2024-07-24	Daggerfly Espionage Group Makes Major Update to Toolset	1f5e4d2f_edr71478518fe76b0efbb75609d3fb6cab06d1b021d6aa30db424f84a5eXxX22Macho.macho	Endpoint Security	IT55	Prevented
2024-07-24	Daggerfly Espionage Group Makes Major Update to Toolset	3_edr764fd74bf13cff9bf1ddd870cbf593b23e2b584ba4465114023870ea6fbefXxX20Macho.macho	Endpoint Security	IT55	Prevented
2024-07-24	Daggerfly Espionage Group Makes Major Update to Toolset	5_edr70cd76bf49cf52e0cb347a68bdcf0590b2eaece134e1b1eba7e8d66261bdbe6XxX28Macho.macho	Endpoint Security	IT55	Prevented
2024-07-24	Daggerfly Espionage Group Makes Major Update to Toolset	dad13b0a9f5fde_edr7bcdda3e5afa10e7d83af0ff39288b9f11a725850b1e6f6313XxX33Macho.m acho	Endpoint Security	IT55	Prevented

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

TLP:AMBER

GLESEC
COMPLETELY PERCEPTI

ASM-VP REPORT

GOAA 07/26/2024

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2024-07-24	Daggerfly Espionage Group Makes Major Update to Toolset	d8a49e688f214553a_edr7525be96cadddec224db19bae3771d14083a2c4c45f28ebXxX32Macho.macho	Endpoint Security	IT55	Prevented
2024-07-24	Daggerfly Espionage Group Makes Major Update to Toolset	hxxp://103.96.131.150	Web Gateway	IT55	Offline/Removed
2024-07-24	Daggerfly Espionage Group Makes Major Update to Toolset	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/daggerfly_espionage_group_makes_major_update_to_toolset_ffdc9c71-da33-4c2c-b4de-c684b12dcded/5c52e41090cdd13e0bfa_browsing7ec11c283f5051347ba02c9868b4fddfd9c3fc452191XxX11Dll.dll?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240724%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240724T062913Z&X-Amz-Expires=600&X-Amz-Signature=eb80fa6fcc9ab9c2d8ef24a778ffa19e47f82bb67bcd1f3e580c28ee8145e663&X-Amz-SignedHeaders=host& x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-24	Daggerfly Espionage Group Makes Major Update to Toolset	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/daggerfly_espionage_group_makes_major_update_to_toolset_ffdc9c71-da33-4c2c-b4de-c684b12dcded/4c3b9a568d8911a2a256fdc2ebe9ff5911a6b2b63c_browsing7784da08a4daf692e93c1aXxX8Elf.elf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240724%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240724T062912Z&X-Amz-Expires=600&X-Amz-Signature=517ccedaf9ed206a7f1ec668848681070ae9bf7d805239fbf3442b931917d760&X-Amz-SignedHeaders=host&x -id=GetObject	Web Gateway	IT55	Penetrated
2024-07-24	Daggerfly Espionage Group Makes Major Update to Toolset	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/daggerfly_espionage_group_makes_major_update_to_toolset_ffdc9c71-da33-4c2c-b4de-c684b12dcded/fce66c26deff6a5b_browsing7320842bc5fa8fe12db991efe6e3edc9c63ffaa3cc5b8cedXxX7Macho.macho?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240724%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240724T062911Z&X-Amz-Expires=600&X-Amz-Signature=fde45a0c2f4e4cf524fb15eb1561e316ce71cff9d0d94f8105d5535c0a0326b7&X-Amz-SignedHeaders=ho st&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-24	Daggerfly Espionage Group Makes Major Update to Toolset	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/daggerfly_espionage_group_makes_major_update_to_toolset_ffdc9c71-da33-4c2c-b4de-c684b12dcded/eff1c0_browsing78895bbb76502f1bbad12be6aa23914a4d208859d848d5f087da8e35e0XxX5Macho.macho?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240724%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240724T062910Z&X-Amz-Expires=600&X-Amz-Signature=501553c8e66adbeab77f5558f84424274d7915c5e0af03afb4554cfe2158483b&X-Amz-SignedHeaders=ho st&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-24	Daggerfly Espionage Group Makes Major Update to Toolset	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/daggerfly_espionage_group_makes_major_update_to_toolset_ffdc9c71-da33-4c2c-b4de-c684b12dcded/3894a8b82338_browsing791764524fddac786a2c5025cad37175877959a06c372b96ef05XxX4Elf.elf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240724%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240724T062908Z&X-Amz-Expires=600&X-Amz-Signature=7e15b2098b1ca6fd362239c06b305715a24bf977acbdf6133b1a237a481805fb&X-Amz-SignedHeaders=host&x -id=GetObject	Web Gateway	IT55	Penetrated
2024-07-23	Cert IL Alert - More MuddyWater IOCs	3fe2_edr71ce6fb0bf62c1165187f71976199a98ba2b1e1ea33f3e53d9e500a3c6d2XxX1Pdf.pdf	Endpoint Security	IT55	Prevented
2024-07-23	Cert IL Alert - More MuddyWater IOCs	4,064e4bb9a425494804_edr7858301f2b75e276a878321b0cc02710e1738b42548caXxX2Zip.zip	Endpoint Security	IT55	Prevented
2024-07-23	Cert IL Alert - More MuddyWater IOCs	bf0b1c094_edr73f05ea4d14640ae14dd4af5cd14f67067041bca45fb12abc3e28b3XxX4Zip.zip	Endpoint Security	IT55	Prevented
2024-07-23	Cert IL Alert - More MuddyWater IOCs	424a9c85f9_edr7aa1aece9480bd658266c366a60ff1d62c31b87ddc15a1913c10e4XxX5Zip.zip	Endpoint Security	IT55	Prevented
2024-07-23	Cert IL Alert - More MuddyWater IOCs	c80c8dd_edr7be3ccf18e327355b880afb5a24d5a0596939458fb13319e05c4d43e9XxX8Zip.zip	Endpoint Security	IT55	Prevented
2024-07-23	Cert IL Alert - More MuddyWater IOCs	960d4c9e_edr79e751be6cad470e4f8e1d3a2b11f76f47597df8619ae41c96ba5809XxX6Exe.exe	Endpoint Security	IT55	Prevented
2024-07-23	Cert IL Alert - More MuddyWater IOCs	99,024abd1f43992698fe6d3b6fa9_edr79c7f061ca73cc01d738440339a8bca199b5XxX13Zip.zip	Endpoint Security	IT55	Prevented

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

ASM-VP REPORT

GOAA 07/26/2024

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2024-07-23	Cert IL Alert - More MuddyWater IOCs	8,340,185bcdda0ec2eb51cfabe4e3b164_edr7a8477c31af7a56d2f1dd3ca0de99b9aXxX12Zip.zip	Endpoint Security	IT55	Prevented
2024-07-23	Cert IL Alert - More MuddyWater IOCs	3a5f_edr7d40e51ddecfa6f081d11f8768383b32f6e65d1860d7afe4336f009614d5XxX7Pdf.pdf	Endpoint Security	IT55	Prevented
2024-07-23	Cert IL Alert - More MuddyWater IOCs	c884531_edr78f5f6aaab0cab2e126b0db27b25a5cfe6905914cc430f6f100b7675cXxX10Zip.zip	Endpoint Security	IT55	Prevented
2024-07-23	Cert IL Alert - More MuddyWater IOCs	hxxp://smartcloudcompany.com	Web Gateway	IT55	Offline/Removed
2024-07-23	Cert IL Alert - More MuddyWater IOCs	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/cer t_il_alert_-_more_muddywater_iocs__5485318d-3c54-4170-b8bf-dbcb42f24f32/7858932c 69d15fdca6f11c4_browsing7169fa99cc5ac83617e28383795baad3f0a400e17XxX16Fpx.fpx?X- Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Crede ntial=AKIAJPJC2Q3D5GWFTK3Q%2F20240723%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date =20240723T103544Z&X-Amz-Expires=600&X-Amz-Signature=28f0f68b6a0d0acb8dc7f38e4405 64fdaf061db819671f4dc31c29d98894eee8&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-23	Cert IL Alert - More MuddyWater IOCs	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/cer t_il_alert_-_more_muddywater_iocs__5485318d-3c54-4170-b8bf-dbcb42f24f32/03dab_br owsing72090588941a1f80ead3e4784fbabe526309e4cf6fa5bb23fbec69aaa2fXxX15Zip.zip?X- Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Crede ntial=AKIAJPJC2Q3D5GWFTK3Q%2F20240723%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date =20240723T103543Z&X-Amz-Expires=600&X-Amz-Signature=5e078c27b9702cbdb2d23632fa4c 6eb5b528df7f56155540299897d858d24bbb&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-23	Cert IL Alert - More MuddyWater IOCs	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/cer t_il_alert_-_more_muddywater_iocs__5485318d-3c54-4170-b8bf-dbcb42f24f32/b8_brows ing703744744555ad841f922995cef5dbca11da22565195d05529f5f9095fbfcaXxX11Exe.exe?X- Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Crede ntial=AKIAJPJC2Q3D5GWFTK3Q%2F20240723%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date =20240723T103543Z&X-Amz-Expires=600&X-Amz-Signature=ea1d7dc9e55091fc5a886cef789e 31d02bbaa38cb850c4939826c18ff69bb09d&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-23	Cert IL Alert - More MuddyWater IOCs	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/cer t_il_alert_-_more_muddywater_iocs__5485318d-3c54-4170-b8bf-dbcb42f24f32/942_brow sing78fa01900fdbfb58d2e373895c045c69c01915edc5349cd6f3e5b7130c472XxX9Exe.exe?X-A mz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Creden tial=AKIAJPJC2Q3D5GWFTK3Q%2F20240723%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date= 20240723T103536Z&X-Amz-Expires=600&X-Amz-Signature=c501f896ee8eb196a2c0f1bd74eb3 5aa1fe003f49c08e8734d9335ccc3ff020c&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-23	Cert IL Alert - More MuddyWater IOCs	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/cer t_il_alert_-_more_muddywater_iocs__5485318d-3c54-4170-b8bf-dbcb42f24f32/73c6_bro wsing77dd3b264e7eb80e26e78ac9df1dba30915b5ce3b1bc1c83db52b9c6b30eXxX3Exe.exe?X-A mz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Creden tial=AKIAJPJC2Q3D5GWFTK3Q%2F20240723%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date= 20240723T103534Z&X-Amz-Expires=600&X-Amz-Signature=6991ae14c98221c63678f326ee2e3 98ba2c3d95d2e881c4b89e4f593f9ddb5f1&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
N/A	Cert IL Alert - More MuddyWater IOCs	3fe2_mail71ce6fb0bf62c1165187f71976199a98ba2b1e1ea33f3e53d9e500a3c6d2XxX1Pdf.pdf	Email Gateway	skywatch@goaa.org	Prevented
N/A	Cert IL Alert - More MuddyWater IOCs	4,064e4bb9a425494804_mail7858301f2b75e276a878321b0cc02710e1738b42548caXxX2Zip.zip	Email Gateway	skywatch@goaa.org	Prevented
N/A	Cert IL Alert - More MuddyWater IOCs	bf0b1c094_mail73f05ea4d14640ae14dd4af5cd14f67067041bca45fb12abc3e28b3XxX4Zip.zip	Email Gateway	skywatch@goaa.org	Prevented
N/A	Cert IL Alert - More MuddyWater IOCs	424a9c85f9_mail7aa1aece9480bd658266c366a60ff1d62c31b87ddc15a1913c10e4XxX5Zip.zip	Email Gateway	skywatch@goaa.org	Prevented
N/A	Cert IL Alert - More MuddyWater IOCs	3a5f_mail7d40e51ddecfa6f081d11f8768383b32f6e65d1860d7afe4336f009614d5XxX7Pdf.pdf	Email Gateway	skywatch@goaa.org	Prevented
N/A	Cert IL Alert - More MuddyWater IOCs	c80c8dd_mail7be3ccf18e327355b880afb5a24d5a0596939458fb13319e05c4d43e9XxX8Zip.zip	Email Gateway	skywatch@goaa.org	Prevented
N/A	Cert IL Alert - More MuddyWater IOCs	c884531_mail78f5f6aaab0cab2e126b0db27b25a5cfe6905914cc430f6f100b7675cXxX10Zip.zi p	Email Gateway	skywatch@goaa.org	Prevented

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

TLP:AMBER

GLESEC
COMPLETELY PERCEPTI

ASM-VP REPORT

GOAA 07/26/2024

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
N/A	Cert IL Alert - More MuddyWater IOCs	8,340,185bcdda0ec2eb51cfabe4e3b164_mail7a8477c31af7a56d2f1dd3ca0de99b9aXxX12Zip.zip	Email Gateway	skywatch@goaa.org	Prevented
N/A	Cert IL Alert - More MuddyWater IOCs	99,024abd1f43992698fe6d3b6fa9_mail79c7f061ca73cc01d738440339a8bca199b5XxX13Zip.zip	Email Gateway	skywatch@goaa.org	Prevented
2024-07-23	WhiteSnake Stealer Delivered In A Multi-Stage Phishing Campaign	c234ce22d4e0a606ba5af02_edr7d6af8b42ee5c2497f7399d7ea682237ce12ada76XxX3Bat.bat	Endpoint Security	IT55	Prevented
2024-07-21	APT41 Adds New Malware To Compromise Entities Across Multiple Sectors	c_edr7dce6c950735bfcf2125be8eb1f3dd468eeb56a1c615c34f95bf38cb58b7d3aXxX56Dll.dll	Endpoint Security	IT55	Prevented
2024-07-21	APT41 Adds New Malware To Compromise Entities Across Multiple Sectors	840_edr7defe0cc29d04b8d0f519b5008d30c09783fe0c63aad5ccb0950fc9a98406XxX76Dll.dll	Endpoint Security	IT55	Prevented
2024-07-21	APT41 Adds New Malware To Compromise Entities Across Multiple Sectors	c3efcb6efad6_edr75613721910a783389a646b2d138c7721df9849b28952d25bcfcXxX78Dll.dll	Endpoint Security	IT55	Prevented
2024-07-21	APT41 Adds New Malware To Compromise Entities Across Multiple Sectors	22a50cea6ad6_edr7a7e8582d2cd4cdc3eaaf57c0fbe8cd062a9b15710166e255a86XxX66Dll.dll	Endpoint Security	IT55	Prevented
2024-07-21	APT41 Adds New Malware To Compromise Entities Across Multiple Sectors	33fd050_edr760e251ab932e5ca4311b494ef72cee157b20537ce773420845302e49XxX74Dll.dll	Endpoint Security	IT55	Prevented
2024-07-21	APT41 Adds New Malware To Compromise Entities Across Multiple Sectors	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/apt41_adds_new_malware_to_compromise_entities_across_multiple_sectors_c50e649f-b6b8-4aac-932c-d0161e9e1fd7/6b3_browsing7e0e0b0586769bc7b32ae3e0bc2f29e8ad2a1d3de07d50bb3e5489e2dd136XxX72Dll.dll?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240721%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240721T073220Z&X-Amz-Expires=600&X-Amz-Signature=1988393901cd11e1d3c364657418354e5ed69eb2892fa96a18ce7a838ed98470&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-21	APT41 Adds New Malware To Compromise Entities Across Multiple Sectors	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/apt41_adds_new_malware_to_compromise_entities_across_multiple_sectors_c50e649f-b6b8-4aac-932c-d0161e9e1fd7/7586e58a569c2a0_browsing7d0b3a710616f48833a040bf3fc57628bbdec7fcb462d565aXxX70Dll.dll?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240721%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240721T073220Z&X-Amz-Expires=600&X-Amz-Signature=bd09c1bc5fc734f547e760c3c1dfd1d518c6169aa072be97c60498e86976a8fc&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-21	APT41 Adds New Malware To Compromise Entities Across Multiple Sectors	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/apt41_adds_new_malware_to_compromise_entities_across_multiple_sectors_c50e649f-b6b8-4aac-932c-d0161e9e1fd7/cdc619_browsing734f4e2aba0137b5fe9faf36896b85dff7cd4a93de562de770777d181aXxX68Dll.dll?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240721%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240721T073220Z&X-Amz-Expires=600&X-Amz-Signature=f1d23715c8d89301c2932ab9333b7f5b62c40fb2b0fea704e69e6b2a24e5db78&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-21	APT41 Adds New Malware To Compromise Entities Across Multiple Sectors	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/apt41_adds_new_malware_to_compromise_entities_across_multiple_sectors_c50e649f-b6b8-4aac-932c-d0161e9e1fd7/e5c_browsing7089eb3297b204aaabdb4a660d125a948ba869d2a7cf3cf7c0098125b5ef5XxX62Dll.dll?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240721%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240721T073219Z&X-Amz-Expires=600&X-Amz-Signature=1bfd0ac8765e6830986103cf26586adaf8b71213fa148a36236352036b07061d&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-21	APT41 Adds New Malware To Compromise Entities Across Multiple Sectors	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/apt41_adds_new_malware_to_compromise_entities_across_multiple_sectors_c50e649f-b6b8-4aac-932c-d0161e9e1fd7/bd058a6fd2034_browsing7f21c38115490aef858d06f26b49b9d7be357297e60bd2934ccXxX60Dll.dll?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240721%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240721T073219Z&X-Amz-Expires=600&X-Amz-Signature=f88e2e16a4e8afa54ec9360585d0fe1f9da723ab58ee408df6bd581a030764ec&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated

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

TLP:AMBER

GLESEC
COMPLETELY PERCEPTI

ASM-VP REPORT

GOAA 07/26/2024

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2024-07-21	APT41 Adds New Malware To Compromise Entities Across Multiple Sectors	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/apt41_adds_new_malware_to_compromise_entities_across_multiple_sectors_c50e649f-b6b8-4aac-932c-d0161e9e1fd7/069ca8ae8a3909aa4_browsing717832d911d646c536fed4c9078667 24f74daf4d740f41aXxX58Dll.dll?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240721%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240721T073218Z&X-Amz-Expires=600&X-Amz-Signature=995c0ce9de4a4d670d5a181156268330a189d5d9b40d5bdcce80f59a7f9d4f45&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-21	APT41 Adds New Malware To Compromise Entities Across Multiple Sectors	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/apt41_adds_new_malware_to_compromise_entities_across_multiple_sectors_c50e649f-b6b8-4aac-932c-d0161e9e1fd7/b0890685b25c6_browsing736827573e9536b2bf8c42dbaf36760fc9 47d461efdb6309aecXxX54Dll.dll?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240721%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240721T073218Z&X-Amz-Expires=600&X-Amz-Signature=195b4c59926431f2edf91ec1e8e8ea9c9e7e6587f36a2cea3ca42fcb28967006&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-21	APT41 Adds New Malware To Compromise Entities Across Multiple Sectors	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/apt41_adds_new_malware_to_compromise_entities_across_multiple_sectors_c50e649f-b6b8-4aac-932c-d0161e9e1fd7/c6a3a1ea84251aed908_browsing702a1f2a565496d583239c5f467f 5dcd0cfc5bfb1a6dbXxX52Dll.dll?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240721%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240721T073217Z&X-Amz-Expires=600&X-Amz-Signature=1c5a4953e5638dc05ff7fe5179a0922b4ec51949cf29a0a40e924c27ba3fc764&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-18	US Cert Alert - Peoples Republic of China PRC Ministry of State Security APT40 Tradecraft in Action	9_edr7daa26c59e0e151f66872147ccd30dd1815bc6e63ec40c288130c6e8a6ea992XxX177Js.js	Endpoint Security	IT55	Prevented
2024-07-18	US Cert Alert - Peoples Republic of China PRC Ministry of State Security APT40 Tradecraft in Action	7c_edr7acd87b47d405da4d6efa2c43599148e12c094970ba198905f0a165d79a78fXxX181Js.js	Endpoint Security	IT55	Prevented
2024-07-18	US Cert Alert - Peoples Republic of China PRC Ministry of State Security APT40 Tradecraft in Action	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/peoples_republic_of_china_prc_ministry_of_state_security_apt40_tradecraft_in_action _9c5c1ae1-be27-41b4-802a-65087a628f32/b2_browsing71e74ed44c3c405da858f29b6dfd4a9 9658dcac7bc83938079ad0dbbdf1b66XxX176Java.java?X-Amz-Algorithm=AWS4-HMAC-SHA256& X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240718%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240718T072147Z&X-Amz-Expires=600&X-Amz-Signature=c1f29889307719f767677b1d0d17cdd98a92bc3c558ba57f320980c107c27fd7&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-18	US Cert Alert - Peoples Republic of China PRC Ministry of State Security APT40 Tradecraft in Action	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/peoples_republic_of_china_prc_ministry_of_state_security_apt40_tradecraft_in_action _9c5c1ae1-be27-41b4-802a-65087a628f32/44369_browsing783a819a38909e89449495fb98c3 f9ba07dd0d2fa55a24a560a89f21a86XxX175Txt.txt?X-Amz-Algorithm=AWS4-HMAC-SHA256&X- Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240718%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240718T072147Z&X-Amz-Expires=600&X-Amz-Signature=eba971fa198b554f8c8f247b8268380c52f64eb97820191c70507edf7dce27e4&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-18	Cert IL Alert - active phishing campaign in Israel	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/cer t_il_alert_-_active_phishing_campaign_in_israel_5e7463a2-b2bc-4457-aa39-264a3c2b dfee/f39c6_browsing7cc82d5766d776ad787c56d48627995cbf3797d7603b790f27cd31cb413XxX1Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240718%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240718T070934Z&X-Amz-Expires=600&X-Amz-Signature=1465425f147add79dc139c808490ad3cf60f84283f67720f61ce9508edbed70c&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-17	BianLian Ransomware Group Continues To Adapt	f9421165e4a62c_edr7a1941b7b3fa73ac6f2149e7ffab3a6a622406baabf1933a2eXxX27Dll.dll	Endpoint Security	IT55	Prevented
2024-07-17	BianLian Ransomware Group Continues To Adapt	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/bianlian_ransomware_group_continues_to_adapt_3fab5dff-c294-4d48-b82f-fd62461303af/834ab96263cca_browsing7b01b3ae6549a9811b56204e714402215ce37fb602732b981d1XxX25Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240717%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240717T074535Z&X-Amz-Expires=600&X-Amz-Signature=d741d327eb4e630992ee41ba4cf5f79d84dc5990510a43749ecf335b89324232&X-Amz-SignedHeaders=host&x-id=GetObj ect	Web Gateway	IT55	Penetrated
2024-07-17	BianLian Ransomware Group Continues To Adapt	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/bianlian_ransomware_group_continues_to_adapt_3fab5dff-c294-4d48-b82f-fd62461303af/b12be86af46b026_browsing7d86fcacef0a58bad0d157a7a044f89a453082b32503bd3c0XxX23Elf .elf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240717%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240717T074533Z&X-Amz-Expires=600&X-Amz-Signature=68284d21e5ed4bd7cc1077d49a6219e53d379d9146d17b6b861c041b43147b68&X-Amz-SignedHeaders=host&x-id=GetObj ect	Web Gateway	IT55	Penetrated

TLP:AMBER

ASM-VP REPORT

GOAA 07/26/2024

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2024-07-17	BianLian Ransomware Group Continues To Adapt	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/bianlian_ransomware_group_continues_to_adapt_3fab5dff-c294-4d48-b82f-fd62461303af/3b309c0_browsing76c26f27f42dbab8c89f05df51c414e87529251dc2d9946e7bc694f29XxX21Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240717%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240717T074531Z&X-Amz-Expires=600&X-Amz-Signature=ede8c637e252e52f9ab14e888b8c21928122b3e66a69d4cd3ce72c656c5f8057&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-17	BianLian Ransomware Group Continues To Adapt	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/bianlian_ransomware_group_continues_to_adapt_3fab5dff-c294-4d48-b82f-fd62461303af/72d91293ff1a9158_browsing7af3997081f65eac819d2ff73655837dc68a447d371ca2f1XxX19Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240717%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240717T074528Z&X-Amz-Expires=600&X-Amz-Signature=70f90fccdcad661233a10b9c66a215f8cf2ae96464fe8d208f65e5e7d8cb36c8&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-17	MuddyWater APT Group Releases BugSleep Backdoor Across The Middle East	ff2ae62ba88e_edr7068fa142bbe67d7b9398e8ae737a43cf36ace1fcf809776c909XxX21Msi.msi	Endpoint Security	IT55	Penetrated
2024-07-17	MuddyWater APT Group Releases BugSleep Backdoor Across The Middle East	7e6b04e1_edr7ae273700cef4dc08349af949dbd4d3418159d607529ae31285e18f7XxX23Msi.msi	Endpoint Security	IT55	Penetrated
2024-07-17	MuddyWater APT Group Releases BugSleep Backdoor Across The Middle East	39da_edr7cc7c627ea4c46f75bcec79e5669236e6b43657dcad099e1b9214527670eXxX27Msi.msi	Endpoint Security	IT55	Penetrated
2024-07-17	MuddyWater APT Group Releases BugSleep Backdoor Across The Middle East	55af6a90ac8863f2_edr7b3fcaa416a0f1e4ff02fb42aa46a7274c6b76aa000aacc2XxX29Msi.msi	Endpoint Security	IT55	Penetrated
2024-07-17	MuddyWater APT Group Releases BugSleep Backdoor Across The Middle East	5df_edr724c220aed7b4878a2a557502a5cefee736406e25ca48ca11a70608f3a1c0XxX39Exe.exe	Endpoint Security	IT55	Prevented
2024-07-17	MuddyWater APT Group Releases BugSleep Backdoor Across The Middle East	960d4c9e_edr79e751be6cad470e4f8e1d3a2b11f76f47597df8619ae41c96ba5809XxX43Exe.exe	Endpoint Security	IT55	Prevented
2024-07-17	MuddyWater APT Group Releases BugSleep Backdoor Across The Middle East	c884531_edr78f5f6aaab0cab2e126b0db27b25a5cfe6905914cc430f6f100b7675cXxX53Zip.zip	Endpoint Security	IT55	Prevented
2024-07-17	MuddyWater APT Group Releases BugSleep Backdoor Across The Middle East	4,064e4bb9a425494804_edr7858301f2b75e276a878321b0cc02710e1738b42548caXxX51Zip.zip	Endpoint Security	IT55	Prevented
2024-07-17	MuddyWater APT Group Releases BugSleep Backdoor Across The Middle East	1c094_edr7258ddb608c879333c941f0738a7f279bc14630f2c8877b82b8046acf91XxX63Zip.zip	Endpoint Security	IT55	Prevented
2024-07-17	MuddyWater APT Group Releases BugSleep Backdoor Across The Middle East	c80c8dd_edr7be3ccf18e327355b880afb5a24d5a0596939458fb13319e05c4d43e9XxX61Zip.zip	Endpoint Security	IT55	Prevented
2024-07-17	MuddyWater APT Group Releases BugSleep Backdoor Across The Middle East	8fbd3_edr74d4659efdc5b5a57ff4168236aeaab6dae4af6b92d99ac28e05f04e5c1XxX55Zip.zip	Endpoint Security	IT55	Prevented

ASM-VP REPORT

GOAA 07/26/2024

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2024-07-17	MuddyWater APT Group Releases BugSleep Backdoor Across The Middle East	424a9c85f9_edr7aa1aece9480bd658266c366a60ff1d62c31b87ddc15a1913c10e4XxX47Zip.zip	Endpoint Security	IT55	Prevented
2024-07-17	MuddyWater APT Group Releases BugSleep Backdoor Across The Middle East	7e14ca8cb_edr7980e85aff4038f489442eace33530fd02e2b9c382a4b6907601beeXxX57Zip.zip	Endpoint Security	IT55	Prevented
2024-07-17	MuddyWater APT Group Releases BugSleep Backdoor Across The Middle East	hxxp://31.171.154.54	Web Gateway	IT55	Offline/Removed
2024-07-17	MuddyWater APT Group Releases BugSleep Backdoor Across The Middle East	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/muddywater_apt_group_releases_bugsleep_backdoor_across_the_middle_east_fc26dd82-ead3-4c1e-a16a-f1243b092248/88_browsing788208316a6cf4025dbabbef703f51d77d475dc735bf826b8d4a13bbd6a3eeXxX59Zip.zip?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240717%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240717T073603Z&X-Amz-Expires=600&X-Amz-Signature=6aa54f2b0d3f9e11ab632941e5c3df475624ad285702dc2482ae4c261d64c082&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-17	MuddyWater APT Group Releases BugSleep Backdoor Across The Middle East	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/muddywater_apt_group_releases_bugsleep_backdoor_across_the_middle_east_fc26dd82-ead3-4c1e-a16a-f1243b092248/e_browsing7896ccb82ae35e1ee5949b187839faab0b51221d510b25882bbe711e57c16d2XxX49Zip.zip?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240717%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240717T073555Z&X-Amz-Expires=600&X-Amz-Signature=672fe28461325c21c4f0fa2c53c8b53d21bb3487530044b4d1e1069a9c924577&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-17	MuddyWater APT Group Releases BugSleep Backdoor Across The Middle East	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/muddywater_apt_group_releases_bugsleep_backdoor_across_the_middle_east_fc26dd82-ead3-4c1e-a16a-f1243b092248/31591fcf6_browsing77a2da2834d2cc99a00ab500918b53900318f6b19ea708eba2b38abXxX45Zip.zip?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240717%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240717T073553Z&X-Amz-Expires=600&X-Amz-Signature=23b13876deeacad123783329b29571c07cc52a645406ef6d25d6cad4dac78f88&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-17	MuddyWater APT Group Releases BugSleep Backdoor Across The Middle East	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/muddywater_apt_group_releases_bugsleep_backdoor_across_the_middle_east_fc26dd82-ead3-4c1e-a16a-f1243b092248/73c6_browsing77dd3b264e7eb80e26e78ac9df1dba30915b5ce3b1bc1c83db52b9c6b30eXxX41Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240717%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240717T073553Z&X-Amz-Expires=600&X-Amz-Signature=2bd8f79bf43fcebba48dce5ed772277dfba8b1fbd5b1705d196d909215aaa1f2&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-17	MuddyWater APT Group Releases BugSleep Backdoor Across The Middle East	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/muddywater_apt_group_releases_bugsleep_backdoor_across_the_middle_east_fc26dd82-ead3-4c1e-a16a-f1243b092248/b8_browsing703744744555ad841f922995cef5dbca11da22565195d05529f5f9095fbfcaXxX37Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240717%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240717T073547Z&X-Amz-Expires=600&X-Amz-Signature=54170cebf2cf35139af9762081a6b6e2da6e312f4ec9231517e9848006a15c78&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-17	MuddyWater APT Group Releases BugSleep Backdoor Across The Middle East	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/muddywater_apt_group_releases_bugsleep_backdoor_across_the_middle_east_fc26dd82-ead3-4c1e-a16a-f1243b092248/942_browsing78fa01900fdbfb58d2e373895c045c69c01915edc5349cd6f3e5b7130c472XxX35Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240717%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240717T073546Z&X-Amz-Expires=600&X-Amz-Signature=e2e51770d3d2d039ac77406881adb44d9a29b13920cc4e552a9d41ce11cc0566&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-17	MuddyWater APT Group Releases BugSleep Backdoor Across The Middle East	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/muddywater_apt_group_releases_bugsleep_backdoor_across_the_middle_east_fc26dd82-ead3-4c1e-a16a-f1243b092248/20aaeac4dbea89b50d011e9becdf51afc1a1a1f254a5f494b80c108fd3c_browsing7f61aXxX33Msi.msi?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240717%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240717T073545Z&X-Amz-Expires=600&X-Amz-Signature=2062a976cf60f3fc531f2f9b2204758c5838614f2e2073c357ef440e7503bbfc&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-17	MuddyWater APT Group Releases BugSleep Backdoor Across The Middle East	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/muddywater_apt_group_releases_bugsleep_backdoor_across_the_middle_east_fc26dd82-ead3-4c1e-a16a-f1243b092248/fb58c54a6d0ed24e85b213f0c48_browsing7f8df05e421d7b07bd2bece3a925a855be93aXxX31Msi.msi?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240717%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240717T073544Z&X-Amz-Expires=600&X-Amz-Signature=b7a4d1cfbe5af8ce282e0db24fc9e8f35ce6674367eb68a06a56cf6c26a4b65b&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated

ASM-VP REPORT

GOAA 07/26/2024

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2024-07-17	MuddyWater APT Group Releases BugSleep Backdoor Across The Middle East	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/mud dywater_apt_group_releases_bugsleep_backdoor_across_the_middle_east_fc26dd82-ead 3-4c1e-a16a-f1243b092248/90f94d98386c1_browsing79a1b98a1f082b0c7487b22403d8d5eb3 db6828725d14392dedXxX25Msi.msi?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sh a256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240717%2Feu-west -1%2Fs3%2Faws4_request&X-Amz-Date=20240717T073540Z&X-Amz-Expires=600&X-Amz-Signa ture=79aefb636d3d420552408260a01b51e184ea3a6287ef8a4f4eb3bd1c29c931c1&X-Amz-Sign edHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
N/A	MuddyWater APT Group Releases BugSleep Backdoor Across The Middle East	424a9c85f9_mail7aa1aece9480bd658266c366a60ff1d62c31b87ddc15a1913c10e4XxX47Zip.zip	Email Gateway	skywatch@goaa.org	Prevented
N/A	MuddyWater APT Group Releases BugSleep Backdoor Across The Middle East	4,064e4bb9a425494804_mail7858301f2b75e276a878321b0cc02710e1738b42548caXxX51Zip.zip	Email Gateway	skywatch@goaa.org	Prevented
N/A	MuddyWater APT Group Releases BugSleep Backdoor Across The Middle East	c884531_mail78f5f6aaab0cab2e126b0db27b25a5cfe6905914cc430f6f100b7675cXxX53Zip.zi p	Email Gateway	skywatch@goaa.org	Prevented
N/A	MuddyWater APT Group Releases BugSleep Backdoor Across The Middle East	8fbd3_mail74d4659efdc5b5a57ff4168236aeaab6dae4af6b92d99ac28e05f04e5c1XxX55Zip.zip	Email Gateway	skywatch@goaa.org	Prevented
N/A	MuddyWater APT Group Releases BugSleep Backdoor Across The Middle East	7e14ca8cb_mail7980e85aff4038f489442eace33530fd02e2b9c382a4b6907601beeXxX57Zip.zip	Email Gateway	skywatch@goaa.org	Prevented
N/A	MuddyWater APT Group Releases BugSleep Backdoor Across The Middle East	c80c8dd_mail7be3ccf18e327355b880afb5a24d5a0596939458fb13319e05c4d43e9XxX61Zip.zi p	Email Gateway	skywatch@goaa.org	Prevented
N/A	MuddyWater APT Group Releases BugSleep Backdoor Across The Middle East	1c094_mail7258ddb608c879333c941f0738a7f279bc14630f2c8877b82b8046acf91XxX63Zip.zip	Email Gateway	skywatch@goaa.org	Prevented
2024-07-17	MuddyWater APT Group Releases BugSleep Backdoor Across The Middle East	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/mud dywater_apt_group_releases_bugsleep_backdoor_across_the_middle_east_fc26dd82-ead 3-4c1e-a16a-f1243b092248/c23f1_browsing7b92b13464a570f737a86c0960d5106868aaa5eac 2f2bac573c3314eb0fXxX19Msi.msi?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sh a256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240717%2Feu-west -1%2Fs3%2Faws4_request&X-Amz-Date=20240717T073536Z&X-Amz-Expires=600&X-Amz-Signa ture=1b8a6d3823705cc2395daedf8c301f31a4ab044bea88ed8828ab2725753c465e&X-Amz-Sign edHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-16	More Akira-related IOCs are spotted in the wild	0b5b31af5956158bfbd14f6cbf4f1bca23c5d16a40dbf3_edr758f3289146c565f43XxX1Exe.exe	Endpoint Security	IT55	Prevented
2024-07-16	ShadowRoot Ransomware Targeting Turkish Businesses	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/sha dowroot_ransomware_targeting_turkish_businesses_bb018787-9844-4121-acab-179bd5f2 61a2/1be40e8ac11d6da8045bd03be3e5_browsing7f0b36b6ab7dc390ff7208a0a4e7688b6b94Xx X43Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOA D&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240716%2Feu-west-1%2Fs3%2Faws4_reque st&X-Amz-Date=20240716T060929Z&X-Amz-Expires=600&X-Amz-Signature=5744bde2e6bf87e 7ba72f98d9bb9f6fcf9b8ed1f43cbf5bb06cc2735a961982f&X-Amz-SignedHeaders=host&x-id= GetObject	Web Gateway	IT55	Penetrated
2024-07-16	ShadowRoot Ransomware Targeting Turkish Businesses	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/sha dowroot_ransomware_targeting_turkish_businesses_bb018787-9844-4121-acab-179bd5f2 61a2/2960a2d4d2fd6b_browsing7b85b8e3ea4c86ec0c13b93bfd3754a7e772a2c74f564b0009Xx X42Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOA D&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240716%2Feu-west-1%2Fs3%2Faws4_reque st&X-Amz-Date=20240716T060928Z&X-Amz-Expires=600&X-Amz-Signature=f240245c7895724 94b49bfcd9f4accdf698691fe45b832c344d2662adda969fe&X-Amz-SignedHeaders=host&x-id= GetObject	Web Gateway	IT55	Penetrated

TLP:AMBER

GLESEC
COMPLETELY PERCEPTI

ASM-VP REPORT

GOAA 07/26/2024

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2024-07-15	Increase In The Exploitation Of Microsoft SmartScreen Vulnerability CVE-2024-21412	58e2b_edr766dec37cc5fcfb63bc16d69627cd87e7e46f0b9f48899889479f12611eXxX20Lnk.lnk	Endpoint Security	IT55	Prevented
2024-07-15	Increase In The Exploitation Of Microsoft SmartScreen Vulnerability CVE-2024-21412	6,481,462f15ad4213f83a3d28304f14496bae1feb8580056959a65_edr7d0ee8981dbXxX21Lnk.lnk	Endpoint Security	IT55	Prevented
2024-07-15	Increase In The Exploitation Of Microsoft SmartScreen Vulnerability CVE-2024-21412	7ee31fa89e9e68f20004bdc31f8f05a95861b6c6_edr78bfa3b57f09fdfad9ef5290XxX22Lnk.lnk	Endpoint Security	IT55	Prevented
2024-07-15	Increase In The Exploitation Of Microsoft SmartScreen Vulnerability CVE-2024-21412	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/increase_in_the_exploitation_of_microsoft_smartscreen_vulnerability_cve-2024-21412_0211ec16-3565-4729-9447-8e445ae4ee88/aceee450c55d616_browsing71c2d3d154b5f77e7f99688b6da8a8f3256a4bae2cdb76a4cXxX26Lnk.lnk?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240715%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240715T060723Z&X-Amz-Expires=600 &X-Amz-Signature=2a22e75d7adeb0912328a1ec6865dce3f8dd9f4341ddd2a529d388b79cb3e52 d&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-15	Increase In The Exploitation Of Microsoft SmartScreen Vulnerability CVE-2024-21412	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/increase_in_the_exploitation_of_microsoft_smartscreen_vulnerability_cve-2024-21412_0211ec16-3565-4729-9447-8e445ae4ee88/81e89_browsing754ae2324c684fce71acafc30f8085870be947e7a76971b4fec1b24b5d1XxX23Lnk.lnk?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240715%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240715T060722Z&X-Amz-Expires=600 &X-Amz-Signature=77bcfd0655da5033f4092aa4211b2cbd2929e250704d9428d86aa3eaf6e025e 4&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-15	Increase In The Exploitation Of Microsoft SmartScreen Vulnerability CVE-2024-21412	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/increase_in_the_exploitation_of_microsoft_smartscreen_vulnerability_cve-2024-21412_0211ec16-3565-4729-9447-8e445ae4ee88/4eccb_browsing7813cee8c8039424aebf69f4269d4a6c2c72d81a001254bcdce80034555XxX19Lnk.lnk?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240715%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240715T060716Z&X-Amz-Expires=600 &X-Amz-Signature=4671e4e8a6e0361e90978c4930c4be3b0c218e19331ccdbacf2e99b4e3e07d7 f&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-15	Increase In The Exploitation Of Microsoft SmartScreen Vulnerability CVE-2024-21412	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/increase_in_the_exploitation_of_microsoft_smartscreen_vulnerability_cve-2024-21412_0211ec16-3565-4729-9447-8e445ae4ee88/4_browsing73abb2c272295473e5556ec7dec06f2018c0a67f208d8ab33de1fb6d40895f5XxX18Lnk.lnk?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240715%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240715T060715Z&X-Amz-Expires=600 &X-Amz-Signature=4a228a4cbd229a9b2675293af4d6a50f1c943c8df9d6bb43b2857e26ac4d2af 6&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-15	Increase In The Exploitation Of Microsoft SmartScreen Vulnerability CVE-2024-21412	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/increase_in_the_exploitation_of_microsoft_smartscreen_vulnerability_cve-2024-21412_0211ec16-3565-4729-9447-8e445ae4ee88/268a0de2468_browsing726a106fd92563a846e764f2ba313e37b5fc0cf76171b0a363f6fXxX17Lnk.lnk?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240715%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240715T060715Z&X-Amz-Expires=600 &X-Amz-Signature=cf926fba8220169bfce68afbe3394dda9c49e321551dd86605546a5f795044f 5&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-15	Increase In The Exploitation Of Microsoft SmartScreen Vulnerability CVE-2024-21412	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/increase_in_the_exploitation_of_microsoft_smartscreen_vulnerability_cve-2024-21412_0211ec16-3565-4729-9447-8e445ae4ee88/2460e_browsing7590e09af09ced6f75c001a9066c18629d956edbe8041f08cd21b7528b2XxX16Lnk.lnk?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240715%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240715T060715Z&X-Amz-Expires=600 &X-Amz-Signature=64b4e39dfabdedca71804dfd15e03de49fdec50545ac48943eda98074f43ab7 f&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-15	Increase In The Exploitation Of Microsoft SmartScreen Vulnerability CVE-2024-21412	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/increase_in_the_exploitation_of_microsoft_smartscreen_vulnerability_cve-2024-21412_0211ec16-3565-4729-9447-8e445ae4ee88/0e2263d4f239a5c39960ffa6b6b688faa_browsing7fc3075e130fe0d4599d5b95ef20647XxX11Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240715%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240715T060713Z&X-Amz-Expires=600 &X-Amz-Signature=7917af833ddfe7b4586e4ffcb2ef5078079a036c53bedde2c1d14514c455eab 9&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-15	Increase In The Exploitation Of Microsoft SmartScreen Vulnerability CVE-2024-21412	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/increase_in_the_exploitation_of_microsoft_smartscreen_vulnerability_cve-2024-21412_0211ec16-3565-4729-9447-8e445ae4ee88/a024a18e2_browsing7707738adcd7b5a740c5a93534b4b8c9d3b947f6d85740af19d17d0XxX10Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240715%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240715T060709Z&X-Amz-Expires=600 &X-Amz-Signature=62c209fa8e6dea6a442e53c2ec88cdf0666b8b6d20aa684807afd53e59d8a01 a&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated

TLP:AMBER

GLESEC
COMPLETELY PERCEPTI

ASM-VP REPORT

GOAA 07/26/2024

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2024-07-15	Increase In The Exploitation Of Microsoft SmartScreen Vulnerability CVE-2024-21412	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/increase_in_the_exploitation_of_microsoft_smartscreen_vulnerability_cve-2024-21412_0211ec16-3565-4729-9447-8e445ae4ee88/a31f222fc28322_browsing7f5e7988d1ad9c0aecd66d58bb7b4d8518ae23e110308dbf91XxX9Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240715%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240715T060705Z&X-Amz-Expires=600& X-Amz-Signature=e565823f5ed4803285835e6c153bbaf607e484749e4a87b480cbc61670243c4c &X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-14	Resurrecting Internet Explorer Threat Actors Using Zero-day Tricks in Internet Shortcut File to Lure Victims CVE-2024-38112	65,142c8f490839a60f490_edr7ab8f28dd9db4258e1cfab2d48e89437ef2188a6e94XxX163Txt.txt	Endpoint Security	IT55	Prevented
2024-07-14	Resurrecting Internet Explorer Threat Actors Using Zero-day Tricks in Internet Shortcut File to Lure Victims CVE-2024-38112	bd_edr710ee53ef3ad872f3f0678117050608a8e073c87045a06a86fb4a7f0e4eff0XxX164Txt.tx t	Endpoint Security	IT55	Prevented
2024-07-14	Dissecting GootLoader With Nodejs	b939ec944_edr7140804710f0ce2a7d33ec89f758ff8e7caab6ee38fe2446e3ac988XxX25Js.js	Endpoint Security	IT55	Prevented
2024-07-14	Dissecting GootLoader With Nodejs	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/dissecting_gootloader_with_nodejs_6e62c6bd-88ff-4cf0-b89c-011f0f83f004/c853d91501111a8_browsing73a027bd3b9b4dab9dd940e89fcfec51efbb6f0db0ba6687bXxX26Js.js?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240714%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240714T113545Z&X-Amz-Expires=600&X-Amz-Signature=4b2de4515dfabad6003761c5fc62a64ee520954a155ef9842bb136583d2e2429&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-14	Silver Fox Threat Group Attack Activities	6_edr7990f3893b800811f36b4d9982e0811f49d0d91791f827d80cf6b8bc258e0ebXxX17Dll.dll	Endpoint Security	IT55	Prevented
2024-07-14	Silver Fox Threat Group Attack Activities	hxxp://6014.anonymousrat6.com	Web Gateway	IT55	Offline/Removed
2024-07-14	Silver Fox Threat Group Attack Activities	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/silver_fox_threat_group_attack_activities_f22c56b3-41f4-4555-bdf0-4416f5d5c642/1bf9dffebe93a422210ac261_browsing7c0de67f975827a1cbe304d79ca93b959fb4628fXxX21Exe.ex e?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240714%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240714T071947Z&X-Amz-Expires=600&X-Amz-Signature=fc286de6cd1427826eee1969dd3b666c4332e94985ca573e844a1039adc9a686&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-14	Silver Fox Threat Group Attack Activities	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/silver_fox_threat_group_attack_activities_f22c56b3-41f4-4555-bdf0-4416f5d5c642/a_browsing790c7e34f45b21f34838260282b8af4b2850ec5e9add93aa3baad8d530cca8dXxX19Ps1.ps 1?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240714%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240714T071947Z&X-Amz-Expires=600&X-Amz-Signature=48cacad4da1ba5aa86f98e0c888f5f22abf1fe33bdb68e371d872bf5d8c305a0&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-14	Silver Fox Threat Group Attack Activities	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/silver_fox_threat_group_attack_activities_f22c56b3-41f4-4555-bdf0-4416f5d5c642/7_browsing7a07a99b53b4f8d8ced56b3e80f3ccaba52692ab7865c1dda3b752739e966b7XxX15Exe.ex e?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240714%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240714T071935Z&X-Amz-Expires=600&X-Amz-Signature=3c24be8dd50dd70db0847886fb5e4f4e9c1201c500cad45a2dd93b88ab0def2a&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-10	Mallox Ransomware Linux Variant Decryptor Found	23ba80_edr78df63ebb313f2f2a2f24dab840e068ddd5cc54bb661db7d010954d2fcXxX18Elf.elf	Endpoint Security	IT55	Prevented
2024-07-10	Mallox Ransomware Linux Variant Decryptor Found	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/mallox_ransomware_linux_variant_decryptor_found_86425878-748d-46f8-a347-18870b072b6c/e1d8095b39af0901618fa2b0d2f620d391f16_browsing7045f6d2e61efca6797f5a322fdXxX12Python.python?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240710%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240710T135951Z&X-Amz-Expires=600&X-Amz-Signature=eef91c24f02de3bfa4c029b0b97438991eac91a62061be54cd4179746d8117a2&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-10	GrimResource - Microsoft Management Console for initial access and evasion	c1bba_edr723f79282dceed4b8c40123c72a5dfcf4e3ff7dd48db8cb6c8772b60b88XxX3Dll.dll	Endpoint Security	IT55	Prevented

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

TLP:AMBER

GLESEC
COMPLETELY PERCEPTI

ASM-VP REPORT

GOAA 07/26/2024

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2024-07-10	GrimResource - Microsoft Management Console for initial access and evasion	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/gri mresource_-_microsoft_management_console_for_initial_access_and_evasion_afba1385 -6119-42c2-92d2-e726eed51d4a/4cb5_browsing75bc114d39f8f1e66d6e7c453987639289a28c d83a7d802744cd99087fd7XxX2Dll.dll?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content - Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240710%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240710T135027Z&X-Amz-Expires=600&X-Amz-Signature=f7c1f93cf56a9e7587fda06f7a509cc5d0754f4c7dcb605ce1305b7aa4184733&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-10	GrimResource - Microsoft Management Console for initial access and evasion	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/gri mresource_-_microsoft_management_console_for_initial_access_and_evasion_afba1385 -6119-42c2-92d2-e726eed51d4a/14bcb_browsing7196143fd2b800385e9b32cfacd837007b0fa ce71a73b546b53310258bbXxX1Xml.xml?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content - Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240710%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240710T135025Z&X-Amz-Expires=600&X-Amz-Signature=288ed54d970acc588e2f4a3de3627d6c346fe2379c57446972fa2e1a33f3b3fb&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-09	Mekotio Banking Trojan Threatens Financial Systems in Latin America	8c_edr7e556beba4a5d026211259114ba686013b5fd5f9cb9e677b2641bd2c2fc5XxX4Pdf.pdf	Endpoint Security	IT55	Prevented
2024-07-09	Mekotio Banking Trojan Threatens Financial Systems in Latin America	439eecb230fb53b81_edr7ae535d6a6d978066134b4b52e49e065e9ddeff5f2bbbd3XxX2Dll.dll	Endpoint Security	IT55	Prevented
2024-07-09	Mekotio Banking Trojan Threatens Financial Systems in Latin America	hxxp://tudoprafrente.co	Web Gateway	IT55	Offline/Removed
2024-07-09	Mekotio Banking Trojan Threatens Financial Systems in Latin America	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/mekotio_banking_trojan_threatens_financial_systems_in_latin_america_43592ade-3b88-4cc8-8ce7-2d504db5127e/e082dc1c11afff40efe2cf92e36ac3_browsing7129b78320b5cc656f4b80488307770eabXxX7Pdf.pdf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240709T122228Z&X-Amz-Expires=600&X-Amz-Signature=7feb4a9989b859c7b00aa1231408437fa03ae5d4673fb915d0a697aefc617e84&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-09	Mekotio Banking Trojan Threatens Financial Systems in Latin America	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/mekotio_banking_trojan_threatens_financial_systems_in_latin_america_43592ade-3b88-4cc8-8ce7-2d504db5127e/b6a82_browsing774b81a9650337163 51d92dd0a75f494069b4b4436d21327c06c917e6e0XxX5Pdf.pdf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240709T122227Z&X-Amz-Expires=600&X-Amz-Signature=2c8d36ca176bb735f93a4c07ae832813160cfb3a254d6f515befc911e02f288e&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
N/A	Mekotio Banking Trojan Threatens Financial Systems in Latin America	8c_mail7e556beba4a5d026211259114ba686013b5fd5f9cb9e677b2641bd2c2fc5XxX4Pdf.pdf	Email Gateway	skywatch@goaa.org	Prevented
2024-07-09	Mekotio Banking Trojan Threatens Financial Systems in Latin America	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/mekotio_banking_trojan_threatens_financial_systems_in_latin_america_43592ade-3b88-4cc8-8ce7-2d504db5127e/a_browsing7112aa5b398fc7a77100164c818b5e17612d828320b4e3e1f895e56b4fd6797XxX1Dll.dll?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240709T122211Z&X-Amz-Expires=600&X-Amz-Signature=6deca2faf5b4e89fd3740de9a77d3ba05b2b1ddd72ed24fbbef5f5882c6c824d&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-09	Turla A Master of Deception	7,091ce9_edr7fb5906680c1b09558bafdf9681a81f5f524677b90fd0f7fc0a05bc00XxX75Exe.exe	Endpoint Security	IT55	Prevented
2024-07-09	Turla A Master of Deception	c2618fb013135485f9f9aa2_edr7983df3371dfdcb7beecde86d02cee0c258d5ed7fXxX77Zip.zip	Endpoint Security	IT55	Prevented
2024-07-09	Turla A Master of Deception	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/turla_a_master_of_deception_5a1a2df0-8d4d-4851-837f-2f4667179131/cac4d4364d20fa343bf681f6544b31995a5_browsing7d8f69ee606c4675db60be5ae8775XxX78Lnk.lnk?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240709T072911Z&X-Amz-Expires=600&X-Amz-Signature=c5faa8688bd7170695c2d231eff9001cfc6ed51978b75ec7735de7cbcc8eb42c&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-09	Turla A Master of Deception	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/turla_a_master_of_deception_5a1a2df0-8d4d-4851-837f-2f4667179131/b6abbeab6e000036c6cdffc5_browsing7c096d796397263e280ea264eba73ac5bab39441XxX76Xml.xml?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240709T072909Z&X-Amz-Expires=600&X-Amz-Signature=7190ff8421c1e70cdccc0eae84238645822002 8151f904782a2ef797ecd419d4&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated

TLP:AMBER

GLESEC
COMPLETELY PERCEPTI

ASM-VP REPORT

GOAA 07/26/2024

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
N/A	Turla A Master of Deception	c2618fb013135485f9f9aa2_mail7983df3371dfdcb7beecde86d02cee0c258d5ed7fXxX77Zip.zi p	Email Gateway	skywatch@goaa.org	Prevented
2024-07-08	Mekotio Banker - Improved Stealth and Ancient Encryption	Mekot2_edrZip.zip	Endpoint Security	IT55	Prevented
2024-07-08	Mekotio Banker - Improved Stealth and Ancient Encryption	Mekot_edr7Bat.bat	Endpoint Security	IT55	Prevented
2024-07-08	Mekotio Banker - Improved Stealth and Ancient Encryption	Mekot8_edrBat.bat	Endpoint Security	IT55	Prevented
2024-07-08	Mekotio Banker - Improved Stealth and Ancient Encryption	Mekot2_edrBat.bat	Endpoint Security	IT55	Prevented
2024-07-08	Mekotio Banker - Improved Stealth and Ancient Encryption	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/mek otio_banker_-_improved_stealth_and_ancient_encryption_4e967f25-7ece-4960-9847-52ab2bfdf231/Mekot10_browsingBat.bat?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Conten t-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240708%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240708T131336Z&X-Amz-Expires=600&X-Amz-Signature=9c12a8ffc0472fca686cb67859e42ab24df7933cbbbee0bf26a5cbead5f0b26d&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-08	Mekotio Banker - Improved Stealth and Ancient Encryption	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/mek otio_banker_-_improved_stealth_and_ancient_encryption_4e967f25-7ece-4960-9847-52ab2bfdf231/Mekot9_browsingBat.bat?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content -Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240708%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240708T131334Z&X-Amz-Expires=600&X-Amz-Signature=eb52610e4e2a30c152364abc6dfbb203cb3f561d182a21a8c79bbbdf4e400a8c&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-08	Mekotio Banker - Improved Stealth and Ancient Encryption	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/mek otio_banker_-_improved_stealth_and_ancient_encryption_4e967f25-7ece-4960-9847-52ab2bfdf231/Mekot6_browsingBat.bat?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content -Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240708%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240708T131327Z&X-Amz-Expires=600&X-Amz-Signature=47cacfb293aec9e077723296d8c599a78fa0fd2a50b750d51ca0e8c714aa6211&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-08	Mekotio Banker - Improved Stealth and Ancient Encryption	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/mek otio_banker_-_improved_stealth_and_ancient_encryption_4e967f25-7ece-4960-9847-52ab2bfdf231/Mekot11_browsingBat.bat?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Conten t-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240708%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240708T131326Z&X-Amz-Expires=600&X-Amz-Signature=5720074f546452d9ccf811e502ea0c982849f19c8f133171be2b0b2203ea82d8&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-08	Mekotio Banker - Improved Stealth and Ancient Encryption	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/mek otio_banker_-_improved_stealth_and_ancient_encryption_4e967f25-7ece-4960-9847-52ab2bfdf231/Mekot12_browsingBat.bat?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Conten t-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240708%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240708T131326Z&X-Amz-Expires=600&X-Amz-Signature=5b0e8737998be2d07d9597e4842ce0204447b926fce97e52ae0ffa60fd81df9a&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-08	Mekotio Banker - Improved Stealth and Ancient Encryption	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/mek otio_banker_-_improved_stealth_and_ancient_encryption_4e967f25-7ece-4960-9847-52ab2bfdf231/Mekot3_browsingBat.bat?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content -Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240708%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240708T131326Z&X-Amz-Expires=600&X-Amz-Signature=3b4176159699debad54410f1f24120c614ef14fc5e80cf89273e844642968b0e&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-08	Mekotio Banker - Improved Stealth and Ancient Encryption	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/mek otio_banker_-_improved_stealth_and_ancient_encryption_4e967f25-7ece-4960-9847-52ab2bfdf231/Mekot4_browsingBat.bat?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content -Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240708%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240708T131325Z&X-Amz-Expires=600&X-Amz-Signature=e2b027202b9e7f6bece0298bfebe129b081a5fcff8a617b43f081bd6738145ba&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-08	Mekotio Banker - Improved Stealth and Ancient Encryption	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/mek otio_banker_-_improved_stealth_and_ancient_encryption_4e967f25-7ece-4960-9847-52ab2bfdf231/Mekot1_browsingBat.bat?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content -Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240708%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240708T131325Z&X-Amz-Expires=600&X-Amz-Signature=834afebe645d7e71d0e209f683768b6b62c28c3456c7c82a27d857babc5ef1a5&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated

TLP:AMBER

GLESEC
COMPLETELY PERCEPTI

ASM-VP REPORT

GOAA 07/26/2024

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2024-07-08	Mekotio Banker - Improved Stealth and Ancient Encryption	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/mek otio_banker_-_improved_stealth_and_ancient_encryption_4e967f25-7ece-4960-9847-52 ab2bfdf231/Mekot5_browsingBat.bat?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content - Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240708%2Feu-w est-1%2Fs3%2Faws4_request&X-Amz-Date=20240708T131324Z&X-Amz-Expires=600&X-Amz-Si gnature=3aca056ca898ca4b88f99c3b5f7353aff89604c6f7dff7fe8d4b6fd11dfb9199&X-Amz-S ignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
N/A	Mekotio Banker - Improved Stealth and Ancient Encryption	Mekot2_mailZip.zip	Email Gateway	skywatch@goaa.org	Prevented
2024-07-08	Mekotio Banker - Improved Stealth and Ancient Encryption	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/mek otio_banker_-_improved_stealth_and_ancient_encryption_4e967f25-7ece-4960-9847-52 ab2bfdf231/Mekot1_browsingZip.zip?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content - Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240708%2Feu-w est-1%2Fs3%2Faws4_request&X-Amz-Date=20240708T131323Z&X-Amz-Expires=600&X-Amz-Si gnature=b544b22809b308da1f2a1cb685669341fa10fa31e2f6752bcce9486472fc817e&X-Amz-S ignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-08	Turning Jenkins Into a Cryptomining Machine From an Attackers Perspective	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/tur ning_jenkins_into_a_cryptomining_machine_from_an_attackers_perspective_46d359f8- 450c-41d3-af01-7ced911e1716/5_browsing7fedfb431a717031f454d4fb2809d1f6d432a9edd9 00b07f0b9f9aca7fb3597XxX28Elf.elf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content - Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240708%2Feu-w est-1%2Fs3%2Faws4_request&X-Amz-Date=20240708T080135Z&X-Amz-Expires=600&X-Amz-Si gnature=f8f6cbcf83dc9c0cad48690bb6a5faec40dc06e432202628820f547f3c271628&X-Amz-S ignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-07	REGRESSHION CVE-2024-6387 A TARGETED EXPLOIT IN THE WILD	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/reg resshion_cve-2024-6387_a_targeted_exploit_in_the_wild__a28da71e-7694-4b72-82ce-5 ac57fca40a1/219f9b69_browsing73c92dfe86b1018344b2113fd79d138509204dda6a5b5839de4 b2de6XxX1Zip.zip?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240707%2Feu-west-1%2Fs3%2Faws4 _request&X-Amz-Date=20240707T145002Z&X-Amz-Expires=600&X-Amz-Signature=f481ee61f 09f9f8b4ee98ba0d7985c1ca25856ccca0aaab0dfb5e93aec8bc2bf&X-Amz-SignedHeaders=host &x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-07	New Threat A Deep Dive Into the Zergeca Botnet	7db9189afd00c2b60b_edr7f892ef1b86d040fb1cf02145c7d2e414ef77ba3335c11XxX3Elf.elf	Endpoint Security	IT55	Prevented
2024-07-07	New Threat A Deep Dive Into the Zergeca Botnet	cea6e4aa15d_edr7c6a2b2c794a660afaf96d43462e0b74436600a2c8a2288ad0c27XxX8Elf.elf	Endpoint Security	IT55	Prevented
2024-07-07	New Threat A Deep Dive Into the Zergeca Botnet	2e9df898_edr7212300815928e0426e9358b1380a1eaba38270d03dd69e421686b5bXxX7Elf.elf	Endpoint Security	IT55	Prevented
2024-07-07	New Threat A Deep Dive Into the Zergeca Botnet	6b81d548c0fbd_edr7a2275bb0d29deca0de96c1584ce7aadaf4f5dac3cb28ee9c29XxX9Elf.elf	Endpoint Security	IT55	Prevented
2024-07-07	New Threat A Deep Dive Into the Zergeca Botnet	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/new _threat_a_deep_dive_into_the_zergeca_botnet_20220833-98bf-4194-849c-b14d387c7fda /b55b194_browsing7a11de7ee2cb3aaede12ce15c85abf2b607d1ebd8f5ed56e3a6ef7c43XxX11E lf.elf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X- Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240707%2Feu-west-1%2Fs3%2Faws4_request&X -Amz-Date=20240707T062056Z&X-Amz-Expires=600&X-Amz-Signature=9d63ae18abc7544a529 d2ae568ae8bf904a1acc7c438be4d1246d806070cd7d7&X-Amz-SignedHeaders=host&x-id=GetO bject	Web Gateway	IT55	Penetrated
2024-07-07	New Threat A Deep Dive Into the Zergeca Botnet	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/new _threat_a_deep_dive_into_the_zergeca_botnet_20220833-98bf-4194-849c-b14d387c7fda /7e62e3e8911c0cb19df34_browsing77df0603fddeff82223e1cc6da7fb1698f512ff2cd2XxX6El f.elf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-A mz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240707%2Feu-west-1%2Fs3%2Faws4_request&X- Amz-Date=20240707T062049Z&X-Amz-Expires=600&X-Amz-Signature=17e92d5e6daac68e0702 39c1c60d0b681548c27e811c1649f1bacf20db7bee68&X-Amz-SignedHeaders=host&x-id=GetOb ject	Web Gateway	IT55	Penetrated
2024-07-07	New Threat A Deep Dive Into the Zergeca Botnet	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/new _threat_a_deep_dive_into_the_zergeca_botnet_20220833-98bf-4194-849c-b14d387c7fda /0dbbe5616de_browsing71c5753768de555203fb9eb2f1e72a8cb5bdce0559bc5cdfa3b2eXxX5El f.elf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-A mz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240707%2Feu-west-1%2Fs3%2Faws4_request&X- Amz-Date=20240707T062046Z&X-Amz-Expires=600&X-Amz-Signature=b87f34e12d25f3da972d db16c5faa9c5cecbe859cc881eb6c10b5586f29cbb28&X-Amz-SignedHeaders=host&x-id=GetOb ject	Web Gateway	IT55	Penetrated
2024-07-04	RisePro Information Stealer	5e1a1b2e2c20bc50b54e02393fa6f26a2b8c2f4d8_edr7f2abdecaca73472b5c5dbaXxX2Exe.exe	Endpoint Security	IT55	Prevented
2024-07-04	RisePro Information Stealer	4f0e839393df_edr72db99a05ade0848979ff375399b104e59a7cc3847d746c17e5cXxX4Exe.exe	Endpoint Security	IT55	Prevented

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

TLP:AMBER

GLESEC
COMPLETELY PERCEPTI

ASM-VP REPORT

GOAA 07/26/2024

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2024-07-04	RisePro Information Stealer	a36d5e_edr790ca17fb6f70884942d868d29c6854054f2db79ed8f4e2d0d16ef1647XxX3Exe.exe	Endpoint Security	IT55	Prevented
2024-07-04	RisePro Information Stealer	56,108c_edr707fcaf87b2220c081db115171ff35811946b3ad2d76105715e8530fbeXxX5Exe.exe	Endpoint Security	IT55	Prevented
2024-07-04	RisePro Information Stealer	a_edr78513831b47f4b35ee9063aa167bf5d05c61559b2ac7f8fb93fa966a36e34d2XxX8Exe.exe	Endpoint Security	IT55	Prevented
2024-07-04	RisePro Information Stealer	b4ad80860c_edr773c79c946c3a4df13e534153bd17ceebad6acedac3156dfe0144cXxX6Exe.exe	Endpoint Security	IT55	Prevented
2024-07-04	RisePro Information Stealer	5_edr719a862d5a32ec56328f8e066a83b6b0577a6965074ca671d0cecce681d5f79XxX12Exe.exe	Endpoint Security	IT55	Prevented
2024-07-04	RisePro Information Stealer	c48eb226b641b382fd4155f10c96aacc585c6e65814865cd_edr762e88b8a5cffd14XxX10Exe.exe	Endpoint Security	IT55	Prevented
2024-07-04	RisePro Information Stealer	c_edr7a40fb4aa017a0d17b535c1857d51f95b7ed8684a1ea860294bf5d897667839XxX15Exe.exe	Endpoint Security	IT55	Prevented
2024-07-04	RisePro Information Stealer	9d540839e_edr75daf4f31eb36271fef6eb16a913446384d07e4d8dbb2602f18bf0fXxX13Exe.exe	Endpoint Security	IT55	Prevented
2024-07-04	RisePro Information Stealer	15dfbd2df433c9_edr725239d6602bdfc56d00db62f88a1769a534d98cad50536c27XxX14Exe.exe	Endpoint Security	IT55	Prevented
2024-07-04	RisePro Information Stealer	cb21be43_edr7c800875400a94b2442bbe02ccaf31ee49e1f440aac378fc2b0b756dXxX24Exe.exe	Endpoint Security	IT55	Prevented
2024-07-04	RisePro Information Stealer	d_edr7c3c01d62fb59e186b2256894fb089c01e1aeda5dbd86a3004f1857a13313adXxX22Exe.exe	Endpoint Security	IT55	Prevented
2024-07-04	RisePro Information Stealer	0d5bb8b8da18abd1f3934103c501abf9b9cd3a6e1656853359a568dca3229_edr765XxX23Exe.exe	Endpoint Security	IT55	Prevented
2024-07-04	RisePro Information Stealer	6,113bc3f3f9_edr72393acff5022f5ba95fb96c3d9038386ada49ccf244fa5f885faXxX16Exe.exe	Endpoint Security	IT55	Prevented
2024-07-04	RisePro Information Stealer	19c98cba0d803_edr7a36b00d2c11cc24d25e1f388ba5093a4b6e9017508371fb34bXxX18Exe.exe	Endpoint Security	IT55	Prevented
2024-07-04	RisePro Information Stealer	f8_edr7dd2b6a63e850b6c2128ec139c6334b572b1c80698fcc30de6f39ffc788f4fXxX25Exe.exe	Endpoint Security	IT55	Prevented
2024-07-04	RisePro Information Stealer	d2cbb_edr7a5ef2ecdf7c6f8c965df5886a18ea0e630009cdedb3692ed1b8c77b487XxX19Exe.exe	Endpoint Security	IT55	Prevented
2024-07-04	RisePro Information Stealer	hxxp://94.156.8.188	Web Gateway	IT55	Offline/Removed
2024-07-04	RisePro Information Stealer	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/risepro_information_stealer_dbcc8998-07d5-4a55-adfd-08a15abf9712/d435d_browsing7cf9077533a7c23129a8d7462e7596505e3990664dd5888fce40652bb14XxX21Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240704%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240704T075921Z&X-Amz-Expires=600&X-Amz-Signature=4c580ee6f1dbeccc160654b67ce410887f0dac85a66ceefca2120b12e1d07f77&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-04	RisePro Information Stealer	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/risepro_information_stealer_dbcc8998-07d5-4a55-adfd-08a15abf9712/0_browsing78b3f37483cfc697fbd67120311e6109843804f5cae9c46f04fa1b51ba7120aXxX20Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240704%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240704T075914Z&X-Amz-Expires=600&X-Amz-Signature=47384eb084998c64a8e48837a28f28093c2d5deb966307f7b7cc5c62a98fa735&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-04	RisePro Information Stealer	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/risepro_information_stealer_dbcc8998-07d5-4a55-adfd-08a15abf9712/ce930238a02a55d_browsing7b6f13fdf9b3306de61c5c25513ed396c7e9a8dbd4c45dbd9XxX17Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240704%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240704T075910Z&X-Amz-Expires=600&X-Amz-Signature=f4e35be937415c396ed18b2b6448be608acb304b80cf763867fe05f90ba2e530&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated

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

TLP:AMBER

GLESEC
COMPLETELY PERCEPTI

ASM-VP REPORT

GOAA 07/26/2024

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2024-07-04	RisePro Information Stealer	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/risepro_information_stealer_dbcc8998-07d5-4a55-adfd-08a15abf9712/6b82e6f228cbb8143b68e1_browsing739f3d083cf6ab0ba9c202ce1ec769bb12c9030619XxX11Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240704%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240704T075903Z&X-Amz-Expires=600&X-Amz-Signature=cb9183d7b8e22cb85087f01067d170a62c74760822feefa8fd23db0a72b86108&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-04	RisePro Information Stealer	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/risepro_information_stealer_dbcc8998-07d5-4a55-adfd-08a15abf9712/30baf54d503_browsing79893b23b24203611da331d436dfc35f2d0a805bac4da0d310489XxX9Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240704%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240704T075856Z&X-Amz-Expires=600&X-Amz-Signature=56c0a290feacd7e02911fc361869803cf93f053c78b572581202ea017fd41b3a&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-04	RisePro Information Stealer	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/risepro_information_stealer_dbcc8998-07d5-4a55-adfd-08a15abf9712/7_browsing7e97faca59d8de34ddc7272791efac41da9ff5b7b175a99e09a255e2701d725XxX7Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240704%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240704T075854Z&X-Amz-Expires=600&X-Amz-Signature=89b1e2a496e5ba53db22d79067ad32037a5bafa6a5a781306f04fd33779d382a&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-04	RisePro Information Stealer	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/risepro_information_stealer_dbcc8998-07d5-4a55-adfd-08a15abf9712/222932_browsing7fa653ffd07f11773ee22eb00e580b6824ce122a1e788f19859aa9dca2XxX1Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240704%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240704T075847Z&X-Amz-Expires=600&X-Amz-Signature=8ce0ccbac1f71ee3f69e12b8ec01ffbb6fce8374026b6a3964725904c3c002d8&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-04	New Ransomware Operator Volcano Demon Serving Up LukaLocker	4e58629158a6c46ad420f_edr729330030f5e0b0ef374e9bb24cd203c89ec3262669XxX35Exe.exe	Endpoint Security	IT55	Prevented
2024-07-04	New Ransomware Operator Volcano Demon Serving Up LukaLocker	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/new_ransomware_operator_volcano_demon_serving_up_lukalocker_46e633a0-07c9-4db4-969c-ca783331cb37/f83abe3d9_browsing717238755f1276c87b3b320d8c30421984a897099ce3741d9143906XxX37Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240704%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240704T062704Z&X-Amz-Expires=600&X-Amz-Signature=00e5aac9dad9d7bbe6d0eb10b3ca6e632e39d828689490d8d91c4833d3a00daa&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-03	Unfurling Hemlock Threat group uses cluster bomb campaigns	8fe4d34a6a245c5acd3d1_edr741213c1dd195468089b1a3fe80adfa6d8d8c94f2d8XxX47Exe.exe	Endpoint Security	IT55	Penetrated
2024-07-03	Unfurling Hemlock Threat group uses cluster bomb campaigns	94,115d0eae0422b6605f0f25841c29b_edr7cc6c029472a983b21d1cedcd7fdcd647XxX35Exe.exe	Endpoint Security	IT55	Prevented
2024-07-03	Unfurling Hemlock Threat group uses cluster bomb campaigns	0ef_edr7459cebfe9bd9102c5eccc16eedddec5931e69bf705aa44aa3c7af584f209XxX38Exe.exe	Endpoint Security	IT55	Prevented
2024-07-03	Unfurling Hemlock Threat group uses cluster bomb campaigns	1f224093b955_edr7dd73caaf1c6a823028c286ddd3414bceb0860e0fe084fb8c2abXxX39Exe.exe	Endpoint Security	IT55	Prevented
2024-07-03	Unfurling Hemlock Threat group uses cluster bomb campaigns	35c55b402e_edr770e25adf57ffbd408a428af9ce21a735474b5d94ccdd4123e68f8XxX41Exe.exe	Endpoint Security	IT55	Prevented
2024-07-03	Unfurling Hemlock Threat group uses cluster bomb campaigns	da4f614c983fa226d813de39093_edr7389ae4d1e043dd86524aa7a5246fd587826bXxX50Exe.exe	Endpoint Security	IT55	Prevented
2024-07-03	Unfurling Hemlock Threat group uses cluster bomb campaigns	569_edr7652d0fd5b4a05ac00f6ec028fd3dc3e34ed7b112c4b8c6048eae72a8d326XxX42Exe.exe	Endpoint Security	IT55	Prevented
2024-07-03	Unfurling Hemlock Threat group uses cluster bomb campaigns	edfb43_edr74d5c586f0690c95ff8cacb36bda6fb4743f20dda5e6f17e7e241edd47XxX51Exe.exe	Endpoint Security	IT55	Prevented

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

TLP:AMBER

GLESEC
COMPLETELY PERCEPTI

ASM-VP REPORT

GOAA 07/26/2024

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2024-07-03	Unfurling Hemlock Threat group uses cluster bomb campaigns	80df101f1f93fa53b3dcbc315d3ec5d8c8330c08b5622ac320_edr7f746d016b66dcXxX46Exe.exe	Endpoint Security	IT55	Prevented
2024-07-03	Unfurling Hemlock Threat group uses cluster bomb campaigns	fd_edr7a9b8e52e2fbcb090d5f5046a73d6e42b421abf063083210889f3fcb47dee0XxX52Exe.exe	Endpoint Security	IT55	Prevented
2024-07-03	Unfurling Hemlock Threat group uses cluster bomb campaigns	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/unfurling_hemlock_threat_group_uses_cluster_bomb_campaigns_e96df6ab-765c-4746-90c1-94ebb0dfb343/be25926929b1aae025_browsing7d7f7614dd5ad637b8fd8e139c68f4d717e3dc9913e3cfXxX49Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240703%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240703T080324Z&X-Amz-Expires=600&X-Amz-Signature=857d02be08d6ab1942d9ced80a5d5bde6334fc47054c570a3cb306d5760d7e30&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-03	Unfurling Hemlock Threat group uses cluster bomb campaigns	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/unfurling_hemlock_threat_group_uses_cluster_bomb_campaigns_e96df6ab-765c-4746-90c1-94ebb0dfb343/7f101603fbb2821504cf2c_browsing71fca0450689dfcd6d1f36e57e27f0392be0f2d1ddXxX45Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240703%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240703T080323Z&X-Amz-Expires=600&X-Amz-Signature=fd2da5638045c4e87a6299cd3dd8dd50e9b35cc7784a594fb05bfcec535049d5&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-03	Unfurling Hemlock Threat group uses cluster bomb campaigns	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/unfurling_hemlock_threat_group_uses_cluster_bomb_campaigns_e96df6ab-765c-4746-90c1-94ebb0dfb343/7d18c6_browsing7c13ec919f3950092319d11eda129c8498e171612e681eebf1c977493dXxX44Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240703%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240703T080323Z&X-Amz-Expires=600&X-Amz-Signature=ed91a80bc2fa44666f16a042ac81dbb5c5648580a2a7762dc0bf3fec2f3ea713&X-Amz-SignedHeaders=ho st&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-03	Unfurling Hemlock Threat group uses cluster bomb campaigns	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/unfurling_hemlock_threat_group_uses_cluster_bomb_campaigns_e96df6ab-765c-4746-90c1-94ebb0dfb343/65923603a6f11_browsing7c7460b8cc69009105208bdfa544b90446580915db8fe127ae8XxX43Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240703%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240703T080317Z&X-Amz-Expires=600&X-Amz-Signature=5c09b307213be76a0f00e4bc07868310957a4f0018e206b16b5aebf11ece7d24&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-03	Unfurling Hemlock Threat group uses cluster bomb campaigns	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/unfurling_hemlock_threat_group_uses_cluster_bomb_campaigns_e96df6ab-765c-4746-90c1-94ebb0dfb343/301a1c9f4e82fc8f5_browsing7577ea399a2591557ff57d337472c3f8482a89c5b4105d5XxX40Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240703%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240703T080315Z&X-Amz-Expires=600&X-Amz-Signature=5bcb76fe6143a118060fe0fbc69cf6da7f1f861a78d444767a5d0090de9608ba&X-Amz-SignedHeaders=ho st&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-03	Unfurling Hemlock Threat group uses cluster bomb campaigns	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/unfurling_hemlock_threat_group_uses_cluster_bomb_campaigns_e96df6ab-765c-4746-90c1-94ebb0dfb343/0c48529d29_browsing79698341e89d6ea5f7e9211fa277e40d3f6a55a8996135944ebdadXxX37Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240703%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240703T080313Z&X-Amz-Expires=600&X-Amz-Signature=2f4d41832318ea79ce33ad3bfc294eb60c9e5c7dd0cdea0fb46b7ec1b092df7b&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-03	Unfurling Hemlock Threat group uses cluster bomb campaigns	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/unfurling_hemlock_threat_group_uses_cluster_bomb_campaigns_e96df6ab-765c-4746-90c1-94ebb0dfb343/3_browsing7b9e74da5fe5e27aaedc25e4aac7678553b6d7d89ec4d99e8b9d0627dcbdc12XxX30Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240703%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240703T080311Z&X-Amz-Expires=600&X-Amz-Signature=6ab9ff6d160413d78e762c5e64dc7fa071f8e089334fc3ef38bbbb54b2ea392d&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-03	Unfurling Hemlock Threat group uses cluster bomb campaigns	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/unfurling_hemlock_threat_group_uses_cluster_bomb_campaigns_e96df6ab-765c-4746-90c1-94ebb0dfb343/229e859dda6cc0bc99a395824f4524693bdd0292b4b9c55d06b4fa382_browsing79b3ea2XxX29Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240703%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240703T080309Z&X-Amz-Expires=600&X-Amz-Signature=fa1a1e05f9641784812c666951e5e188366b77fb5d9b5cc5198a5c96866f0c08&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-03	Supply Chain Compromise Leads to Trojanized Installers	4df9b_edr7da9590990230ed2ab9b4c3d399cf770ed7f6c36a8a10285375fd5a292fXxX18Exe.exe	Endpoint Security	IT55	Prevented

LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

TLP:AMBER

GLESEC
COMPLETELY PERCEPTI

ASM-VP REPORT

GOAA 07/26/2024

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2024-07-03	Supply Chain Compromise Leads to Trojanized Installers	6f49_edr756749d175058f15d5f3c80c8a7d46e80ec3e5eb9fb31f4346abdb72a0e7XxX20Exe.exe	Endpoint Security	IT55	Prevented
2024-07-03	Supply Chain Compromise Leads to Trojanized Installers	70bce9c228aacbdadaaf18596c0eb308c102382d04632b01b826e9db96210093_edrXxX21Exe.exe	Endpoint Security	IT55	Prevented
2024-07-03	Supply Chain Compromise Leads to Trojanized Installers	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/supply_chain_compromise_leads_to_trojanized_installers_d393005f-03bd-4d35-af94-aff4991999c4/fdc84cb0845f8_browsing7a39b29027d6433f4a1bbd8c5b808280235cf867a6b0b7a91ebXxX28Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240703%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240703T080043Z&X-Amz-Expires=600&X-Amz-Signature=c8c87a80e65f43c4513c1f406269a6ee0c8069c9a045e6159e3379bfa555f0ae&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-03	Supply Chain Compromise Leads to Trojanized Installers	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/supply_chain_compromise_leads_to_trojanized_installers_d393005f-03bd-4d35-af94-aff4991999c4/de4e032880_browsing71cdebe5c26913888b135fb2424132856cc892baea9792d6c66249XxX26Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240703%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240703T080042Z&X-Amz-Expires=600&X-Amz-Signature=f578869f64bbf06fa282edc89864c442cd3f0d9f07b3a64d8d6a412eab53d56c&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-03	Supply Chain Compromise Leads to Trojanized Installers	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/supply_chain_compromise_leads_to_trojanized_installers_d393005f-03bd-4d35-af94-aff4991999c4/bfa99c41aecc814de5b9eb839_browsing7a27e516c8b0a4e31edd9ed1304da6c996b4aaXxX23Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240703%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240703T080038Z&X-Amz-Expires=600&X-Amz-Signature=5cb70b37a29b38fbbf0d9a9fc9793ae18469c3e2dd887de29e8b900c22e6165e&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-03	Supply Chain Compromise Leads to Trojanized Installers	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/supply_chain_compromise_leads_to_trojanized_installers_d393005f-03bd-4d35-af94-aff4991999c4/2eae4f06f2c3_browsing76c6206c632ac93f4e8c4b3e0e63eca3118e883f8ac479b2f852XxX10Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240703%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240703T080019Z&X-Amz-Expires=600&X-Amz-Signature=50c32ffb1731d7377cc6cd292bcd2dc2ba2cfb2e363325678b61b5299f1f130c&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-21	APT41 Adds New Malware To Compromise Entities Across Multiple Sectors	69ca8ae8a3909aa4_edr717832d911d646c536fed4c907866724f74daf4d740f41aXxX58Dll.dll	Endpoint Security	IT55	Prevented
2024-07-21	APT41 Adds New Malware To Compromise Entities Across Multiple Sectors	bd058a6fd2034_edr7f21c38115490aef858d06f26b49b9d7be357297e60bd2934ccXxX60Dll.dll	Endpoint Security	IT55	Prevented
2024-07-21	APT41 Adds New Malware To Compromise Entities Across Multiple Sectors	7,586e58a569c2a0_edr7d0b3a710616f48833a040bf3fc57628bbdec7fcb462d565aXxX70Dll.dll	Endpoint Security	IT55	Prevented
2024-07-21	APT41 Adds New Malware To Compromise Entities Across Multiple Sectors	e5c_edr7089eb3297b204aaabdb4a660d125a948ba869d2a7cf3cf7c0098125b5ef5XxX62Dll.dll	Endpoint Security	IT55	Prevented
2024-07-21	APT41 Adds New Malware To Compromise Entities Across Multiple Sectors	cdc619_edr734f4e2aba0137b5fe9faf36896b85dff7cd4a93de562de770777d181aXxX68Dll.dll	Endpoint Security	IT55	Prevented
2024-07-21	APT41 Adds New Malware To Compromise Entities Across Multiple Sectors	hxxp://152.89.244.185/conn.exe	Web Gateway	IT55	Offline/Removed
2024-07-21	APT41 Adds New Malware To Compromise Entities Across Multiple Sectors	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/apt41_adds_new_malware_to_compromise_entities_across_multiple_sectors_c50e649f-b6b8-4aac-932c-d0161e9e1fd7/c3efcb6efad6_browsing75613721910a783389a646b2d138c7721df9849b28952d25bcfcXxX78Dll.dll?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240721%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240721T073227Z&X-Amz-Expires=600&X-Amz-Signature=978ba734f0c753d12591c6ee635cdc743ee0ca7e18ffd1a3fc4e9f95375afad2&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated

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

TLP:AMBER

GLESEC
COMPLETELY PERCEPTI

ASM-VP REPORT

GOAA 07/26/2024

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2024-07-21	APT41 Adds New Malware To Compromise Entities Across Multiple Sectors	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/apt41_adds_new_malware_to_compromise_entities_across_multiple_sectors_c50e649f-b6b8-4aac-932c-d0161e9e1fd7/840_browsing7defe0cc29d04b8d0f519b5008d30c09783fe0c63aad5ccb0950fc9a98406XxX76Dll.dll?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240721%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240721T073226Z&X-Amz-Expires=600&X-Amz-Signature=1635ec3a941d3c8981f919543b3f4ebad9b2b9c8ad388ffbde5a76f4e5d0fe8c&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-21	APT41 Adds New Malware To Compromise Entities Across Multiple Sectors	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/apt41_adds_new_malware_to_compromise_entities_across_multiple_sectors_c50e649f-b6b8-4aac-932c-d0161e9e1fd7/33fd050_browsing760e251ab932e5ca4311b494ef72cee157b20537ce773420845302e49XxX74Dll.dll?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240721%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240721T073226Z&X-Amz-Expires=600&X-Amz-Signature=543cbe824d1ced583da350c41184bac3b01442a30ee73de2f8dd4b1b5d0c1e87&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-21	APT41 Adds New Malware To Compromise Entities Across Multiple Sectors	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/apt41_adds_new_malware_to_compromise_entities_across_multiple_sectors_c50e649f-b6b8-4aac-932c-d0161e9e1fd7/22a50cea6ad6_browsing7a7e8582d2cd4cdc3eaaf57c0fbe8cd062a9b15710166e255a86XxX66Dll.dll?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240721%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240721T073219Z&X-Amz-Expires=600&X-Amz-Signature=d3ecfa21573c77e22e3e761881bb925c837e6d7dabc804a69c821145324cde39&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-21	APT41 Adds New Malware To Compromise Entities Across Multiple Sectors	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/apt41_adds_new_malware_to_compromise_entities_across_multiple_sectors_c50e649f-b6b8-4aac-932c-d0161e9e1fd7/c_browsing7dce6c950735bfcf2125be8eb1f3dd468eeb56a1c615c34f95bf38cb58b7d3aXxX56Dll.dll?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240721%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240721T073218Z&X-Amz-Expires=600&X-Amz-Signature=6abd6cae2349d726b6c0b2c453afc4c0b30f5f53873fe9a49afc1c68825a1af2&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-18	US Cert Alert - Peoples Republic of China PRC Ministry of State Security APT40 Tradecraft in Action	44,369_edr783a819a38909e89449495fb98c3f9ba07dd0d2fa55a24a560a89f21a86XxX175Txt.txt	Endpoint Security	IT55	Prevented
2024-07-18	US Cert Alert - Peoples Republic of China PRC Ministry of State Security APT40 Tradecraft in Action	b2_edr71e74ed44c3c405da858f29b6dfd4a99658dcac7bc83938079ad0dbbdf1b66XxX176Java.j ava	Endpoint Security	IT55	Prevented
2024-07-18	US Cert Alert - Peoples Republic of China PRC Ministry of State Security APT40 Tradecraft in Action	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/peoples_republic_of_china_prc_ministry_of_state_security_apt40_tradecraft_in_action_9c5c1ae1-be27-41b4-802a-65087a628f32/7c_browsing7acd87b47d405da4d6efa2c43599148e12c094970ba198905f0a165d79a78fXxX181Js.js?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Am z-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240718%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240718T072148Z&X-Amz-Expires=600 &X-Amz-Signature=233cfc39810e4532a53fa015b6f33f68bed43cd12ee4d364fe9b27dcb20c483 5&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-18	US Cert Alert - Peoples Republic of China PRC Ministry of State Security APT40 Tradecraft in Action	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/peoples_republic_of_china_prc_ministry_of_state_security_apt40_tradecraft_in_action_9c5c1ae1-be27-41b4-802a-65087a628f32/9_browsing7daa26c59e0e151f66872147ccd30dd1815bc6e63ec40c288130c6e8a6ea992XxX177Js.js?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Am z-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240718%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240718T072148Z&X-Amz-Expires=600 &X-Amz-Signature=fc4c454fbf245d53301ffaa221324c29ca2a5019504c2d0659d868e0092b9ce a&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-18	Cert IL Alert - active phishing campaign in Israel	f39c6_edr7cc82d5766d776ad787c56d48627995cbf3797d7603b790f27cd31cb413XxX1Exe.exe	Endpoint Security	IT55	Prevented
2024-07-17	BianLian Ransomware Group Continues To Adapt	72d91293ff1a9158_edr7af3997081f65eac819d2ff73655837dc68a447d371ca2f1XxX19Exe.exe	Endpoint Security	IT55	Prevented
2024-07-17	BianLian Ransomware Group Continues To Adapt	834ab96263cca_edr7b01b3ae6549a9811b56204e714402215ce37fb602732b981d1XxX25Exe.exe	Endpoint Security	IT55	Prevented
2024-07-17	BianLian Ransomware Group Continues To Adapt	3b309c0_edr76c26f27f42dbab8c89f05df51c414e87529251dc2d9946e7bc694f29XxX21Exe.exe	Endpoint Security	IT55	Prevented

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

TLP:AMBER

ASM-VP REPORT

GOAA 07/26/2024

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2024-07-17	BianLian Ransomware Group Continues To Adapt	b12be86af46b026_edr7d86fcacef0a58bad0d157a7a044f89a453082b32503bd3c0XxX23Elf.elf	Endpoint Security	IT55	Prevented
2024-07-17	BianLian Ransomware Group Continues To Adapt	hxxp://104.238.61.20	Web Gateway	IT55	Offline/Removed
2024-07-17	BianLian Ransomware Group Continues To Adapt	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/bianlian_ransomware_group_continues_to_adapt_3fab5dff-c294-4d48-b82f-fd62461303af/f9421165e4a62c_browsing7a1941b7b3fa73ac6f2149e7ffab3a6a622406baabf1933a2eXxX27Dll .dll?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Am z-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240717%2Feu-west-1%2Fs3%2Faws4_request&X-A mz-Date=20240717T074537Z&X-Amz-Expires=600&X-Amz-Signature=d8eddb3bdb9cb40898e63581fffbca21872803b503c7a8737930fb6a42f7c408&X-Amz-SignedHeaders=host&x-id=GetObj ect	Web Gateway	IT55	Penetrated
2024-07-17	MuddyWater APT Group Releases BugSleep Backdoor Across The Middle East	c23f1_edr7b92b13464a570f737a86c0960d5106868aaa5eac2f2bac573c3314eb0fXxX19Msi.msi	Endpoint Security	IT55	Penetrated
2024-07-17	MuddyWater APT Group Releases BugSleep Backdoor Across The Middle East	90f94d98386c1_edr79a1b98a1f082b0c7487b22403d8d5eb3db6828725d14392dedXxX25Msi.msi	Endpoint Security	IT55	Penetrated
2024-07-17	MuddyWater APT Group Releases BugSleep Backdoor Across The Middle East	fb58c54a6d0ed24e85b213f0c48_edr7f8df05e421d7b07bd2bece3a925a855be93aXxX31Msi.msi	Endpoint Security	IT55	Penetrated
2024-07-17	MuddyWater APT Group Releases BugSleep Backdoor Across The Middle East	20aaeac4dbea89b50d011e9becdf51afc1a1a1f254a5f494b80c108fd3c_edr7f61aXxX33Msi.msi	Endpoint Security	IT55	Penetrated
2024-07-17	MuddyWater APT Group Releases BugSleep Backdoor Across The Middle East	31,591fcf6_edr77a2da2834d2cc99a00ab500918b53900318f6b19ea708eba2b38abXxX45Zip.zip	Endpoint Security	IT55	Penetrated
2024-07-17	MuddyWater APT Group Releases BugSleep Backdoor Across The Middle East	88_edr788208316a6cf4025dbabbef703f51d77d475dc735bf826b8d4a13bbd6a3eeXxX59Zip.zip	Endpoint Security	IT55	Penetrated
2024-07-17	MuddyWater APT Group Releases BugSleep Backdoor Across The Middle East	942_edr78fa01900fdbfb58d2e373895c045c69c01915edc5349cd6f3e5b7130c472XxX35Exe.exe	Endpoint Security	IT55	Prevented
2024-07-17	MuddyWater APT Group Releases BugSleep Backdoor Across The Middle East	b8_edr7037447445555ad841f922995cef5dbca11da22565195d05529f5f9095fbfcaXxX37Exe.exe	Endpoint Security	IT55	Prevented
2024-07-17	MuddyWater APT Group Releases BugSleep Backdoor Across The Middle East	73c6_edr77dd3b264e7eb80e26e78ac9df1dba30915b5ce3b1bc1c83db52b9c6b30eXxX41Exe.exe	Endpoint Security	IT55	Prevented
2024-07-17	MuddyWater APT Group Releases BugSleep Backdoor Across The Middle East	e_edr7896ccb82ae35e1ee5949b187839faab0b51221d510b25882bbe711e57c16d2XxX49Zip.zip	Endpoint Security	IT55	Prevented

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

TLP:AMBER

GLESEC
COMPLETELY PERCEPTI

ASM-VP REPORT

GOAA 07/26/2024

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2024-07-17	MuddyWater APT Group Releases BugSleep Backdoor Across The Middle East	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/muddywater_apt_group_releases_bugsleep_backdoor_across_the_middle_east_fc26dd82-ead3-4c1e-a16a-f1243b092248/1c094_browsing7258ddb608c879333c941f0738a7f279bc14630f2c8877b82b8046acf91XxX63Zip.zip?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240717%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240717T073605Z&X-Amz-Expires=600&X-Amz-Signature=9997754def165c8c397732c0eb97b54e7fba875c14de4062effa580a36a53d8e&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-17	MuddyWater APT Group Releases BugSleep Backdoor Across The Middle East	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/muddywater_apt_group_releases_bugsleep_backdoor_across_the_middle_east_fc26dd82-ead3-4c1e-a16a-f1243b092248/c80c8dd_browsing7be3ccf18e327355b880afb5a24d5a0596939458fb13319e05c4d43e9XxX61Zip.zip?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240717%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240717T073604Z&X-Amz-Expires=600&X-Amz-Signature=5503873c66550d457222ff81e856094791600f6a395af07411dbea44b8c697f8&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-17	MuddyWater APT Group Releases BugSleep Backdoor Across The Middle East	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/muddywater_apt_group_releases_bugsleep_backdoor_across_the_middle_east_fc26dd82-ead3-4c1e-a16a-f1243b092248/7e14ca8cb_browsing7980e85aff4038f489442eace33530fd02e2b9c382a4b6907601beeXxX57Zip.zip?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240717%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240717T073557Z&X-Amz-Expires=600&X-Amz-Signature=f4938aab7bb9b47988149b98b395baef27b62b3e01eeaa32858c05c9db45cf73&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-17	MuddyWater APT Group Releases BugSleep Backdoor Across The Middle East	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/muddywater_apt_group_releases_bugsleep_backdoor_across_the_middle_east_fc26dd82-ead3-4c1e-a16a-f1243b092248/8fbd3_browsing74d4659efdc5b5a57ff4168236aeaab6dae4af6b92d99ac28e05f04e5c1XxX55Zip.zip?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240717%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240717T073556Z&X-Amz-Expires=600&X-Amz-Signature=1da8222031784 87ef16314c98c9cca68a14625f99b6b45e11b1e9455468ba612&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-17	MuddyWater APT Group Releases BugSleep Backdoor Across The Middle East	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/muddywater_apt_group_releases_bugsleep_backdoor_across_the_middle_east_fc26dd82-ead3-4c1e-a16a-f1243b092248/c884531_browsing78f5f6aaab0cab2e126b0db27b25a5cfe6905914cc430f6f100b7675cXxX53Zip.zip?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240717%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240717T073556Z&X-Amz-Expires=600&X-Amz-Signature=fb5878fd8f1de0556b2bf2e3204e3bc2e840c59a8148e14ffa367ae5688385f0&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-17	MuddyWater APT Group Releases BugSleep Backdoor Across The Middle East	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/muddywater_apt_group_releases_bugsleep_backdoor_across_the_middle_east_fc26dd82-ead3-4c1e-a16a-f1243b092248/4064e4bb9a425494804_browsing7858301f2b75e276a878321b0cc02710e1738b42548caXxX51Zip.zip?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240717%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240717T073556Z&X-Amz-Expires=600&X-Amz-Signature=e4c96c20ec8b9cf306b99333f9e8404823e3c6db41d89a970b571f52b51f9418&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-17	MuddyWater APT Group Releases BugSleep Backdoor Across The Middle East	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/muddywater_apt_group_releases_bugsleep_backdoor_across_the_middle_east_fc26dd82-ead3-4c1e-a16a-f1243b092248/424a9c85f9_browsing7aa1aece9480bd658266c366a60ff1d62c31b87ddc15a1913c10e4XxX47Zip.zip?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240717%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240717T073554Z&X-Amz-Expires=600&X-Amz-Signature=c87cff5528c9161f0f84bcb87e391005737b1b0ed7553913a2931382841e52b8&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-17	MuddyWater APT Group Releases BugSleep Backdoor Across The Middle East	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/muddywater_apt_group_releases_bugsleep_backdoor_across_the_middle_east_fc26dd82-ead3-4c1e-a16a-f1243b092248/960d4c9e_browsing79e751be6cad470e4f8e1d3a2b11f76f47597df8619ae41c96ba5809XxX43Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240717%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240717T073553Z&X-Amz-Expires=600&X-Amz-Signature=a9ed360c1076c9472576e9f28d51047bd1c0a3464e7e935fdec51b3f02aa45b9&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-17	MuddyWater APT Group Releases BugSleep Backdoor Across The Middle East	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/muddywater_apt_group_releases_bugsleep_backdoor_across_the_middle_east_fc26dd82-ead3-4c1e-a16a-f1243b092248/5df_browsing724c220aed7b4878a2a557502a5cefee736406e25ca48ca11a70608f3a1c0XxX39Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240717%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240717T073553Z&X-Amz-Expires=600&X-Amz-Signature=14ccf0dae5fdd1b456d8c05113609b3f473059a252f74b17feddacb97726a363&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-17	MuddyWater APT Group Releases BugSleep Backdoor Across The Middle East	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/muddywater_apt_group_releases_bugsleep_backdoor_across_the_middle_east_fc26dd82-ead3-4c1e-a16a-f1243b092248/55af6a90ac8863f2_browsing7b3fcaa416a0f1e4ff02fb42aa46a7274c6b76aa000aacc2XxX29Msi.msi?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240717%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240717T073543Z&X-Amz-Expires=600&X-Amz-Signature=38c5a970d4390ccd9c04af00d48eb22973e82583a52819dedb41e880e85a36a1&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated

LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

TLP:AMBER

GLESEC
COMPLETELY PERCEPTI

ASM-VP REPORT

GOAA 07/26/2024

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2024-07-17	MuddyWater APT Group Releases BugSleep Backdoor Across The Middle East	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/mud dywater_apt_group_releases_bugsleep_backdoor_across_the_middle_east_fc26dd82-ead 3-4c1e-a16a-f1243b092248/39da_browsing7cc7c627ea4c46f75bcec79e5669236e6b43657dca d099e1b9214527670eXxX27Msi.msi?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sh a256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240717%2Feu-west -1%2Fs3%2Faws4_request&X-Amz-Date=20240717T073541Z&X-Amz-Expires=600&X-Amz-Signa ture=af479c50833e2e8ac9a8967feddb6fe9378b67b8f7e012515ed002716dafba1a&X-Amz-Sign edHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-17	MuddyWater APT Group Releases BugSleep Backdoor Across The Middle East	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/mud dywater_apt_group_releases_bugsleep_backdoor_across_the_middle_east_fc26dd82-ead 3-4c1e-a16a-f1243b092248/7e6b04e1_browsing7ae273700cef4dc08349af949dbd4d3418159d 607529ae31285e18f7XxX23Msi.msi?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sh a256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240717%2Feu-west -1%2Fs3%2Faws4_request&X-Amz-Date=20240717T073539Z&X-Amz-Expires=600&X-Amz-Signa ture=6eaeaf44d4835b859eb7a95ba9a6000fb980e4fd1becc70d8818e6cc283411e6&X-Amz-Sign edHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-17	MuddyWater APT Group Releases BugSleep Backdoor Across The Middle East	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/mud dywater_apt_group_releases_bugsleep_backdoor_across_the_middle_east_fc26dd82-ead 3-4c1e-a16a-f1243b092248/ff2ae62ba88e_browsing7068fa142bbe67d7b9398e8ae737a43cf3 6ace1fcf809776c909XxX21Msi.msi?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sh a256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240717%2Feu-west -1%2Fs3%2Faws4_request&X-Amz-Date=20240717T073538Z&X-Amz-Expires=600&X-Amz-Signa ture=7cdb798ff8d4a03cf6456d7fda0bc4bde8f49dd30fb9eeedbbd5312fbed998cf&X-Amz-Sign edHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
N/A	MuddyWater APT Group Releases BugSleep Backdoor Across The Middle East	31,591fcf6_mail77a2da2834d2cc99a00ab500918b53900318f6b19ea708eba2b38abXxX45Zip.zip	Email Gateway	skywatch@goaa.org	Prevented
N/A	MuddyWater APT Group Releases BugSleep Backdoor Across The Middle East	e_mail7896ccb82ae35e1ee5949b187839faab0b51221d510b25882bbe711e57c16d2XxX49Zip.zi p	Email Gateway	skywatch@goaa.org	Prevented
N/A	MuddyWater APT Group Releases BugSleep Backdoor Across The Middle East	88_mail788208316a6cf4025dbabbef703f51d77d475dc735bf826b8d4a13bbd6a3eeXxX59Zip.zip	Email Gateway	skywatch@goaa.org	Prevented
2024-07-16	More Akira-related IOCs are spotted in the wild	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/mor e_akira-related_iocs_are_spotted_in_the_wild_fe6d82bc-2544-42cd-a62b-22e9d378156 6/0b5b31af5956158bfbd14f6cbf4f1bca23c5d16a40dbf3_browsing758f3289146c565f43XxX1E xe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240716%2Feu-west-1%2Fs3%2Faws4_request&X -Amz-Date=20240716T092021Z&X-Amz-Expires=600&X-Amz-Signature=d9c076e2872c30a6cd3 c9352dfc99935cdd39972b2aee3d2f7e952ca1c9febdb&X-Amz-SignedHeaders=host&x-id=GetO bject	Web Gateway	IT55	Penetrated
2024-07-16	ShadowRoot Ransomware Targeting Turkish Businesses	2,960a2d4d2fd6b_edr7b85b8e3ea4c86ec0c13b93bfd3754a7e772a2c74f564b0009XxX42Exe.exe	Endpoint Security	IT55	Prevented
2024-07-16	ShadowRoot Ransomware Targeting Turkish Businesses	1be40e8ac11d6da8045bd03be3e5_edr7f0b36b6ab7dc390ff7208a0a4e7688b6b94XxX43Exe.exe	Endpoint Security	IT55	Prevented
2024-07-15	Increase In The Exploitation Of Microsoft SmartScreen Vulnerability CVE-2024-21412	a31f222fc28322_edr7f5e7988d1ad9c0aecd66d58bb7b4d8518ae23e110308dbf91XxX9Exe.exe	Endpoint Security	IT55	Prevented
2024-07-15	Increase In The Exploitation Of Microsoft SmartScreen Vulnerability CVE-2024-21412	a024a18e2_edr7707738adcd7b5a740c5a93534b4b8c9d3b947f6d85740af19d17d0XxX10Exe.exe	Endpoint Security	IT55	Penetrated
2024-07-15	Increase In The Exploitation Of Microsoft SmartScreen Vulnerability CVE-2024-21412	2,460e_edr7590e09af09ced6f75c001a9066c18629d956edbe8041f08cd21b7528b2XxX16Lnk.lnk	Endpoint Security	IT55	Prevented
2024-07-15	Increase In The Exploitation Of Microsoft SmartScreen Vulnerability CVE-2024-21412	4eccb_edr7813cee8c8039424aebf69f4269d4a6c2c72d81a001254bcdce80034555XxX19Lnk.lnk	Endpoint Security	IT55	Prevented

TLP:AMBER

GLESEC
COMPLETELY PERCEPTI

ASM-VP REPORT

GOAA 07/26/2024

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2024-07-15	Increase In The Exploitation Of Microsoft SmartScreen Vulnerability CVE-2024-21412	0e2263d4f239a5c39960ffa6b6b688faa_edr7fc3075e130fe0d4599d5b95ef20647XxX11Exe.exe	Endpoint Security	IT55	Prevented
2024-07-15	Increase In The Exploitation Of Microsoft SmartScreen Vulnerability CVE-2024-21412	aceee450c55d616_edr71c2d3d154b5f77e7f99688b6da8a8f3256a4bae2cdb76a4cXxX26Lnk.lnk	Endpoint Security	IT55	Prevented
2024-07-15	Increase In The Exploitation Of Microsoft SmartScreen Vulnerability CVE-2024-21412	268a0de2468_edr726a106fd92563a846e764f2ba313e37b5fc0cf76171b0a363f6fXxX17Lnk.lnk	Endpoint Security	IT55	Prevented
2024-07-15	Increase In The Exploitation Of Microsoft SmartScreen Vulnerability CVE-2024-21412	81e89_edr754ae2324c684fce71acafc30f8085870be947e7a76971b4fec1b24b5d1XxX23Lnk.lnk	Endpoint Security	IT55	Prevented
2024-07-15	Increase In The Exploitation Of Microsoft SmartScreen Vulnerability CVE-2024-21412	4_edr73abb2c272295473e5556ec7dec06f2018c0a67f208d8ab33de1fb6d40895f5XxX18Lnk.lnk	Endpoint Security	IT55	Prevented
2024-07-15	Increase In The Exploitation Of Microsoft SmartScreen Vulnerability CVE-2024-21412	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/increase_in_the_exploitation_of_microsoft_smartscreen_vulnerability_cve-2024-21412_0211ec16-3565-4729-9447-8e445ae4ee88/7ee31fa89e9e68f20004bdc31f8f05a95861b6c6_browsing78bfa3b57f09fdfad9ef5290XxX22Lnk.lnk?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240715%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240715T060717Z&X-Amz-Expires=600&X-Amz-Signature=e29b72877210d7a5570f5afd2277e875d88186f01c892312e2f74d952c5ef57b&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-15	Increase In The Exploitation Of Microsoft SmartScreen Vulnerability CVE-2024-21412	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/increase_in_the_exploitation_of_microsoft_smartscreen_vulnerability_cve-2024-21412_0211ec16-3565-4729-9447-8e445ae4ee88/6481462f15ad4213f83a3d28304f14496bae1feb8580056959a65_browsing7d0ee8981dbXxX21Lnk.lnk?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240715%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240715T060716Z&X-Amz-Expires=600&X-Amz-Signature=d46db1dee533debd431b21301edc55303d37220807f55916e00a89df1482249f&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-15	Increase In The Exploitation Of Microsoft SmartScreen Vulnerability CVE-2024-21412	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/increase_in_the_exploitation_of_microsoft_smartscreen_vulnerability_cve-2024-21412_0211ec16-3565-4729-9447-8e445ae4ee88/58e2b_browsing766dec37cc5fcfb63bc16d69627cd87e7e46f0b9f48899889479f12611eXxX20Lnk.lnk?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240715%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240715T060716Z&X-Amz-Expires=600&X-Amz-Signature=59e36d947c3a994eba6f93aa90529a27d22d952dd54fabca0fa78d709146f3ea&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-14	Resurrecting Internet Explorer Threat Actors Using Zero-day Tricks in Internet Shortcut File to Lure Victims CVE-2024-38112	hxxps://cbmelipilla.cl	Web Gateway	IT55	Blocked
2024-07-14	Resurrecting Internet Explorer Threat Actors Using Zero-day Tricks in Internet Shortcut File to Lure Victims CVE-2024-38112	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/resurrecting_internet_explorer_threat_actors_using_zero-day_tricks_in_internet_shortcut_file_to_lure_victims_cve-2024-38112_5e2c3d19-9fd2-4aad-858f-c73d2fcd9f32/bd_browsing710ee53ef3ad872f3f0678117050608a8e073c87045a06a86fb4a7f0e4eff0XxX164Txt .txt?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240714%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240714T113659Z&X-Amz-Expires=600&X-Amz-Signature=c252f49767f87f77b7add545afad681d73dec893e070a5ccfc6209c2bba84309&X-Amz-SignedHeaders=host&x-id=GetObj ect	Web Gateway	IT55	Penetrated
2024-07-14	Resurrecting Internet Explorer Threat Actors Using Zero-day Tricks in Internet Shortcut File to Lure Victims CVE-2024-38112	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/resurrecting_internet_explorer_threat_actors_using_zero-day_tricks_in_internet_shortcut_file_to_lure_victims_cve-2024-38112_5e2c3d19-9fd2-4aad-858f-c73d2fcd9f32/65142c8f490839a60f490_browsing7ab8f28dd9db4258e1cfab2d48e89437ef2188a6e94XxX163Txt .txt?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240714%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240714T113658Z&X-Amz-Expires=600&X-Amz-Signature=939889353b38ab0e28610c80507d6682c9b1fe729b93e07b32c2af53397b43e3&X-Amz-SignedHeaders=host&x-id=GetObj ect	Web Gateway	IT55	Penetrated

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

TLP:AMBER

GLESEC
COMPLETELY PERCEPTI

ASM-VP REPORT

GOAA 07/26/2024

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2024-07-14	Dissecting GootLoader With Nodejs	c853d91501111a8_edr73a027bd3b9b4dab9dd940e89fcfec51efbb6f0db0ba6687bXxX26Js.js	Endpoint Security	IT55	Prevented
2024-07-14	Dissecting GootLoader With Nodejs	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/dissecting_gootloader_with_nodejs_6e62c6bd-88ff-4cf0-b89c-011f0f83f004/b939ec944_browsing7140804710f0ce2a7d33ec89f758ff8e7caab6ee38fe2446e3ac988XxX25Js.js?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240714%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240714T113544Z&X-Amz-Expires=600&X-Amz-Signature=86402a25af8768fe49ca3431f1347df2c23d7761fd4ce728edef926b78ee9d3f&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-14	Silver Fox Threat Group Attack Activities	7_edr7a07a99b53b4f8d8ced56b3e80f3ccaba52692ab7865c1dda3b752739e966b7XxX15Exe.exe	Endpoint Security	IT55	Prevented
2024-07-14	Silver Fox Threat Group Attack Activities	1bf9dffebe93a422210ac261_edr7c0de67f975827a1cbe304d79ca93b959fb4628fXxX21Exe.exe	Endpoint Security	IT55	Prevented
2024-07-14	Silver Fox Threat Group Attack Activities	a_edr790c7e34f45b21f34838260282b8af4b2850ec5e9add93aa3baad8d530cca8dXxX19Ps1.ps1	Endpoint Security	IT55	Prevented
2024-07-14	Silver Fox Threat Group Attack Activities	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/silver_fox_threat_group_attack_activities_f22c56b3-41f4-4555-bdf0-4416f5d5c642/6_browsing7990f3893b800811f36b4d9982e0811f49d0d91791f827d80cf6b8bc258e0ebXxX17Dll.dl l?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240714%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240714T071946Z&X-Amz-Expires=600&X-Amz-Signature=19c5097b04091b99e3180693e6211219c239e021cb016493261d2bca945e138e&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-10	Mallox Ransomware Linux Variant Decryptor Found	e1d8095b39af0901618fa2b0d2f620d391f16_edr7045f6d2e61efca6797f5a322fdXxX12Python. python	Endpoint Security	IT55	Prevented
2024-07-10	Mallox Ransomware Linux Variant Decryptor Found	hxxp://91.215.85.142	Web Gateway	IT55	Offline/Removed
2024-07-10	Mallox Ransomware Linux Variant Decryptor Found	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/mallox_ransomware_linux_variant_decryptor_found_86425878-748d-46f8-a347-18870b072b6c/23ba80_browsing78df63ebb313f2f2a2f24dab840e068ddd5cc54bb661db7d010954d2fcXxX18Elf.elf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240710%2Feu-west-1%2Fs3%2Faws4_request& X-Amz-Date=20240710T135952Z&X-Amz-Expires=600&X-Amz-Signature=1db03caf1a8c7054c674cd7e23ae27d5b2c997739fe9d1218bb4a9c4e96d372d&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-10	GrimResource - Microsoft Management Console for initial access and evasion	14bcb_edr7196143fd2b800385e9b32cfacd837007b0face71a73b546b53310258bbXxX1Xml.xml	Endpoint Security	IT55	Prevented
2024-07-10	GrimResource - Microsoft Management Console for initial access and evasion	4cb5_edr75bc114d39f8f1e66d6e7c453987639289a28cd83a7d802744cd99087fd7XxX2Dll.dll	Endpoint Security	IT55	Prevented
2024-07-10	GrimResource - Microsoft Management Console for initial access and evasion	14bcb_mail7196143fd2b800385e9b32cfacd837007b0face71a73b546b53310258bbXxX1Xml.xml	Email Gateway	skywatch@goaa.org	Penetrated
2024-07-10	GrimResource - Microsoft Management Console for initial access and evasion	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/grimresource_-_microsoft_management_console_for_initial_access_and_evasion_afba1385 -6119-42c2-92d2-e726eed51d4a/c1bba_browsing723f79282dceed4b8c40123c72a5dfcf4e3ff7dd48db8cb6c8772b60b88XxX3Dll.dll?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240710%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240710T135027Z&X-Amz-Expires=600&X-Amz-Signature=bd24f17647a2b573d52a0b4f13dbf88954e28d809f2c7b0d08626a90255a7142&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-09	Mekotio Banking Trojan Threatens Financial Systems in Latin America	a_edr7112aa5b398fc7a77100164c818b5e17612d828320b4e3e1f895e56b4fd6797XxX1Dll.dll	Endpoint Security	IT55	Prevented
2024-07-09	Mekotio Banking Trojan Threatens Financial Systems in Latin America	e082dc1c11afff40efe2cf92e36ac3_edr7129b78320b5cc656f4b80488307770eabXxX7Pdf.pdf	Endpoint Security	IT55	Prevented

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

ASM-VP REPORT

GOAA 07/26/2024

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2024-07-09	Mekotio Banking Trojan Threatens Financial Systems in Latin America	b6a82_edr774b81a965033716351d92dd0a75f494069b4b4436d21327c06c917e6e0XxX5Pdf.pdf	Endpoint Security	IT55	Prevented
2024-07-09	Mekotio Banking Trojan Threatens Financial Systems in Latin America	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/mekotio_banking_trojan_threatens_financial_systems_in_latin_america_43592ade-3b88-4cc8-8ce7-2d504db5127e/008c_browsing7e556beba4a5d026211259114ba686013b5fd5f9cb9e677b2641bd2c2fc5XxX4Pdf.pdf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240709T122227Z&X-Amz-Expires=600&X-Amz-Signature=1a7e888573a980faadff4f469e32632aab84e158865b324864828dfa9b4dc3f7&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-09	Mekotio Banking Trojan Threatens Financial Systems in Latin America	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/mekotio_banking_trojan_threatens_financial_systems_in_latin_america_43592ade-3b88-4cc8-8ce7-2d504db5127e/439eecb230fb53b81_browsing7ae535d6a6d978066134b4b52e49e065e9ddeff5f2bbbd3XxX2Dll.dll?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240709T122219Z&X-Amz-Expires=600&X-Amz-Signature=b646911ea2c8f3f39674c1bf48d535cf7fd018c74369c72c464b9f745a26260c&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
N/A	Mekotio Banking Trojan Threatens Financial Systems in Latin America	b6a82_mail774b81a965033716351d92dd0a75f494069b4b4436d21327c06c917e6e0XxX5Pdf.pdf	Email Gateway	skywatch@goaa.org	Prevented
N/A	Mekotio Banking Trojan Threatens Financial Systems in Latin America	e082dc1c11afff40efe2cf92e36ac3_mail7129b78320b5cc656f4b80488307770eabXxX7Pdf.pdf	Email Gateway	skywatch@goaa.org	Prevented
2024-07-09	Turla A Master of Deception	b6abbeab6e000036c6cdffc5_edr7c096d796397263e280ea264eba73ac5bab39441XxX76Xml.xml	Endpoint Security	IT55	Prevented
2024-07-09	Turla A Master of Deception	cac4d4364d20fa343bf681f6544b31995a5_edr7d8f69ee606c4675db60be5ae8775XxX78Lnk.lnk	Endpoint Security	IT55	Prevented
2024-07-09	Turla A Master of Deception	hxxp://files.philbendeck.com/article/	Web Gateway	IT55	Offline/Removed
2024-07-09	Turla A Master of Deception	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/turla_a_master_of_deception_5a1a2df0-8d4d-4851-837f-2f4667179131/c2618fb013135485f9f9aa2_browsing7983df3371dfdcb7beecde86d02cee0c258d5ed7fXxX77Zip.zip?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240709T072910Z&X-Amz-Expires=600&X-Amz-Signature=9e5655cc19e6689d1b870592c68ccdc485b95b87f43ad4b412589a37e20adf7e&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-09	Turla A Master of Deception	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/turla_a_master_of_deception_5a1a2df0-8d4d-4851-837f-2f4667179131/7091ce9_browsing7fb5906680c1b09558bafdf9681a81f5f524677b90fd0f7fc0a05bc00XxX75Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240709T072908Z&X-Amz-Expires=600&X-Amz-Signature=0f8dd89ab0c02bf4c5c555e8dbd7f04f8702b521a40406fce3bf583cbca77a6d&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-08	Mekotio Banker - Improved Stealth and Ancient Encryption	Mekot1_edrZip.zip	Endpoint Security	IT55	Prevented
2024-07-08	Mekotio Banker - Improved Stealth and Ancient Encryption	Mekot5_edrBat.bat	Endpoint Security	IT55	Prevented
2024-07-08	Mekotio Banker - Improved Stealth and Ancient Encryption	Mekot12_edrBat.bat	Endpoint Security	IT55	Prevented
2024-07-08	Mekotio Banker - Improved Stealth and Ancient Encryption	Mekot9_edrBat.bat	Endpoint Security	IT55	Prevented
2024-07-08	Mekotio Banker - Improved Stealth and Ancient Encryption	Mekot6_edrBat.bat	Endpoint Security	IT55	Prevented

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

TLP:AMBER

GLESEC
COMPLETELY PERCEPTI

ASM-VP REPORT

GOAA 07/26/2024

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2024-07-08	Mekotio Banker - Improved Stealth and Ancient Encryption	Mekot11_edrBat.bat	Endpoint Security	IT55	Prevented
2024-07-08	Mekotio Banker - Improved Stealth and Ancient Encryption	Mekot4_edrBat.bat	Endpoint Security	IT55	Prevented
2024-07-08	Mekotio Banker - Improved Stealth and Ancient Encryption	Mekot10_edrBat.bat	Endpoint Security	IT55	Prevented
2024-07-08	Mekotio Banker - Improved Stealth and Ancient Encryption	Mekot3_edrBat.bat	Endpoint Security	IT55	Prevented
2024-07-08	Mekotio Banker - Improved Stealth and Ancient Encryption	Mekot1_edrBat.bat	Endpoint Security	IT55	Prevented
2024-07-08	Mekotio Banker - Improved Stealth and Ancient Encryption	hxxp://40.90.192.58/factura0001450000g9.zip	Web Gateway	IT55	Offline/Removed
2024-07-08	Mekotio Banker - Improved Stealth and Ancient Encryption	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/mek otio_banker_-_improved_stealth_and_ancient_encryption_4e967f25-7ece-4960-9847-52ab2bfdf231/Mekot8_browsingBat.bat?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240708%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240708T131335Z&X-Amz-Expires=600&X-Amz-Signature=74b8ab3c53c7f24eed555c86f6acbd35eb1a0898393adb50c759ab9da7d505d2&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-08	Mekotio Banker - Improved Stealth and Ancient Encryption	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/mek otio_banker_-_improved_stealth_and_ancient_encryption_4e967f25-7ece-4960-9847-52ab2bfdf231/Mekot2_browsingBat.bat?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240708%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240708T131325Z&X-Amz-Expires=600&X-Amz-Signature=ec679927e7ffb049037bbda8866dfa6b386d365b4d5dc399952100aaf86352a3&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-08	Mekotio Banker - Improved Stealth and Ancient Encryption	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/mek otio_banker_-_improved_stealth_and_ancient_encryption_4e967f25-7ece-4960-9847-52ab2bfdf231/Mekot_browsing7Bat.bat?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240708%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240708T131324Z&X-Amz-Expires=600&X-Amz-Signature=bfaaf575053e799b7de16f404e88fac20e499da65f118f1ed20d3f79e70e68d0&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-08	Turning Jenkins Into a Cryptomining Machine From an Attackers Perspective	5_edr7fedfb431a717031f454d4fb2809d1f6d432a9edd900b07f0b9f9aca7fb3597XxX28Elf.elf	Endpoint Security	IT55	Prevented
2024-07-07	REGRESSHION CVE-2024-6387 A TARGETED EXPLOIT IN THE WILD	219f9b69_edr73c92dfe86b1018344b2113fd79d138509204dda6a5b5839de4b2de6XxX1Zip.zip	Endpoint Security	IT55	Prevented
2024-07-07	REGRESSHION CVE-2024-6387 A TARGETED EXPLOIT IN THE WILD	hxxp://108.174.58.28	Web Gateway	IT55	Penetrated
N/A	REGRESSHION CVE-2024-6387 A TARGETED EXPLOIT IN THE WILD	219f9b69_mail73c92dfe86b1018344b2113fd79d138509204dda6a5b5839de4b2de6XxX1Zip.zip	Email Gateway	skywatch@goaa.org	Failed
2024-07-07	New Threat A Deep Dive Into the Zergeca Botnet	0dbbe5616de_edr71c5753768de555203fb9eb2f1e72a8cb5bdce0559bc5cdfa3b2eXxX5Elf.elf	Endpoint Security	IT55	Prevented
2024-07-07	New Threat A Deep Dive Into the Zergeca Botnet	b55b194_edr7a11de7ee2cb3aaede12ce15c85abf2b607d1ebd8f5ed56e3a6ef7c43XxX11Elf.elf	Endpoint Security	IT55	Prevented

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

TLP:AMBER

GLESEC
COMPLETELY PERCEPTI

ASM-VP REPORT

GOAA 07/26/2024

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2024-07-07	New Threat A Deep Dive Into the Zergeca Botnet	7e62e3e8911c0cb19df34_edr77df0603fddeff82223e1cc6da7fb1698f512ff2cd2XxX6Elf.elf	Endpoint Security	IT55	Prevented
2024-07-07	New Threat A Deep Dive Into the Zergeca Botnet	hxxp://84.54.51.82	Web Gateway	IT55	Offline/Removed
2024-07-07	New Threat A Deep Dive Into the Zergeca Botnet	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/new_threat_a_deep_dive_into_the_zergeca_botnet_20220833-98bf-4194-849c-b14d387c7fda/6b81d548c0fbd_browsing7a2275bb0d29deca0de96c1584ce7aadaf4f5dac3cb28ee9c29XxX9El f.elf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-A mz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240707%2Feu-west-1%2Fs3%2Faws4_request&X- Amz-Date=20240707T062054Z&X-Amz-Expires=600&X-Amz-Signature=ce35176b176125c46ee5 02d5cf58af985a4288414551989ff4c3c515a6c83ee9&X-Amz-SignedHeaders=host&x-id=GetOb ject	Web Gateway	IT55	Penetrated
2024-07-07	New Threat A Deep Dive Into the Zergeca Botnet	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/new_threat_a_deep_dive_into_the_zergeca_botnet_20220833-98bf-4194-849c-b14d387c7fda/cea6e4aa15d_browsing7c6a2b2c794a660afaf96d43462e0b74436600a2c8a2288ad0c27XxX8El f.elf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-A mz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240707%2Feu-west-1%2Fs3%2Faws4_request&X- Amz-Date=20240707T062052Z&X-Amz-Expires=600&X-Amz-Signature=967eb3b1cf53d84fa034 2786b6470c552de497b3de042b4c9f1ca40dedc856f1&X-Amz-SignedHeaders=host&x-id=GetOb ject	Web Gateway	IT55	Penetrated
2024-07-07	New Threat A Deep Dive Into the Zergeca Botnet	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/new_threat_a_deep_dive_into_the_zergeca_botnet_20220833-98bf-4194-849c-b14d387c7fda/2e9df898_browsing7212300815928e0426e9358b1380a1eaba38270d03dd69e421686b5bXxX7El f.elf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-A mz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240707%2Feu-west-1%2Fs3%2Faws4_request&X- Amz-Date=20240707T062052Z&X-Amz-Expires=600&X-Amz-Signature=5e30441e9e8665780e12 a15d7c0fd62874f07d911ab2e221560d86bc8e054c9a&X-Amz-SignedHeaders=host&x-id=GetOb ject	Web Gateway	IT55	Penetrated
2024-07-07	New Threat A Deep Dive Into the Zergeca Botnet	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/new_threat_a_deep_dive_into_the_zergeca_botnet_20220833-98bf-4194-849c-b14d387c7fda/7db9189afd00c2b60b_browsing7f892ef1b86d040fb1cf02145c7d2e414ef77ba3335c11XxX3El f.elf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-A mz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240707%2Feu-west-1%2Fs3%2Faws4_request&X- Amz-Date=20240707T062041Z&X-Amz-Expires=600&X-Amz-Signature=6cd3b921e5af9ae4e73a 75ceea1076bbf18e38cc8bb814bd23195e1796279a2f&X-Amz-SignedHeaders=host&x-id=GetOb ject	Web Gateway	IT55	Penetrated
2024-07-04	RisePro Information Stealer	222,932_edr7fa653ffd07f11773ee22eb00e580b6824ce122a1e788f19859aa9dca2XxX1Exe.exe	Endpoint Security	IT55	Prevented
2024-07-04	RisePro Information Stealer	7_edr7e97faca59d8de34ddc7272791efac41da9ff5b7b175a99e09a255e2701d725XxX7Exe.exe	Endpoint Security	IT55	Prevented
2024-07-04	RisePro Information Stealer	30baf54d503_edr79893b23b24203611da331d436dfc35f2d0a805bac4da0d310489XxX9Exe.exe	Endpoint Security	IT55	Prevented
2024-07-04	RisePro Information Stealer	6b82e6f228cbb8143b68e1_edr739f3d083cf6ab0ba9c202ce1ec769bb12c9030619XxX11Exe.exe	Endpoint Security	IT55	Prevented
2024-07-04	RisePro Information Stealer	0_edr78b3f37483cfc697fbd67120311e6109843804f5cae9c46f04fa1b51ba7120aXxX20Exe.exe	Endpoint Security	IT55	Prevented
2024-07-04	RisePro Information Stealer	ce930238a02a55d_edr7b6f13fdf9b3306de61c5c25513ed396c7e9a8dbd4c45dbd9XxX17Exe.exe	Endpoint Security	IT55	Prevented
2024-07-04	RisePro Information Stealer	d435d_edr7cf9077533a7c23129a8d7462e7596505e3990664dd5888fce40652bb14XxX21Exe.exe	Endpoint Security	IT55	Prevented
2024-07-04	RisePro Information Stealer	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/risepro_information_stealer_dbcc8998-07d5-4a55-adfd-08a15abf9712/f8_browsing7dd2b6a63e850b6c2128ec139c6334b572b1c80698fcc30de6f39ffc788f4fXxX25Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240704%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240704T075926Z&X-Amz-Expires=600&X-Amz-Signature=bd508d50aea0230e52ff464e22d4905e18843428e765915fceda2983ef565e22&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-04	RisePro Information Stealer	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/risepro_information_stealer_dbcc8998-07d5-4a55-adfd-08a15abf9712/cb21be43_browsing7c800875400a94b2442bbe02ccaf31ee49e1f440aac378fc2b0b756dXxX24Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240704%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240704T075925Z&X-Amz-Expires=600&X-Amz-Signature=7e55cf41bdf091da463307e3d9ba9db27a8d77441f16ba24c41325195a24be7b&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-04	RisePro Information Stealer	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/risepro_information_stealer_dbcc8998-07d5-4a55-adfd-08a15abf9712/0d5bb8b8da18abd1f3934103c501abf9b9cd3a6e1656853359a568dca3229_browsing765XxX23Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240704%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240704T075924Z&X-Amz-Expires=600&X-Amz-Signature=c3c7b9fa4ffb8d50510621b4af91344f3c87224c072ab8ca43d5f293754b86bf&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated

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

TLP:AMBER

ASM-VP REPORT

GOAA 07/26/2024

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2024-07-04	RisePro Information Stealer	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/risepro_information_stealer_dbcc8998-07d5-4a55-adfd-08a15abf9712/d_browsing7c3c01d62fb59e186b2256894fb089c01e1aeda5dbd86a3004f1857a13313adXxX22Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240704%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240704T075923Z&X-Amz-Expires=600&X-Amz-Signature=5c8a55070b5bd4517e13062cd7f8c24d758065df665a47c4cfad2f8f34ab4888&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-04	RisePro Information Stealer	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/risepro_information_stealer_dbcc8998-07d5-4a55-adfd-08a15abf9712/d2cbb_browsing7a5ef2ecdf7c6f8c965df5886a18ea0e630009cdedb3692ed1b8c77b487XxX19Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240704%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240704T075913Z&X-Amz-Expires=600&X-Amz-Signature=0bd7637d5be3ad90cc4dc8d921b05f73743b0a5d902a2e45e6e7309de60a9a80&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-04	RisePro Information Stealer	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/risepro_information_stealer_dbcc8998-07d5-4a55-adfd-08a15abf9712/19c98cba0d803_browsing7a36b00d2c11cc24d25e1f388ba5093a4b6e9017508371fb34bXxX18Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240704%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240704T075912Z&X-Amz-Expires=600&X-Amz-Signature=4465e62007d99732fb94aa74fceb3c2433bcd21a494aedf60c1ba8f8c836e600&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-04	RisePro Information Stealer	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/risepro_information_stealer_dbcc8998-07d5-4a55-adfd-08a15abf9712/6113bc3f3f9_browsing72393acff5022f5ba95fb96c3d9038386ada49ccf244fa5f885faXxX16Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240704%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240704T075909Z&X-Amz-Expires=600&X-Amz-Signature=0caf3ffa4bebbca769a111aafbb8e129fe3fbf6aeb32d93bb4ebf97bec34bdce&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-04	RisePro Information Stealer	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/risepro_information_stealer_dbcc8998-07d5-4a55-adfd-08a15abf9712/c_browsing7a40fb4aa017a0d17b535c1857d51f95b7ed8684a1ea860294bf5d897667839XxX15Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240704%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240704T075909Z&X-Amz-Expires=600&X-Amz-Signature=12471175f6b4c1e18e7550ba46f28c109b19fa108dcc61d40c0428565c02077e&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-04	RisePro Information Stealer	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/risepro_information_stealer_dbcc8998-07d5-4a55-adfd-08a15abf9712/15dfbd2df433c9_browsing725239d6602bdfc56d00db62f88a1769a534d98cad50536c27XxX14Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240704%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240704T075907Z&X-Amz-Expires=600&X-Amz-Signature=91ebffe27af59d6b039e7f25e5dffe80142ba96cd21d367730b702d01681d4fc&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-04	RisePro Information Stealer	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/risepro_information_stealer_dbcc8998-07d5-4a55-adfd-08a15abf9712/9d540839e_browsing75daf4f31eb36271fef6eb16a913446384d07e4d8dbb2602f18bf0fXxX13Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240704%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240704T075906Z&X-Amz-Expires=600&X-Amz-Signature=dfc69e1808ef3f47e5188d790b05ff4daa2079b97fdabe7256535afb1fdc6496&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-04	RisePro Information Stealer	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/risepro_information_stealer_dbcc8998-07d5-4a55-adfd-08a15abf9712/5_browsing719a862d5a32ec56328f8e066a83b6b0577a6965074ca671d0cecce681d5f79XxX12Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240704%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240704T075905Z&X-Amz-Expires=600&X-Amz-Signature=3e4888ad201a66cdfb524d2667ecbe932cbc760472217aeedbe8f2d651623353&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-04	RisePro Information Stealer	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/risepro_information_stealer_dbcc8998-07d5-4a55-adfd-08a15abf9712/c48eb226b641b382fd4155f10c96aacc585c6e65814865cd_browsing762e88b8a5cffd14XxX10Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240704%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240704T075857Z&X-Amz-Expires=600&X-Amz-Signature=f3f73217258e77489178ec10878c25fc2b138c487bf1948cdb04586895ceb730&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-04	RisePro Information Stealer	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/risepro_information_stealer_dbcc8998-07d5-4a55-adfd-08a15abf9712/a_browsing78513831b47f4b35ee9063aa167bf5d05c61559b2ac7f8fb93fa966a36e34d2XxX8Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240704%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240704T075855Z&X-Amz-Expires=600&X-Amz-Signature=dac3ef3b62bb77dd71d1435a2c6c4838ad5be99308461b3756f9d842ea6b84de&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-04	RisePro Information Stealer	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/risepro_information_stealer_dbcc8998-07d5-4a55-adfd-08a15abf9712/b4ad80860c_browsing773c79c946c3a4df13e534153bd17ceebad6acedac3156dfe0144cXxX6Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240704%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240704T075853Z&X-Amz-Expires=600&X-Amz-Signature=35805a39893d475abbe9119a31dea306dca435dcce3233d4ad7149eab38da583&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated

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

TLP:AMBER

ASM-VP REPORT

GOAA 07/26/2024

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2024-07-04	RisePro Information Stealer	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/risepro_information_stealer_dbcc8998-07d5-4a55-adfd-08a15abf9712/56108c_browsing707fcaf87b2220c081db115171ff35811946b3ad2d76105715e8530fbeXxX5Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240704%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240704T075851Z&X-Amz-Expires=600&X-Amz-Signature=174ce2f580799be519c0a488b58d7a738dde9b6e3da771000878c67a7718e248&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-04	RisePro Information Stealer	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/risepro_information_stealer_dbcc8998-07d5-4a55-adfd-08a15abf9712/4f0e839393df_browsing72db99a05ade0848979ff375399b104e59a7cc3847d746c17e5cXxX4Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240704%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240704T075850Z&X-Amz-Expires=600&X-Amz-Signature=b3140111129385e27cebedee91123d9356d186374da6a57d4a5e2d30a956bc97&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-04	RisePro Information Stealer	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/risepro_information_stealer_dbcc8998-07d5-4a55-adfd-08a15abf9712/a36d5e_browsing790ca17fb6f70884942d868d29c6854054f2db79ed8f4e2d0d16ef1647XxX3Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240704%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240704T075850Z&X-Amz-Expires=600&X-Amz-Signature=3bc1e1d7ee34448d86037231660b0e75e9b6281f520679e2aeda55a92902bf2a&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-04	RisePro Information Stealer	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/risepro_information_stealer_dbcc8998-07d5-4a55-adfd-08a15abf9712/5e1a1b2e2c20bc50b54e02393fa6f26a2b8c2f4d8_browsing7f2abdecaca73472b5c5dbaXxX2Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240704%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240704T075849Z&X-Amz-Expires=600&X-Amz-Signature=7899a8fc3ab95b0541e3d11a5111c445b4cbb37e9ae3ed3baebc7695ce1507d8&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-04	New Ransomware Operator Volcano Demon Serving Up LukaLocker	f83abe3d9_edr717238755f1276c87b3b320d8c30421984a897099ce3741d9143906XxX37Exe.exe	Endpoint Security	IT55	Prevented
2024-07-04	New Ransomware Operator Volcano Demon Serving Up LukaLocker	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/new_ransomware_operator_volcano_demon_serving_up_lukalocker_46e633a0-07c9-4db4-969c-ca783331cb37/4e58629158a6c46ad420f_browsing729330030f5e0b0ef374e9bb24cd203c89ec3262669XxX35Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240704%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240704T062702Z&X-Amz-Expires=600&X-Amz-Signature=a47d9caadb947dee0c09cbbbcd57816575ac14d78af1182449faafb953ba507f&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-03	Unfurling Hemlock Threat group uses cluster bomb campaigns	229e859dda6cc0bc99a395824f4524693bdd0292b4b9c55d06b4fa382_edr79b3ea2XxX29Exe.exe	Endpoint Security	IT55	Prevented
2024-07-03	Unfurling Hemlock Threat group uses cluster bomb campaigns	3_edr7b9e74da5fe5e27aaedc25e4aac7678553b6d7d89ec4d99e8b9d0627dcbdc12XxX30Exe.exe	Endpoint Security	IT55	Prevented
2024-07-03	Unfurling Hemlock Threat group uses cluster bomb campaigns	be25926929b1aae025_edr7d7f7614dd5ad637b8fd8e139c68f4d717e3dc9913e3cfXxX49Exe.exe	Endpoint Security	IT55	Prevented
2024-07-03	Unfurling Hemlock Threat group uses cluster bomb campaigns	0c48529d29_edr79698341e89d6ea5f7e9211fa277e40d3f6a55a8996135944ebdadXxX37Exe.exe	Endpoint Security	IT55	Prevented
2024-07-03	Unfurling Hemlock Threat group uses cluster bomb campaigns	301a1c9f4e82fc8f5_edr7577ea399a2591557ff57d337472c3f8482a89c5b4105d5XxX40Exe.exe	Endpoint Security	IT55	Prevented
2024-07-03	Unfurling Hemlock Threat group uses cluster bomb campaigns	7f101603fbb2821504cf2c_edr71fca0450689dfcd6d1f36e57e27f0392be0f2d1ddXxX45Exe.exe	Endpoint Security	IT55	Prevented
2024-07-03	Unfurling Hemlock Threat group uses cluster bomb campaigns	7d18c6_edr7c13ec919f3950092319d11eda129c8498e171612e681eebf1c977493dXxX44Exe.exe	Endpoint Security	IT55	Prevented
2024-07-03	Unfurling Hemlock Threat group uses cluster bomb campaigns	65,923,603a6f11_edr7c7460b8cc69009105208bdfa544b90446580915db8fe127ae8XxX43Exe.exe	Endpoint Security	IT55	Prevented

TLP:AMBER

GLESEC
COMPLETELY PERCEPTI

ASM-VP REPORT

GOAA 07/26/2024

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2024-07-03	Unfurling Hemlock Threat group uses cluster bomb campaigns	hxxp://77.91.68.29/fks/	Web Gateway	IT55	Offline/Removed
2024-07-03	Unfurling Hemlock Threat group uses cluster bomb campaigns	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/unf urling_hemlock_threat_group_uses_cluster_bomb_campaigns_e96df6ab-765c-4746-90c1-94ebb0dfb343/fd_browsing7a9b8e52e2fbcb090d5f5046a73d6e42b421abf063083210889f3fcb 47dee0XxX52Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNE D-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240703%2Feu-west-1%2Fs3%2Faw s4_request&X-Amz-Date=20240703T080326Z&X-Amz-Expires=600&X-Amz-Signature=7d20d49 fb143be9dc0603dec2bd68e950e7f88e40bc7739251fc05096cfa0e0c&X-Amz-SignedHeaders=ho st&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-03	Unfurling Hemlock Threat group uses cluster bomb campaigns	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/unf urling_hemlock_threat_group_uses_cluster_bomb_campaigns_e96df6ab-765c-4746-90c1-94ebb0dfb343/edfb43_browsing74d5c586f0690c95ff8cacb36bda6fb4743f20dda5e6f17e7e24 1edd47XxX51Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNE D-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240703%2Feu-west-1%2Fs3%2Faw s4_request&X-Amz-Date=20240703T080325Z&X-Amz-Expires=600&X-Amz-Signature=a80c4dc 30fd034bb54cbbd9e4352654533f6cb3201cae425f8d9f67a073c173a&X-Amz-SignedHeaders=ho st&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-03	Unfurling Hemlock Threat group uses cluster bomb campaigns	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/unf urling_hemlock_threat_group_uses_cluster_bomb_campaigns_e96df6ab-765c-4746-90c1-94ebb0dfb343/da4f614c983fa226d813de39093_browsing7389ae4d1e043dd86524aa7a5246fd5 87826bXxX50Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNE D-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240703%2Feu-west-1%2Fs3%2Faw s4_request&X-Amz-Date=20240703T080325Z&X-Amz-Expires=600&X-Amz-Signature=b2d5004 e27ef1e35af2c176cd121b9c2a6ab939e28c5f981833c65b93072da45&X-Amz-SignedHeaders=ho st&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-03	Unfurling Hemlock Threat group uses cluster bomb campaigns	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/unf urling_hemlock_threat_group_uses_cluster_bomb_campaigns_e96df6ab-765c-4746-90c1-94ebb0dfb343/8fe4d34a6a245c5acd3d1_browsing741213c1dd195468089b1a3fe80adfa6d8d8c 94f2d8XxX47Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNE D-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240703%2Feu-west-1%2Fs3%2Faw s4_request&X-Amz-Date=20240703T080324Z&X-Amz-Expires=600&X-Amz-Signature=718b10e c516f45c6af33ca1970abd223ff6b6d89c4b5de72aa400cefe43aa358&X-Amz-SignedHeaders=ho st&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-03	Unfurling Hemlock Threat group uses cluster bomb campaigns	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/unf urling_hemlock_threat_group_uses_cluster_bomb_campaigns_e96df6ab-765c-4746-90c1-94ebb0dfb343/80df101f1f93fa53b3dcbc315d3ec5d8c8330c08b5622ac320_browsing7f746d01 6b66dcXxX46Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNE D-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240703%2Feu-west-1%2Fs3%2Faw s4_request&X-Amz-Date=20240703T080324Z&X-Amz-Expires=600&X-Amz-Signature=1b5ee21 aa36759ab26ec077c0586ca2303644fad1a6cbfd7532d8318ddbe6920&X-Amz-SignedHeaders=ho st&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-03	Unfurling Hemlock Threat group uses cluster bomb campaigns	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/unf urling_hemlock_threat_group_uses_cluster_bomb_campaigns_e96df6ab-765c-4746-90c1-94ebb0dfb343/569_browsing7652d0fd5b4a05ac00f6ec028fd3dc3e34ed7b112c4b8c6048eae72 a8d326XxX42Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNE D-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240703%2Feu-west-1%2Fs3%2Faw s4_request&X-Amz-Date=20240703T080316Z&X-Amz-Expires=600&X-Amz-Signature=ad20f79 f684f5bed7147491b20c0e7fe3de262e82e33e8297bd0ea08fee040fe&X-Amz-SignedHeaders=ho st&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-03	Unfurling Hemlock Threat group uses cluster bomb campaigns	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/unf urling_hemlock_threat_group_uses_cluster_bomb_campaigns_e96df6ab-765c-4746-90c1-94ebb0dfb343/35c55b402e_browsing770e25adf57ffbd408a428af9ce21a735474b5d94ccdd412 3e68f8XxX41Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNE D-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240703%2Feu-west-1%2Fs3%2Faw s4_request&X-Amz-Date=20240703T080316Z&X-Amz-Expires=600&X-Amz-Signature=a136767 7df2f872fc8710301d3dd37b6451f41cd600dd0e6e8bff777f87d38f4&X-Amz-SignedHeaders=ho st&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-03	Unfurling Hemlock Threat group uses cluster bomb campaigns	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/unf urling_hemlock_threat_group_uses_cluster_bomb_campaigns_e96df6ab-765c-4746-90c1-94ebb0dfb343/1f224093b955_browsing7dd73caaf1c6a823028c286ddd3414bceb0860e0fe084f b8c2abXxX39Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNE D-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240703%2Feu-west-1%2Fs3%2Faw s4_request&X-Amz-Date=20240703T080315Z&X-Amz-Expires=600&X-Amz-Signature=7ad31bb bf45836a838102a8b72d8c6e94875c0f59ee715fa299ab2bc42e7ee50&X-Amz-SignedHeaders=ho st&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-03	Unfurling Hemlock Threat group uses cluster bomb campaigns	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/unf urling_hemlock_threat_group_uses_cluster_bomb_campaigns_e96df6ab-765c-4746-90c1-94ebb0dfb343/0ef_browsing7459cebfe9bd9102c5eccc16eedddec5931e69bf705aa44aa3c7af5 84f209XxX38Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNE D-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240703%2Feu-west-1%2Fs3%2Faw s4_request&X-Amz-Date=20240703T080313Z&X-Amz-Expires=600&X-Amz-Signature=a944d69 b50324a75af2cf082efc86383e77b0393384c31100456381ca1bd7a00&X-Amz-SignedHeaders=ho st&x-id=GetObject	Web Gateway	IT55	Penetrated

LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

TLP:AMBER

ASM-VP REPORT

GOAA 07/26/2024

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2024-07-03	Unfurling Hemlock Threat group uses cluster bomb campaigns	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/unfurling_hemlock_threat_group_uses_cluster_bomb_campaigns_e96df6ab-765c-4746-90c1-94ebb0dfb343/94115d0eae0422b6605f0f25841c29b_browsing7cc6c029472a983b21d1cedcd7fdcd647XxX35Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240703%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240703T080312Z&X-Amz-Expires=600&X-Amz-Signature=1f3138feda766329c845d8f8f5228928b3fc7372682708d399c3e0a21c952908&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-03	Supply Chain Compromise Leads to Trojanized Installers	2eae4f06f2c3_edr76c6206c632ac93f4e8c4b3e0e63eca3118e883f8ac479b2f852XxX10Exe.exe	Endpoint Security	IT55	Prevented
2024-07-03	Supply Chain Compromise Leads to Trojanized Installers	fdc84cb0845f8_edr7a39b29027d6433f4a1bbd8c5b808280235cf867a6b0b7a91ebXxX28Exe.exe	Endpoint Security	IT55	Prevented
2024-07-03	Supply Chain Compromise Leads to Trojanized Installers	bfa99c41aecc814de5b9eb839_edr7a27e516c8b0a4e31edd9ed1304da6c996b4aaaXxX23Exe.exe	Endpoint Security	IT55	Prevented
2024-07-03	Supply Chain Compromise Leads to Trojanized Installers	de4e032880_edr71cdebe5c26913888b135fb2424132856cc892baea9792d6c66249XxX26Exe.exe	Endpoint Security	IT55	Prevented
2024-07-03	Supply Chain Compromise Leads to Trojanized Installers	hxxp://170.130.34.114	Web Gateway	IT55	Offline/Removed
2024-07-03	Supply Chain Compromise Leads to Trojanized Installers	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/supply_chain_compromise_leads_to_trojanized_installers_d393005f-03bd-4d35-af94-aff4991999c4/70bce9c228aacbdadaaf18596c0eb308c102382d04632b01b826e9db96210093_browsingXxX21Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240703%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240703T080038Z&X-Amz-Expires=600&X-Amz-Signature=ed504db716db6dab88227a8aac4b322dd251fb49d3e058aa98406d83b281397e&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-03	Supply Chain Compromise Leads to Trojanized Installers	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/supply_chain_compromise_leads_to_trojanized_installers_d393005f-03bd-4d35-af94-aff4991999c4/6f49_browsing756749d175058f15d5f3c80c8a7d46e80ec3e5eb9fb31f4346abdb72a0e7XxX20Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240703%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240703T080033Z&X-Amz-Expires=600&X-Amz-Signature=e3e31636fc1f3bb1088f07e81b6e5228437d97bb9610ef4e9f8acf370ec6dc49&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated
2024-07-03	Supply Chain Compromise Leads to Trojanized Installers	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/supply_chain_compromise_leads_to_trojanized_installers_d393005f-03bd-4d35-af94-aff4991999c4/4df9b_browsing7da9590990230ed2ab9b4c3d399cf770ed7f6c36a8a10285375fd5a292fXxX18Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240703%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240703T080030Z&X-Amz-Expires=600&X-Amz-Signature=06d39cde2a032c03600ac68ffafbfd297d0b67ffab12e17225551abe4ffbae33&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	IT55	Penetrated

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

Threats

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

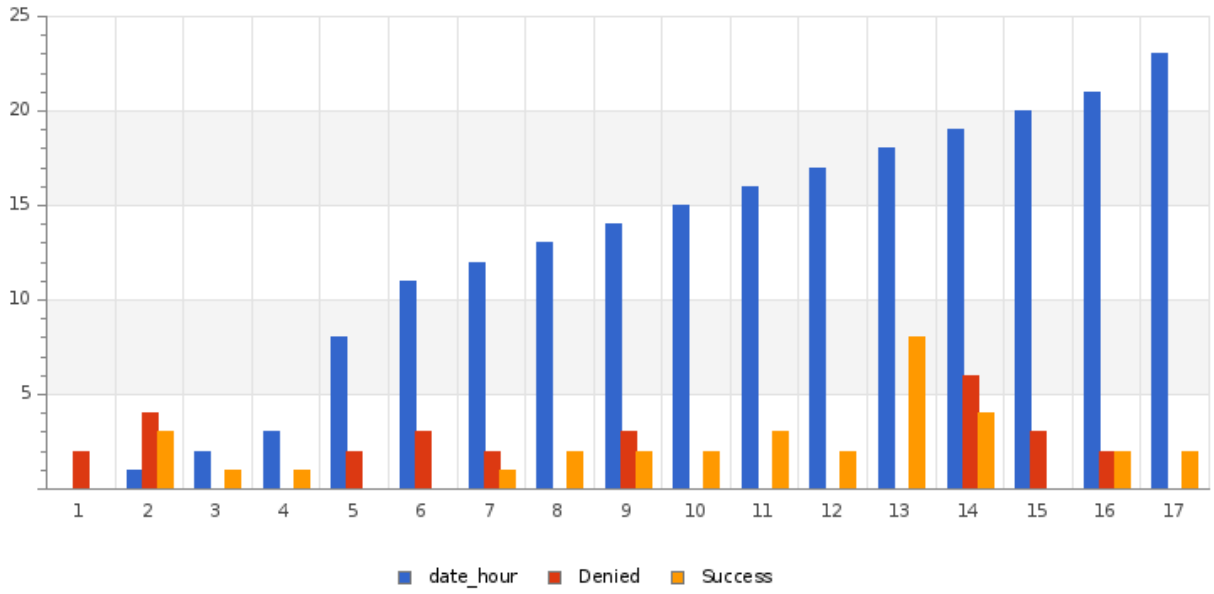
Trusted Access

MSS-TAS

Total Users *

7

Average Authentications by Hour of the Day



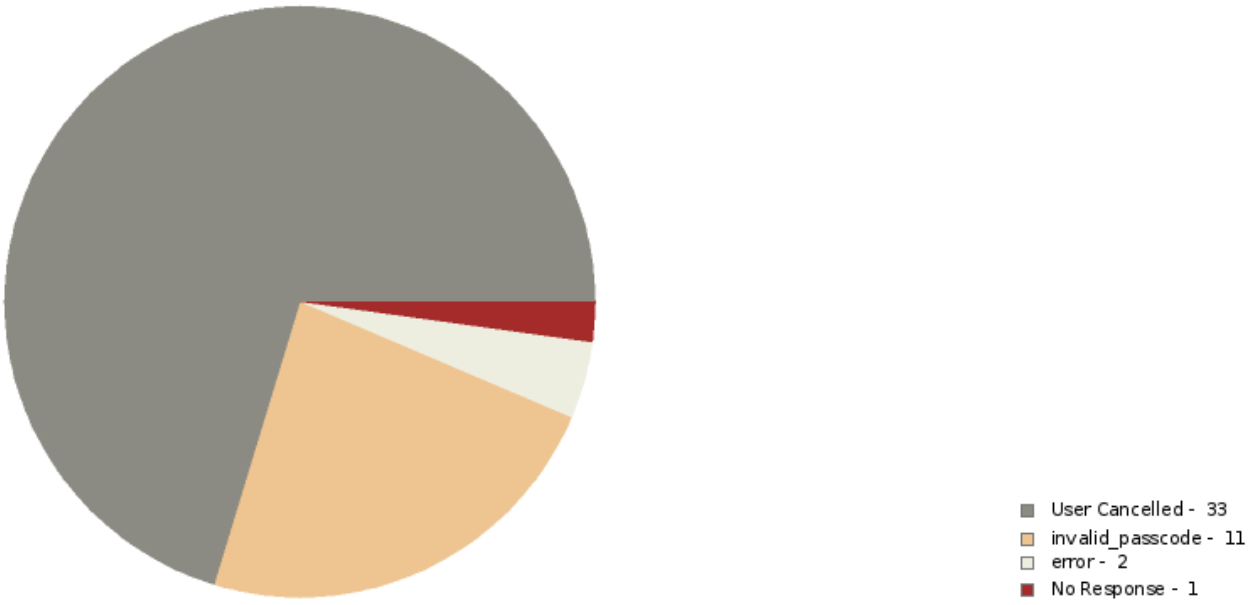
LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

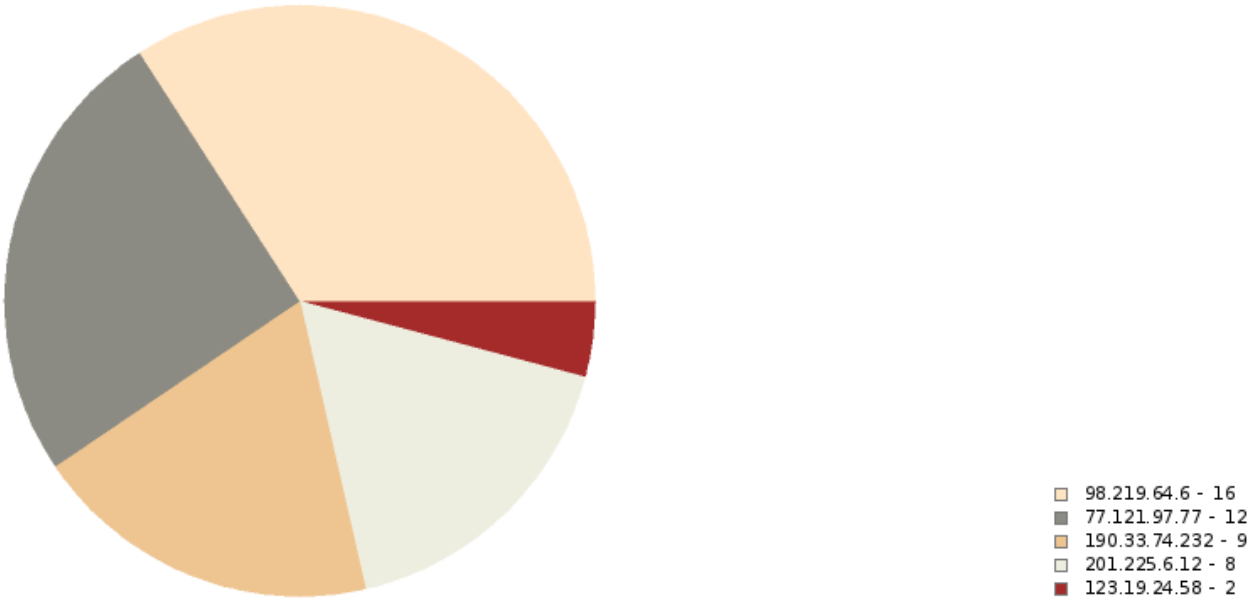
ASM-VP REPORT

GOAA 07/26/2024

Top of Failed Authentications *



Top Authentications Failed by IPs *

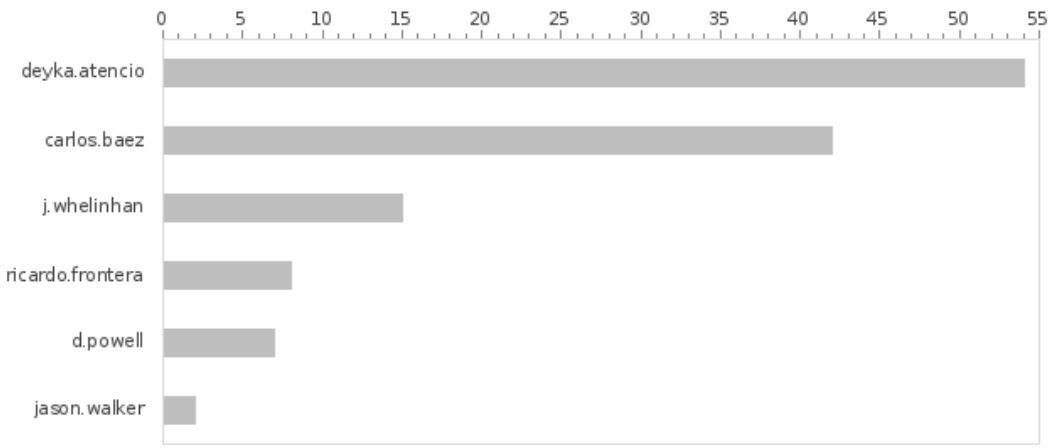


LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

ASM-VP REPORT

GOAA 07/26/2024

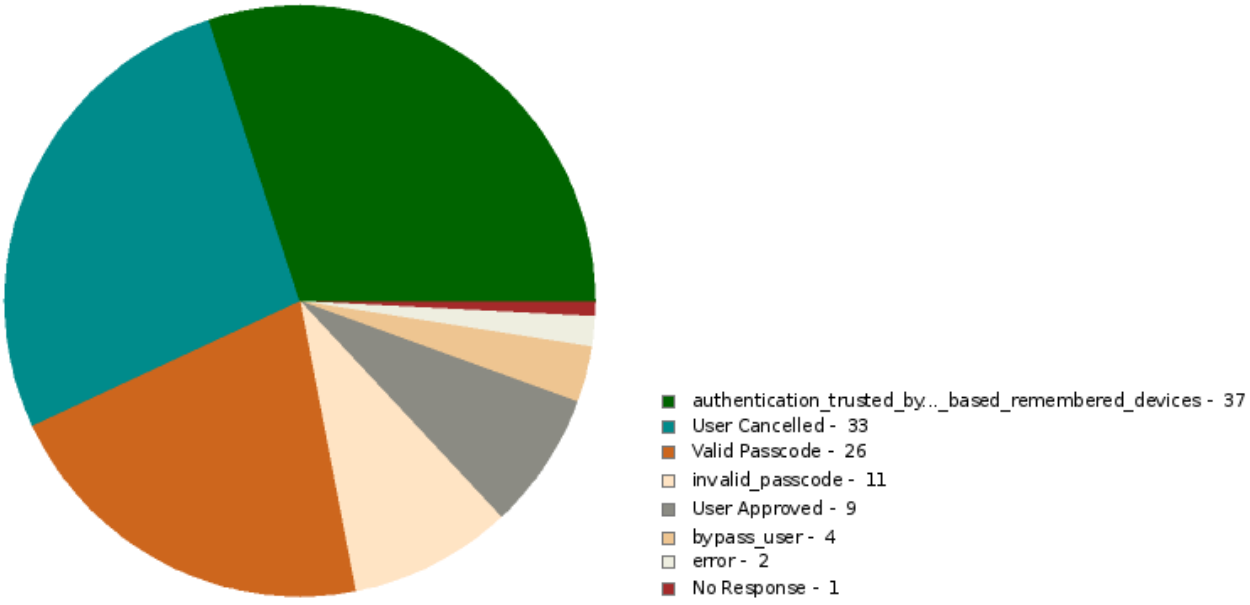
Top Authenticated Users *



Most Active Applications *

app	Denied	Success	Total
Skywatch	34	52	86
Cymulate	13	29	42

Authentication Status in the Last 24 Hours *



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

ASM-VP REPORT

GOAA 07/26/2024

Users with failed authentications *

user	Time	src_ip
carlos.baez	Mon Jul 15 20:53:23 2,024 UTC	190.33.74.232
carlos.baez	Mon Jul 15 20:54:40 2,024 UTC	190.33.74.232
deyka.atencio	Mon Jul 15 11:01:26 2,024 UTC	98.219.64.6
deyka.atencio	Mon Jul 15 11:02:19 2,024 UTC	77.121.97.77
deyka.atencio	Thu Jul 11 14:58:14 2,024 UTC	77.121.97.77
deyka.atencio	Mon Jul 15 19:33:22 2,024 UTC	190.33.74.232
carlos.baez	Mon Jul 15 19:43:08 2,024 UTC	190.33.74.232
carlos.baez	Mon Jul 15 19:43:59 2,024 UTC	190.33.74.232
deyka.atencio	Sat Jul 13 1:17:13 2,024 UTC	98.219.64.6
deyka.atencio	Sat Jul 13 1:23:14 2,024 UTC	98.219.64.6
deyka.atencio	Sat Jul 13 1:23:18 2,024 UTC	98.219.64.6
deyka.atencio	Sat Jul 13 1:42:00 2,024 UTC	98.219.64.6
carlos.baez	Tue Jul 16 1:39:31 2,024 UTC	201.225.6.12
carlos.baez	Tue Jul 16 1:54:49 2,024 UTC	201.225.6.12
deyka.atencio	Mon Jul 15 8:10:17 2,024 UTC	123.19.24.58
deyka.atencio	Mon Jul 15 8:10:26 2,024 UTC	123.19.24.58
deyka.atencio	Wed Jul 10 21:20:18 2,024 UTC	98.219.64.6
deyka.atencio	Wed Jul 10 21:20:30 2,024 UTC	98.219.64.6
deyka.atencio	Thu Jul 11 12:48:53 2,024 UTC	77.121.97.77
deyka.atencio	Thu Jul 11 12:50:45 2,024 UTC	77.121.97.77
carlos.baez	Mon Jul 15 20:07:09 2,024 UTC	190.33.74.232
deyka.atencio	Mon Jul 15 11:02:16 2,024 UTC	77.121.97.77
deyka.atencio	Thu Jul 11 14:58:17 2,024 UTC	77.121.97.77
deyka.atencio	Thu Jul 11 14:58:28 2,024 UTC	77.121.97.77
deyka.atencio	Thu Jul 11 14:59:16 2,024 UTC	77.121.97.77
deyka.atencio	Thu Jul 11 14:59:18 2,024 UTC	77.121.97.77
deyka.atencio	Thu Jul 11 14:59:29 2,024 UTC	77.121.97.77
deyka.atencio	Mon Jul 15 19:33:10 2,024 UTC	190.33.74.232
carlos.baez	Mon Jul 15 19:54:18 2,024 UTC	190.33.74.232
carlos.baez	Mon Jul 15 19:56:16 2,024 UTC	190.33.74.232
deyka.atencio	Sat Jul 13 1:23:00 2,024 UTC	98.219.64.6
deyka.atencio	Sat Jul 13 1:23:46 2,024 UTC	98.219.64.6
deyka.atencio	Sat Jul 13 1:23:55 2,024 UTC	98.219.64.6
deyka.atencio	Sat Jul 13 1:24:01 2,024 UTC	98.219.64.6

user	Time	src_ip
deyka.atencio	Sat Jul 13 1:32:04 2,024 UTC	98.219.64.6
deyka.atencio	Fri Jul 12 0:45:01 2,024 UTC	98.219.64.6
deyka.atencio	Fri Jul 12 0:45:12 2,024 UTC	98.219.64.6
carlos.baez	Tue Jul 16 14:02:32 2,024 UTC	201.225.6.12
carlos.baez	Tue Jul 16 14:03:02 2,024 UTC	201.225.6.12
carlos.baez	Tue Jul 16 1:39:49 2,024 UTC	201.225.6.12
carlos.baez	Tue Jul 16 1:41:48 2,024 UTC	201.225.6.12
carlos.baez	Tue Jul 16 1:50:20 2,024 UTC	201.225.6.12
carlos.baez	Tue Jul 16 1:54:20 2,024 UTC	201.225.6.12
deyka.atencio	Wed Jul 10 21:20:39 2,024 UTC	98.219.64.6
deyka.atencio	Wed Jul 10 21:34:12 2,024 UTC	98.219.64.6
deyka.atencio	Thu Jul 11 12:48:49 2,024 UTC	77.121.97.77
deyka.atencio	Thu Jul 11 12:49:57 2,024 UTC	77.121.97.77

Authentications left as No response by Users *

Username	IP Address	Time
deyka.atencio	98.219.64.6	Sat Jul 13 1:42:00 2,024 UTC

Users with Invalid Passcode *

Username	Time	IP Address
carlos.baez	Tue Jul 16 1:39:49 2,024 UTC	201.225.6.12
deyka.atencio	Thu Jul 11 14:58:17 2,024 UTC	77.121.97.77
deyka.atencio	Thu Jul 11 14:58:28 2,024 UTC	77.121.97.77
deyka.atencio	Thu Jul 11 14:59:18 2,024 UTC	77.121.97.77
deyka.atencio	Thu Jul 11 14:59:29 2,024 UTC	77.121.97.77
deyka.atencio	Mon Jul 15 19:33:10 2,024 UTC	190.33.74.232
deyka.atencio	Fri Jul 12 0:45:12 2,024 UTC	98.219.64.6
deyka.atencio	Mon Jul 15 8:10:26 2,024 UTC	123.19.24.58
deyka.atencio	Thu Jul 11 12:48:53 2,024 UTC	77.121.97.77
deyka.atencio	Mon Jul 15 11:02:19 2,024 UTC	77.121.97.77
deyka.atencio	Mon Jul 15 19:33:22 2,024 UTC	190.33.74.232

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

ASM-VP REPORT

GOAA 07/26/2024

Call timed out by Users *

Username	Time	IP Address
deyka.atencio	Sat Jul 13 1:42:00 2,024 UTC	98.219.64.6

Authentications Cancelled by the Users *

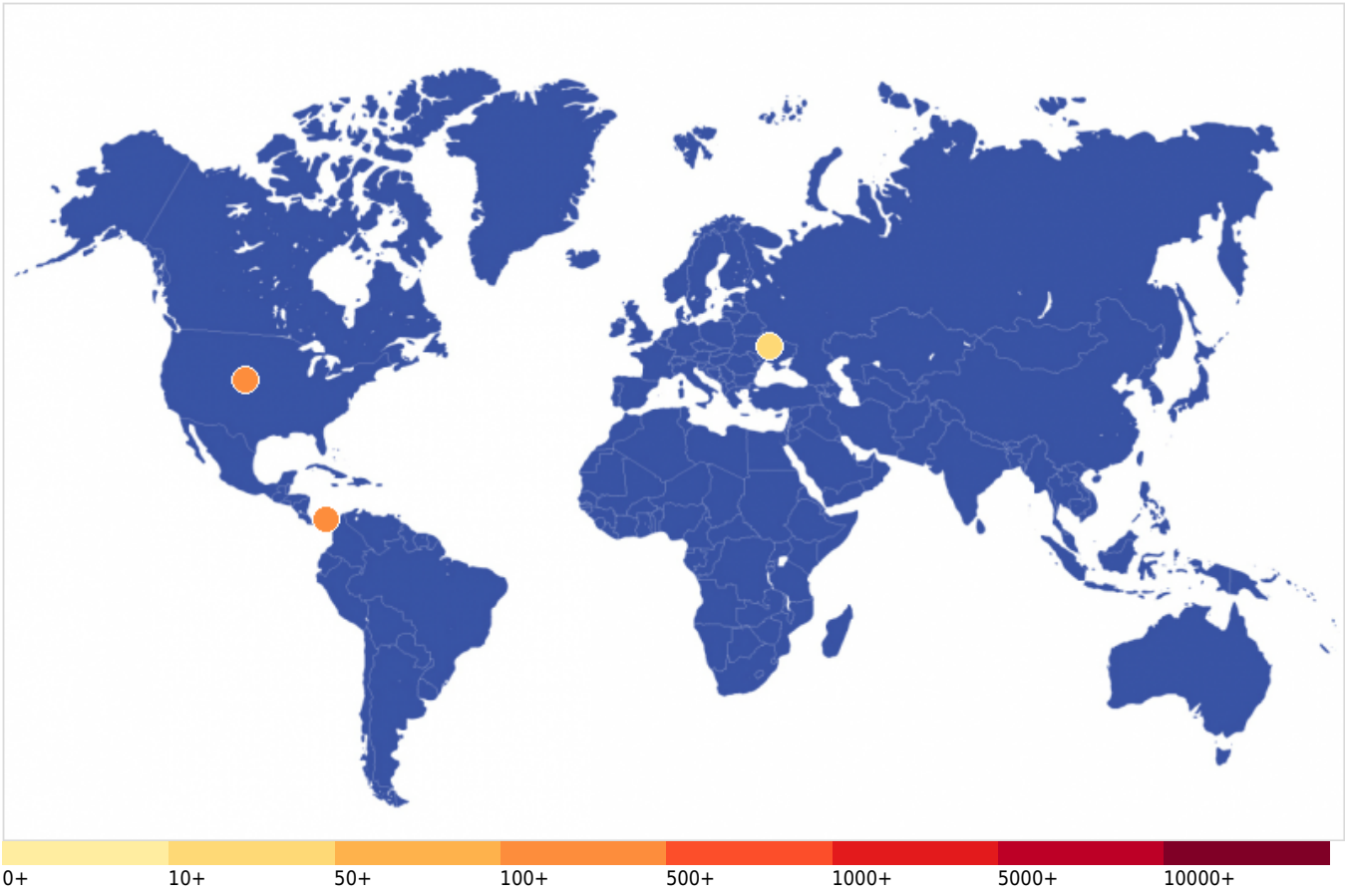
Username	Time	IP Address
carlos.baez	Mon Jul 15 20:53:23 2,024 UTC	190.33.74.232
carlos.baez	Mon Jul 15 20:54:40 2,024 UTC	190.33.74.232
deyka.atencio	Mon Jul 15 11:01:26 2,024 UTC	98.219.64.6
deyka.atencio	Thu Jul 11 14:58:14 2,024 UTC	77.121.97.77
carlos.baez	Mon Jul 15 19:43:08 2,024 UTC	190.33.74.232
carlos.baez	Mon Jul 15 19:43:59 2,024 UTC	190.33.74.232
deyka.atencio	Sat Jul 13 1:17:13 2,024 UTC	98.219.64.6
deyka.atencio	Sat Jul 13 1:23:14 2,024 UTC	98.219.64.6
deyka.atencio	Sat Jul 13 1:23:18 2,024 UTC	98.219.64.6
carlos.baez	Tue Jul 16 1:39:31 2,024 UTC	201.225.6.12
carlos.baez	Tue Jul 16 1:54:49 2,024 UTC	201.225.6.12
deyka.atencio	Mon Jul 15 8:10:17 2,024 UTC	123.19.24.58
deyka.atencio	Wed Jul 10 21:20:18 2,024 UTC	98.219.64.6
deyka.atencio	Wed Jul 10 21:20:30 2,024 UTC	98.219.64.6
deyka.atencio	Thu Jul 11 12:50:45 2,024 UTC	77.121.97.77
carlos.baez	Mon Jul 15 20:07:09 2,024 UTC	190.33.74.232
deyka.atencio	Mon Jul 15 11:02:16 2,024 UTC	77.121.97.77
deyka.atencio	Thu Jul 11 14:59:16 2,024 UTC	77.121.97.77
carlos.baez	Mon Jul 15 19:54:18 2,024 UTC	190.33.74.232
carlos.baez	Mon Jul 15 19:56:16 2,024 UTC	190.33.74.232
deyka.atencio	Sat Jul 13 1:23:00 2,024 UTC	98.219.64.6
deyka.atencio	Sat Jul 13 1:23:46 2,024 UTC	98.219.64.6
deyka.atencio	Sat Jul 13 1:32:04 2,024 UTC	98.219.64.6
deyka.atencio	Fri Jul 12 0:45:01 2,024 UTC	98.219.64.6
carlos.baez	Tue Jul 16 14:02:32 2,024 UTC	201.225.6.12
carlos.baez	Tue Jul 16 14:03:02 2,024 UTC	201.225.6.12
carlos.baez	Tue Jul 16 1:41:48 2,024 UTC	201.225.6.12
carlos.baez	Tue Jul 16 1:50:20 2,024 UTC	201.225.6.12
carlos.baez	Tue Jul 16 1:54:20 2,024 UTC	201.225.6.12

ASM-VP REPORT

GOAA 07/26/2024

Username	Time	IP Address
deyka.atencio	Wed Jul 10 21:20:39 2,024 UTC	98.219.64.6
deyka.atencio	Wed Jul 10 21:34:12 2,024 UTC	98.219.64.6
deyka.atencio	Thu Jul 11 12:48:49 2,024 UTC	77.121.97.77
deyka.atencio	Thu Jul 11 12:49:57 2,024 UTC	77.121.97.77

Most Successful Authenticated Countries *

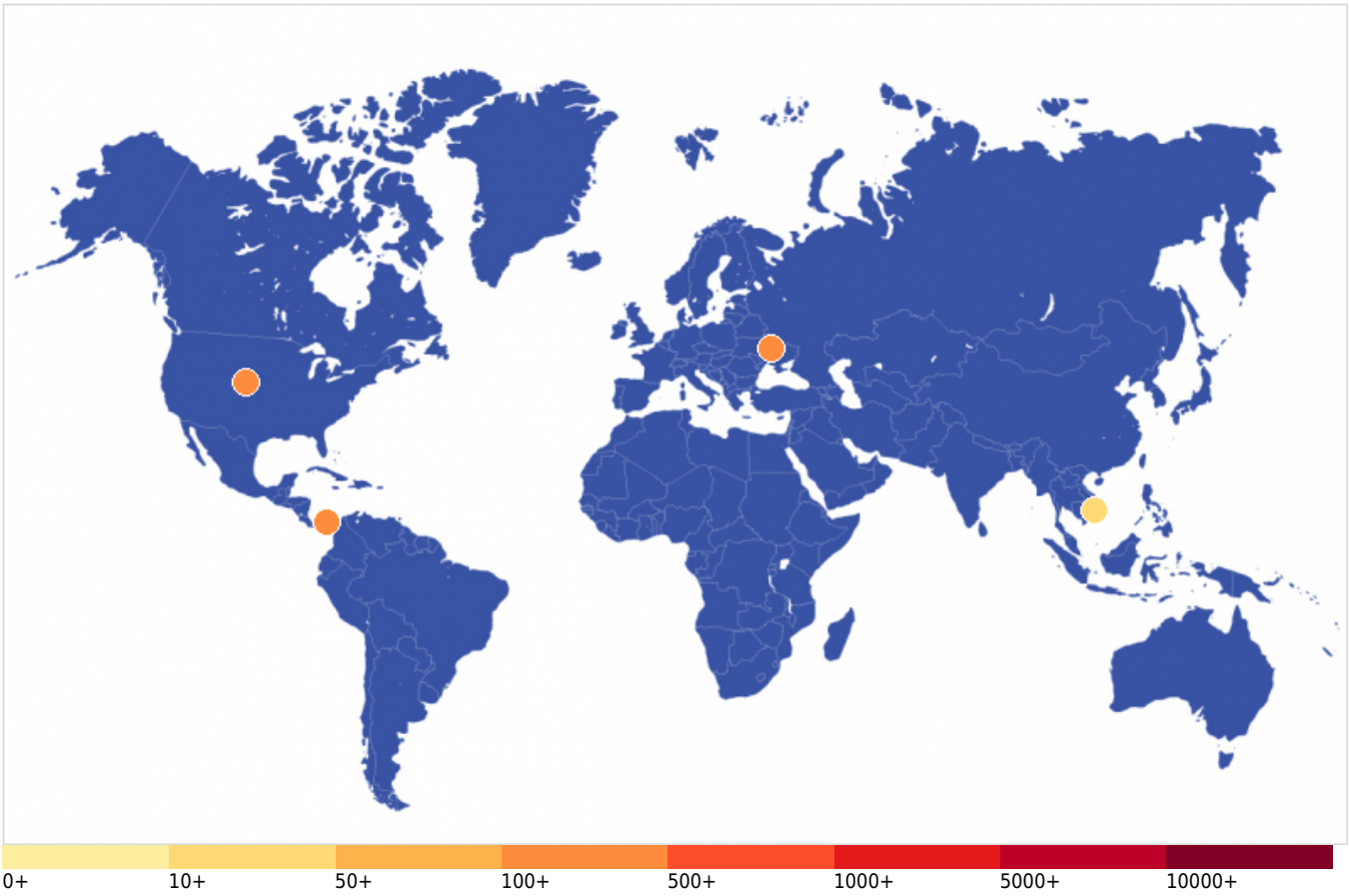


Countries with Most Failed Authentications *

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

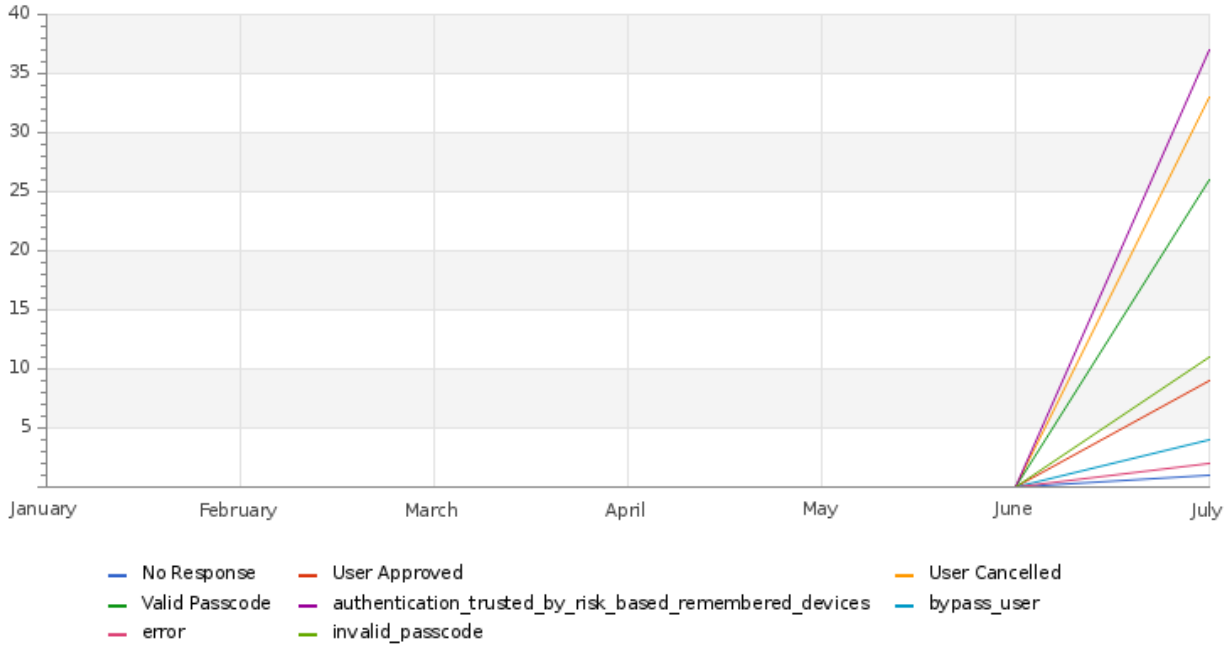
ASM-VP REPORT

GOAA 07/26/2024

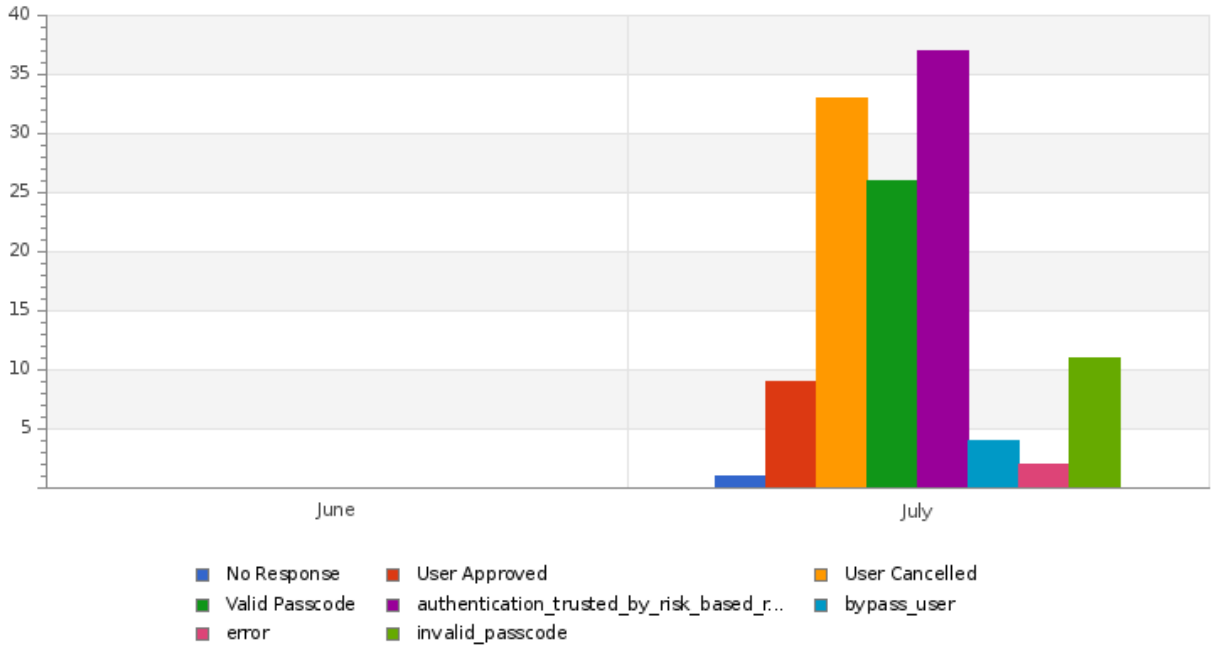


LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

Trusted Access In Last 6 Months



Successful and Failed Authentications *

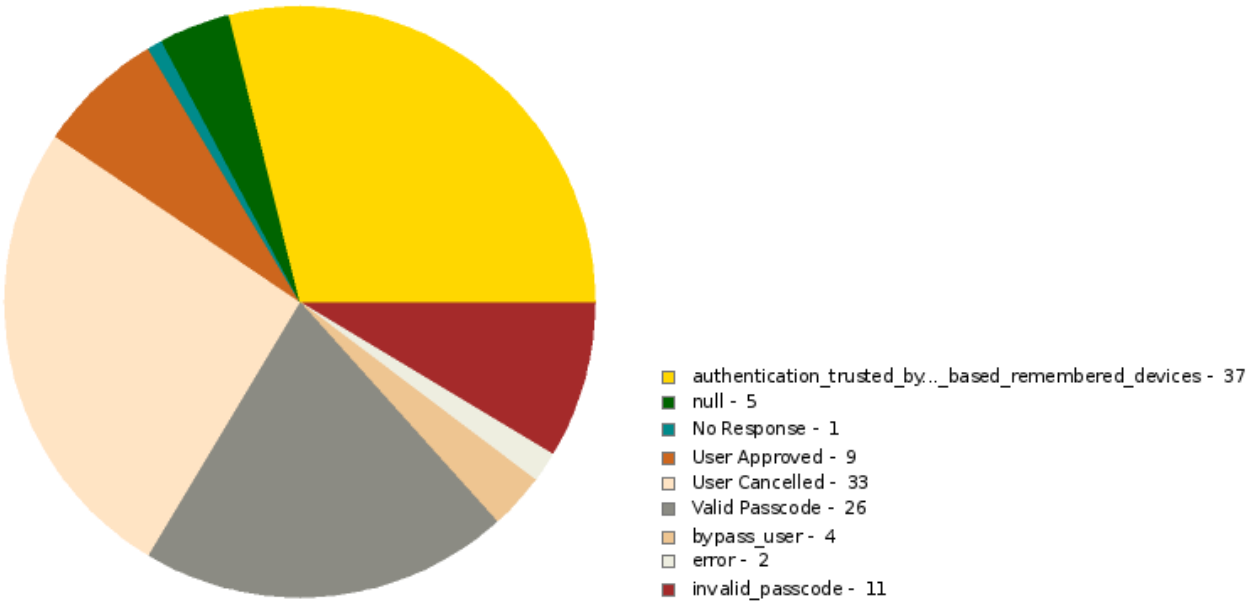


LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

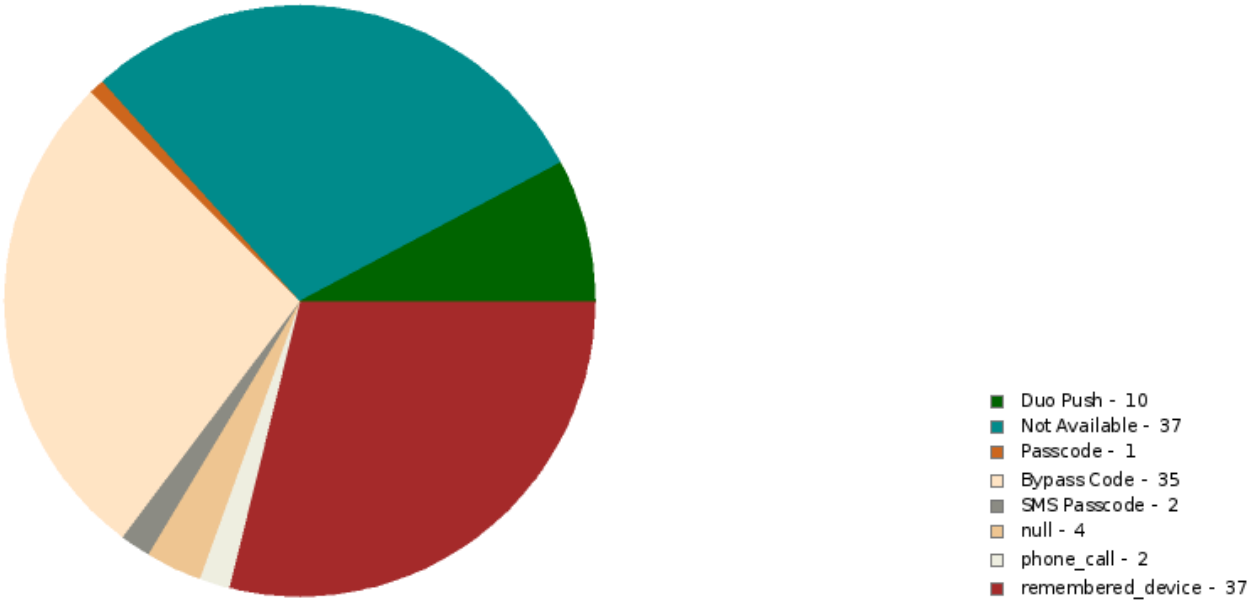
ASM-VP REPORT

GOAA 07/26/2024

Successful Authentications *



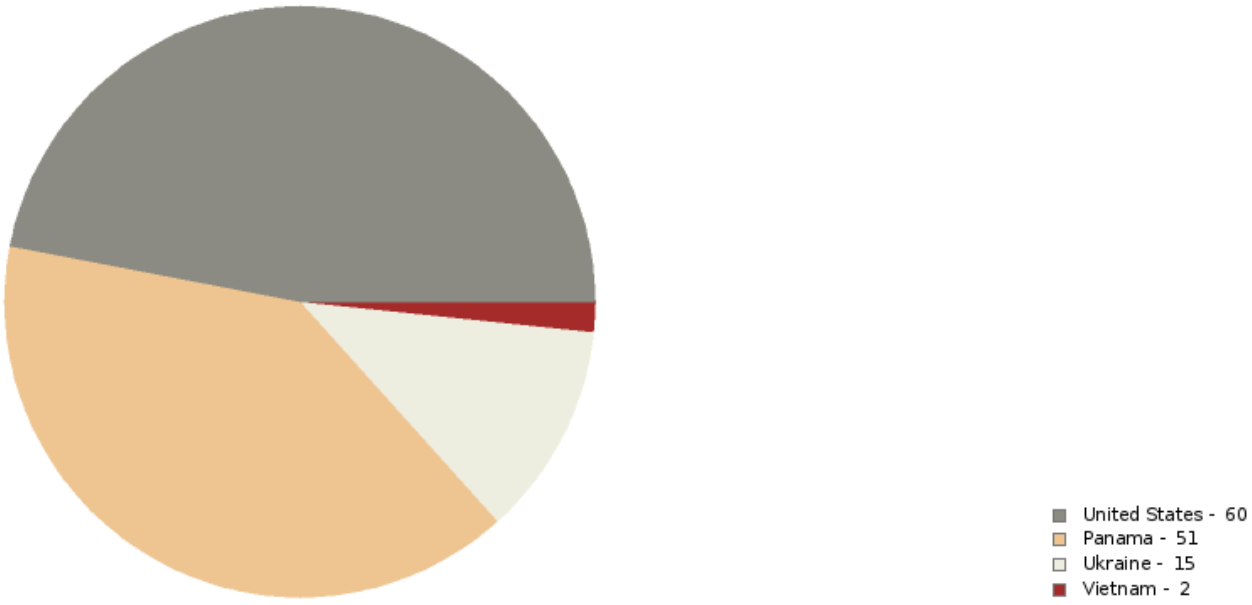
Successful Authentications by Factor *



LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

Authentication Per Country *



MSS-USB

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