TLP:AMBER

ASM-VP REPORT

ORGANO JUDICIAL

July 26, 2023

TLP AMBER
ASM-VP REPORT

About this report

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

Assets

MSS-VME

Overview

Vulnerability Level

4%

Discovered Hosts

13

Vulnerable Hosts

5

Executive Summary Vulnerability Severity Distribution

Scanner	critical	high	medium	low
Organo Judicial	2	2	9	1

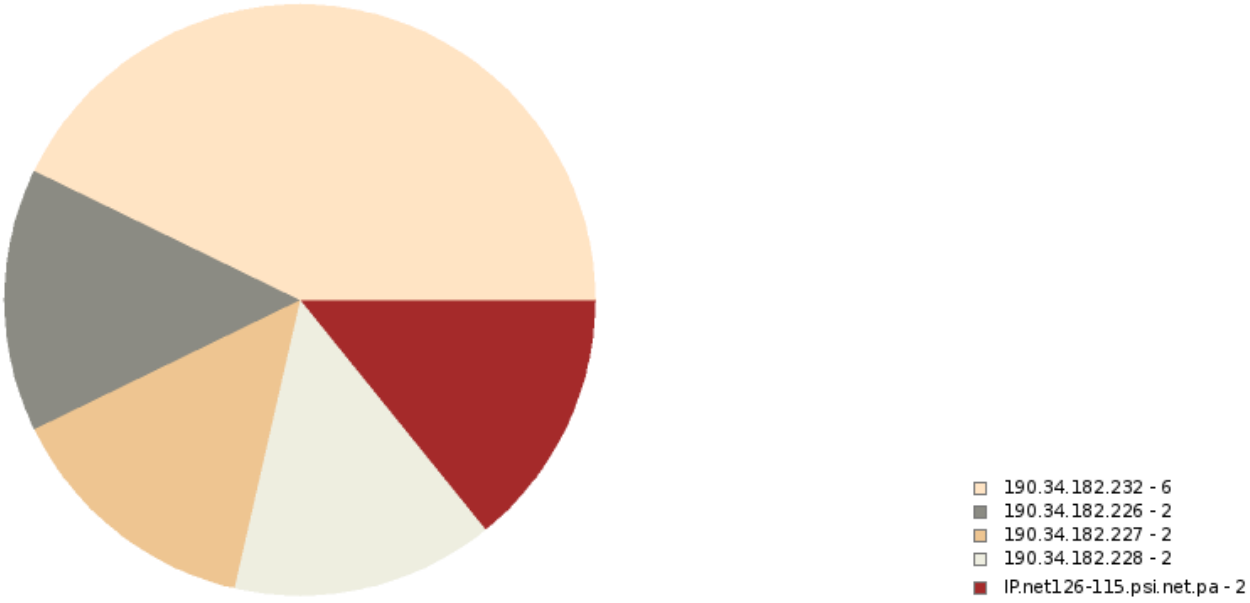
LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

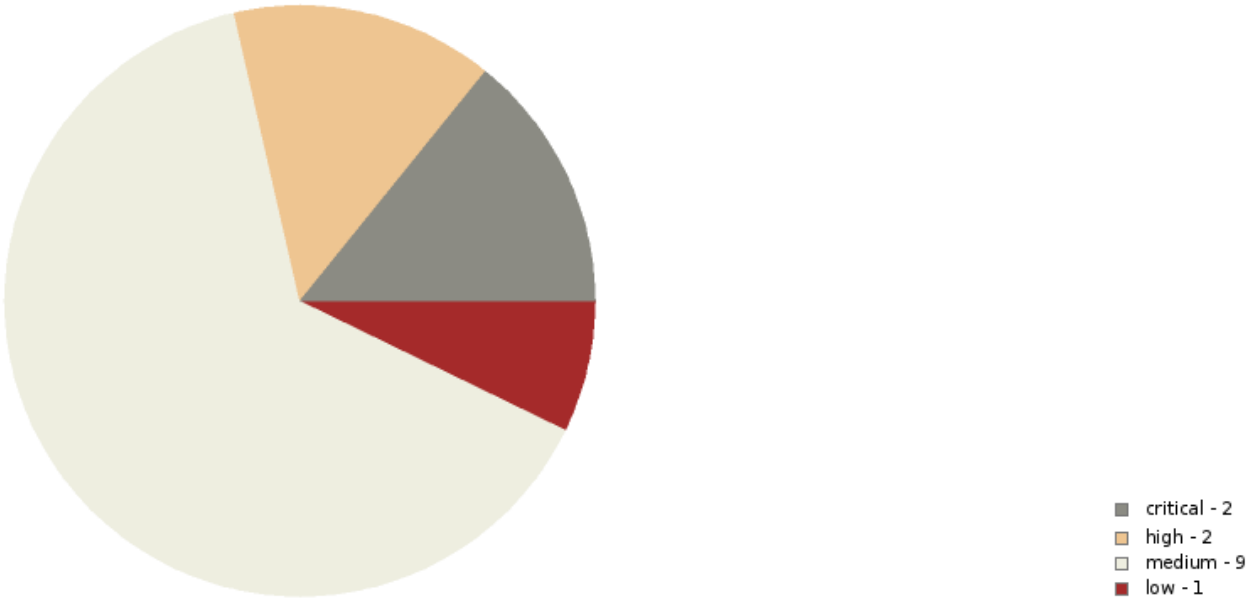
ASM-VP REPORT

Organo Judicial 07/26/2023

Most Vulnerable Host *



Vulnerability Distribution



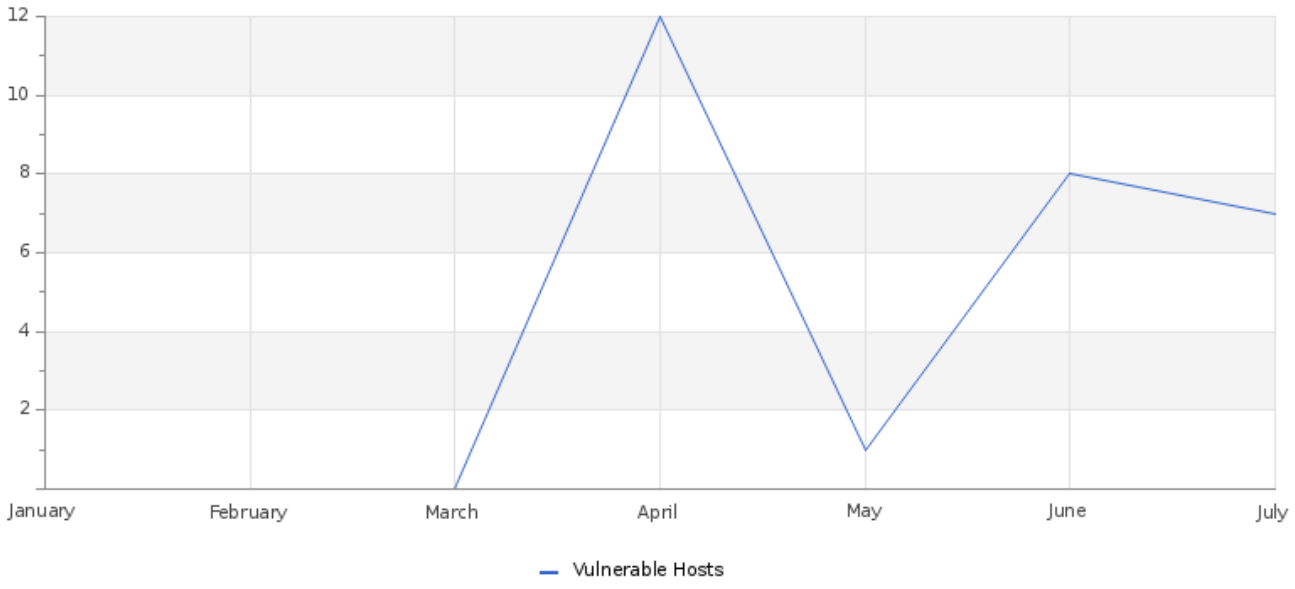
LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

Top 10 Most Common Vulnerabilities

Vulnerability
TLS Version 1.00 Protocol Detection
TLS Version 1.10 Protocol Deprecated
CGI Generic SQL Injection Detection (potential, 2nd order, 2nd pass)
Microsoft IIS 6.00 Unsupported Version Detection
Microsoft Windows 2,000 Unsupported Installation Detection
Unsupported Web Server Detection
Web Application Potentially Vulnerable to Clickjacking
Web Server PROPFIND Method Internal IP Disclosure

History

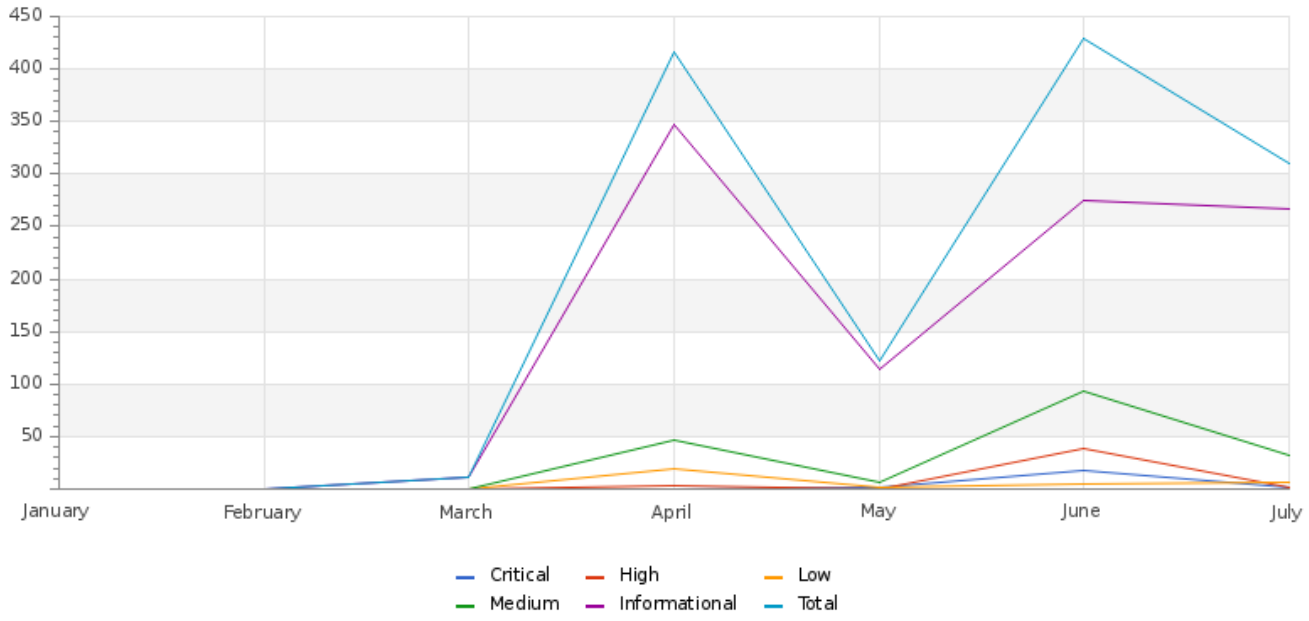
Vulnerable Host History



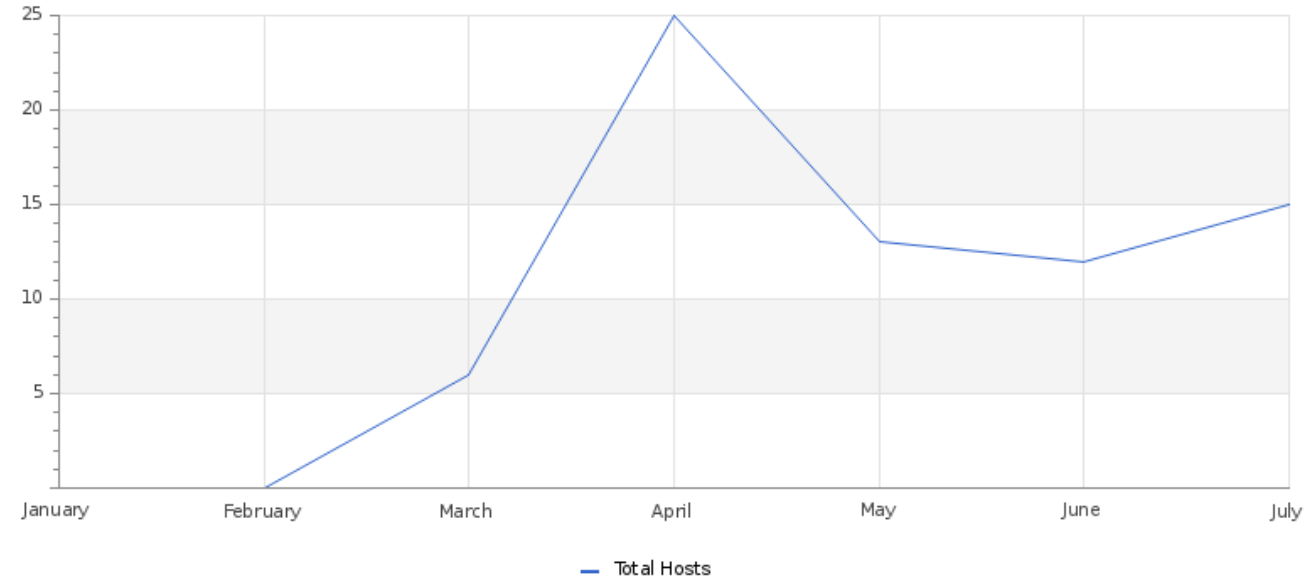
ASM-VP REPORT

Organo Judicial 07/26/2023

Vulnerability Severity History



Discovered Host History



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

Vulnerabilities Compared To Previous Month

dest	Previous	Current
190.34.182.226	6	2
190.34.182.227	6	2
190.34.182.228	6	2
190.34.182.232	7	6
190.34.182.234	39	0
190.34.182.239	8	0
190.34.182.241	32	0
190.34.182.243	10	0
190.34.182.246	39	0
190.34.182.250	19	0
IP.net126-115.psi.net.pa	6	2
IP.net126-116.psi.net.pa	6	0
IP.net126-117.psi.net.pa	6	0

Open Port Monitoring

Open Ports

ip	hostname	port	status	protocol	service
190.34.182.232		80	open	tcp	www
190.34.182.232		443	open	tcp	No Service Detected
190.34.182.227		25	open	tcp	smtp
190.34.182.227		80	open	tcp	www
190.34.182.227		264	open	tcp	fw1
190.34.182.227		443	open	tcp	www
200.46.126.116	IP.net126-116.psi.net.pa	25	open	tcp	smtp
200.46.126.116	IP.net126-116.psi.net.pa	80	open	tcp	www
200.46.126.116	IP.net126-116.psi.net.pa	264	open	tcp	fw1
200.46.126.116	IP.net126-116.psi.net.pa	443	open	tcp	www
200.46.126.116	IP.net126-116.psi.net.pa	18264	open	tcp	www
190.34.182.234		443	open	tcp	www
190.34.182.250		443	open	tcp	www
190.34.182.241		443	open	tcp	www

ASM-VP REPORT

Organo Judicial 07/26/2023

ip	hostname	port	status	protocol	service
200.46.126.115	IP.net126-115.psi.net.pa	25	open	tcp	smtp
200.46.126.115	IP.net126-115.psi.net.pa	80	open	tcp	www
200.46.126.115	IP.net126-115.psi.net.pa	264	open	tcp	fw1
200.46.126.115	IP.net126-115.psi.net.pa	443	open	tcp	www
200.46.126.115	IP.net126-115.psi.net.pa	18264	open	tcp	www
190.34.182.228		25	open	tcp	smtp
190.34.182.228		80	open	tcp	www
190.34.182.228		264	open	tcp	fw1
190.34.182.228		443	open	tcp	www
190.34.182.228		18264	open	tcp	www
190.34.182.226		25	open	tcp	smtp
190.34.182.226		80	open	tcp	www
190.34.182.226		264	open	tcp	fw1
190.34.182.226		443	open	tcp	www
200.46.126.117	IP.net126-117.psi.net.pa	25	open	tcp	smtp
200.46.126.117	IP.net126-117.psi.net.pa	80	open	tcp	www
200.46.126.117	IP.net126-117.psi.net.pa	264	open	tcp	fw1
200.46.126.117	IP.net126-117.psi.net.pa	443	open	tcp	www
200.46.126.117	IP.net126-117.psi.net.pa	18264	open	tcp	www
190.34.182.239		80	open	tcp	www
190.34.182.239		443	open	tcp	www
190.34.182.246		443	open	tcp	www

Vulnerability

MSS-BAS Email

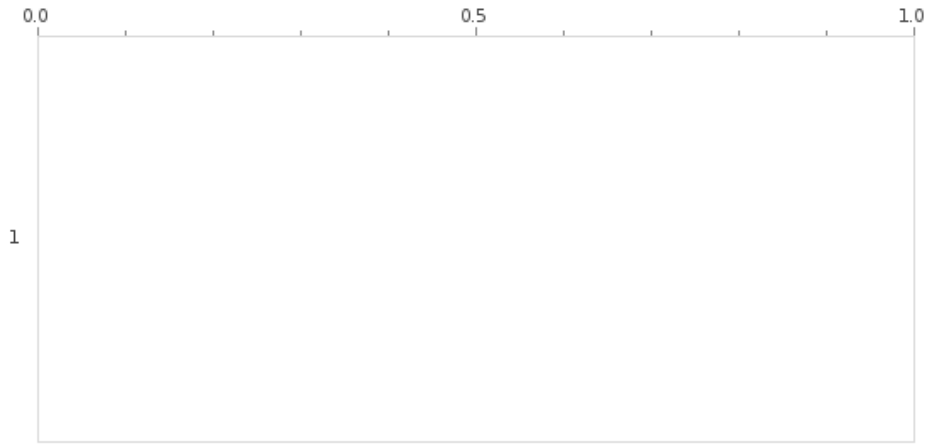
Cymulate Score

1%

Simulation Summary

Penetrated : 0 / Total Tests: 0

Emails Sent

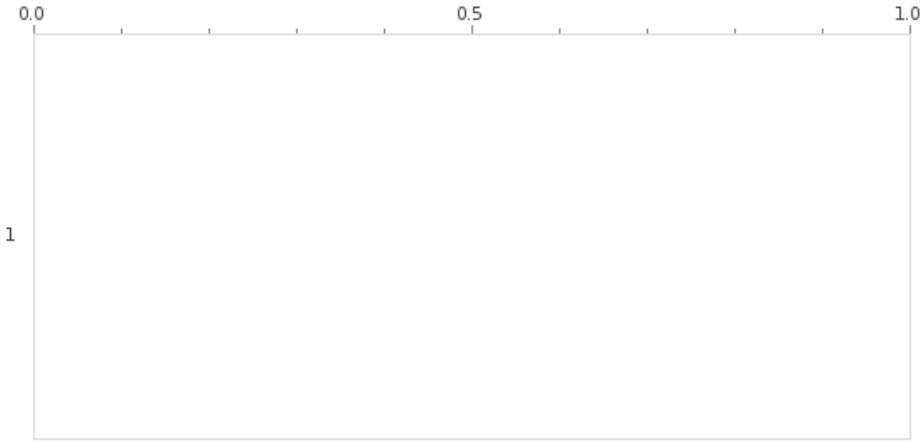


TLP:AMBER

ASM-VP REPORT

Organo Judicial 07/26/2023

Emails Penetrated



Percent Penetrated

%

Simulations Sent/Penetrated

Category	Penetrated	Total

MSS-BAS Web

Cymulate Score

54%

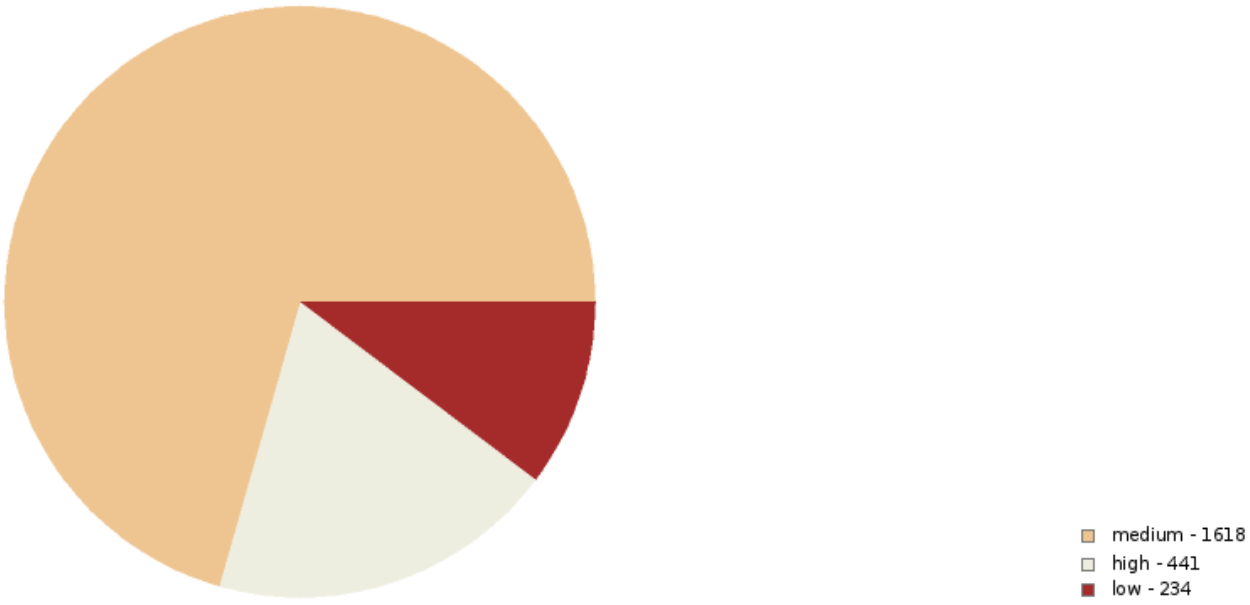
Simulation Summary

Penetrated : 3,605 / Total Tests: 13,385

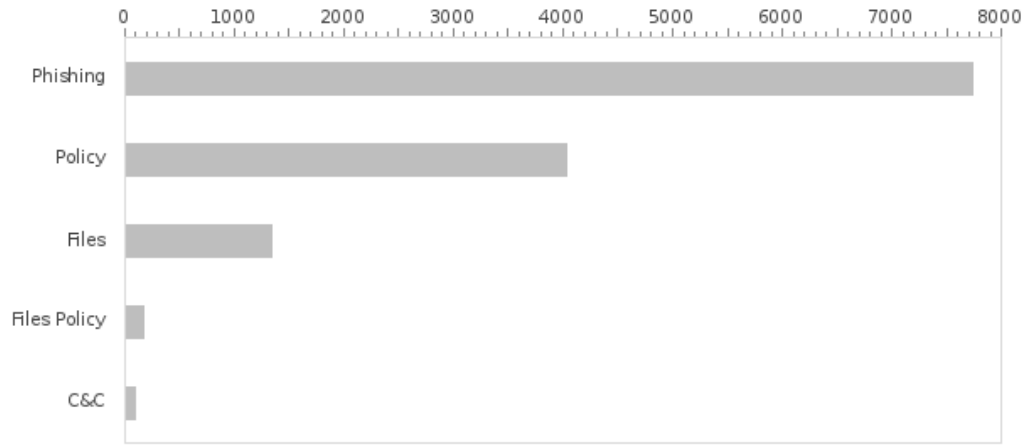
ASM-VP REPORT

Organo Judicial 07/26/2023

Penetrations by Severity



Browsing Sent

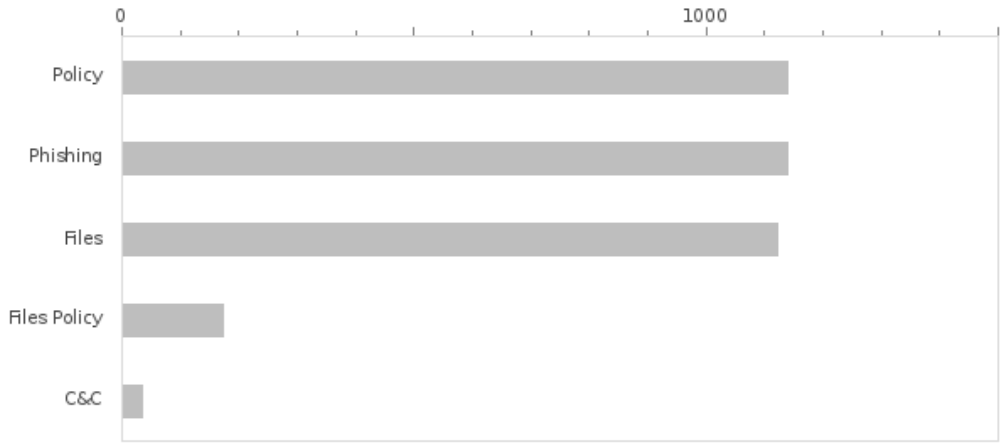


LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

ASM-VP REPORT

Organo Judicial 07/26/2023

Browsing Penetrated



Percent Penetrated

27%

Simulations Sent/Penetrated

Category	Penetrated	Total
Phishing	1138	7740
Policy	1140	4035
Files	1121	1338
Files Policy	172	174
C&C	34	98

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

Security Validation

MSS-BAS EDR

Simulation Summary

Penetrated : 0 / Sent : 0

Worm based code execution

penetrated : 0 / Total tests : 0

Percent Penetrated

%

MSS-BAS IMTHREAT

Cymulate Score

45%

Percent Penetrated

32%

Simulation Summary

Penetrated: 193 / Total: 596

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

TLP:AMBER

ASM-VP REPORT

Organo Judicial 07/26/2023

Immediate Threats Campaigns

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-07-25	Ransomware Spotlight Play	Ransomwarebgjacdgace_edr7Exe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-07-25	Ransomware Spotlight Play	Ransomwarebgjacdgace10_edrExe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-07-25	Ransomware Spotlight Play	Ransomwarebgjacdgace4_edrExe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-07-26	India Cert Alert - Mallox Ransomware Targeting Unsecured MS SQL Servers	Mallboxbgjadhhiij_edr7Exe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-07-26	India Cert Alert - Mallox Ransomware Targeting Unsecured MS SQL Servers	Mallboxbgjadhhiij15_edrBat.bat	Endpoint Security	88E1000GMSYS	Penetrated
2023-07-26	India Cert Alert - Mallox Ransomware Targeting Unsecured MS SQL Servers	Mallboxbgjadhhiij4_edrExe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-07-26	India Cert Alert - Mallox Ransomware Targeting Unsecured MS SQL Servers	Mallboxbgjadhhiij5_edrExe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-07-26	India Cert Alert - Mallox Ransomware Targeting Unsecured MS SQL Servers	Mallboxbgjadhhiij3_edrExe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-07-26	India Cert Alert - Mallox Ransomware Targeting Unsecured MS SQL Servers	Mallboxbgjadhhiij2_edrExe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-07-26	India Cert Alert - Mallox Ransomware Targeting Unsecured MS SQL Servers	Mallboxbgjadhhiij12_edrPs1.ps1	Endpoint Security	88E1000GMSYS	Blocked
2023-07-26	India Cert Alert - Mallox Ransomware Targeting Unsecured MS SQL Servers	Mallboxbgjadhhiij13_edrPs1.ps1	Endpoint Security	88E1000GMSYS	Blocked
2023-07-26	India Cert Alert - Mallox Ransomware Targeting Unsecured MS SQL Servers	Mallboxbgjadhhiij10_edrPs1.ps1	Endpoint Security	88E1000GMSYS	Blocked
2023-07-26	India Cert Alert - Mallox Ransomware Targeting Unsecured MS SQL Servers	Mallboxbgjadhhiij9_edrPs1.ps1	Endpoint Security	88E1000GMSYS	Blocked
2023-07-26	India Cert Alert - Mallox Ransomware Targeting Unsecured MS SQL Servers	Mallboxbgjadhhiij1_edrExe.exe	Endpoint Security	88E1000GMSYS	Blocked

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

ASM-VP REPORT

Organo Judicial 07/26/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-07-26	India Cert Alert - Mallox Ransomware Targeting Unsecured MS SQL Servers	hxxp://185.170.144.153	Web Gateway	88E1000GMSYS	Offline/Removed
2023-07-26	India Cert Alert - Mallox Ransomware Targeting Unsecured MS SQL Servers	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ind ia_cert_alert_-_mallox_ransomware_targeting_unsecured_ms_sql_servers_a88804f4-9b a8-4e9a-89c8-0cf1c679ae06/Mallboxbgjadhhiij8_browsingPs1.ps1?X-Amz-Algorithm=AWS 4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3 D5GWFTK3Q%2F20230726%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230726T135119Z &X-Amz-Expires=600&X-Amz-Signature=3a845a383a10309ca2a9f1e3887209a3f10226d0376da 5dd5db8be1821b9263b&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-26	India Cert Alert - Mallox Ransomware Targeting Unsecured MS SQL Servers	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ind ia_cert_alert_-_mallox_ransomware_targeting_unsecured_ms_sql_servers_a88804f4-9b a8-4e9a-89c8-0cf1c679ae06/Mallboxbgjadhhiij11_browsingPs1.ps1?X-Amz-Algorithm=AW S4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q 3D5GWFTK3Q%2F20230726%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230726T135118 Z&X-Amz-Expires=600&X-Amz-Signature=04cfb5b51e0d5c17ff24b2fdac6a0a2232ffa2095ef0 32bc7dc515dbf5698f00&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-26	India Cert Alert - Mallox Ransomware Targeting Unsecured MS SQL Servers	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ind ia_cert_alert_-_mallox_ransomware_targeting_unsecured_ms_sql_servers_a88804f4-9b a8-4e9a-89c8-0cf1c679ae06/Mallboxbgjadhhiij14_browsingBat.bat?X-Amz-Algorithm=AW S4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q 3D5GWFTK3Q%2F20230726%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230726T135111 Z&X-Amz-Expires=600&X-Amz-Signature=825ced1306ad3d9741c204928ee1a8addb3e077e62c2 bc7471d415db3d253f9f&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-26	India Cert Alert - Mallox Ransomware Targeting Unsecured MS SQL Servers	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ind ia_cert_alert_-_mallox_ransomware_targeting_unsecured_ms_sql_servers_a88804f4-9b a8-4e9a-89c8-0cf1c679ae06/Mallboxbgjadhhiij6_browsingExe.exe?X-Amz-Algorithm=AWS 4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3 D5GWFTK3Q%2F20230726%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230726T135101Z &X-Amz-Expires=600&X-Amz-Signature=0cf3469ff1e1b55b1a0c6ace7653819d34a36a4cce8bb b8c7cd05d44aa023d0a&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-26	First-ever Open-Source Software Supply Chain Attacks	Firsteverbgjacahebh49_edrExe.exe	Endpoint Security	88E1000GMSYS	Penetrated
2023-07-26	First-ever Open-Source Software Supply Chain Attacks	Firsteverbgjacahebh54_edrElf.elf	Endpoint Security	88E1000GMSYS	Blocked
2023-07-26	First-ever Open-Source Software Supply Chain Attacks	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/fir st-ever_open-source_software_supply_chain_attacks_6df0d247-55bd-4848-a6e9-ebf2f8 cd6517/Firsteverbgjacahebh52_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X- Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F2023 0726%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230726T074836Z&X-Amz-Expires=6 00&X-Amz-Signature=89dc6f8d5c0ccd14e75b69134f8f262befed8e37e49506e47e29da0db4b7f 83a&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-26	First-ever Open-Source Software Supply Chain Attacks	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/fir st-ever_open-source_software_supply_chain_attacks_6df0d247-55bd-4848-a6e9-ebf2f8 cd6517/Firsteverbgjacahebh51_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X- Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F2023 0726%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230726T074828Z&X-Amz-Expires=6 00&X-Amz-Signature=96256aa5ec34348f19ca6e6565ecf5854d6ceb2a3b4413e5401312024f553 a47&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-26	New Reptile Rootkit Malware Attacking Linux Systems Using Port Knocking	Newbgjadaaiej1_edrSh.sh	Endpoint Security	88E1000GMSYS	Penetrated
2023-07-26	New Reptile Rootkit Malware Attacking Linux Systems Using Port Knocking	Newbgjadaaiej3_edrO.o	Endpoint Security	88E1000GMSYS	Blocked
2023-07-26	New Reptile Rootkit Malware Attacking Linux Systems Using Port Knocking	Newbgjadaaiej8_edrO.o	Endpoint Security	88E1000GMSYS	Blocked
2023-07-26	New Reptile Rootkit Malware Attacking Linux Systems Using Port Knocking	Newbgjadaaiej2_edrO.o	Endpoint Security	88E1000GMSYS	Blocked

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

ASM-VP REPORT

Organo Judicial 07/26/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-07-26	New Reptile Rootkit Malware Attacking Linux Systems Using Port Knocking	Newbgjadaaiej9_edrElf.elf	Endpoint Security	88E1000GMSYS	Blocked
2023-07-26	New Reptile Rootkit Malware Attacking Linux Systems Using Port Knocking	Newbgjadaaiej6_edrElf.elf	Endpoint Security	88E1000GMSYS	Blocked
2023-07-26	New Reptile Rootkit Malware Attacking Linux Systems Using Port Knocking	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/new_reptile_rootkit_malware_attacking_linux_systems_using_port_knocking_c90e131d-0bd0-4024-978d-6ccdbb54f8c0/Newbgjadaaiej_browsing7Elf.elf?X-Amz-Algorithm=AWS4-HM AC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GW FTK3Q%2F20230726%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230726T074229Z&X-Amz-Expires=600&X-Amz-Signature=c77a83a0d61e93d1fe41e04d1df631d6a4d4ee5ed3b5eaccc de38ee521522798&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-26	New Reptile Rootkit Malware Attacking Linux Systems Using Port Knocking	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/new_reptile_rootkit_malware_attacking_linux_systems_using_port_knocking_c90e131d-0bd0-4024-978d-6ccdbb54f8c0/NewbgjadaaiejO.o?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230726%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230726T074227Z&X-Amz-Expires=600&X-Amz-Signature=e0696d88c7bf0003c6fb52f986aeaff6113dcc733cafa9191ca7cfe0e823404d&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-26	New Reptile Rootkit Malware Attacking Linux Systems Using Port Knocking	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/new_reptile_rootkit_malware_attacking_linux_systems_using_port_knocking_c90e131d-0bd0-4024-978d-6ccdbb54f8c0/NewbgjadaaiejO.o?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230726%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230726T074225Z&X-Amz-Expires=600&X-Amz-Signature=d5e56a1959b644f1ef23595adf6a7b8c090f6e283db76715ded1d1f9e55b9403&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-25	Ransomware Spotlight Play	Ransomwarebgjacdgace2_edrExe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-07-25	Ransomware Spotlight Play	Ransomwarebgjacdgace8_edrExe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-07-25	Ransomware Spotlight Play	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ransomware_spotlight_play_9c7a6699-8793-486d-b28c-2b289d802cf8/Ransomwarebgjacdgace14_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNE D-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230725%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230725T060209Z&X-Amz-Expires=600&X-Amz-Signature=cba716fdf82231c070dd4caef38b1cb4a8140a6ca3627b9ac721219ca770be9f&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-25	Ransomware Spotlight Play	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ransomware_spotlight_play_9c7a6699-8793-486d-b28c-2b289d802cf8/Ransomwarebgjacdgace12_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNE D-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230725%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230725T060208Z&X-Amz-Expires=600&X-Amz-Signature=014839510bc6685bf6642a3780d902a66c3b8e98515d99e5e1c017f150b77e99&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-25	Ransomware Spotlight Play	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ransomware_spotlight_play_9c7a6699-8793-486d-b28c-2b289d802cf8/Ransomwarebgjacdgace11_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNE D-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230725%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230725T060203Z&X-Amz-Expires=600&X-Amz-Signature=34cf12c90c08701025a15f92a7ead3e0e1a1f23d17b3fd754413b4c94413ef85&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-25	Ransomware Spotlight Play	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ransomware_spotlight_play_9c7a6699-8793-486d-b28c-2b289d802cf8/Ransomwarebgjacdgace9_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED - PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230725%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230725T060202Z&X-Amz-Expires=600&X-Amz-Signature=a3d9de6e3ee828ab4c3f21e240cfc53d50b61b7a8006ef7958cadeede1fbdf5b&X-Amz-SignedHeaders=hos t&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-25	Ransomware Spotlight Play	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ransomware_spotlight_play_9c7a6699-8793-486d-b28c-2b289d802cf8/Ransomwarebgjacdgace5_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED - PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230725%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230725T060159Z&X-Amz-Expires=600&X-Amz-Signature=e2076b7ca3ce2243be8ca03f80f4d3009cc6abfc2b50d3e6f750b6efb944d0f0&X-Amz-SignedHeaders=hos t&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-25	Ransomware Spotlight Play	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ransomware_spotlight_play_9c7a6699-8793-486d-b28c-2b289d802cf8/Ransomwarebgjacdgace3_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED - PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230725%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230725T060158Z&X-Amz-Expires=600&X-Amz-Signature=7c657314a8a83491242e94634f71fb9e46a59d4bdceb0a129f4489096550f16e&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated

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

ASM-VP REPORT

Organo Judicial 07/26/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-07-25	Ransomware Spotlight Play	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ransomware_spotlight_play_9c7a6699-8793-486d-b28c-2b289d802cf8/Ransomwarebgjacdgace1_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230725%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230725T060145Z&X-Amz-Expires=600&X-Amz-Signature=21764fbc82c7e518aceb4d2174a8ab54405f92fc116cadc5b19e0ac67b333a5f&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-24	UAC-0006 Distributes SmokeLoader Through Phishing Emails (CERT-UA6999)	Uac0006bgijhdcdcg13_edrHtml.html	Endpoint Security	88E1000GMSYS	Blocked
2023-07-24	UAC-0006 Distributes SmokeLoader Through Phishing Emails (CERT-UA6999)	Uac0006bgijhdcdcg14_edrZip.zip	Endpoint Security	88E1000GMSYS	Blocked
2023-07-24	UAC-0006 Distributes SmokeLoader Through Phishing Emails (CERT-UA6999)	Uac0006bgijhdcdcg20_edrExe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-07-24	UAC-0006 Distributes SmokeLoader Through Phishing Emails (CERT-UA6999)	hxxp://193.106.174.173	Web Gateway	88E1000GMSYS	Offline/Removed
2023-07-24	UAC-0006 Distributes SmokeLoader Through Phishing Emails (CERT-UA6999)	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/uac-0006_distributes_smokeloader_through_phishing_emails_%28cert-ua6999%29_8b19babc-f0b4-4e71-8fb3-facdc03755d6/Uac0006bgijhdcdcg16_browsingZip.zip?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230724%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230724T070035Z&X-Amz-Expires=600&X-Amz-Signature=fc9a36937988114f8a63978553b0ed8c7368a372d7a5be0584545b768cab6086&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-24	UAC-0006 Distributes SmokeLoader Through Phishing Emails (CERT-UA6999)	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/uac-0006_distributes_smokeloader_through_phishing_emails_%28cert-ua6999%29_8b19babc-f0b4-4e71-8fb3-facdc03755d6/Uac0006bgijhdcdcg19_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230724%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230724T070035Z&X-Amz-Expires=600&X-Amz-Signature=b840dd24d25eab85239ffb58702dbc7ff7bab264bca32a21da5c2c96116f2b37&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-24	UAC-0006 Distributes SmokeLoader Through Phishing Emails (CERT-UA6999)	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/uac-0006_distributes_smokeloader_through_phishing_emails_%28cert-ua6999%29_8b19babc-f0b4-4e71-8fb3-facdc03755d6/Uac0006bgijhdcdcg15_browsingZip.zip?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230724%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230724T070034Z&X-Amz-Expires=600&X-Amz-Signature=edb9cdac08070a5446841072abfa616aabcccfca95803ec396bbe326660e56da&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-24	UAC-0006 Distributes SmokeLoader Through Phishing Emails (CERT-UA6999)	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/uac-0006_distributes_smokeloader_through_phishing_emails_%28cert-ua6999%29_8b19babc-f0b4-4e71-8fb3-facdc03755d6/Uac0006bgijhdcdcg21_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230724%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230724T070033Z&X-Amz-Expires=600&X-Amz-Signature=d7a832eb986ba0adcf05fc9d001bd04814f04d919afc7d45e14bce09ebb38a72&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-24	UAC-0006 Distributes SmokeLoader Through Phishing Emails (CERT-UA6999)	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/uac-0006_distributes_smokeloader_through_phishing_emails_%28cert-ua6999%29_8b19babc-f0b4-4e71-8fb3-facdc03755d6/Uac0006bgijhdcdcg1_browsing7Php.php?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230724%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230724T070026Z&X-Amz-Expires=600&X-Amz-Signature=a5421e19a6494fd52530e8ffe9e0306687aea8101357e39938a09b67c44fefc4&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-24	Ursnif campaign in Italy	hxxp://109.105.198.129/pictures/...	Web Gateway	88E1000GMSYS	Offline/Removed
2023-07-24	Ursnif campaign in Italy	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ursnif_campaign_in_italy_dcb21441-3f3a-4596-a36a-f8929756993e/UrsnifbgijhigahI4_browsingPs1.ps1?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230724%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230724T065530Z&X-Amz-Expires=600&X-Amz-Signature=ea9d5e6ed2ad8ffd3a8aa12c5d11b00f1f6cee80b761422f5580d4610a223305&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated

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

ASM-VP REPORT

Organo Judicial 07/26/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-07-24	Ursnif campaign in Italy	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/urs nif_campaign_in_italy_dcb21441-3f3a-4596-a36a-f8929756993e/Ursnifbgijhigahi1_bro wsingDll.dll?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYL OAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230724%2Feu-west-1%2Fs3%2Faws4_req uest&X-Amz-Date=20230724T065527Z&X-Amz-Expires=600&X-Amz-Signature=194f06cf4a24a d2a9fd7799846fb4c7b706d858f931aca8d6f773a122412fac0&X-Amz-SignedHeaders=host&x-i d=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-23	Manipulated Caiman: The Sophisticated Snare of Mexico's Banking Predator	Manipulatedcaimanbgjabaaibd15_edrExe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-07-23	Manipulated Caiman: The Sophisticated Snare of Mexico's Banking Predator	Manipulatedcaimanbgjabaaibd11_edrExe.exe	Endpoint Security	88E1000GMSYS	Penetrated
2023-07-23	Manipulated Caiman: The Sophisticated Snare of Mexico's Banking Predator	Manipulatedcaimanbgjabaaibd14_edrJs.js	Endpoint Security	88E1000GMSYS	Blocked
2023-07-23	Manipulated Caiman: The Sophisticated Snare of Mexico's Banking Predator	Manipulatedcaimanbgjabaaibd12_edrExe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-07-23	Manipulated Caiman: The Sophisticated Snare of Mexico's Banking Predator	Manipulatedcaimanbgjabaaibd3_edrExe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-07-23	Manipulated Caiman: The Sophisticated Snare of Mexico's Banking Predator	Manipulatedcaimanbgjabaaibd8_edrExe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-07-23	Manipulated Caiman: The Sophisticated Snare of Mexico's Banking Predator	Manipulatedcaimanbgjabaaibd_edr7Exe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-07-23	Manipulated Caiman: The Sophisticated Snare of Mexico's Banking Predator	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/man ipulated_caiman%3A_the_sophisticated_snare_of_mexico%27s_banking_predator_4b5849 7a-83ae-4fdd-bb38-8219794cb25b/Manipulatedcaimanbgjabaaibd1_browsingExe.exe?X-Am z-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credent ial=AKIAJPJC2Q3D5GWFTK3Q%2F20230723%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=2 0230723T085427Z&X-Amz-Expires=600&X-Amz-Signature=0491a62dfe221ffff07417eccda4d8 445b4a8214e670c4f33b041e8bbeab740b&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-23	Manipulated Caiman: The Sophisticated Snare of Mexico's Banking Predator	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/man ipulated_caiman%3A_the_sophisticated_snare_of_mexico%27s_banking_predator_4b5849 7a-83ae-4fdd-bb38-8219794cb25b/Manipulatedcaimanbgjabaaibd2_browsingExe.exe?X-Am z-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credent ial=AKIAJPJC2Q3D5GWFTK3Q%2F20230723%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=2 0230723T085427Z&X-Amz-Expires=600&X-Amz-Signature=113b43de0f25971215607d70321a84 5999177caeb047cb8a105e1ebca333bcf0&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-23	Manipulated Caiman: The Sophisticated Snare of Mexico's Banking Predator	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/man ipulated_caiman%3A_the_sophisticated_snare_of_mexico%27s_banking_predator_4b5849 7a-83ae-4fdd-bb38-8219794cb25b/Manipulatedcaimanbgjabaaibd4_browsingExe.exe?X-Am z-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credent ial=AKIAJPJC2Q3D5GWFTK3Q%2F20230723%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=2 0230723T085426Z&X-Amz-Expires=600&X-Amz-Signature=bbaf3a6764eb74ae2c0aa13382ff51 b4b47021f3385496ce8edf608ed9337466&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-23	Manipulated Caiman: The Sophisticated Snare of Mexico's Banking Predator	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/man ipulated_caiman%3A_the_sophisticated_snare_of_mexico%27s_banking_predator_4b5849 7a-83ae-4fdd-bb38-8219794cb25b/Manipulatedcaimanbgjabaaibd5_browsingExe.exe?X-Am z-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credent ial=AKIAJPJC2Q3D5GWFTK3Q%2F20230723%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=2 0230723T085424Z&X-Amz-Expires=600&X-Amz-Signature=2b7465d1860a6a5fb51d951405d690 ddec83150009ba1b311b66093ee8f90a7c&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-23	Manipulated Caiman: The Sophisticated Snare of Mexico's Banking Predator	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/man ipulated_caiman%3A_the_sophisticated_snare_of_mexico%27s_banking_predator_4b5849 7a-83ae-4fdd-bb38-8219794cb25b/Manipulatedcaimanbgjabaaibd6_browsingExe.exe?X-Am z-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credent ial=AKIAJPJC2Q3D5GWFTK3Q%2F20230723%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=2 0230723T085417Z&X-Amz-Expires=600&X-Amz-Signature=d2539f209bcc6e18bece3d5f786e0d 02eeb5eb0294041732fa410312779150ef&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated

TLP:AMBER

GLESEC
COMPLETELY PERCEPTI

ASM-VP REPORT

Organo Judicial 07/26/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-07-23	Manipulated Caiman: The Sophisticated Snare of Mexico's Banking Predator	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/manipulated_caiman%3A_the_sophisticated_snare_of_mexico%27s_banking_predator_4b58497a-83ae-4fdd-bb38-8219794cb25b/Manipulatedcaimanbgjabaaibd9_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230723%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230723T085403Z&X-Amz-Expires=600&X-Amz-Signature=33950823fd820f089c6854242a721ca440ae9e0135a46b5a88298773c6b3ac43&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-23	Manipulated Caiman: The Sophisticated Snare of Mexico's Banking Predator	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/manipulated_caiman%3A_the_sophisticated_snare_of_mexico%27s_banking_predator_4b58497a-83ae-4fdd-bb38-8219794cb25b/Manipulatedcaimanbgjabaaibd10_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230723%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230723T085403Z&X-Amz-Expires=600&X-Amz-Signature=ac011453f1c290103cfda846f7b410003adb61fe48bf9295c03fc22ca6b0f993&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-23	Manipulated Caiman: The Sophisticated Snare of Mexico's Banking Predator	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/manipulated_caiman%3A_the_sophisticated_snare_of_mexico%27s_banking_predator_4b58497a-83ae-4fdd-bb38-8219794cb25b/Manipulatedcaimanbgjabaaibd13_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230723%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230723T085401Z&X-Amz-Expires=600&X-Amz-Signature=f5711e35eb56311a8b081bbec9cb9bc55069ae683839a4d0120654f3adf0a76c&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-23	A Look Into Space Pirates Unconventional Techniques Attack Vectors And Tools	Abgijibigeg18_edrDll.dll	Endpoint Security	88E1000GMSYS	Penetrated
2023-07-23	A Look Into Space Pirates Unconventional Techniques Attack Vectors And Tools	Abgijibigeg21_edrDll.dll	Endpoint Security	88E1000GMSYS	Penetrated
2023-07-23	A Look Into Space Pirates Unconventional Techniques Attack Vectors And Tools	Abgijibigeg64_edrExe.exe	Endpoint Security	88E1000GMSYS	Penetrated
2023-07-23	A Look Into Space Pirates Unconventional Techniques Attack Vectors And Tools	Abgijibigeg63_edrExe.exe	Endpoint Security	88E1000GMSYS	Penetrated
2023-07-23	A Look Into Space Pirates Unconventional Techniques Attack Vectors And Tools	Abgijibigeg66_edrExe.exe	Endpoint Security	88E1000GMSYS	Penetrated
2023-07-23	A Look Into Space Pirates Unconventional Techniques Attack Vectors And Tools	Abgijibigeg58_edrExe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-07-23	A Look Into Space Pirates Unconventional Techniques Attack Vectors And Tools	Abgijibigeg23_edrDll.dll	Endpoint Security	88E1000GMSYS	Blocked
2023-07-23	A Look Into Space Pirates Unconventional Techniques Attack Vectors And Tools	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/a_look_into_space_pirates_unconventional_techniques_attack_vectors_and_tools_995867 c2-733c-4527-bde5-5c324ac95e6d/Abgijibigeg6_browsing7Exe.exe?X-Amz-Algorithm=AWS 4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230723%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230723T064053Z&X-Amz-Expires=600&X-Amz-Signature=acd824f22e556b3f514f2ab7b01c19960579e6e5ade984a500429281e7e38909&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-23	A Look Into Space Pirates Unconventional Techniques Attack Vectors And Tools	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/a_look_into_space_pirates_unconventional_techniques_attack_vectors_and_tools_995867 c2-733c-4527-bde5-5c324ac95e6d/Abgijibigeg65_browsingExe.exe?X-Amz-Algorithm=AWS 4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230723%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230723T064050Z&X-Amz-Expires=600&X-Amz-Signature=47821cf36bdd455befd90366c31b85c9d5813061f0349f950be59e6a2a0867ad&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated

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

TLP:AMBER

GLESEC
COMPLETELY PERCEPTI

ASM-VP REPORT

Organo Judicial 07/26/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-07-23	A Look Into Space Pirates Unconventional Techniques Attack Vectors And Tools	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/a_look_into_space_pirates_unconventional_techniques_attack_vectors_and_tools_995867 c2-733c-4527-bde5-5c324ac95e6d/Abgijibigeg62_browsingExe.exe?X-Amz-Algorithm=AWS 4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3 D5GWFTK3Q%2F20230723%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230723T064038Z &X-Amz-Expires=600&X-Amz-Signature=7692247330acff4b4c4323072ce03f8781ed0a55e828a c17818e9b18c2b4ea62&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-23	A Look Into Space Pirates Unconventional Techniques Attack Vectors And Tools	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/a_look_into_space_pirates_unconventional_techniques_attack_vectors_and_tools_995867 c2-733c-4527-bde5-5c324ac95e6d/Abgijibigeg30_browsingDll.dll?X-Amz-Algorithm=AWS 4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3 D5GWFTK3Q%2F20230723%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230723T064032Z &X-Amz-Expires=600&X-Amz-Signature=c75397c2e9f8aa2e7c807a8bd0225df2b5a79316abda8 dd338404f628ff48c09&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-23	A Look Into Space Pirates Unconventional Techniques Attack Vectors And Tools	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/a_look_into_space_pirates_unconventional_techniques_attack_vectors_and_tools_995867 c2-733c-4527-bde5-5c324ac95e6d/Abgijibigeg28_browsingDll.dll?X-Amz-Algorithm=AWS 4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3 D5GWFTK3Q%2F20230723%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230723T064032Z &X-Amz-Expires=600&X-Amz-Signature=2c8790df1b75b89296c254a7a9bf93f9422f0fd9e99bc 5c5e429b32a5a41fa7a&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-23	A Look Into Space Pirates Unconventional Techniques Attack Vectors And Tools	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/a_look_into_space_pirates_unconventional_techniques_attack_vectors_and_tools_995867 c2-733c-4527-bde5-5c324ac95e6d/Abgijibigeg24_browsingDll.dll?X-Amz-Algorithm=AWS 4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3 D5GWFTK3Q%2F20230723%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230723T064030Z &X-Amz-Expires=600&X-Amz-Signature=cf8db055c4f94b2939f541a8a673eb02642339b9b52c2 cfd3b71413682675d91&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-23	A Look Into Space Pirates Unconventional Techniques Attack Vectors And Tools	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/a_look_into_space_pirates_unconventional_techniques_attack_vectors_and_tools_995867 c2-733c-4527-bde5-5c324ac95e6d/Abgijibigeg22_browsingDll.dll?X-Amz-Algorithm=AWS 4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3 D5GWFTK3Q%2F20230723%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230723T064029Z &X-Amz-Expires=600&X-Amz-Signature=7a79a3b4cd665c9671e4cb3a646cdf2f8f7e3e5408dd4 8fba35220b9755a31f0&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-23	Threat Actor Launches ScarLeteel 2.00	Threatbgijdaabfc2_edrSh.sh	Endpoint Security	88E1000GMSYS	Blocked
2023-07-23	Threat Actor Launches ScarLeteel 2.00	Threatbgijdaabfc4_edrSh.sh	Endpoint Security	88E1000GMSYS	Blocked
2023-07-23	Threat Actor Launches ScarLeteel 2.00	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/threat_actor_launches_scarleteel_2.0_5c3a31c4-d75d-4f35-8a4e-ab9dc96ff553/Threatbgijdaabfc3_browsingSh.sh?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230723%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230723T063750Z&X-Amz-Expires=600&X-Amz-Signature=c4fe484b6eb4d49cff6a104ab960fd7ab01d0384a83f17ba7208aa2e948cd058&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-20	The Turla APT Group Uses Multiple Malware Families To Exfiltrate Data (CERT-UA6981)	hxxps://mail.kzp.bg/outlook/api/logoff.aspx	Web Gateway	88E1000GMSYS	Offline/Removed
2023-07-20	The Turla APT Group Uses Multiple Malware Families To Exfiltrate Data (CERT-UA6981)	Thebgijibifhf1_edrDll.dll	Endpoint Security	88E1000GMSYS	Blocked
2023-07-20	DDoS Botnet Targets Zyxel Vulnerability (CVE-2023-28771)	Ddosbgijibiigd_edr78Elf.elf	Endpoint Security	88E1000GMSYS	Blocked
2023-07-20	DDoS Botnet Targets Zyxel Vulnerability (CVE-2023-28771)	Ddosbgijibiigd86_edrElf.elf	Endpoint Security	88E1000GMSYS	Blocked
2023-07-20	DDoS Botnet Targets Zyxel Vulnerability (CVE-2023-28771)	Ddosbgijibiigd80_edrElf.elf	Endpoint Security	88E1000GMSYS	Blocked
2023-07-20	DDoS Botnet Targets Zyxel Vulnerability (CVE-2023-28771)	Ddosbgijibiigd84_edrElf.elf	Endpoint Security	88E1000GMSYS	Blocked
2023-07-20	DDoS Botnet Targets Zyxel Vulnerability (CVE-2023-28771)	hxxp://109.207.200.44	Web Gateway	88E1000GMSYS	Offline/Removed

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

TLP:AMBER

GLESEC
COMPLETELY PERCEPTI

ASM-VP REPORT

Organo Judicial 07/26/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-07-20	DDoS Botnet Targets Zyxel Vulnerability (CVE-2023-28771)	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ddos_botnet_targets_zyxel_vulnerability_%28cve-2023-28771%29_726e7b63-4627-4776-a657-7c9d9a38820c/Ddosbgijibiigd83_browsingElf.elf?X-Amz-Algorithm=AWS4-HMAC-SHA256 &X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230720%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230720T053405Z&X-Amz-Expires=600&X-Amz-Signature=fa1f77dabdbeb680c91c317e74d92f79d139d3fc0da7320487c54f6fbdb12efb&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-20	DDoS Botnet Targets Zyxel Vulnerability (CVE-2023-28771)	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ddos_botnet_targets_zyxel_vulnerability_%28cve-2023-28771%29_726e7b63-4627-4776-a657-7c9d9a38820c/Ddosbgijibiigd82_browsingElf.elf?X-Amz-Algorithm=AWS4-HMAC-SHA256 &X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230720%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230720T053404Z&X-Amz-Expires=600&X-Amz-Signature=164cdda35a54b60f4a7dc4be1972ca306fa18d67f790c9c8437dac6bab614b31&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-20	DDoS Botnet Targets Zyxel Vulnerability (CVE-2023-28771)	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ddos_botnet_targets_zyxel_vulnerability_%28cve-2023-28771%29_726e7b63-4627-4776-a657-7c9d9a38820c/Ddosbgijibiigd81_browsingElf.elf?X-Amz-Algorithm=AWS4-HMAC-SHA256 &X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230720%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230720T053403Z&X-Amz-Expires=600&X-Amz-Signature=ce6c64cf3e5840439be7adb16593880d2da2a4fa9ea4f8e5b8b0398b8055d428&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-20	DDoS Botnet Targets Zyxel Vulnerability (CVE-2023-28771)	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ddos_botnet_targets_zyxel_vulnerability_%28cve-2023-28771%29_726e7b63-4627-4776-a657-7c9d9a38820c/Ddosbgijibiigd_browsing79Elf.elf?X-Amz-Algorithm=AWS4-HMAC-SHA256 &X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230720%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230720T053402Z&X-Amz-Expires=600&X-Amz-Signature=4621f556015ac21a132c85fb018fc00a12d2f8693d94448398de8bcc1fd32de8&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-20	DDoS Botnet Targets Zyxel Vulnerability (CVE-2023-28771)	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ddos_botnet_targets_zyxel_vulnerability_%28cve-2023-28771%29_726e7b63-4627-4776-a657-7c9d9a38820c/Ddosbgijibiigd_browsing77Elf.elf?X-Amz-Algorithm=AWS4-HMAC-SHA256 &X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230720%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230720T053358Z&X-Amz-Expires=600&X-Amz-Signature=c87fe9977236e5f4c0618d2da4c1c8f7cabbfd1a2bc2f093aca4bcd023b6d266&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-18	Infamous Meduza Stealer	Infamousbgijcbdjad11_edrExe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-07-18	Infamous Meduza Stealer	Infamousbgijcbdjad14_edrExe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-07-18	Infamous Meduza Stealer	Infamousbgijcbdjad1_edr7Exe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-07-18	Infamous Meduza Stealer	Infamousbgijcbdjad13_edrExe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-07-18	Infamous Meduza Stealer	Infamousbgijcbdjad16_edrExe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-07-18	Infamous Meduza Stealer	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/infamous_meduza_stealer_21000adb-78d3-4a28-94c3-8427f297ac31/Infamousbgijcbdjad21_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230718%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230718T065248Z&X-Amz-Expires=600&X-Amz-Signature=ba7cc48412c3e1bab37dba48baf8b394833ef0c3e81739aee6a378f8c2ac451e&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-18	Infamous Meduza Stealer	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/infamous_meduza_stealer_21000adb-78d3-4a28-94c3-8427f297ac31/Infamousbgijcbdjad20_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230718%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230718T065247Z&X-Amz-Expires=600&X-Amz-Signature=fbf283a8c15dde6e71387e8d06359844b1ff2f42b8b48b942160bcfc03f07b88&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-18	Infamous Meduza Stealer	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/infamous_meduza_stealer_21000adb-78d3-4a28-94c3-8427f297ac31/Infamousbgijcbdjad12_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230718%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230718T065245Z&X-Amz-Expires=600&X-Amz-Signature=db858f9bf0e3d6cfe22ca96d31578ccc02c747bd4fb64f15689ed0b0c24e9692&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-18	Infamous Meduza Stealer	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/infamous_meduza_stealer_21000adb-78d3-4a28-94c3-8427f297ac31/Infamousbgijcbdjad15_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230718%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230718T065243Z&X-Amz-Expires=600&X-Amz-Signature=04e02f9e0de4dfd728944ceb1d8537f58b4882746168eaaa66d3e5dfe6d3ad05&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-18	Infamous Meduza Stealer	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/infamous_meduza_stealer_21000adb-78d3-4a28-94c3-8427f297ac31/Infamousbgijcbdjad18_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230718%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230718T065242Z&X-Amz-Expires=600&X-Amz-Signature=3408615f754b9a9c3818c7e94d583653994f5159b05bdf30da41b92d39039cec&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated

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

TLP:AMBER

GLESEC
COMPLETELY PERCEPTI

ASM-VP REPORT

Organo Judicial 07/26/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-07-18	Infamous Meduza Stealer	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/infamous_meduza_stealer_21000adb-78d3-4a28-94c3-8427f297ac31/Infamousbgijcbdjad19_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230718%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230718T065232Z&X-Amz-Expires=600&X-Amz-Signature=8c6ccd1fc054bbcc602c4b7398690ee485a6cab92567fb73bac9b44539373c55&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-18	APT36 Delivers Crimson RAT Using Pilgrimage Security Briefing Lure	Apt36bgijdaafca_edr77Exe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-07-18	APT36 Delivers Crimson RAT Using Pilgrimage Security Briefing Lure	Apt36bgijdaafca80_edrDocx.docx	Endpoint Security	88E1000GMSYS	Penetrated
2023-07-18	APT36 Delivers Crimson RAT Using Pilgrimage Security Briefing Lure	Apt36bgijdaafca81_edrZip.zip	Endpoint Security	88E1000GMSYS	Penetrated
2023-07-18	APT36 Delivers Crimson RAT Using Pilgrimage Security Briefing Lure	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/apt36_delivers_crimson_rat_using_pilgrimage_security_briefing_lure_d3803684-14d2-4b40-97f4-11d6c9cba750/Apt36bgijdaafca_browsing79Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230718%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230718T055530Z&X-Amz-Expires=600&X-Amz-Signature=db79a716885b9c95a150b3be234670d1847bff1adcd923e44c81cb19c53e7745&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Blocked
2023-07-10	Operation Brainleeches Targets Microsoft 365 Users	Operationbgiihibied11_edrJs.js	Endpoint Security	OMY-EDIF-HE-LS	Penetrated
2023-07-10	Operation Brainleeches Targets Microsoft 365 Users	hxxp://137.184.153.238	Web Gateway	OMY-EDIF-HE-LS	Offline/Removed
2023-07-10	TeamTNT Targets Cloud Native Environments	Teamtntbgiigjfdih1_edrElf.elf	Endpoint Security	OMY-EDIF-HE-LS	Penetrated
2023-07-10	TeamTNT Targets Cloud Native Environments	Teamtntbgiigjfdih2_edrElf.elf	Endpoint Security	OMY-EDIF-HE-LS	Blocked
2023-07-09	US Cert Alert - (AA23-187A) Increased Truebot Activity Infects U.S. And Canada Networks	Truebotbgiiijfbga9_edrDll.dll	Endpoint Security	OMY-EDIF-HE-LS	Blocked
2023-07-09	US Cert Alert - (AA23-187A) Increased Truebot Activity Infects U.S. And Canada Networks	Truebotbgiiijfbga5_edrExe.exe	Endpoint Security	OMY-EDIF-HE-LS	Blocked
2023-07-09	US Cert Alert - (AA23-187A) Increased Truebot Activity Infects U.S. And Canada Networks	Truebotbgiiijfbga8_edrDll.dll	Endpoint Security	OMY-EDIF-HE-LS	Blocked
2023-07-09	US Cert Alert - (AA23-187A) Increased Truebot Activity Infects U.S. And Canada Networks	Truebotbgiiijfbga6_edrExe.exe	Endpoint Security	OMY-EDIF-HE-LS	Blocked
2023-07-09	US Cert Alert - (AA23-187A) Increased Truebot Activity Infects U.S. And Canada Networks	Truebotbgiiijfbga2_edrExe.exe	Endpoint Security	OMY-EDIF-HE-LS	Blocked
2023-07-09	US Cert Alert - (AA23-187A) Increased Truebot Activity Infects U.S. And Canada Networks	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/us_cert_alert_-_%28aa23-187a%29_increased_truebot_activity_infects_u.s.and_canada_networks_c18bd470-6c4d-4289-a966-659944d071c9/Truebotbgiiijfbga_browsing7Dll.dll? X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230709T103014Z&X-Amz-Expires=600&X-Amz-Signature=1aff5fae03fa4969cffeaf7406d89ab0b2d80f28b9bdca8cdee3b84c73e4b848&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY-EDIF-HE-LS	Penetrated

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

TLP:AMBER

GLESEC
COMPLETELY PERCEPTI

ASM-VP REPORT

Organo Judicial 07/26/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-07-09	US Cert Alert - (AA23-187A) Increased Truebot Activity Infects U.S. And Canada Networks	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/us_ cert_alert_-_%28aa23-187a%29_increased_truebot_activity_infects_u.s.and_canada_networks_c18bd470-6c4d-4289-a966-659944d071c9/Truebotbgiiijfbga4_browsingExe.exe? X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230709T103012Z&X-Amz-Expires=600&X-Amz-Signature=21d7a60aefc40078b038ce4316678b26211b540310f93e34bbfc4ba47b47c09f&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY-EDIF-HE-LS	Penetrated
2023-07-09	US Cert Alert - (AA23-187A) Increased Truebot Activity Infects U.S. And Canada Networks	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/us_ cert_alert_-_%28aa23-187a%29_increased_truebot_activity_infects_u.s.and_canada_networks_c18bd470-6c4d-4289-a966-659944d071c9/Truebotbgiiijfbga3_browsingExe.exe? X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230709T102925Z&X-Amz-Expires=600&X-Amz-Signature=2e39fe3c15105d27d54bdd638c418687f56b6b5e023bf5ff8f455f77780b645d&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY-EDIF-HE-LS	Penetrated
2023-07-09	US Cert Alert - (AA23-187A) Increased Truebot Activity Infects U.S. And Canada Networks	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/us_ cert_alert_-_%28aa23-187a%29_increased_truebot_activity_infects_u.s.and_canada_networks_c18bd470-6c4d-4289-a966-659944d071c9/Truebotbgiiijfbga1_browsingExe.exe? X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230709T102902Z&X-Amz-Expires=600&X-Amz-Signature=ababa0aedb770b81584bdd904ef0f307292f57f7412a15f60876c6b05c6d56d5&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY-EDIF-HE-LS	Penetrated
2023-07-09	Buddyransome	Buddyransombgiiiijacb1_edrExe.exe	Endpoint Security	OMY-EDIF-HE-LS	Blocked
2023-07-09	Buddyransome	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/buddyransome_8cb491e4-5136-4deb-8e19-2027964f5bd2/Buddyransombgiiiijacb2_browsingEx e.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-A mz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230709%2Feu-west-1%2Fs3%2Faws4_request&X- Amz-Date=20230709T080307Z&X-Amz-Expires=600&X-Amz-Signature=d78fab77aaef3866c371e72c2d51eb966ab7b4f5582cf9887dbad32b4a5e493c&X-Amz-SignedHeaders=host&x-id=GetOb ject	Web Gateway	OMY-EDIF-HE-LS	Penetrated
2023-07-09	Threat Profile UNC3944	Threatbgiigjfhhb_edr75Exe.exe	Endpoint Security	OMY-EDIF-HE-LS	Blocked
2023-07-09	Threat Profile UNC3944	Threatbgiigjfhhb_edr72Exe.exe	Endpoint Security	OMY-EDIF-HE-LS	Blocked
2023-07-09	Threat Profile UNC3944	Threatbgiigjfhhb_edr73Exe.exe	Endpoint Security	OMY-EDIF-HE-LS	Blocked
2023-07-09	Threat Profile UNC3944	Threatbgiigjfhhb_edr77Exe.exe	Endpoint Security	OMY-EDIF-HE-LS	Penetrated
2023-07-09	Threat Profile UNC3944	Threatbgiigjfhhb_edr76Exe.exe	Endpoint Security	OMY-EDIF-HE-LS	Penetrated
2023-07-09	Threat Profile UNC3944	Threatbgiigjfhhb84_edrExe.exe	Endpoint Security	OMY-EDIF-HE-LS	Penetrated
2023-07-09	Threat Profile UNC3944	Threatbgiigjfhhb85_edrExe.exe	Endpoint Security	OMY-EDIF-HE-LS	Penetrated
2023-07-09	Threat Profile UNC3944	Threatbgiigjfhhb_edr79Exe.exe	Endpoint Security	OMY-EDIF-HE-LS	Penetrated
2023-07-09	Threat Profile UNC3944	Threatbgiigjfhhb83_edrExe.exe	Endpoint Security	OMY-EDIF-HE-LS	Penetrated
2023-07-09	Threat Profile UNC3944	Threatbgiigjfhhb80_edrExe.exe	Endpoint Security	OMY-EDIF-HE-LS	Penetrated
2023-07-09	Threat Profile UNC3944	Threatbgiigjfhhb82_edrExe.exe	Endpoint Security	OMY-EDIF-HE-LS	Penetrated
2023-07-09	Threat Profile UNC3944	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/threat_profile_unc3944_f7ba8a64-eecc-477f-a86e-0cbdccc2a0c9/Threatbgiigjfhhb81_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230709T060447Z&X-Amz-Expires=600&X-Amz-Signature=4f473264532c3ca92fabcf6bb0ab266bcfed1f990fe2e9fc6a962595f4c65947&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY-EDIF-HE-LS	Penetrated
2023-07-09	Threat Profile UNC3944	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/threat_profile_unc3944_f7ba8a64-eecc-477f-a86e-0cbdccc2a0c9/Threatbgiigjfhhb_browsing78Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230709T060443Z&X-Amz-Expires=600&X-Amz-Signature=182a16b5020f8bd63a112a6a35aac09f7455cf1f4fa2f4532a00d74fca2f6dcd&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY-EDIF-HE-LS	Penetrated
2023-07-09	Threat Profile UNC3944	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/threat_profile_unc3944_f7ba8a64-eecc-477f-a86e-0cbdccc2a0c9/Threatbgiigjfhhb_browsing74Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230709T060433Z&X-Amz-Expires=600&X-Amz-Signature=abcf08fabaeec39129ea8af9018ed6b0501c0962e927095b2d61a6f6e9ea4757&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY-EDIF-HE-LS	Penetrated

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

ASM-VP REPORT

Organo Judicial 07/26/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-07-09	Threat Profile UNC3944	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/threat_profile_unc3944_f7ba8a64-eecc-477f-a86e-0cbdccc2a0c9/Threatbgiigjfhhb_browsing71Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230709T060430Z&X-Amz-Expires=600&X-Amz-Signature=a159fd50add116dd76df2e4770d009fa4f6bafedfb584a56211dc9eadfedc92c&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY-EDIF-HE-LS	Penetrated
2023-07-09	Threat Profile UNC3944	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/threat_profile_unc3944_f7ba8a64-eecc-477f-a86e-0cbdccc2a0c9/Threatbgiigjfhhb_browsi ng70Elf.elf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLO AD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230709%2Feu-west-1%2Fs3%2Faws4_requ est&X-Amz-Date=20230709T060414Z&X-Amz-Expires=600&X-Amz-Signature=c2f28df4515e5079c1367d9580d6c68014decdbfbcac98c8cc874063fb59be65&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY-EDIF-HE-LS	Penetrated
2023-07-09	Threat Profile UNC3944	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/threat_profile_unc3944_f7ba8a64-eecc-477f-a86e-0cbdccc2a0c9/Threatbgiigjfhhb66_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230709T060407Z&X-Amz-Expires=600&X-Amz-Signature=fb42d6546de30eba6befc876f96ed6e7f7c87b4d38a7237a6d01847d6744d583&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY-EDIF-HE-LS	Penetrated
2023-07-06	PhonyC2 Framework Used By MuddyWater	Phonyc2bgiigaijja5_edrPs1.ps1	Endpoint Security	OMY	Penetrated
2023-07-06	PhonyC2 Framework Used By MuddyWater	hxxp://164.132.237.79	Web Gateway	OMY	Offline/Removed
2023-07-06	PhonyC2 Framework Used By MuddyWater	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/phonyc2_framework_used_by_muddywater_055285f0-d830-4652-b2b3-c438a424a18e/Phonyc2bgiigaijja10_browsingJs.js?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230706%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230706T050246Z&X-Amz-Expires=600&X-Amz-Signature=4362bbd08874f258a5daa09b01af3d6d6b6397fb6ee35b8501958d3e55d78fec&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY	Penetrated
2023-07-06	PhonyC2 Framework Used By MuddyWater	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/phonyc2_framework_used_by_muddywater_055285f0-d830-4652-b2b3-c438a424a18e/Phonyc2bgiigaijja9_browsingJs.js?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UN SIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230706%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230706T050245Z&X-Amz-Expires=600&X-Amz-Signature=01a4e4182697f8288884496726cbaa3189f97cad0e1b6fbbf2ebc4a99107089f&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY	Penetrated
2023-07-05	The suspected Maha grass organization uses the WarHawk backdoor variant Spyder to spy on many countries	Thebgiifccegi21_edrExe.exe	Endpoint Security	OMY	Penetrated
2023-07-05	The suspected Maha grass organization uses the WarHawk backdoor variant Spyder to spy on many countries	Thebgiifccegi18_edrExe.exe	Endpoint Security	OMY	Blocked
2023-07-05	The suspected Maha grass organization uses the WarHawk backdoor variant Spyder to spy on many countries	Thebgiifccegi10_edrExe.exe	Endpoint Security	OMY	Blocked
2023-07-05	The suspected Maha grass organization uses the WarHawk backdoor variant Spyder to spy on many countries	Thebgiifccegi14_edrExe.exe	Endpoint Security	OMY	Blocked
2023-07-05	The suspected Maha grass organization uses the WarHawk backdoor variant Spyder to spy on many countries	hxxp://192.169.7.142	Web Gateway	OMY	Offline/Removed

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

TLP:AMBER

GLESEC
COMPLETELY PERCEPTI

ASM-VP REPORT

Organo Judicial 07/26/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-07-05	The suspected Maha grass organization uses the WarHawk backdoor variant Spyder to spy on many countries	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/the_suspected_maha_grass_organization_uses_the_warhawk_backdoor_variant_spyder_to_spy_on_many_countries_b12092f9-cbef-4912-87fe-16158033afbc/Thebgiifccegi20_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230705%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230705T050518Z&X-Amz-Expires=600&X-Amz-Signature=cc1dc02da1c1bee6d0a0bdd8f60f93aff6d7dfa812b7fa9fc15c89781eb19ead&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY	Penetrated
2023-07-05	The suspected Maha grass organization uses the WarHawk backdoor variant Spyder to spy on many countries	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/the_suspected_maha_grass_organization_uses_the_warhawk_backdoor_variant_spyder_to_spy_on_many_countries_b12092f9-cbef-4912-87fe-16158033afbc/Thebgiifccegi19_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230705%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230705T050516Z&X-Amz-Expires=600&X-Amz-Signature=8ca5632125c7852177e088f5bd0bff6667056a8334a400deea5ae943e66c38c1&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY	Penetrated
2023-07-05	The suspected Maha grass organization uses the WarHawk backdoor variant Spyder to spy on many countries	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/the_suspected_maha_grass_organization_uses_the_warhawk_backdoor_variant_spyder_to_spy_on_many_countries_b12092f9-cbef-4912-87fe-16158033afbc/Thebgiifccegi1_browsing7Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230705%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230705T050515Z&X-Amz-Expires=600&X-Amz-Signature=a5acfdf19339a28be095a7507bbdb8c530472eedc4cd3b2dbdde57546da9c2a66&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY	Penetrated
2023-07-05	The suspected Maha grass organization uses the WarHawk backdoor variant Spyder to spy on many countries	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/the_suspected_maha_grass_organization_uses_the_warhawk_backdoor_variant_spyder_to_spy_on_many_countries_b12092f9-cbef-4912-87fe-16158033afbc/Thebgiifccegi13_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230705%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230705T050513Z&X-Amz-Expires=600&X-Amz-Signature=2caf31d6c47d6dc2569b3d1dc8b37934ad0610375175b859c6a1040834fb0772&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY	Penetrated
2023-07-05	The suspected Maha grass organization uses the WarHawk backdoor variant Spyder to spy on many countries	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/the_suspected_maha_grass_organization_uses_the_warhawk_backdoor_variant_spyder_to_spy_on_many_countries_b12092f9-cbef-4912-87fe-16158033afbc/Thebgiifccegi9_browsin gExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD& X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230705%2Feu-west-1%2Fs3%2Faws4_request &X-Amz-Date=20230705T050509Z&X-Amz-Expires=600&X-Amz-Signature=9b1ee1e9a6c8dfd38902a9569819041b20daf69697754a4b09246e63c58fe48a&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY	Penetrated
2023-07-04	The DPRK strikes using a new variant of RUSTBUCKET	Thebgiiecjcjg12_edr7Macho.macho	Endpoint Security	OMY	Penetrated
2023-07-04	The DPRK strikes using a new variant of RUSTBUCKET	Thebgiiecjcjg129_edrMacho.macho	Endpoint Security	OMY	Penetrated
2023-07-04	The DPRK strikes using a new variant of RUSTBUCKET	Thebgiiecjcjg132_edrMacho.macho	Endpoint Security	OMY	Penetrated
2023-07-04	The DPRK strikes using a new variant of RUSTBUCKET	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/the_dprk_strikes_using_a_new_variant_of_rustbucket_5ef1bf2d-e849-470a-b237-647c9e112e12/Thebgiiecjcjg131_browsingMacho.macho?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230704%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230704T061340Z&X-Amz-Expires=600& X-Amz-Signature=2152a7e2ad7859a0bf07d0707b213ab1a68e79fbb61bfcbb066482fca7c57d18 &X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY	Penetrated
2023-07-04	The DPRK strikes using a new variant of RUSTBUCKET	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/the_dprk_strikes_using_a_new_variant_of_rustbucket_5ef1bf2d-e849-470a-b237-647c9e112e12/Thebgiiecjcjg126_browsingMacho.macho?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230704%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230704T061326Z&X-Amz-Expires=600& X-Amz-Signature=d3113d06a5b8effcd2f8410929c6881f43ce9a9de30c785afae87dc9e1efe44e &X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY	Penetrated
2023-07-04	The DPRK strikes using a new variant of RUSTBUCKET	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/the_dprk_strikes_using_a_new_variant_of_rustbucket_5ef1bf2d-e849-470a-b237-647c9e112e12/Thebgiiecjcjg125_browsingMacho.macho?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230704%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230704T061322Z&X-Amz-Expires=600& X-Amz-Signature=fc5ae0dca0029c4fec43e4328a668db533362b6da5f8df7446f6e9ebf73e0865 &X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY	Penetrated
2023-07-04	The DPRK strikes using a new variant of RUSTBUCKET	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/the_dprk_strikes_using_a_new_variant_of_rustbucket_5ef1bf2d-e849-470a-b237-647c9e112e12/Thebgiiecjcjg122_browsingMacho.macho?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230704%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230704T061311Z&X-Amz-Expires=600& X-Amz-Signature=bcee76ee6370c3c40f7d723271f5fe172cad3363e0e41d249d3d83428bafc52e &X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY	Penetrated

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

TLP:AMBER

GLESEC
COMPLETELY PERCEPTI

ASM-VP REPORT

Organo Judicial 07/26/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-07-03	Word Document with an Online Attached Template	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/word_document_with_an_online_attached_template_10c61f38-086a-4f78-980a-6d2253adcd93/Matryoshkabgiididgjd3_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230703%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230703T113621Z&X-Amz-Expires=600&X-Amz-Signature=9d818b981923c64d0f677f1856aa660b29ecd43d1b16bdf99545adcbc2ee5def&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY	Penetrated
2023-07-03	Word Document with an Online Attached Template	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/word_document_with_an_online_attached_template_10c61f38-086a-4f78-980a-6d2253adcd93/Matryoshkabgiididgjd1_browsingDocx.docx?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230703%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230703T113620Z&X-Amz-Expires=600&X-Amz-Signature=a1f53a12def379c033d5c4d31672c833aeeba3e2771bba105237af5bb01b404a&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY	Penetrated
2023-07-03	Word Document with an Online Attached Template	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/word_document_with_an_online_attached_template_10c61f38-086a-4f78-980a-6d2253adcd93/Matryoshkabgiididgjd2_browsingRtf.rtf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230703%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230703T113618Z&X-Amz-Expires=600&X-Amz-Signature=6930a71760c35441357e030b39ea40d572c0138b1adfc4618cbda2f76425dcbb&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY	Penetrated
2023-07-03	New Qakbot (Qbot) activity	Qbotbgiidicbbd1_edrDll.dll	Endpoint Security	OMY	Blocked
2023-07-03	New Qakbot (Qbot) activity	Qbotbgiidicbbd2_edrJs.js	Endpoint Security	OMY	Blocked
2023-07-03	New Qakbot (Qbot) activity	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/new_qakbot_%28qbot%29_activity_f5a2f41e-fc87-429d-b4af-e3e89d8c012f/Qbotbgiidicbbd3_browsingZip.zip?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230703%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230703T111525Z&X-Amz-Expires=600&X-Amz-Signature=6fa1662bfa7c72cce5aba43dee6f3b0cab9558744b961476839253ee2976a668&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY	Penetrated
2023-07-03	Mirai Campaign Leveraging Multiple IoT Exploits	Miraibgihfhcccf2_edrElf.elf	Endpoint Security	OMY	Blocked
2023-07-03	Mirai Campaign Leveraging Multiple IoT Exploits	Miraibgihfhcccf3_edrElf.elf	Endpoint Security	OMY	Blocked
2023-07-03	Mirai Campaign Leveraging Multiple IoT Exploits	Miraibgihfhcccf6_edrElf.elf	Endpoint Security	OMY	Blocked
2023-07-03	Mirai Campaign Leveraging Multiple IoT Exploits	Miraibgihfhcccf5_edrElf.elf	Endpoint Security	OMY	Blocked
2023-07-03	Mirai Campaign Leveraging Multiple IoT Exploits	Miraibgihfhcccf12_edrElf.elf	Endpoint Security	OMY	Blocked
2023-07-03	Mirai Campaign Leveraging Multiple IoT Exploits	Miraibgihfhcccf_edr7Elf.elf	Endpoint Security	OMY	Blocked
2023-07-03	Mirai Campaign Leveraging Multiple IoT Exploits	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/mirai_campaign_leveraging_multiple_iot_exploits_29e3fabb-a46e-42e6-9931-6276108ef13d/Miraibgihfhcccf13_browsingElf.elf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230703%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230703T083532Z&X-Amz-Expires=600&X-Amz-Signature=24589dce531b48117c54f4eb370ad5c70def5bb00e2115b05e030738411c0a4a&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY	Penetrated
2023-07-03	Mirai Campaign Leveraging Multiple IoT Exploits	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/mirai_campaign_leveraging_multiple_iot_exploits_29e3fabb-a46e-42e6-9931-6276108ef13d/Miraibgihfhcccf11_browsingElf.elf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230703%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230703T083530Z&X-Amz-Expires=600&X-Amz-Signature=d8c42774d75cbdc266b1796c8f87436a71735bbd9e23e7849b9362d548048dc2&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY	Penetrated
2023-07-03	Mirai Campaign Leveraging Multiple IoT Exploits	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/mirai_campaign_leveraging_multiple_iot_exploits_29e3fabb-a46e-42e6-9931-6276108ef13d/Miraibgihfhcccf10_browsingElf.elf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230703%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230703T083529Z&X-Amz-Expires=600&X-Amz-Signature=b888bc6dd9fb5255424cce378c4422dacf8eb861540ec47f9addbb21470ff417&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY	Penetrated

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

TLP:AMBER

ASM-VP REPORT

Organo Judicial 07/26/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-07-03	Mirai Campaign Leveraging Multiple IoT Exploits	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/mir ai_campaign_leveraging_multiple_iot_exploits_29e3fabb-a46e-42e6-9931-6276108ef13 d/Miraibgihfhcccf9_browsingElf.elf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Conten t-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230703%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230703T083529Z&X-Amz-Expires=600&X-Amz-S ignature=26994715316c73e532091d793e52ccb3181b3750c239cb3112838fe3cce9e84a&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY	Penetrated
2023-07-03	Mirai Campaign Leveraging Multiple IoT Exploits	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/mir ai_campaign_leveraging_multiple_iot_exploits_29e3fabb-a46e-42e6-9931-6276108ef13 d/Miraibgihfhcccf8_browsingElf.elf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Conten t-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230703%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230703T083528Z&X-Amz-Expires=600&X-Amz-S ignature=06d471ae706672c8ab2eb944b4cd938acc5ef2344a1c2397582d02fd2c56eed6&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY	Penetrated
2023-07-03	Mirai Campaign Leveraging Multiple IoT Exploits	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/mir ai_campaign_leveraging_multiple_iot_exploits_29e3fabb-a46e-42e6-9931-6276108ef13 d/Miraibgihfhcccf4_browsingElf.elf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Conten t-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230703%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230703T083524Z&X-Amz-Expires=600&X-Amz-S ignature=8451d32e42eeafa236bc2a95c3efbc768a681f58705e0e0a6690038b4870ef0c&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY	Penetrated
2023-07-03	Mirai Campaign Leveraging Multiple IoT Exploits	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/mir ai_campaign_leveraging_multiple_iot_exploits_29e3fabb-a46e-42e6-9931-6276108ef13 d/Miraibgihfhcccf1_browsingElf.elf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Conten t-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230703%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230703T083520Z&X-Amz-Expires=600&X-Amz-S ignature=7f1c7ded8a78c20ed1e83cc32489685f06efdc3decf43d280cfb8ff726940533&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY	Penetrated
2023-07-02	Gh0stBins RAT Analysis	Gh0stbinsbgihjbhhhb1_edrExe.exe	Endpoint Security	OMY	Blocked
2023-07-02	Gh0stBins RAT Analysis	Gh0stbinsbgihjbhhhb4_edrDll.dll	Endpoint Security	OMY	Penetrated
2023-07-02	Gh0stBins RAT Analysis	Gh0stbinsbgihjbhhhb3_edrDll.dll	Endpoint Security	OMY	Penetrated
2023-07-02	Gh0stBins RAT Analysis	hxxp://193.134.208.217	Web Gateway	OMY	Offline/Removed
2023-06-29	8Base Ransomware - A Heavy Hitting Player	Eightbasebgiiacggfh4_edrExe.exe	Endpoint Security	OMY	Blocked
2023-06-29	Tracing The Footsteps Of Red Wolf	Tracingbgiiaaecbg1_edrIso.iso	Endpoint Security	OMY	Penetrated
2023-06-29	Tracing The Footsteps Of Red Wolf	Tracingbgiiaaecbg2_edrLnk.lnk	Endpoint Security	OMY	Penetrated
2023-06-29	Tracing The Footsteps Of Red Wolf	Tracingbgiiaaecbg3_edrDll.dll	Endpoint Security	OMY	Blocked
2023-06-28	Wagner Ransomware Cyber Recruitment	Wagnerbgihjbhidd5_edrExe.exe	Endpoint Security	OMY	Blocked
2023-06-26	Operation Magalenha - Long-Running Campaign Pursues Portuguese Credentials and PII	Magalenhabgihgjegca10_edr7Exe.exe	Endpoint Security	OMY	Blocked
2023-06-26	Operation Magalenha - Long-Running Campaign Pursues Portuguese Credentials and PII	Magalenhabgihgjegca105_edrExe.exe	Endpoint Security	OMY	Penetrated
2023-06-26	Operation Magalenha - Long-Running Campaign Pursues Portuguese Credentials and PII	Magalenhabgihgjegca103_edrExe.exe	Endpoint Security	OMY	Penetrated

TLP:AMBER

GLESEC
COMPLETELY PERCEPTI

ASM-VP REPORT

Organo Judicial 07/26/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-06-26	Operation Magalenha - Long-Running Campaign Pursues Portuguese Credentials and PII	Magalenhabgihgjegca91_edrExe.exe	Endpoint Security	OMY	Penetrated
2023-06-26	Operation Magalenha - Long-Running Campaign Pursues Portuguese Credentials and PII	Magalenhabgihgjegca90_edrExe.exe	Endpoint Security	OMY	Penetrated
2023-06-26	Operation Magalenha - Long-Running Campaign Pursues Portuguese Credentials and PII	Magalenhabgihgjegca102_edrExe.exe	Endpoint Security	OMY	Blocked
2023-06-26	Operation Magalenha - Long-Running Campaign Pursues Portuguese Credentials and PII	Magalenhabgihgjegca93_edrExe.exe	Endpoint Security	OMY	Blocked
2023-06-26	Operation Magalenha - Long-Running Campaign Pursues Portuguese Credentials and PII	hxxp://94.228.121.36	Web Gateway	OMY	Offline/Removed
2023-06-26	Operation Magalenha - Long-Running Campaign Pursues Portuguese Credentials and PII	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/operation_magalenha_-_long-running_campaign_pursues_portuguese_credentials_and_pii_39302ab3-8137-4c47-8629-bc09e763c579/Magalenhabgihgjegca92_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230626%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230626T134005Z&X-Amz-Expires=600&X-Amz-Signature=f57f00dcbe1adfa7cbe1e083416a9f64d614a78ce204e38a72013cb1411f6e1b&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY	Penetrated
2023-06-26	Operation Magalenha - Long-Running Campaign Pursues Portuguese Credentials and PII	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/operation_magalenha_-_long-running_campaign_pursues_portuguese_credentials_and_pii_39302ab3-8137-4c47-8629-bc09e763c579/Magalenhabgihgjegca94_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230626%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230626T133915Z&X-Amz-Expires=600&X-Amz-Signature=2ee4816dc7e8a432d023214fa7a6d41a188e78059456d8d52923b9134cc85372&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY	Penetrated
2023-06-26	Operation Magalenha - Long-Running Campaign Pursues Portuguese Credentials and PII	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/operation_magalenha_-_long-running_campaign_pursues_portuguese_credentials_and_pii_39302ab3-8137-4c47-8629-bc09e763c579/Magalenhabgihgjegca9_browsing7Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230626%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230626T133802Z&X-Amz-Expires=600&X-Amz-Signature=d82bbb4e2b58762e11f012fe25023033bd5f0917a2d608ee616e9a5eb3dc1422&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY	Penetrated
2023-06-26	Operation Magalenha - Long-Running Campaign Pursues Portuguese Credentials and PII	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/operation_magalenha_-_long-running_campaign_pursues_portuguese_credentials_and_pii_39302ab3-8137-4c47-8629-bc09e763c579/Magalenhabgihgjegca98_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230626%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230626T133555Z&X-Amz-Expires=600&X-Amz-Signature=d933d01f696f4d6f4cb55b3e7d1aae597961d0947f8b06e32e8148032f3fd78d&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY	Penetrated
2023-06-26	Operation Magalenha - Long-Running Campaign Pursues Portuguese Credentials and PII	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/operation_magalenha_-_long-running_campaign_pursues_portuguese_credentials_and_pii_39302ab3-8137-4c47-8629-bc09e763c579/Magalenhabgihgjegca99_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230626%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230626T133113Z&X-Amz-Expires=600&X-Amz-Signature=30ff68efa21a122d652a6248115446d214d010555b023fd4609add6cde8e7d16&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY	Penetrated

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

ASM-VP REPORT

Organo Judicial 07/26/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-06-26	Operation Magalenha - Long-Running Campaign Pursues Portuguese Credentials and PII	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/operation_magalenha_-_long-running_campaign_pursues_portuguese_credentials_and_pii_39302ab3-8137-4c47-8629-bc09e763c579/Magalenhabgihgjegca100_browsingExe.exe?X-Am z-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230626%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230626T132609Z&X-Amz-Expires=600&X-Amz-Signature=bcead03efb9c9bddd27262d2f93260153b18d978365b0049598346a7827125ae&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY	Blocked
2023-06-26	Operation Magalenha - Long-Running Campaign Pursues Portuguese Credentials and PII	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/operation_magalenha_-_long-running_campaign_pursues_portuguese_credentials_and_pii_39302ab3-8137-4c47-8629-bc09e763c579/Magalenhabgihgjegca101_browsingExe.exe?X-Am z-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230626%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230626T132104Z&X-Amz-Expires=600&X-Amz-Signature=0b1973054fc169764dd9f8dc4e89674f78b73ab61d8b2020949029095d34ca97&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY	Blocked
2023-06-26	Operation Magalenha - Long-Running Campaign Pursues Portuguese Credentials and PII	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/operation_magalenha_-_long-running_campaign_pursues_portuguese_credentials_and_pii_39302ab3-8137-4c47-8629-bc09e763c579/Magalenhabgihgjegca104_browsingExe.exe?X-Am z-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230626%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230626T130552Z&X-Amz-Expires=600&X-Amz-Signature=322b4cde637543b570878704dfb5385dbe4a75c7126d6f67ff623775e31130cc&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY	Blocked
2023-06-26	Crysis And Venus Ransomware Installed Via RDP	Crysisbgihfhcije1_edr79Exe.exe	Endpoint Security	OMY	Blocked
N/A	Crysis And Venus Ransomware Installed Via RDP	Crysisbgihfhcije190_edrExe.exe	Endpoint Security	OMY	Blocked
2023-06-26	Crysis And Venus Ransomware Installed Via RDP	Crysisbgihfhcije194_edrExe.exe	Endpoint Security	OMY	Blocked
2023-06-26	Crysis And Venus Ransomware Installed Via RDP	Crysisbgihfhcije185_edrExe.exe	Endpoint Security	OMY	Blocked
2023-06-26	Crysis And Venus Ransomware Installed Via RDP	Crysisbgihfhcije186_edrExe.exe	Endpoint Security	OMY	Blocked
2023-06-26	Crysis And Venus Ransomware Installed Via RDP	Crysisbgihfhcije183_edrDll.dll	Endpoint Security	OMY	Blocked
2023-06-26	Crysis And Venus Ransomware Installed Via RDP	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/crysis_and_venus_ransomware_installed_via_rdp_f8741241-ed45-4a8f-8e68-09566cd32555/Crysisbgihfhcije188_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Conte nt-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230626%2Feu - west-1%2Fs3%2Faws4_request&X-Amz-Date=20230626T062954Z&X-Amz-Expires=600&X-Amz-Signature=a7959b27519930e6ae75b50f63c9ad8a8240ec15b24ec86f607f9f5e91134002&X-Amz - SignedHeaders=host&x-id=GetObject	Web Gateway	OMY	Penetrated
2023-06-26	Crysis And Venus Ransomware Installed Via RDP	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/crysis_and_venus_ransomware_installed_via_rdp_f8741241-ed45-4a8f-8e68-09566cd32555/Crysisbgihfhcije184_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Conte nt-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230626%2Feu - west-1%2Fs3%2Faws4_request&X-Amz-Date=20230626T062951Z&X-Amz-Expires=600&X-Amz-Signature=7518a1b485518e5ad3330e4f9d8833ae8c2baac34de71e33ad3ec0060f7040f7&X-Amz - SignedHeaders=host&x-id=GetObject	Web Gateway	OMY	Penetrated
2023-06-26	Crysis And Venus Ransomware Installed Via RDP	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/crysis_and_venus_ransomware_installed_via_rdp_f8741241-ed45-4a8f-8e68-09566cd32555/Crysisbgihfhcije182_browsingDll.dll?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Conte nt-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230626%2Feu - west-1%2Fs3%2Faws4_request&X-Amz-Date=20230626T062950Z&X-Amz-Expires=600&X-Amz-Signature=84309457b122445e585e9dcd96fba0ad468616d2101d3e573f7819f52464fe35&X-Amz - SignedHeaders=host&x-id=GetObject	Web Gateway	OMY	Penetrated
2023-06-26	Crysis And Venus Ransomware Installed Via RDP	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/crysis_and_venus_ransomware_installed_via_rdp_f8741241-ed45-4a8f-8e68-09566cd32555/Crysisbgihfhcije181_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Conte nt-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230626%2Feu - west-1%2Fs3%2Faws4_request&X-Amz-Date=20230626T062949Z&X-Amz-Expires=600&X-Amz-Signature=53ba2440f22c3a28f967587de199434ca41f7b3e64193250cfd96315505dcda9&X-Amz - SignedHeaders=host&x-id=GetObject	Web Gateway	OMY	Penetrated
2023-06-26	Crysis And Venus Ransomware Installed Via RDP	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/crysis_and_venus_ransomware_installed_via_rdp_f8741241-ed45-4a8f-8e68-09566cd32555/Crysisbgihfhcije180_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Conte nt-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230626%2Feu - west-1%2Fs3%2Faws4_request&X-Amz-Date=20230626T062948Z&X-Amz-Expires=600&X-Amz-Signature=4da2b6c143e4224e7967566b903e7c4baedbc4368bab5972515afd1a3ad73b45&X-Amz - SignedHeaders=host&x-id=GetObject	Web Gateway	OMY	Penetrated

TLP:AMBER

GLESEC
COMPLETELY PERCEPTI

ASM-VP REPORT

Organo Judicial 07/26/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-07-26	India Cert Alert - Mallox Ransomware Targeting Unsecured MS SQL Servers	Mallboxbgjadhhiij14_edrBat.bat	Endpoint Security	88E1000GMSYS	Penetrated
2023-07-26	India Cert Alert - Mallox Ransomware Targeting Unsecured MS SQL Servers	Mallboxbgjadhhiij6_edrExe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-07-26	India Cert Alert - Mallox Ransomware Targeting Unsecured MS SQL Servers	Mallboxbgjadhhiij8_edrPs1.ps1	Endpoint Security	88E1000GMSYS	Blocked
2023-07-26	India Cert Alert - Mallox Ransomware Targeting Unsecured MS SQL Servers	Mallboxbgjadhhiij11_edrPs1.ps1	Endpoint Security	88E1000GMSYS	Blocked
2023-07-26	India Cert Alert - Mallox Ransomware Targeting Unsecured MS SQL Servers	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ind ia_cert_alert_-_mallox_ransomware_targeting_unsecured_ms_sql_servers_a88804f4-9b a8-4e9a-89c8-0cf1c679ae06/Mallboxbgjadhhiij9_browsingPs1.ps1?X-Amz-Algorithm=AWS 4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3 D5GWFTK3Q%2F20230726%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230726T135119Z &X-Amz-Expires=600&X-Amz-Signature=ee8dd2d8ca951745eb1074257d157de423e9f57ad843a 367b76de1e56c8b864a&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-26	India Cert Alert - Mallox Ransomware Targeting Unsecured MS SQL Servers	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ind ia_cert_alert_-_mallox_ransomware_targeting_unsecured_ms_sql_servers_a88804f4-9b a8-4e9a-89c8-0cf1c679ae06/Mallboxbgjadhhiij10_browsingPs1.ps1?X-Amz-Algorithm=AW S4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q 3D5GWFTK3Q%2F20230726%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230726T135118 Z&X-Amz-Expires=600&X-Amz-Signature=ada529c76668e98f4ba4046ca9fe72614ee8234c94bb 405bb3b3671a0821f231&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-26	India Cert Alert - Mallox Ransomware Targeting Unsecured MS SQL Servers	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ind ia_cert_alert_-_mallox_ransomware_targeting_unsecured_ms_sql_servers_a88804f4-9b a8-4e9a-89c8-0cf1c679ae06/Mallboxbgjadhhiij12_browsingPs1.ps1?X-Amz-Algorithm=AW S4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q 3D5GWFTK3Q%2F20230726%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230726T135117 Z&X-Amz-Expires=600&X-Amz-Signature=14b837c9c27da2895b44452f7630cbdcb5140ecea3f5 cd865c02bff003ca3849&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-26	India Cert Alert - Mallox Ransomware Targeting Unsecured MS SQL Servers	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ind ia_cert_alert_-_mallox_ransomware_targeting_unsecured_ms_sql_servers_a88804f4-9b a8-4e9a-89c8-0cf1c679ae06/Mallboxbgjadhhiij13_browsingPs1.ps1?X-Amz-Algorithm=AW S4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q 3D5GWFTK3Q%2F20230726%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230726T135112 Z&X-Amz-Expires=600&X-Amz-Signature=b103e6ae46852c2c61fe93620569d1104bafafbd299f 4c803ebcf942bfd714b9&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-26	India Cert Alert - Mallox Ransomware Targeting Unsecured MS SQL Servers	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ind ia_cert_alert_-_mallox_ransomware_targeting_unsecured_ms_sql_servers_a88804f4-9b a8-4e9a-89c8-0cf1c679ae06/Mallboxbgjadhhiij15_browsingBat.bat?X-Amz-Algorithm=AW S4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q 3D5GWFTK3Q%2F20230726%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230726T135111 Z&X-Amz-Expires=600&X-Amz-Signature=74271b86478019929a659601d9733c6de00cd30f5250 aff468178c00bcb2d1af&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-26	India Cert Alert - Mallox Ransomware Targeting Unsecured MS SQL Servers	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ind ia_cert_alert_-_mallox_ransomware_targeting_unsecured_ms_sql_servers_a88804f4-9b a8-4e9a-89c8-0cf1c679ae06/Mallboxbgjadhhiij1_browsingExe.exe?X-Amz-Algorithm=AWS 4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3 D5GWFTK3Q%2F20230726%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230726T135109Z &X-Amz-Expires=600&X-Amz-Signature=479ab68dcbd84c6eee57d305a092a835c9210bf67094d d4baafbe8752456bef6&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-26	India Cert Alert - Mallox Ransomware Targeting Unsecured MS SQL Servers	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ind ia_cert_alert_-_mallox_ransomware_targeting_unsecured_ms_sql_servers_a88804f4-9b a8-4e9a-89c8-0cf1c679ae06/Mallboxbgjadhhiij2_browsingExe.exe?X-Amz-Algorithm=AWS 4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3 D5GWFTK3Q%2F20230726%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230726T135106Z &X-Amz-Expires=600&X-Amz-Signature=7443e7a772145655c6d5b77942457b220af83700baa15 6846ee8d71183ef7078&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-26	India Cert Alert - Mallox Ransomware Targeting Unsecured MS SQL Servers	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ind ia_cert_alert_-_mallox_ransomware_targeting_unsecured_ms_sql_servers_a88804f4-9b a8-4e9a-89c8-0cf1c679ae06/Mallboxbgjadhhiij3_browsingExe.exe?X-Amz-Algorithm=AWS 4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3 D5GWFTK3Q%2F20230726%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230726T135105Z &X-Amz-Expires=600&X-Amz-Signature=1b9ec2fecc6eb97fd08326c66ca5eb1a0040fd49b2257 6ba4c0717caaeb862f8&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated

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

TLP:AMBER

GLESEC
COMPLETELY PERCEPTI

ASM-VP REPORT

Organo Judicial 07/26/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-07-26	India Cert Alert - Mallox Ransomware Targeting Unsecured MS SQL Servers	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ind ia_cert_alert_-_mallox_ransomware_targeting_unsecured_ms_sql_servers_a88804f4-9b a8-4e9a-89c8-0cf1c679ae06/Mallboxbgjadhhiij4_browsingExe.exe?X-Amz-Algorithm=AWS 4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3 D5GWFTK3Q%2F20230726%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230726T135102Z &X-Amz-Expires=600&X-Amz-Signature=550c2930373a98f39e6a9cb41e7e6a25b15416bfbf0ef e0a8cfce3fed9204dca&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-26	India Cert Alert - Mallox Ransomware Targeting Unsecured MS SQL Servers	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ind ia_cert_alert_-_mallox_ransomware_targeting_unsecured_ms_sql_servers_a88804f4-9b a8-4e9a-89c8-0cf1c679ae06/Mallboxbgjadhhiij5_browsingExe.exe?X-Amz-Algorithm=AWS 4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3 D5GWFTK3Q%2F20230726%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230726T135102Z &X-Amz-Expires=600&X-Amz-Signature=a6b783080b36726e91fa7ddb3d71c4e754f95d650beb0 0a17e59055f40cd1bd3&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-26	India Cert Alert - Mallox Ransomware Targeting Unsecured MS SQL Servers	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ind ia_cert_alert_-_mallox_ransomware_targeting_unsecured_ms_sql_servers_a88804f4-9b a8-4e9a-89c8-0cf1c679ae06/Mallboxbgjadhhiij_browsing7Exe.exe?X-Amz-Algorithm=AWS 4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3 D5GWFTK3Q%2F20230726%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230726T135059Z &X-Amz-Expires=600&X-Amz-Signature=f87a38951bc8587e1266b089ce856c6954d4af7124e8e 7ee12cb96904e720d13&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-26	First-ever Open-Source Software Supply Chain Attacks	Firsteverbgjacahebh52_edrExe.exe	Endpoint Security	88E1000GMSYS	Penetrated
2023-07-26	First-ever Open-Source Software Supply Chain Attacks	Firsteverbgjacahebh51_edrExe.exe	Endpoint Security	88E1000GMSYS	Penetrated
2023-07-25	Ransomware Spotlight Play	Ransomwarebgjacdgace11_edrExe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-07-25	Ransomware Spotlight Play	Ransomwarebgjacdgace3_edrExe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-07-25	Ransomware Spotlight Play	Ransomwarebgjacdgace14_edrExe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-07-25	Ransomware Spotlight Play	Ransomwarebgjacdgace12_edrExe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-07-25	Ransomware Spotlight Play	Ransomwarebgjacdgace5_edrExe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-07-25	Ransomware Spotlight Play	Ransomwarebgjacdgace9_edrExe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-07-26	First-ever Open-Source Software Supply Chain Attacks	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/fir st-ever_open-source_software_supply_chain_attacks_6df0d247-55bd-4848-a6e9-ebf2f8 cd6517/Firsteverbgjacahebh54_browsingElf.elf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X- Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F2023 0726%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230726T074842Z&X-Amz-Expires=6 00&X-Amz-Signature=9944ec23388278ec33577da9d01cc89f69555b04ba7e868bcb1899ec00794 cd4&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-26	First-ever Open-Source Software Supply Chain Attacks	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/fir st-ever_open-source_software_supply_chain_attacks_6df0d247-55bd-4848-a6e9-ebf2f8 cd6517/Firsteverbgjacahebh49_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X- Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F2023 0726%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230726T074820Z&X-Amz-Expires=6 00&X-Amz-Signature=8133dad235969a7de0bc1c084d0d8ef85fadc44d5e8363bedb078a5009bb5 276&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-26	New Reptile Rootkit Malware Attacking Linux Systems Using Port Knocking	Newbgjadaaiej4_edrO.o	Endpoint Security	88E1000GMSYS	Blocked
2023-07-26	New Reptile Rootkit Malware Attacking Linux Systems Using Port Knocking	Newbgjadaaiej5_edrO.o	Endpoint Security	88E1000GMSYS	Blocked
2023-07-26	New Reptile Rootkit Malware Attacking Linux Systems Using Port Knocking	Newbgjadaaiej_edr7Elf.elf	Endpoint Security	88E1000GMSYS	Blocked
2023-07-26	New Reptile Rootkit Malware Attacking Linux Systems Using Port Knocking	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/new _reptile_rootkit_malware_attacking_linux_systems_using_port_knocking_c90e131d-0b d0-4024-978d-6ccdbb54f8c0/Newbgjadaaiej9_browsingElf.elf?X-Amz-Algorithm=AWS4-HM AC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GW FTK3Q%2F20230726%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230726T074230Z&X-Amz-Expires=600&X-Amz-Signature=fe45253d58061c565b2d75860e93bfdfcf06fb1472537183b eeb7b9250268d0d&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated

TLP:AMBER

ASM-VP REPORT

Organo Judicial 07/26/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-07-26	New Reptile Rootkit Malware Attacking Linux Systems Using Port Knocking	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/new_reptile_rootkit_malware_attacking_linux_systems_using_port_knocking_c90e131d-0bd0-4024-978d-6ccdbb54f8c0/NewbgjadaaiejJ8_browsingO.o?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230726%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230726T074229Z&X-Amz-Expires=600&X-Amz-Signature=9c809ac1883316adc5457bcd1f11c8f11ce7b317cdf41163cca977ac336693f8&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-26	New Reptile Rootkit Malware Attacking Linux Systems Using Port Knocking	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/new_reptile_rootkit_malware_attacking_linux_systems_using_port_knocking_c90e131d-0bd0-4024-978d-6ccdbb54f8c0/NewbgjadaaiejJ6_browsingElf.elf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230726%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230726T074228Z&X-Amz-Expires=600&X-Amz-Signature=5e822541e5dd64afda1e119873684f30fd56fa62712ad568c0ba7de9c0b19d12&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-26	New Reptile Rootkit Malware Attacking Linux Systems Using Port Knocking	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/new_reptile_rootkit_malware_attacking_linux_systems_using_port_knocking_c90e131d-0bd0-4024-978d-6ccdbb54f8c0/NewbgjadaaiejJ3_browsingO.o?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230726%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230726T074223Z&X-Amz-Expires=600&X-Amz-Signature=b84ca75ed8ae044712af550dc031d1df7ef3d840ba3d935cbc254ef3979f3d49&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-26	New Reptile Rootkit Malware Attacking Linux Systems Using Port Knocking	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/new_reptile_rootkit_malware_attacking_linux_systems_using_port_knocking_c90e131d-0bd0-4024-978d-6ccdbb54f8c0/NewbgjadaaiejJ2_browsingO.o?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230726%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230726T074218Z&X-Amz-Expires=600&X-Amz-Signature=454654c2085ab65c436bb23bef9ea69a8872f3620a79d2a935291e4cba0edb85&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-26	New Reptile Rootkit Malware Attacking Linux Systems Using Port Knocking	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/new_reptile_rootkit_malware_attacking_linux_systems_using_port_knocking_c90e131d-0bd0-4024-978d-6ccdbb54f8c0/NewbgjadaaiejJ1_browsingSh.sh?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230726%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230726T074216Z&X-Amz-Expires=600&X-Amz-Signature=1f4135aa3188989f2900bd8e288ad4d182f1b3f064907c54a910192504231dc2&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-25	Ransomware Spotlight Play	Ransomwarebgjacdgace1_edrExe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-07-25	Ransomware Spotlight Play	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ransomware_spotlight_play_9c7a6699-8793-486d-b28c-2b289d802cf8/Ransomwarebgjacdgace10_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230725%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230725T060202Z&X-Amz-Expires=600&X-Amz-Signature=e9b04948460fafabe83ac5dab2972b8547af2990a2459a27f3602b663e043db3&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-25	Ransomware Spotlight Play	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ransomware_spotlight_play_9c7a6699-8793-486d-b28c-2b289d802cf8/Ransomwarebgjacdgace8_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230725%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230725T060200Z&X-Amz-Expires=600&X-Amz-Signature=7ebe5b4abaebd6f54ef6877ef44f5674fbfa6e2408632ee013e91d893f27b964&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-25	Ransomware Spotlight Play	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ransomware_spotlight_play_9c7a6699-8793-486d-b28c-2b289d802cf8/Ransomwarebgjacdgace_browsing7Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230725%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230725T060159Z&X-Amz-Expires=600&X-Amz-Signature=3d6d579f77ab2e4587082a503a56d462043d22c1d941baf1e0c07a7d661a47f1&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-25	Ransomware Spotlight Play	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ransomware_spotlight_play_9c7a6699-8793-486d-b28c-2b289d802cf8/Ransomwarebgjacdgace4_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230725%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230725T060158Z&X-Amz-Expires=600&X-Amz-Signature=ee8a646cf55163e0563c85bdff978fe3965062f1cb9f83f63a66223e33b608b5&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-25	Ransomware Spotlight Play	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ransomware_spotlight_play_9c7a6699-8793-486d-b28c-2b289d802cf8/Ransomwarebgjacdgace2_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230725%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230725T060148Z&X-Amz-Expires=600&X-Amz-Signature=d66a404a1ffa8b0f93aada2a6dac556bdedfa356d98092a5ceaa64ee624bc3df&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-24	UAC-0006 Distributes SmokeLoader Through Phishing Emails (CERT-UA6999)	Uac0006bgijhdcdcg21_edrExe.exe	Endpoint Security	88E1000GMSYS	Blocked

TLP:AMBER

ASM-VP REPORT

Organo Judicial 07/26/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-07-24	UAC-0006 Distributes SmokeLoader Through Phishing Emails (CERT-UA6999)	Uac0006bgijhdcdcg16_edrZip.zip	Endpoint Security	88E1000GMSYS	Blocked
2023-07-24	UAC-0006 Distributes SmokeLoader Through Phishing Emails (CERT-UA6999)	Uac0006bgijhdcdcg19_edrExe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-07-24	UAC-0006 Distributes SmokeLoader Through Phishing Emails (CERT-UA6999)	Uac0006bgijhdcdcg1_edr7Php.php	Endpoint Security	88E1000GMSYS	Blocked
2023-07-24	UAC-0006 Distributes SmokeLoader Through Phishing Emails (CERT-UA6999)	Uac0006bgijhdcdcg15_edrZip.zip	Endpoint Security	88E1000GMSYS	Blocked
2023-07-24	UAC-0006 Distributes SmokeLoader Through Phishing Emails (CERT-UA6999)	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/uac-0006_distributes_smokeloader_through_phishing_emails_%28cert-ua6999%29_8b19babc-f0b4-4e71-8fb3-facdc03755d6/Uac0006bgijhdcdcg20_browsingExe.exe?X-Amz-Algorithm =AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230724%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230724T070032Z&X-Amz-Expires=600&X-Amz-Signature=0e3cfec066253b9e3f7b04a3dcdd291f146bd170331ce6d899516e15c00def97&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-24	UAC-0006 Distributes SmokeLoader Through Phishing Emails (CERT-UA6999)	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/uac-0006_distributes_smokeloader_through_phishing_emails_%28cert-ua6999%29_8b19babc-f0b4-4e71-8fb3-facdc03755d6/Uac0006bgijhdcdcg14_browsingZip.zip?X-Amz-Algorithm =AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230724%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230724T070030Z&X-Amz-Expires=600&X-Amz-Signature=4133c0811a90b9955ee89612150135ceaa6ea097240f41d3402b6c8a4c5ebe99&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-24	UAC-0006 Distributes SmokeLoader Through Phishing Emails (CERT-UA6999)	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/uac-0006_distributes_smokeloader_through_phishing_emails_%28cert-ua6999%29_8b19babc-f0b4-4e71-8fb3-facdc03755d6/Uac0006bgijhdcdcg13_browsingHtml.html?X-Amz-Algorit hm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230724%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230724T070027Z&X-Amz-Expires=600&X-Amz-Signature=21516f857181c40e17333bb7ee2d5228b2c5912a20e84486b6cda5eda4d216ee&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-24	Ursnif campaign in Italy	Ursnifbgijhigahi4_edrPs1.ps1	Endpoint Security	88E1000GMSYS	Penetrated
2023-07-24	Ursnif campaign in Italy	Ursnifbgijhigahi1_edrDll.dll	Endpoint Security	88E1000GMSYS	Blocked
2023-07-23	Manipulated Caiman: The Sophisticated Snare of Mexico's Banking Predator	Manipulatedcaimanbgjabaaibd5_edrExe.exe	Endpoint Security	88E1000GMSYS	Penetrated
2023-07-23	Manipulated Caiman: The Sophisticated Snare of Mexico's Banking Predator	Manipulatedcaimanbgjabaaibd6_edrExe.exe	Endpoint Security	88E1000GMSYS	Penetrated
2023-07-23	Manipulated Caiman: The Sophisticated Snare of Mexico's Banking Predator	Manipulatedcaimanbgjabaaibd4_edrExe.exe	Endpoint Security	88E1000GMSYS	Penetrated
2023-07-23	Manipulated Caiman: The Sophisticated Snare of Mexico's Banking Predator	Manipulatedcaimanbgjabaaibd13_edrExe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-07-23	Manipulated Caiman: The Sophisticated Snare of Mexico's Banking Predator	Manipulatedcaimanbgjabaaibd1_edrExe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-07-23	Manipulated Caiman: The Sophisticated Snare of Mexico's Banking Predator	Manipulatedcaimanbgjabaaibd2_edrExe.exe	Endpoint Security	88E1000GMSYS	Blocked

TLP:AMBER

ASM-VP REPORT

Organo Judicial 07/26/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-07-23	Manipulated Caiman: The Sophisticated Snare of Mexico's Banking Predator	Manipulatedcaimanbgjabaaibd9_edrExe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-07-23	Manipulated Caiman: The Sophisticated Snare of Mexico's Banking Predator	Manipulatedcaimanbgjabaaibd10_edrExe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-07-23	Manipulated Caiman: The Sophisticated Snare of Mexico's Banking Predator	hxxp://45.153.240.94	Web Gateway	88E1000GMSYS	Offline/Removed
2023-07-23	Manipulated Caiman: The Sophisticated Snare of Mexico's Banking Predator	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/manipulated_caiman%3A_the_sophisticated_snare_of_mexico%27s_banking_predator_4b58497a-83ae-4fdd-bb38-8219794cb25b/Manipulatedcaimanbgjabaaibd3_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230723%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230723T085427Z&X-Amz-Expires=600&X-Amz-Signature=90d5ab59a331f53bd04686fe4d7e4c352fb319757963f28992eb89976d806c17&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-23	Manipulated Caiman: The Sophisticated Snare of Mexico's Banking Predator	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/manipulated_caiman%3A_the_sophisticated_snare_of_mexico%27s_banking_predator_4b58497a-83ae-4fdd-bb38-8219794cb25b/Manipulatedcaimanbgjabaaibd_browsing7Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230723%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230723T085414Z&X-Amz-Expires=600&X-Amz-Signature=6e1389bf32f7b67b6277c3303ddee2497b0cae457a5719fd0da6881295ddf466&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-23	Manipulated Caiman: The Sophisticated Snare of Mexico's Banking Predator	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/manipulated_caiman%3A_the_sophisticated_snare_of_mexico%27s_banking_predator_4b58497a-83ae-4fdd-bb38-8219794cb25b/Manipulatedcaimanbgjabaaibd8_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230723%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230723T085412Z&X-Amz-Expires=600&X-Amz-Signature=1741014a3f4f5ca89b6853c6b0c3122920745e2e6d65170d03392f5b0e1976f8&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-23	Manipulated Caiman: The Sophisticated Snare of Mexico's Banking Predator	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/manipulated_caiman%3A_the_sophisticated_snare_of_mexico%27s_banking_predator_4b58497a-83ae-4fdd-bb38-8219794cb25b/Manipulatedcaimanbgjabaaibd11_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230723%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230723T085402Z&X-Amz-Expires=600&X-Amz-Signature=92407f881b06506bc8a1b6885b1f6967767825bf5c9097451fdf9134ac141d89&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-23	Manipulated Caiman: The Sophisticated Snare of Mexico's Banking Predator	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/manipulated_caiman%3A_the_sophisticated_snare_of_mexico%27s_banking_predator_4b58497a-83ae-4fdd-bb38-8219794cb25b/Manipulatedcaimanbgjabaaibd12_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230723%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230723T085402Z&X-Amz-Expires=600&X-Amz-Signature=fa195fa2b8875d67db2b4fb75ece7f67a92ba4c535dd7ce0cb16883e259555b3&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-23	Manipulated Caiman: The Sophisticated Snare of Mexico's Banking Predator	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/manipulated_caiman%3A_the_sophisticated_snare_of_mexico%27s_banking_predator_4b58497a-83ae-4fdd-bb38-8219794cb25b/Manipulatedcaimanbgjabaaibd14_browsingJs.js?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230723%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230723T085401Z&X-Amz-Expires=600&X-Amz-Signature=9fb28f58995eace2a58286da2b8a7d39ff2e4092f272be952bf5d804ec802939&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-23	Manipulated Caiman: The Sophisticated Snare of Mexico's Banking Predator	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/manipulated_caiman%3A_the_sophisticated_snare_of_mexico%27s_banking_predator_4b58497a-83ae-4fdd-bb38-8219794cb25b/Manipulatedcaimanbgjabaaibd15_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230723%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230723T085359Z&X-Amz-Expires=600&X-Amz-Signature=73b90e4dad93fedf3d3b2ad8638165cea1fcd4298a8ca7621c9355eddf8fca7c&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-23	A Look Into Space Pirates Unconventional Techniques Attack Vectors And Tools	Abgijibigeg22_edrDll.dll	Endpoint Security	88E1000GMSYS	Penetrated
2023-07-23	A Look Into Space Pirates Unconventional Techniques Attack Vectors And Tools	Abgijibigeg65_edrExe.exe	Endpoint Security	88E1000GMSYS	Penetrated

ASM-VP REPORT

Organo Judicial 07/26/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-07-23	A Look Into Space Pirates Unconventional Techniques Attack Vectors And Tools	Abgijibigeg28_edrDll.dll	Endpoint Security	88E1000GMSYS	Penetrated
2023-07-23	A Look Into Space Pirates Unconventional Techniques Attack Vectors And Tools	Abgijibigeg62_edrExe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-07-23	A Look Into Space Pirates Unconventional Techniques Attack Vectors And Tools	Abgijibigeg30_edrDll.dll	Endpoint Security	88E1000GMSYS	Blocked
2023-07-23	A Look Into Space Pirates Unconventional Techniques Attack Vectors And Tools	Abgijibigeg24_edrDll.dll	Endpoint Security	88E1000GMSYS	Blocked
2023-07-23	A Look Into Space Pirates Unconventional Techniques Attack Vectors And Tools	Abgijibigeg6_edr7Exe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-07-23	A Look Into Space Pirates Unconventional Techniques Attack Vectors And Tools	hxxps://beachdrivingfun.com	Web Gateway	88E1000GMSYS	Penetrated
2023-07-23	A Look Into Space Pirates Unconventional Techniques Attack Vectors And Tools	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/a_look_into_space_pirates_unconventional_techniques_attack_vectors_and_tools_995867 c2-733c-4527-bde5-5c324ac95e6d/Abgijibigeg66_browsingExe.exe?X-Amz-Algorithm=AWS 4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3 D5GWFTK3Q%2F20230723%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230723T064052Z &X-Amz-Expires=600&X-Amz-Signature=f839faf1d60e17a7a307a760e190b17f1d386a7724731 b7e306aac1739d19e87&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-23	A Look Into Space Pirates Unconventional Techniques Attack Vectors And Tools	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/a_look_into_space_pirates_unconventional_techniques_attack_vectors_and_tools_995867 c2-733c-4527-bde5-5c324ac95e6d/Abgijibigeg64_browsingExe.exe?X-Amz-Algorithm=AWS 4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3 D5GWFTK3Q%2F20230723%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230723T064048Z &X-Amz-Expires=600&X-Amz-Signature=8f0a770fe58a86142b7838e670d3d8d5b0e0afe63799c 4694629ee0b956f1206&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-23	A Look Into Space Pirates Unconventional Techniques Attack Vectors And Tools	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/a_look_into_space_pirates_unconventional_techniques_attack_vectors_and_tools_995867 c2-733c-4527-bde5-5c324ac95e6d/Abgijibigeg63_browsingExe.exe?X-Amz-Algorithm=AWS 4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3 D5GWFTK3Q%2F20230723%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230723T064041Z &X-Amz-Expires=600&X-Amz-Signature=f7a0b1da791b982a45dbdcd6ded95a7a6d3526edac6b3 b55b5507775089439b7&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-23	A Look Into Space Pirates Unconventional Techniques Attack Vectors And Tools	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/a_look_into_space_pirates_unconventional_techniques_attack_vectors_and_tools_995867 c2-733c-4527-bde5-5c324ac95e6d/Abgijibigeg58_browsingExe.exe?X-Amz-Algorithm=AWS 4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3 D5GWFTK3Q%2F20230723%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230723T064034Z &X-Amz-Expires=600&X-Amz-Signature=70865b77eddae35912b9a4294345c34024dc15aebf981 b834d18859808f3198e&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-23	A Look Into Space Pirates Unconventional Techniques Attack Vectors And Tools	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/a_look_into_space_pirates_unconventional_techniques_attack_vectors_and_tools_995867 c2-733c-4527-bde5-5c324ac95e6d/Abgijibigeg23_browsingDll.dll?X-Amz-Algorithm=AWS 4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3 D5GWFTK3Q%2F20230723%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230723T064030Z &X-Amz-Expires=600&X-Amz-Signature=814394f01f8f9010230f16a7701a99660c0e3c4ecea70 28fa97f2cf349fa0d0d&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-23	A Look Into Space Pirates Unconventional Techniques Attack Vectors And Tools	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/a_look_into_space_pirates_unconventional_techniques_attack_vectors_and_tools_995867 c2-733c-4527-bde5-5c324ac95e6d/Abgijibigeg21_browsingDll.dll?X-Amz-Algorithm=AWS 4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3 D5GWFTK3Q%2F20230723%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230723T064028Z &X-Amz-Expires=600&X-Amz-Signature=59e920237bf5848fa1caae13bb68d80eeff2f453d8894 c762d982d79a35503e4&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated

ASM-VP REPORT

Organo Judicial 07/26/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-07-23	A Look Into Space Pirates Unconventional Techniques Attack Vectors And Tools	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/a_look_into_space_pirates_unconventional_techniques_attack_vectors_and_tools_995867 c2-733c-4527-bde5-5c324ac95e6d/Abgijibigeg18_browsingDll.dll?X-Amz-Algorithm=AWS 4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230723%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230723T064027Z&X-Amz-Expires=600&X-Amz-Signature=660c721e2dcc3c55efee43eefbe53762f1b099c7f8148a09163a029deb0c4005&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-23	Threat Actor Launches ScarLeteel 2.00	Threatbgijdaabfc3_edrSh.sh	Endpoint Security	88E1000GMSYS	Blocked
2023-07-23	Threat Actor Launches ScarLeteel 2.00	hxxp://175.102.182.6	Web Gateway	88E1000GMSYS	Offline/Removed
2023-07-23	Threat Actor Launches ScarLeteel 2.00	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/threat_actor_launches_scarleteel_2.0_5c3a31c4-d75d-4f35-8a4e-ab9dc96ff553/Threatbgijdaabfc4_browsingSh.sh?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230723%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230723T063752Z&X-Amz-Expires=600&X-Amz-Signature=af5ad8c61c610b52b77ec88464e72dad810b3de81a001bbfcce2041b220be649&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-23	Threat Actor Launches ScarLeteel 2.00	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/threat_actor_launches_scarleteel_2.0_5c3a31c4-d75d-4f35-8a4e-ab9dc96ff553/Threatbgijdaabfc2_browsingSh.sh?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230723%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230723T063752Z&X-Amz-Expires=600&X-Amz-Signature=b6539763a3bad2698080d81a8e9b6b24de1173c1b6dd74c8f15eb8705018ee87&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-20	The Turla APT Group Uses Multiple Malware Families To Exfiltrate Data (CERT-UA6981)	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/the_turla_apt_group_uses_multiple_malware_families_to_exfiltrate_data_%28cert-ua6981%29_a81930dd-7462-451c-a175-656d5b0b5612/Thebgijibifhf1_browsingDll.dll?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230720%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230720T053726Z&X-Amz-Expires=600&X-Amz-Signature=6aa3a5adbccd2c55413df180a6399ef15f37912228a5571cd841cbeb3cc25e20&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-20	DDoS Botnet Targets Zyxel Vulnerability (CVE-2023-28771)	Ddosbgijibiigd_edr77Elf.elf	Endpoint Security	88E1000GMSYS	Blocked
2023-07-20	DDoS Botnet Targets Zyxel Vulnerability (CVE-2023-28771)	Ddosbgijibiigd82_edrElf.elf	Endpoint Security	88E1000GMSYS	Blocked
2023-07-20	DDoS Botnet Targets Zyxel Vulnerability (CVE-2023-28771)	Ddosbgijibiigd81_edrElf.elf	Endpoint Security	88E1000GMSYS	Blocked
2023-07-20	DDoS Botnet Targets Zyxel Vulnerability (CVE-2023-28771)	Ddosbgijibiigd83_edrElf.elf	Endpoint Security	88E1000GMSYS	Blocked
2023-07-20	DDoS Botnet Targets Zyxel Vulnerability (CVE-2023-28771)	Ddosbgijibiigd_edr79Elf.elf	Endpoint Security	88E1000GMSYS	Blocked
2023-07-20	DDoS Botnet Targets Zyxel Vulnerability (CVE-2023-28771)	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ddos_botnet_targets_zyxel_vulnerability_%28cve-2023-28771%29_726e7b63-4627-4776-a657-7c9d9a38820c/Ddosbgijibiigd86_browsingElf.elf?X-Amz-Algorithm=AWS4-HMAC-SHA256 &X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230720%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230720T053408Z&X-Amz-Expires=600&X-Amz-Signature=f3d583a170ee1ff80a10a5b3a1f4fcaa0d283e71667ee7d8c245b9c219773b4a&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-20	DDoS Botnet Targets Zyxel Vulnerability (CVE-2023-28771)	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ddos_botnet_targets_zyxel_vulnerability_%28cve-2023-28771%29_726e7b63-4627-4776-a657-7c9d9a38820c/Ddosbgijibiigd84_browsingElf.elf?X-Amz-Algorithm=AWS4-HMAC-SHA256 &X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230720%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230720T053406Z&X-Amz-Expires=600&X-Amz-Signature=6119b074d9d2f095d83253a697c4befed2b6d5b6d3d61cf9e2acff1e1af0d782&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-20	DDoS Botnet Targets Zyxel Vulnerability (CVE-2023-28771)	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ddos_botnet_targets_zyxel_vulnerability_%28cve-2023-28771%29_726e7b63-4627-4776-a657-7c9d9a38820c/Ddosbgijibiigd80_browsingElf.elf?X-Amz-Algorithm=AWS4-HMAC-SHA256 &X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230720%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230720T053403Z&X-Amz-Expires=600&X-Amz-Signature=fff02df44b9754bb75be90643878fff4cc16f99f753c507e7c5c63e350ce8243&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated

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

TLP:AMBER

GLESEC
COMPLETELY PERCEPTI

ASM-VP REPORT

Organo Judicial 07/26/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-07-20	DDoS Botnet Targets Zyxel Vulnerability (CVE-2023-28771)	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ddos_botnet_targets_zyxel_vulnerability_%28cve-2023-28771%29_726e7b63-4627-4776-a657-7c9d9a38820c/Ddosbgijibiigd_browsing78Elf.elf?X-Amz-Algorithm=AWS4-HMAC-SHA256 &X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230720%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230720T053401Z&X-Amz-Expires=600&X-Amz-Signature=fc122dc2ac575ea6a0a4f5916f9210bd8ab6b18df0d60ea0b781fd142c6711d9&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-18	Infamous Meduza Stealer	Infamousbgijcbdjad20_edrExe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-07-18	Infamous Meduza Stealer	Infamousbgijcbdjad15_edrExe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-07-18	Infamous Meduza Stealer	Infamousbgijcbdjad18_edrExe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-07-18	Infamous Meduza Stealer	Infamousbgijcbdjad21_edrExe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-07-18	Infamous Meduza Stealer	Infamousbgijcbdjad12_edrExe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-07-18	Infamous Meduza Stealer	Infamousbgijcbdjad19_edrExe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-07-18	Infamous Meduza Stealer	hxxp://79.137.203.37	Web Gateway	88E1000GMSYS	Offline/Removed
2023-07-18	Infamous Meduza Stealer	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/infamous_meduza_stealer_21000adb-78d3-4a28-94c3-8427f297ac31/Infamousbgijcbdjad1_browsing7Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230718%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230718T065254Z&X-Amz-Expires=600&X-Amz-Signature=cfec4d974c18af431683ce1b9d946fdffe1462a75994d5aec807322e60a1e7b5&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-18	Infamous Meduza Stealer	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/infamous_meduza_stealer_21000adb-78d3-4a28-94c3-8427f297ac31/Infamousbgijcbdjad13_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230718%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230718T065247Z&X-Amz-Expires=600&X-Amz-Signature=f715abe0206c5b36775b04245480e10fccd6055ccca099e7e0e4836e8051e8b6&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-18	Infamous Meduza Stealer	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/infamous_meduza_stealer_21000adb-78d3-4a28-94c3-8427f297ac31/Infamousbgijcbdjad11_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230718%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230718T065246Z&X-Amz-Expires=600&X-Amz-Signature=36c43fdd2855e1851d69b017469133671c39b3ad63c570fd02511aee99757399&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-18	Infamous Meduza Stealer	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/infamous_meduza_stealer_21000adb-78d3-4a28-94c3-8427f297ac31/Infamousbgijcbdjad16_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230718%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230718T065244Z&X-Amz-Expires=600&X-Amz-Signature=8f31036c710e73b649be57e28d4a65f37b2be715793d60e66ae3511ddc50bff6&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-18	Infamous Meduza Stealer	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/infamous_meduza_stealer_21000adb-78d3-4a28-94c3-8427f297ac31/Infamousbgijcbdjad14_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230718%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230718T065239Z&X-Amz-Expires=600&X-Amz-Signature=131471988991ca632909d4722b0c8065dc70db3c400a0d72718277d48e384daa&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-18	APT36 Delivers Crimson RAT Using Pilgrimage Security Briefing Lure	Apt36bgijdaafca_edr79Exe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-07-18	APT36 Delivers Crimson RAT Using Pilgrimage Security Briefing Lure	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/apt36_delivers_crimson_rat_using_pilgrimage_security_briefing_lure_d3803684-14d2-4b40-97f4-11d6c9cba750/Apt36bgijdaafca_browsing77Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230718%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230718T055559Z&X-Amz-Expires=600&X-Amz-Signature=600d28400377fb552782fcb31b80c1a74826518945ad0c7d1278beabd58f04b6&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Blocked
2023-07-18	APT36 Delivers Crimson RAT Using Pilgrimage Security Briefing Lure	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/apt36_delivers_crimson_rat_using_pilgrimage_security_briefing_lure_d3803684-14d2-4b40-97f4-11d6c9cba750/Apt36bgijdaafca80_browsingDocx.docx?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230718%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230718T055550Z&X-Amz-Expires=600&X-Amz-Signature=48e4b8fdfe4ff39425623bf0dea85e2436c2bc7951ee2b521962831a3b83e078&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated

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

TLP:AMBER

GLESEC
COMPLETELY PERCEPTI

ASM-VP REPORT

Organo Judicial 07/26/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-07-18	APT36 Delivers Crimson RAT Using Pilgrimage Security Briefing Lure	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/apt36_delivers_crimson_rat_using_pilgrimage_security_briefing_lure_d3803684-14d2-4b40-97f4-11d6c9cba750/Apt36bgijdaafca81_browsingZip.zip?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230718%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230718T055549Z&X-Amz-Expires=600&X-Amz-Signature=e4471a13ada51a88ba5a0d021fbe04cb1c170e4c19d5342400ef05bbc4fa0404&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-07-10	Operation Brainleeches Targets Microsoft 365 Users	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/operation_brainleeches_targets_microsoft_365_users_acac1185-0d7f-47a2-8dfc-ddea7a245502/Operationbgiihibied11_browsingJs.js?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz- Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230710 %2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230710T102412Z&X-Amz-Expires=600&X -Amz-Signature=80125575e6fe17c463df8223fad2acde83d33cdd5ea341fd1f3018fb5c135aae& X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY-EDIF-HE-LS	Penetrated
2023-07-10	TeamTNT Targets Cloud Native Environments	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/teamtnt_targets_cloud_native_environments_b865aebc-e863-4bd8-b32b-3f6ee3bd2645/Teamtntbgiigjfdih2_browsingElf.elf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230710%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230710T072516Z&X-Amz-Expires=600&X-Amz-Signature=56e72621ef1465e5ec2df967e03fb6aa8601420005f74a06abcfbe951b4ad8f3&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY-EDIF-HE-LS	Penetrated
2023-07-10	TeamTNT Targets Cloud Native Environments	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/teamtnt_targets_cloud_native_environments_b865aebc-e863-4bd8-b32b-3f6ee3bd2645/Teamtntbgiigjfdih1_browsingElf.elf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230710%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230710T072511Z&X-Amz-Expires=600&X-Amz-Signature=4a4e5ac5bd26d68c9029e5dbae88b1a18e477054a1b7be27a3726686061f7097&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY-EDIF-HE-LS	Penetrated
2023-07-09	US Cert Alert - (AA23-187A) Increased Truebot Activity Infects U.S. And Canada Networks	Truebotbgiiijfbga3_edrExe.exe	Endpoint Security	OMY-EDIF-HE-LS	Penetrated
2023-07-09	US Cert Alert - (AA23-187A) Increased Truebot Activity Infects U.S. And Canada Networks	Truebotbgiiijfbga1_edrExe.exe	Endpoint Security	OMY-EDIF-HE-LS	Blocked
2023-07-09	US Cert Alert - (AA23-187A) Increased Truebot Activity Infects U.S. And Canada Networks	Truebotbgiiijfbga4_edrExe.exe	Endpoint Security	OMY-EDIF-HE-LS	Blocked
2023-07-09	US Cert Alert - (AA23-187A) Increased Truebot Activity Infects U.S. And Canada Networks	Truebotbgiiijfbga_edr7Dll.dll	Endpoint Security	OMY-EDIF-HE-LS	Blocked
2023-07-09	US Cert Alert - (AA23-187A) Increased Truebot Activity Infects U.S. And Canada Networks	hxxp://45.227.253.102	Web Gateway	OMY-EDIF-HE-LS	Offline/Removed
2023-07-09	US Cert Alert - (AA23-187A) Increased Truebot Activity Infects U.S. And Canada Networks	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/us_ cert_alert_-_%28aa23-187a%29_increased_truebot_activity_infects_u.s.and_canada_networks_c18bd470-6c4d-4289-a966-659944d071c9/Truebotbgiiijfbga9_browsingDll.dll? X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230709T103016Z&X-Amz-Expires=600&X-Amz-Signature=7a38aa8c36298394f8b0147677d60699ab8851fb93b740077788ade190ad928b&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY-EDIF-HE-LS	Penetrated
2023-07-09	US Cert Alert - (AA23-187A) Increased Truebot Activity Infects U.S. And Canada Networks	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/us_ cert_alert_-_%28aa23-187a%29_increased_truebot_activity_infects_u.s.and_canada_networks_c18bd470-6c4d-4289-a966-659944d071c9/Truebotbgiiijfbga8_browsingDll.dll? X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230709T103015Z&X-Amz-Expires=600&X-Amz-Signature=29d8584bd831da026d7c41d5fee094e7076b1adf4ae893ba1a3464f68afcff0f&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY-EDIF-HE-LS	Penetrated
2023-07-09	US Cert Alert - (AA23-187A) Increased Truebot Activity Infects U.S. And Canada Networks	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/us_ cert_alert_-_%28aa23-187a%29_increased_truebot_activity_infects_u.s.and_canada_networks_c18bd470-6c4d-4289-a966-659944d071c9/Truebotbgiiijfbga6_browsingExe.exe? X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230709T103013Z&X-Amz-Expires=600&X-Amz-Signature=e49ca622eac7d57181f9e0e4da013b4d0a13bd55d4a2ddaed1d98a207e381fc2&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY-EDIF-HE-LS	Penetrated

TLP:AMBER

GLESEC
COMPLETELY PERCEPTI

ASM-VP REPORT

Organo Judicial 07/26/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-07-09	US Cert Alert - (AA23-187A) Increased Truebot Activity Infects U.S. And Canada Networks	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/us_ cert_alert_-_%28aa23-187a%29_increased_truebot_activity_infects_u.s.and_canada_networks_c18bd470-6c4d-4289-a966-659944d071c9/Truebotbgiiijfbga5_browsingExe.exe? X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230709T103011Z&X-Amz-Expires=600&X-Amz-Signature=4efcbb51ee9e60622a092d4a4afbc6e03b26c9e53b2f45295c07af4af1c02e06&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY-EDIF-HE-LS	Penetrated
2023-07-09	US Cert Alert - (AA23-187A) Increased Truebot Activity Infects U.S. And Canada Networks	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/us_ cert_alert_-_%28aa23-187a%29_increased_truebot_activity_infects_u.s.and_canada_networks_c18bd470-6c4d-4289-a966-659944d071c9/Truebotbgiiijfbga2_browsingExe.exe? X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230709T102914Z&X-Amz-Expires=600&X-Amz-Signature=691800ef513eff97210170d4f9f627295433ffbd289221ae17b42277f28414cc&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY-EDIF-HE-LS	Penetrated
2023-07-09	Buddyransome	Buddyransombgiiiijacb2_edrExe.exe	Endpoint Security	OMY-EDIF-HE-LS	Blocked
2023-07-09	Buddyransome	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/buddyransome_8cb491e4-5136-4deb-8e19-2027964f5bd2/Buddyransombgiiiijacb1_browsingEx e.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-A mz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230709%2Feu-west-1%2Fs3%2Faws4_request&X- Amz-Date=20230709T080313Z&X-Amz-Expires=600&X-Amz-Signature=ba9c6a60e2996e4dce8549edda081cdd3c2fad814ed31b73b234ba322032ea2f&X-Amz-SignedHeaders=host&x-id=GetOb ject	Web Gateway	OMY-EDIF-HE-LS	Penetrated
2023-07-09	Threat Profile UNC3944	Threatbgiigjfhhb66_edrExe.exe	Endpoint Security	OMY-EDIF-HE-LS	Blocked
2023-07-09	Threat Profile UNC3944	Threatbgiigjfhhb_edr74Exe.exe	Endpoint Security	OMY-EDIF-HE-LS	Penetrated
2023-07-09	Threat Profile UNC3944	Threatbgiigjfhhb_edr71Exe.exe	Endpoint Security	OMY-EDIF-HE-LS	Penetrated
2023-07-09	Threat Profile UNC3944	Threatbgiigjfhhb_edr70Elf.elf	Endpoint Security	OMY-EDIF-HE-LS	Blocked
2023-07-09	Threat Profile UNC3944	Threatbgiigjfhhb81_edrExe.exe	Endpoint Security	OMY-EDIF-HE-LS	Penetrated
2023-07-09	Threat Profile UNC3944	Threatbgiigjfhhb_edr78Exe.exe	Endpoint Security	OMY-EDIF-HE-LS	Penetrated
2023-07-09	Threat Profile UNC3944	hxxp://149.28.110.16	Web Gateway	OMY-EDIF-HE-LS	Offline/Removed
2023-07-09	Threat Profile UNC3944	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/threat_profile_unc3944_f7ba8a64-eecc-477f-a86e-0cbdccc2a0c9/Threatbgiigjfhhb85_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230709T060455Z&X-Amz-Expires=600&X-Amz-Signature=7462e5493bbe55b85a79e8e61a5cbc2b0a5f778b278337ce49479a71a1d9cb3e&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY-EDIF-HE-LS	Penetrated
2023-07-09	Threat Profile UNC3944	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/threat_profile_unc3944_f7ba8a64-eecc-477f-a86e-0cbdccc2a0c9/Threatbgiigjfhhb84_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230709T060452Z&X-Amz-Expires=600&X-Amz-Signature=abf8a65f62d1bcbe34f18e3b32ffb9d8a62c8cdfcc5d00297db1884ae518d213&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY-EDIF-HE-LS	Penetrated
2023-07-09	Threat Profile UNC3944	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/threat_profile_unc3944_f7ba8a64-eecc-477f-a86e-0cbdccc2a0c9/Threatbgiigjfhhb83_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230709T060451Z&X-Amz-Expires=600&X-Amz-Signature=eac380184643cec2bbfa13bc9068a57c07755197f4d39e52b64cc30b8a3635e9&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY-EDIF-HE-LS	Penetrated
2023-07-09	Threat Profile UNC3944	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/threat_profile_unc3944_f7ba8a64-eecc-477f-a86e-0cbdccc2a0c9/Threatbgiigjfhhb82_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230709T060450Z&X-Amz-Expires=600&X-Amz-Signature=0eb168ea4b4f15717aa8c1f66eb819633c4f4db079a172f6997c80dd7363c2a8&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY-EDIF-HE-LS	Penetrated
2023-07-09	Threat Profile UNC3944	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/threat_profile_unc3944_f7ba8a64-eecc-477f-a86e-0cbdccc2a0c9/Threatbgiigjfhhb80_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230709T060446Z&X-Amz-Expires=600&X-Amz-Signature=e19341df10aaed59939f65c53cc67239e61b34ce45a09fea4b250375ba10e28d&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY-EDIF-HE-LS	Penetrated
2023-07-09	Threat Profile UNC3944	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/threat_profile_unc3944_f7ba8a64-eecc-477f-a86e-0cbdccc2a0c9/Threatbgiigjfhhb_browsing79Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230709T060445Z&X-Amz-Expires=600&X-Amz-Signature=b089e01dbfc5633f32c3d1d81a3ed00886fdad95b85087f5b96a7a95a5446788&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY-EDIF-HE-LS	Penetrated

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

TLP:AMBER

ASM-VP REPORT

Organo Judicial 07/26/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-07-09	Threat Profile UNC3944	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/threat_profile_unc3944_f7ba8a64-eecc-477f-a86e-0cbdccc2a0c9/ThreatbgiigjfhhbbrowsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230709T060439Z&X-Amz-Expires=600&X-Amz-Signature=53a645143aa8bf9b02116859b4b12ece6e9aecbb5185507f35b46059f3307cf1&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY-EDIF-HE-LS	Penetrated
2023-07-09	Threat Profile UNC3944	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/threat_profile_unc3944_f7ba8a64-eecc-477f-a86e-0cbdccc2a0c9/ThreatbgiigjfhhbbrowsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230709T060436Z&X-Amz-Expires=600&X-Amz-Signature=bff96956a9fc7d82c6b75d9c7be9df612af4dc02faaaf2bcb1452e2c2b353c7a&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY-EDIF-HE-LS	Penetrated
2023-07-09	Threat Profile UNC3944	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/threat_profile_unc3944_f7ba8a64-eecc-477f-a86e-0cbdccc2a0c9/ThreatbgiigjfhhbbrowsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230709T060436Z&X-Amz-Expires=600&X-Amz-Signature=a5ac82f9fa5d6b0fecf4e710bfabfddf7641d71f3eeaf7edeaf657040aaa5266&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY-EDIF-HE-LS	Penetrated
2023-07-09	Threat Profile UNC3944	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/threat_profile_unc3944_f7ba8a64-eecc-477f-a86e-0cbdccc2a0c9/ThreatbgiigjfhhbbrowsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230709T060433Z&X-Amz-Expires=600&X-Amz-Signature=2f5479f8afc6c07cff22ba0f3005e6fa8f217c1e4585375541b5bee5e8d29e38&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY-EDIF-HE-LS	Penetrated
2023-07-09	Threat Profile UNC3944	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/threat_profile_unc3944_f7ba8a64-eecc-477f-a86e-0cbdccc2a0c9/ThreatbgiigjfhhbbrowsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230709T060432Z&X-Amz-Expires=600&X-Amz-Signature=ae1647eb7f924e3a71fa07338aae2fcb390d905db23cd0ced152a3b8cbcf9666&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY-EDIF-HE-LS	Penetrated
2023-07-06	PhonyC2 Framework Used By MuddyWater	Phonyc2bgiigaijja10_edrJs.js	Endpoint Security	OMY	Blocked
2023-07-06	PhonyC2 Framework Used By MuddyWater	Phonyc2bgiigaijja9_edrJs.js	Endpoint Security	OMY	Blocked
2023-07-06	PhonyC2 Framework Used By MuddyWater	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/phonyc2_framework_used_by_muddywater_055285f0-d830-4652-b2b3-c438a424a18e/Phonyc2bgiigaijja5_browsingPs1.ps1?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230706%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230706T050244Z&X-Amz-Expires=600&X-Amz-Signature=ca293c1e5575c84327a88df08310e54f79f6c65096b99c3a279e031dddc25f0e&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY	Penetrated
2023-07-05	The suspected Maha grass organization uses the WarHawk backdoor variant Spyder to spy on many countries	Thebgiifccegi9_edrExe.exe	Endpoint Security	OMY	Blocked
2023-07-05	The suspected Maha grass organization uses the WarHawk backdoor variant Spyder to spy on many countries	Thebgiifccegi20_edrExe.exe	Endpoint Security	OMY	Penetrated
2023-07-05	The suspected Maha grass organization uses the WarHawk backdoor variant Spyder to spy on many countries	Thebgiifccegi19_edrExe.exe	Endpoint Security	OMY	Blocked
2023-07-05	The suspected Maha grass organization uses the WarHawk backdoor variant Spyder to spy on many countries	Thebgiifccegi13_edrExe.exe	Endpoint Security	OMY	Blocked

TLP:AMBER

GLESEC
COMPLETELY PERCEPTI

ASM-VP REPORT

Organo Judicial 07/26/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-07-05	The suspected Maha grass organization uses the WarHawk backdoor variant Spyder to spy on many countries	Thebgiifccegi1_edr7Exe.exe	Endpoint Security	OMY	Blocked
2023-07-05	The suspected Maha grass organization uses the WarHawk backdoor variant Spyder to spy on many countries	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/the_suspected_maha_grass_organization_uses_the_warhawk_backdoor_variant_spyder_to_spy_on_many_countries_b12092f9-cbef-4912-87fe-16158033afbc/Thebgiifccegi21_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230705%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230705T050519Z&X-Amz-Expires=600&X-Amz-Signature=7d65d6d70d39f786a25d9287f5f741977c0a3e67e6e062bb36d187fd5b123645&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY	Penetrated
2023-07-05	The suspected Maha grass organization uses the WarHawk backdoor variant Spyder to spy on many countries	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/the_suspected_maha_grass_organization_uses_the_warhawk_backdoor_variant_spyder_to_spy_on_many_countries_b12092f9-cbef-4912-87fe-16158033afbc/Thebgiifccegi18_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230705%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230705T050516Z&X-Amz-Expires=600&X-Amz-Signature=9bb5fbd98f512f3349adb8fa28054c96c599ed4656c4ee650820a7b15ad97f2e&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY	Penetrated
2023-07-05	The suspected Maha grass organization uses the WarHawk backdoor variant Spyder to spy on many countries	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/the_suspected_maha_grass_organization_uses_the_warhawk_backdoor_variant_spyder_to_spy_on_many_countries_b12092f9-cbef-4912-87fe-16158033afbc/Thebgiifccegi14_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230705%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230705T050514Z&X-Amz-Expires=600&X-Amz-Signature=388e40749bcc53e88b32fd7fe9cca5837a87e0aea1b70c6226dd7f09ea300315&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY	Penetrated
2023-07-05	The suspected Maha grass organization uses the WarHawk backdoor variant Spyder to spy on many countries	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/the_suspected_maha_grass_organization_uses_the_warhawk_backdoor_variant_spyder_to_spy_on_many_countries_b12092f9-cbef-4912-87fe-16158033afbc/Thebgiifccegi10_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230705%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230705T050513Z&X-Amz-Expires=600&X-Amz-Signature=5729a9c2f405e87dcc66a57d3732b77a95c43036e3efc5ff3390ea39b210f186&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY	Penetrated
2023-07-04	The DPRK strikes using a new variant of RUSTBUCKET	Thebgiiecjcjg122_edrMacho.macho	Endpoint Security	OMY	Blocked
2023-07-04	The DPRK strikes using a new variant of RUSTBUCKET	Thebgiiecjcjg131_edrMacho.macho	Endpoint Security	OMY	Penetrated
2023-07-04	The DPRK strikes using a new variant of RUSTBUCKET	Thebgiiecjcjg126_edrMacho.macho	Endpoint Security	OMY	Blocked
2023-07-04	The DPRK strikes using a new variant of RUSTBUCKET	Thebgiiecjcjg125_edrMacho.macho	Endpoint Security	OMY	Blocked
2023-07-04	The DPRK strikes using a new variant of RUSTBUCKET	hxxp://companydeck.online	Web Gateway	OMY	Blocked
2023-07-04	The DPRK strikes using a new variant of RUSTBUCKET	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/the_dprk_strikes_using_a_new_variant_of_rustbucket_5ef1bf2d-e849-470a-b237-647c9e112e12/Thebgiiecjcjg132_browsingMacho.macho?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230704%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230704T061341Z&X-Amz-Expires=600& X-Amz-Signature=82b3bc3120f6ca6454781da5f5a2369cac781374cd5bdaa9155d71bb69e46617 &X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY	Penetrated
2023-07-04	The DPRK strikes using a new variant of RUSTBUCKET	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/the_dprk_strikes_using_a_new_variant_of_rustbucket_5ef1bf2d-e849-470a-b237-647c9e112e12/Thebgiiecjcjg129_browsingMacho.macho?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230704%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230704T061337Z&X-Amz-Expires=600& X-Amz-Signature=9fd13b9cbcfeb58f45fcf8655b5ed13eecf6821f8c3eaf91362005146eaedfe2 &X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY	Penetrated
2023-07-04	The DPRK strikes using a new variant of RUSTBUCKET	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/the_dprk_strikes_using_a_new_variant_of_rustbucket_5ef1bf2d-e849-470a-b237-647c9e112e12/Thebgiiecjcjg12_browsing7Macho.macho?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230704%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230704T061331Z&X-Amz-Expires=600& X-Amz-Signature=84e1c4e7bb67bbbeaa87180a7bbc5b1eeac792fa55c0972c96c1dffcdbe871db &X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY	Penetrated

TLP:AMBER

GLESEC
COMPLETELY PERCEPTI

ASM-VP REPORT

Organo Judicial 07/26/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-07-03	Word Document with an Online Attached Template	Matryoshkabgiididgjd2_edrRtf.rtf	Endpoint Security	OMY	Blocked
2023-07-03	Word Document with an Online Attached Template	Matryoshkabgiididgjd3_edrExe.exe	Endpoint Security	OMY	Blocked
2023-07-03	Word Document with an Online Attached Template	Matryoshkabgiididgjd1_edrDocx.docx	Endpoint Security	OMY	Blocked
2023-07-03	New Qakbot (Qbot) activity	Qbotbgiidicbbd3_edrZip.zip	Endpoint Security	OMY	Blocked
2023-07-03	New Qakbot (Qbot) activity	hxxps://brotherocean.com	Web Gateway	OMY	Blocked
2023-07-03	New Qakbot (Qbot) activity	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/new_qakbot_%28qbot%29_activity_f5a2f41e-fc87-429d-b4af-e3e89d8c012f/Qbotbgiidicbbd2_browsingJs.js?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230703%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230703T111524Z&X-Amz-Expires=600&X-Amz-Signature=b21b8243d53fb0bfc18feea5b4bea11ff3d1adfd5b8b6e86996b3f1515b83834&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY	Penetrated
2023-07-03	New Qakbot (Qbot) activity	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/new_qakbot_%28qbot%29_activity_f5a2f41e-fc87-429d-b4af-e3e89d8c012f/Qbotbgiidicbbd1_browsingDll.dll?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230703%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230703T111515Z&X-Amz-Expires=600&X-Amz-Signature=388d96b9c75ac0973757d141a88fc8562eff0c7857369700699960009 23d10c0&X-Amz-SignedHeaders=host &x-id=GetObject	Web Gateway	OMY	Penetrated
2023-07-03	Mirai Campaign Leveraging Multiple IoT Exploits	Miraibgihfhcccf1_edrElf.elf	Endpoint Security	OMY	Blocked
2023-07-03	Mirai Campaign Leveraging Multiple IoT Exploits	Miraibgihfhcccf11_edrElf.elf	Endpoint Security	OMY	Penetrated
2023-07-03	Mirai Campaign Leveraging Multiple IoT Exploits	Miraibgihfhcccf4_edrElf.elf	Endpoint Security	OMY	Penetrated
2023-07-03	Mirai Campaign Leveraging Multiple IoT Exploits	Miraibgihfhcccf13_edrElf.elf	Endpoint Security	OMY	Blocked
2023-07-03	Mirai Campaign Leveraging Multiple IoT Exploits	Miraibgihfhcccf9_edrElf.elf	Endpoint Security	OMY	Blocked
2023-07-03	Mirai Campaign Leveraging Multiple IoT Exploits	Miraibgihfhcccf10_edrElf.elf	Endpoint Security	OMY	Blocked
2023-07-03	Mirai Campaign Leveraging Multiple IoT Exploits	Miraibgihfhcccf8_edrElf.elf	Endpoint Security	OMY	Blocked
2023-07-03	Mirai Campaign Leveraging Multiple IoT Exploits	hxxp://185.225.74.251/sparc	Web Gateway	OMY	Blocked
2023-07-03	Mirai Campaign Leveraging Multiple IoT Exploits	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/miraii_campaign_leveraging_multiple_iot_exploits_29e3fabb-a46e-42e6-9931-6276108ef13d/Miraibgihfhcccf12_browsingElf.elf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230703%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230703T083531Z&X-Amz-Expires=600&X-Amz-Signature=836a08df5eca6802c28cb1ec5c29eb5e0a9a908e9bb6c3a0f73dc03097391122&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY	Penetrated
2023-07-03	Mirai Campaign Leveraging Multiple IoT Exploits	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/miraii_campaign_leveraging_multiple_iot_exploits_29e3fabb-a46e-42e6-9931-6276108ef13d/Miraibgihfhcccf_browsing7Elf.elf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230703%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230703T083527Z&X-Amz-Expires=600&X-Amz-Signature=9241bfeae51347a1201f6373175e429aa0f3699b92f2320150268afa8f84f10a&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY	Penetrated

ASM-VP REPORT

Organo Judicial 07/26/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-07-03	Mirai Campaign Leveraging Multiple IoT Exploits	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/mir ai_campaign_leveraging_multiple_iot_exploits_29e3fabb-a46e-42e6-9931-6276108ef13 d/Miraibgihfhcccf6_browsingElf.elf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Conten t-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230703%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230703T083526Z&X-Amz-Expires=600&X-Amz-S ignature=95917aae783fbae69f04021f2f640e55f6d9f7247ba8d2f39dea3d44a38253f7&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY	Penetrated
2023-07-03	Mirai Campaign Leveraging Multiple IoT Exploits	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/mir ai_campaign_leveraging_multiple_iot_exploits_29e3fabb-a46e-42e6-9931-6276108ef13 d/Miraibgihfhcccf5_browsingElf.elf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Conten t-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230703%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230703T083525Z&X-Amz-Expires=600&X-Amz-S ignature=ef99f53f76d097deb49b1e91a4a0557605c05ef2efb7c481eba863f548f17f2d&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY	Penetrated
2023-07-03	Mirai Campaign Leveraging Multiple IoT Exploits	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/mir ai_campaign_leveraging_multiple_iot_exploits_29e3fabb-a46e-42e6-9931-6276108ef13 d/Miraibgihfhcccf3_browsingElf.elf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Conten t-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230703%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230703T083523Z&X-Amz-Expires=600&X-Amz-S ignature=ffa28ff43194cfe8feee07a0b6f6840a3fe5e2169690e2df50e1acab1df5eedf&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY	Penetrated
2023-07-03	Mirai Campaign Leveraging Multiple IoT Exploits	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/mir ai_campaign_leveraging_multiple_iot_exploits_29e3fabb-a46e-42e6-9931-6276108ef13 d/Miraibgihfhcccf2_browsingElf.elf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Conten t-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230703%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230703T083522Z&X-Amz-Expires=600&X-Amz-S ignature=d23ca35755f26d03cb01c643eb4a5a53d1311a34e0c0982fabef65a5fa8fe29f&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY	Penetrated
2023-07-02	Gh0stBins RAT Analysis	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/gh0 stbins_rat_analysis_c3247a6f-a237-42c1-b6a7-bc7b5a1e890a/Gh0stbinsbgihjbhhhb4_br owsingDll.dll?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAY LOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230702%2Feu-west-1%2Fs3%2Faws4_re quest&X-Amz-Date=20230702T053321Z&X-Amz-Expires=600&X-Amz-Signature=b4936440b4c0 5fb317787cc6127a71ad003ec8e275aab886319de4a63b80d50f&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY	Penetrated
2023-07-02	Gh0stBins RAT Analysis	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/gh0 stbins_rat_analysis_c3247a6f-a237-42c1-b6a7-bc7b5a1e890a/Gh0stbinsbgihjbhhhb3_br owsingDll.dll?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAY LOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230702%2Feu-west-1%2Fs3%2Faws4_re quest&X-Amz-Date=20230702T053320Z&X-Amz-Expires=600&X-Amz-Signature=0d63d2297a3c 8a2c08327688d592852d9313e542078fa8e2230d92fa637a4a3c&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY	Penetrated
2023-07-02	Gh0stBins RAT Analysis	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/gh0 stbins_rat_analysis_c3247a6f-a237-42c1-b6a7-bc7b5a1e890a/Gh0stbinsbgihjbhhhb1_br owsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAY LOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230702%2Feu-west-1%2Fs3%2Faws4_re quest&X-Amz-Date=20230702T053307Z&X-Amz-Expires=600&X-Amz-Signature=ac3eb84d7c9b 4be51a7e435cd391bde240711b038476da98cdb0acf8d0dc8672&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY	Penetrated
2023-06-29	8Base Ransomware - A Heavy Hitting Player	Eightbasebgiiacggfh1_edrExe.exe	Endpoint Security	OMY	Blocked
2023-06-29	8Base Ransomware - A Heavy Hitting Player	Eightbasebgiiacggfh3_edrExe.exe	Endpoint Security	OMY	Blocked
2023-06-29	8Base Ransomware - A Heavy Hitting Player	Eightbasebgiiacggfh2_edrExe.exe	Endpoint Security	OMY	Blocked
2023-06-29	Tracing The Footsteps Of Red Wolf	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/tra cing_the_footsteps_of_red_wolf_4c0c8a2b-4185-4f42-9746-029b05056114/Tracingbgiia aecbg3_browsingDll.dll?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNS IGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230629%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230629T060229Z&X-Amz-Expires=600&X-Amz-Signature=6d2 dc0f03d58732e9e787cef51c38181f25485448c889ae0f53fa25b383e2922&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY	Penetrated
2023-06-29	Tracing The Footsteps Of Red Wolf	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/tra cing_the_footsteps_of_red_wolf_4c0c8a2b-4185-4f42-9746-029b05056114/Tracingbgiia aecbg2_browsingLnk.lnk?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNS IGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230629%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230629T060229Z&X-Amz-Expires=600&X-Amz-Signature=771 e766d9d3ab55d6d488facdfe1176074810865754090535186d72a34bb5641&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY	Penetrated

TLP:AMBER

ASM-VP REPORT

Organo Judicial 07/26/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-06-29	Tracing The Footsteps Of Red Wolf	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/tracing_the_footsteps_of_red_wolf_4c0c8a2b-4185-4f42-9746-029b05056114/Tracingbgiiaaecbg1_browsingIso.iso?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230629%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230629T060218Z&X-Amz-Expires=600&X-Amz-Signature=ff06688e5a83eb410bab37526f6347779470eb5458b404535cfcd653672ab799&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY	Penetrated
2023-06-28	Wagner Ransomware Cyber Recruitment	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/wagner_ransomware_cyber_recruitment_8554ca68-cbf7-4a40-9e5c-35fa77b13e87/Wagnerbgihjbhidd5_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230628%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230628T064400Z&X-Amz-Expires=600&X-Amz-Signature=975e75e27d8bd5f565c46a12a075c697d4bf6fd020a151fdd9054c71d6603d41&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY	Blocked
2023-06-26	Operation Magalenha - Long-Running Campaign Pursues Portuguese Credentials and PII	Magalenhabgihgjegca100_edrExe.exe	Endpoint Security	OMY	Penetrated
2023-06-26	Operation Magalenha - Long-Running Campaign Pursues Portuguese Credentials and PII	Magalenhabgihgjegca98_edrExe.exe	Endpoint Security	OMY	Penetrated
2023-06-26	Operation Magalenha - Long-Running Campaign Pursues Portuguese Credentials and PII	Magalenhabgihgjegca94_edrExe.exe	Endpoint Security	OMY	Penetrated
2023-06-26	Operation Magalenha - Long-Running Campaign Pursues Portuguese Credentials and PII	Magalenhabgihgjegca9_edr7Exe.exe	Endpoint Security	OMY	Penetrated
2023-06-26	Operation Magalenha - Long-Running Campaign Pursues Portuguese Credentials and PII	Magalenhabgihgjegca104_edrExe.exe	Endpoint Security	OMY	Blocked
2023-06-26	Operation Magalenha - Long-Running Campaign Pursues Portuguese Credentials and PII	Magalenhabgihgjegca99_edrExe.exe	Endpoint Security	OMY	Blocked
2023-06-26	Operation Magalenha - Long-Running Campaign Pursues Portuguese Credentials and PII	Magalenhabgihgjegca101_edrExe.exe	Endpoint Security	OMY	Blocked
2023-06-26	Operation Magalenha - Long-Running Campaign Pursues Portuguese Credentials and PII	Magalenhabgihgjegca92_edrExe.exe	Endpoint Security	OMY	Blocked

TLP:AMBER

GLESEC
COMPLETELY PERCEPTI

ASM-VP REPORT

Organo Judicial 07/26/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-06-26	Operation Magalenha - Long-Running Campaign Pursues Portuguese Credentials and PII	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/operation_magalenha_-_long-running_campaign_pursues_portuguese_credentials_and_pii_39302ab3-8137-4c47-8629-bc09e763c579/Magalenhabgihgjegca90_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230626%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230626T134114Z&X-Amz-Expires=600&X-Amz-Signature=a94d15e38cf59f00cefdec9a1c44ab479ddac2d4fc4e934ee16590291082737f&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY	Penetrated
2023-06-26	Operation Magalenha - Long-Running Campaign Pursues Portuguese Credentials and PII	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/operation_magalenha_-_long-running_campaign_pursues_portuguese_credentials_and_pii_39302ab3-8137-4c47-8629-bc09e763c579/Magalenhabgihgjegca91_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230626%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230626T134024Z&X-Amz-Expires=600&X-Amz-Signature=5497c15c97ee853cc0145af6bc1cc00f1ccef60e1bc7dd6eb78442c456991f52&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY	Penetrated
2023-06-26	Operation Magalenha - Long-Running Campaign Pursues Portuguese Credentials and PII	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/operation_magalenha_-_long-running_campaign_pursues_portuguese_credentials_and_pii_39302ab3-8137-4c47-8629-bc09e763c579/Magalenhabgihgjegca93_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230626%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230626T133944Z&X-Amz-Expires=600&X-Amz-Signature=6af5d763d57acf80ff4e12a17df66085c29c3bd7678a9f1bea8e8f8e9d0079e2&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY	Penetrated
2023-06-26	Operation Magalenha - Long-Running Campaign Pursues Portuguese Credentials and PII	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/operation_magalenha_-_long-running_campaign_pursues_portuguese_credentials_and_pii_39302ab3-8137-4c47-8629-bc09e763c579/Magalenhabgihgjegca102_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230626%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230626T131601Z&X-Amz-Expires=600&X-Amz-Signature=558c85f567127c709de3474705e04fdded7ed7ca2fbf9265934c9030183934e4&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY	Blocked
2023-06-26	Operation Magalenha - Long-Running Campaign Pursues Portuguese Credentials and PII	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/operation_magalenha_-_long-running_campaign_pursues_portuguese_credentials_and_pii_39302ab3-8137-4c47-8629-bc09e763c579/Magalenhabgihgjegca103_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230626%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230626T131056Z&X-Amz-Expires=600&X-Amz-Signature=a85e8b890b17ad5d9330460274c6441293a2b57be93fb7ee6efbc2cdc5a096ec&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY	Blocked
2023-06-26	Operation Magalenha - Long-Running Campaign Pursues Portuguese Credentials and PII	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/operation_magalenha_-_long-running_campaign_pursues_portuguese_credentials_and_pii_39302ab3-8137-4c47-8629-bc09e763c579/Magalenhabgihgjegca105_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230626%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230626T130046Z&X-Amz-Expires=600&X-Amz-Signature=7451b433faf915349474e09fdd77e24fdcd3fde75be7603950e44c097c7cd53f&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY	Blocked
2023-06-26	Operation Magalenha - Long-Running Campaign Pursues Portuguese Credentials and PII	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/operation_magalenha_-_long-running_campaign_pursues_portuguese_credentials_and_pii_39302ab3-8137-4c47-8629-bc09e763c579/Magalenhabgihgjegca10_browsing7Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230626%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230626T125542Z&X-Amz-Expires=600&X-Amz-Signature=5767409976fb012a08fee440e306132c174513be0f2a1d3120c274c0229895c2&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY	Blocked
2023-06-26	Crysis And Venus Ransomware Installed Via RDP	Crysisbgihfhcije181_edrExe.exe	Endpoint Security	OMY	Blocked
2023-06-26	Crysis And Venus Ransomware Installed Via RDP	Crysisbgihfhcije184_edrExe.exe	Endpoint Security	OMY	Penetrated
2023-06-26	Crysis And Venus Ransomware Installed Via RDP	Crysisbgihfhcije180_edrExe.exe	Endpoint Security	OMY	Blocked
2023-06-26	Crysis And Venus Ransomware Installed Via RDP	Crysisbgihfhcije188_edrExe.exe	Endpoint Security	OMY	Blocked
2023-06-26	Crysis And Venus Ransomware Installed Via RDP	Crysisbgihfhcije182_edrDll.dll	Endpoint Security	OMY	Blocked
2023-06-26	Crysis And Venus Ransomware Installed Via RDP	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/crysis_and_venus_ransomware_installed_via_rdp_f8741241-ed45-4a8f-8e68-09566cd32555/Crysisbgihfhcije194_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230626%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230626T062955Z&X-Amz-Expires=600&X-Amz-Signature=57015ad6da05eab11200468e623297d39a3c22e2d74d7664450dc20ab5c88513&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY	Penetrated

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

TLP:AMBER

ASM-VP REPORT

Organo Judicial 07/26/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-06-26	Crysis And Venus Ransomware Installed Via RDP	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/crysis_and_venus_ransomware_installed_via_rdp_f8741241-ed45-4a8f-8e68-09566cd32555/Crysisbgihfhcije190_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230626%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230626T062954Z&X-Amz-Expires=600&X-Amz-Signature=cff1c01fb60df3c6f6951d17019a91f6d5c85e3ef5f84b3e8f9936715b9913cf&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY	Penetrated
2023-06-26	Crysis And Venus Ransomware Installed Via RDP	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/crysis_and_venus_ransomware_installed_via_rdp_f8741241-ed45-4a8f-8e68-09566cd32555/Crysisbgihfhcije186_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230626%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230626T062953Z&X-Amz-Expires=600&X-Amz-Signature=aa669cd338958498042b32fdfae54778ab1b370c233e158892ea463c511c3704&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY	Penetrated
2023-06-26	Crysis And Venus Ransomware Installed Via RDP	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/crysis_and_venus_ransomware_installed_via_rdp_f8741241-ed45-4a8f-8e68-09566cd32555/Crysisbgihfhcije185_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230626%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230626T062952Z&X-Amz-Expires=600&X-Amz-Signature=0c6d638b8a25e57fa5803879fa6eda3d4c04e67d2e189934e0641e29d55d1ac8&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY	Penetrated
2023-06-26	Crysis And Venus Ransomware Installed Via RDP	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/crysis_and_venus_ransomware_installed_via_rdp_f8741241-ed45-4a8f-8e68-09566cd32555/Crysisbgihfhcije183_browsingDll.dll?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230626%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230626T062950Z&X-Amz-Expires=600&X-Amz-Signature=ec66eef3815b9b3f38cbe69246d1fec605262dfb6720d3d5ad6ef41077c8b939&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY	Penetrated
2023-06-26	Crysis And Venus Ransomware Installed Via RDP	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/crysis_and_venus_ransomware_installed_via_rdp_f8741241-ed45-4a8f-8e68-09566cd32555/Crysisbgihfhcije1_browsing79Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230626%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230626T062946Z&X-Amz-Expires=600&X-Amz-Signature=838335f94c38e9f18ac94ad2f3da95a7bc52169f6863db2839a427a207257bd1&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	OMY	Penetrated

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

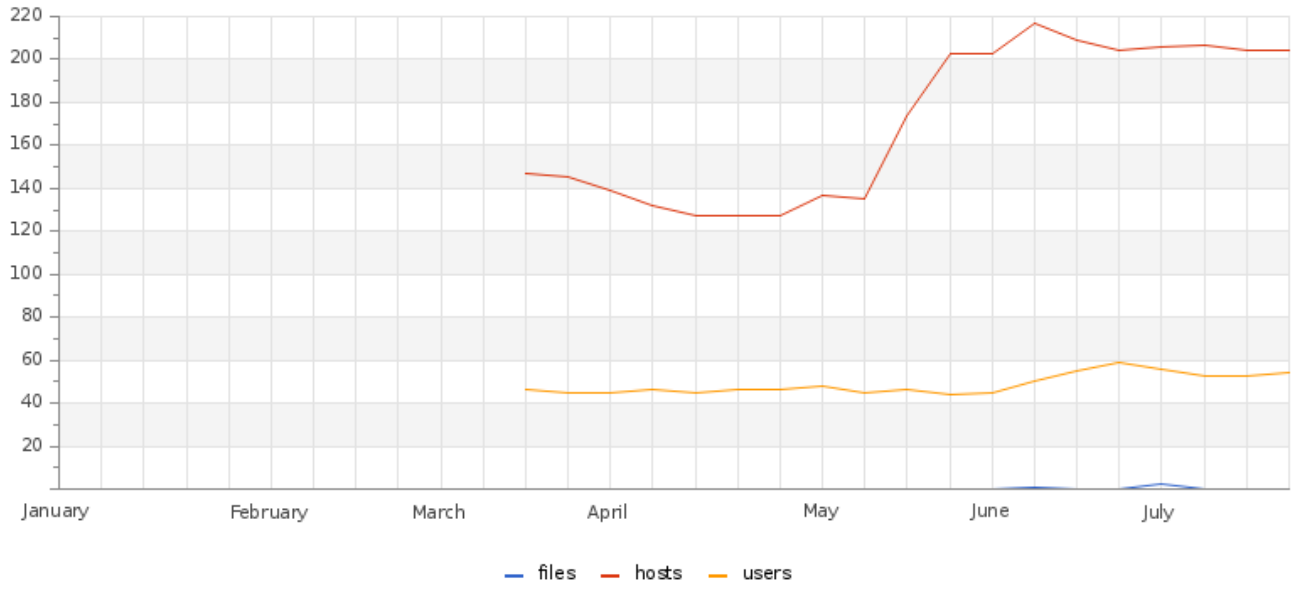
Threats

MSS-EDR

Average Threat - User Defined

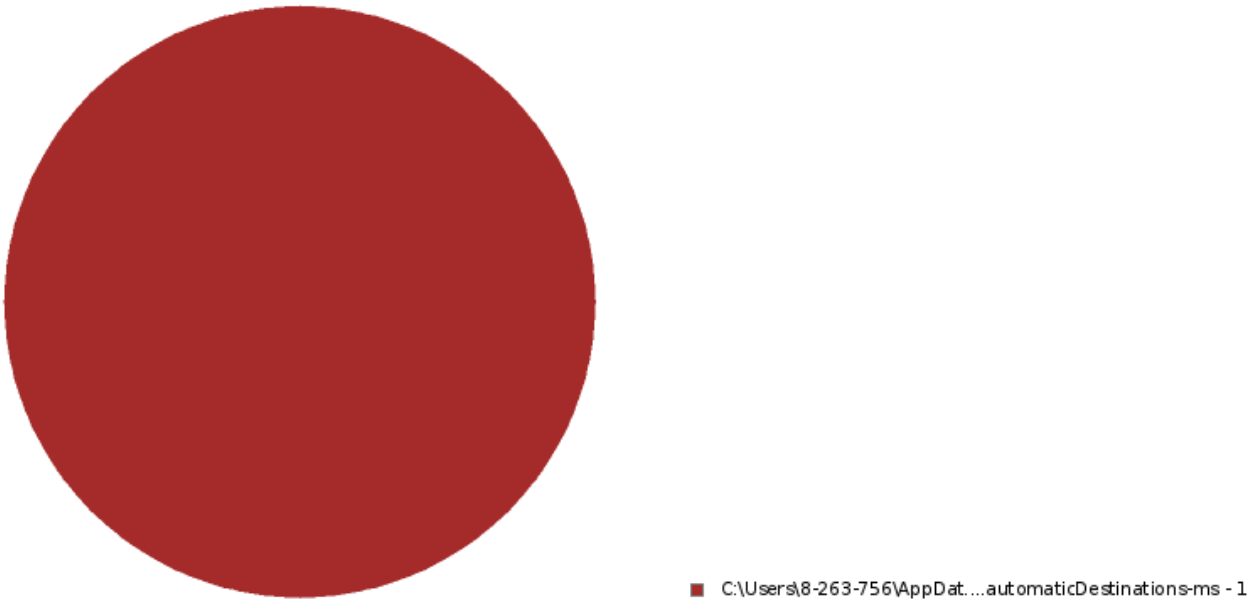
81

Threat Score

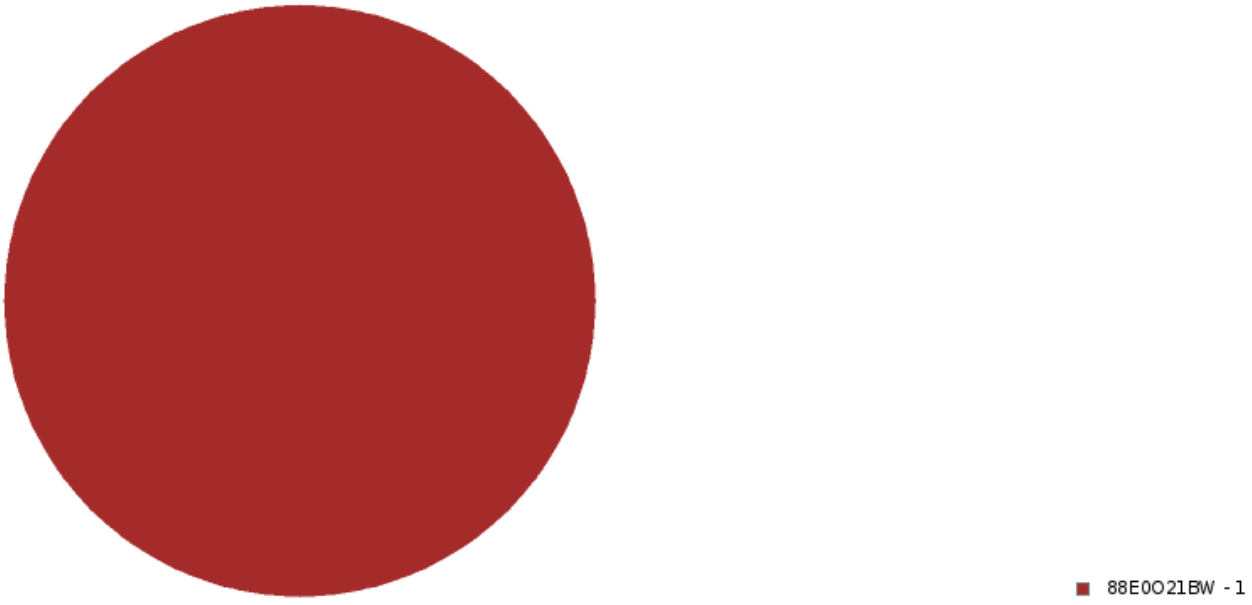


LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

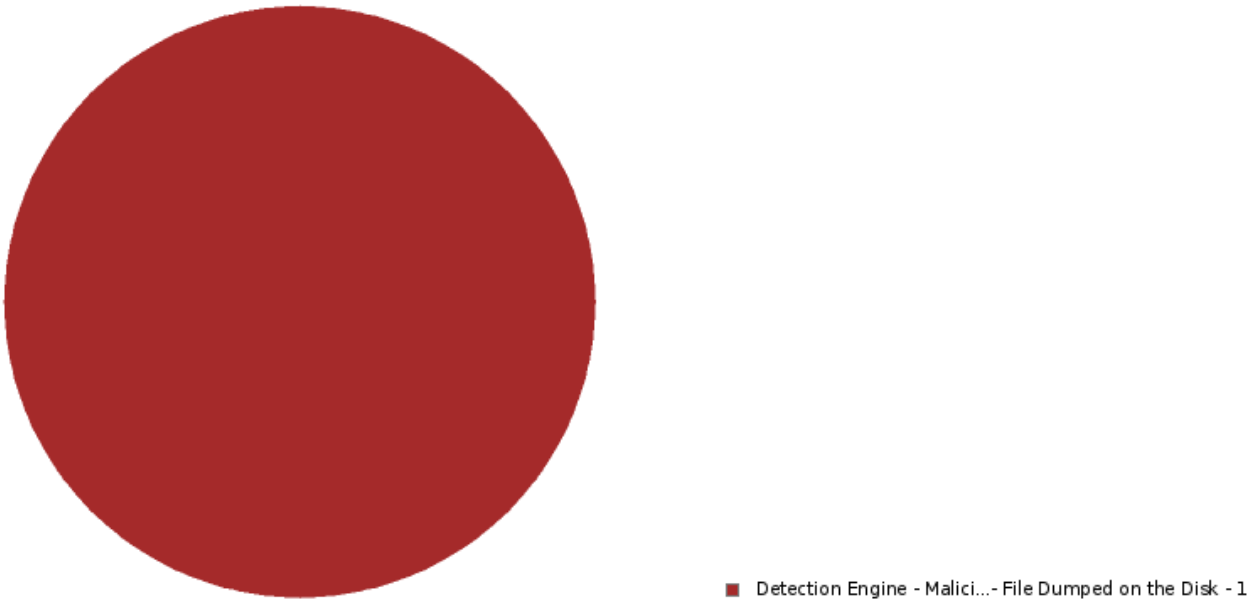
Events by File Path - User Defined



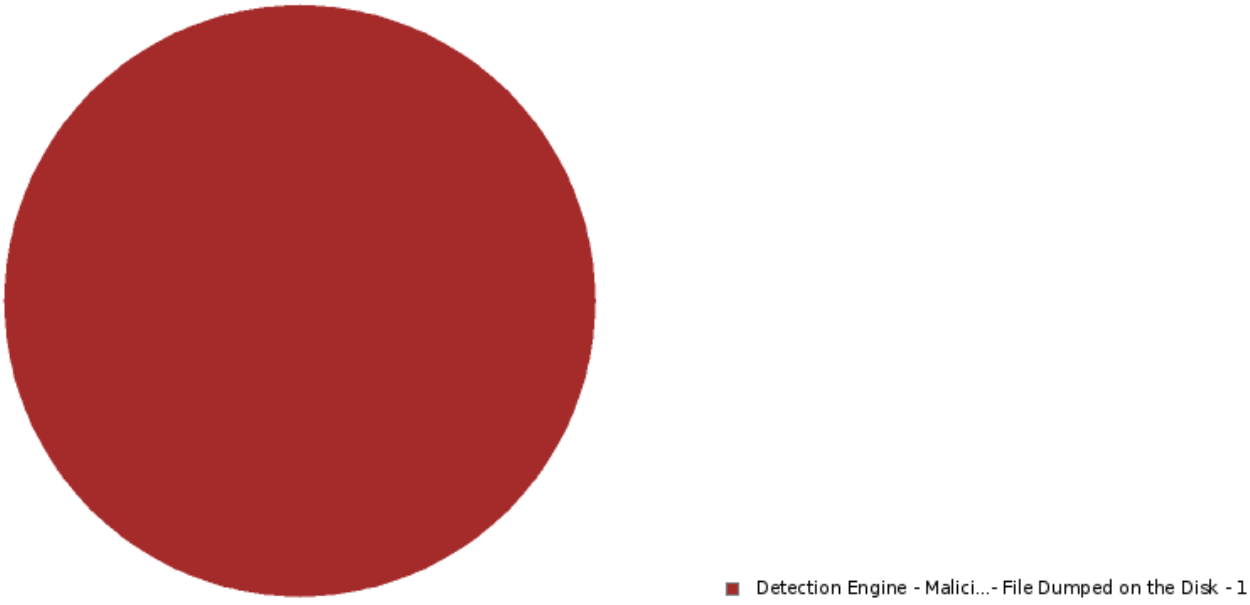
Events by Host Name - User Defined



Events by Event Name - User Defined



High Severity Events by Event Name - User Defined



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

ASM-VP REPORT

Organo Judicial 07/26/2023

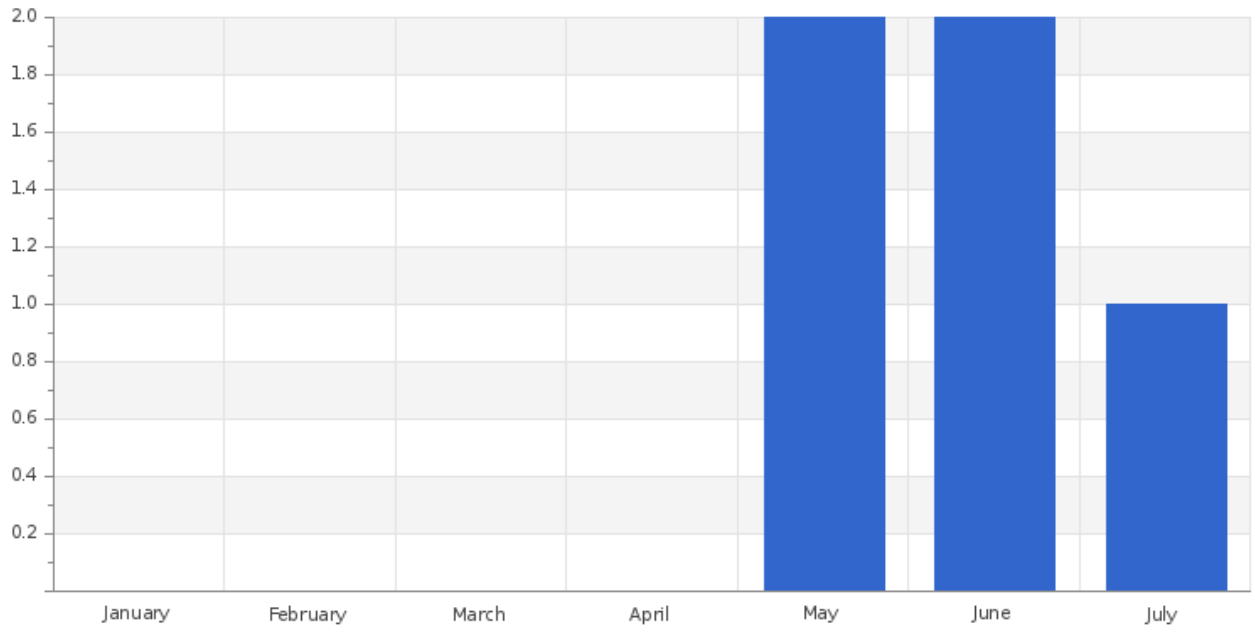
Brute Force Detection by Ratio - User Defined

Host \ User Name	Ratio (Bad : Good)	Probability
88e0o21cq\administrador	39 : 141	0.28
88e0o20d4\administrador	5 : 31	0.16
88e0o20a9\administrador	1 : 32	0.03
88e0o20bc\administrador	1 : 72	0.01

High Severity Events

Host	File Path	Severity	count
88E0O21BW	C:\Users\8-263-756\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\dd7c3b1adb1c168b.automaticDestinations-ms	5	1

Events



Total Hosts - User Defined

88

High Severity Events by File Path - User Defined

File Path	Severity	Event Count
C:\Users\8-263-756\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\dd7c3b1adb1c168b.automaticDestinations-ms	5	1

High Severity Events by Host Name - User Defined

Host	Severity	Event Count
88E0O21BW	5	1

MSS-DDOS

Total Attacks over 24 hours

243797

Critical Attacks over 24 hours

229039

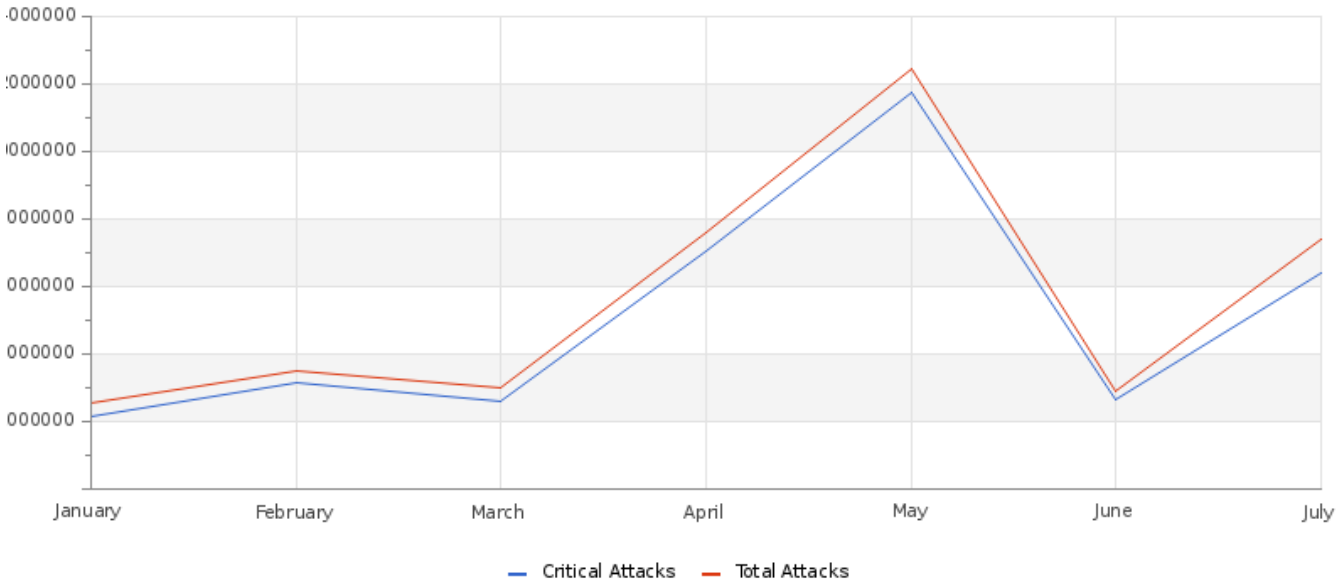
LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

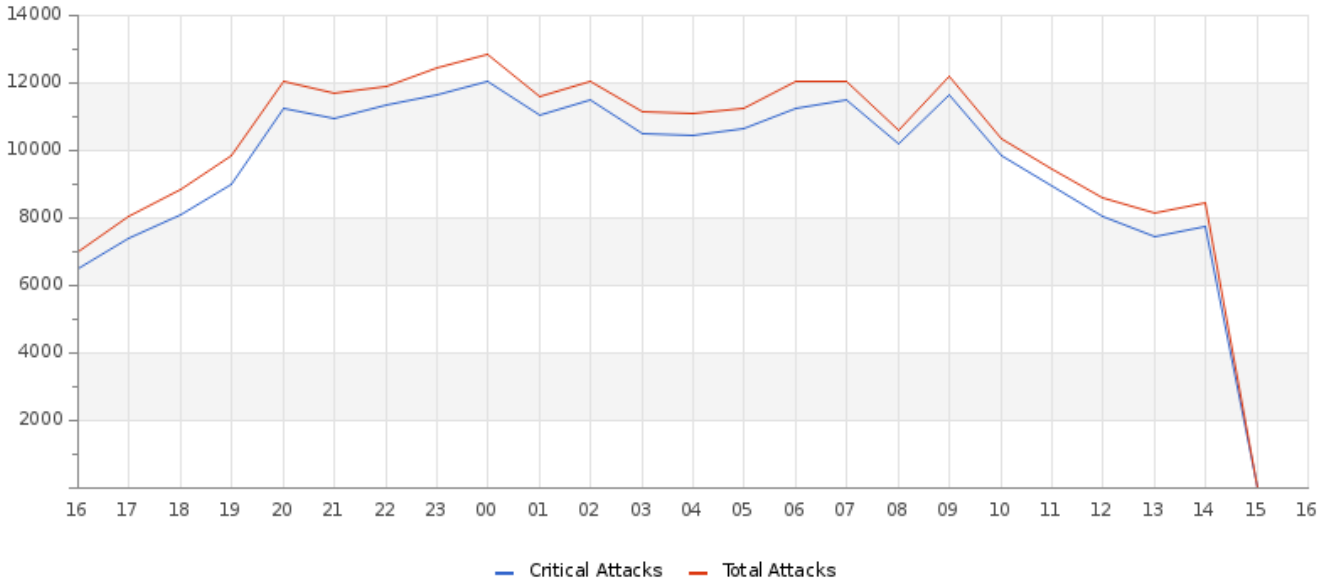
ASM-VP REPORT

Organo Judicial 07/26/2023

Total & Critical Attacks Per Month In Last 6 Months



Executive Summary - Critical and Total Attacks In Past 24 Hours



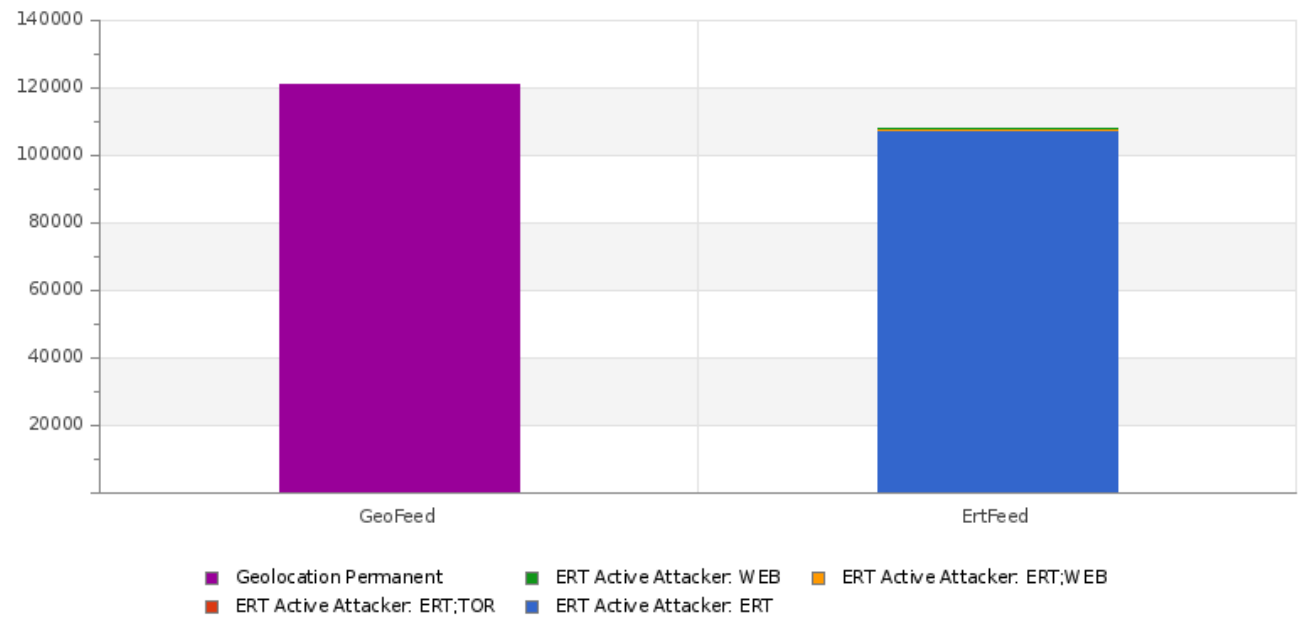
LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

TLP:AMBER

ASM-VP REPORT

Organo Judicial 07/26/2023

Critical Attacks Blocked



Executive Summary - Most Common Attack Durations

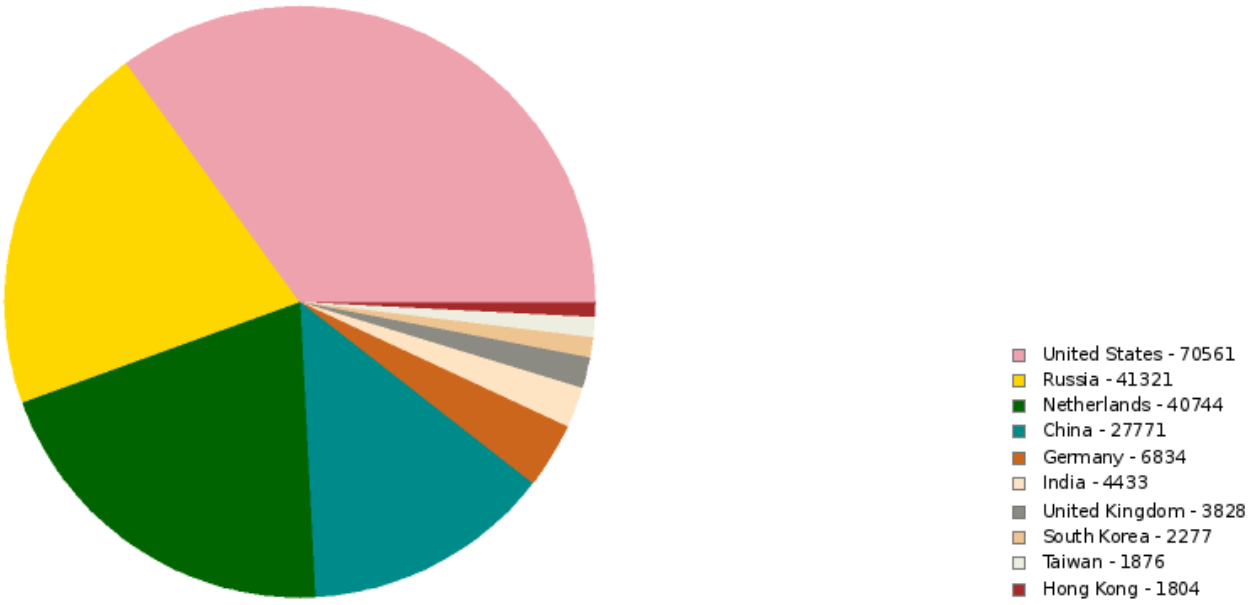
range	Access	Anomalies	Anti-Scanning	ErtFeed	GeoFeed
Less Than A Minute	1	1	12	30583	1
One to Five Minutes	0	3	1	178	11
Thirty to Sixty Minutes	41	12	0	0	75
Ten to Thirty Minutes	2	10	0	0	92
Five to Ten Minutes	0	0	1	1	2

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

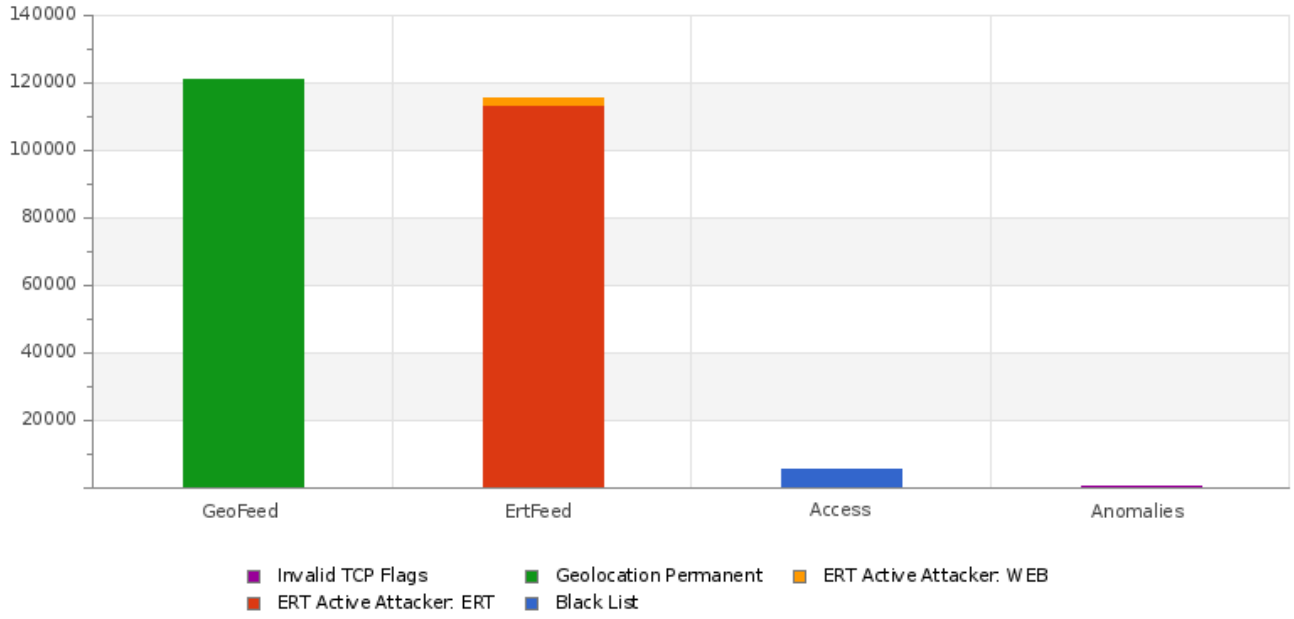
ASM-VP REPORT

Organo Judicial 07/26/2023

Executive Summary - Top Attacking Countries



Types of Blocked Attacks

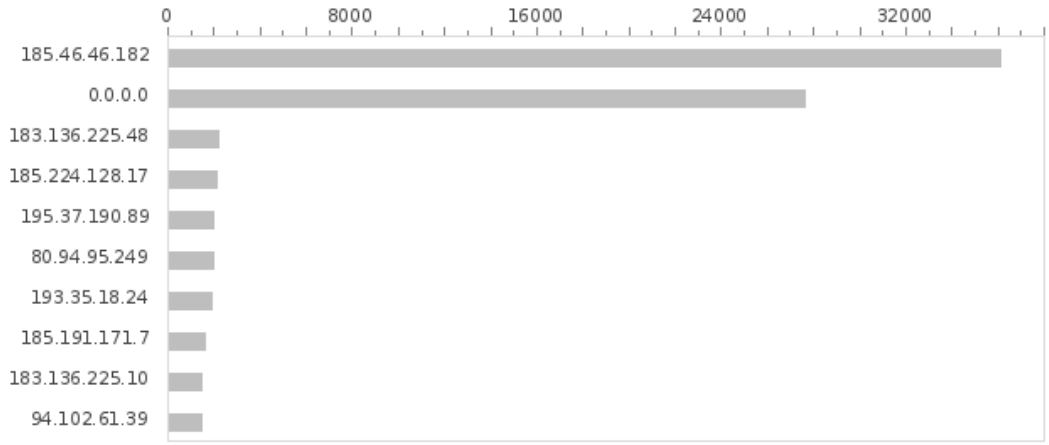


LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

ASM-VP REPORT

Organo Judicial 07/26/2023

Top Attack Sources



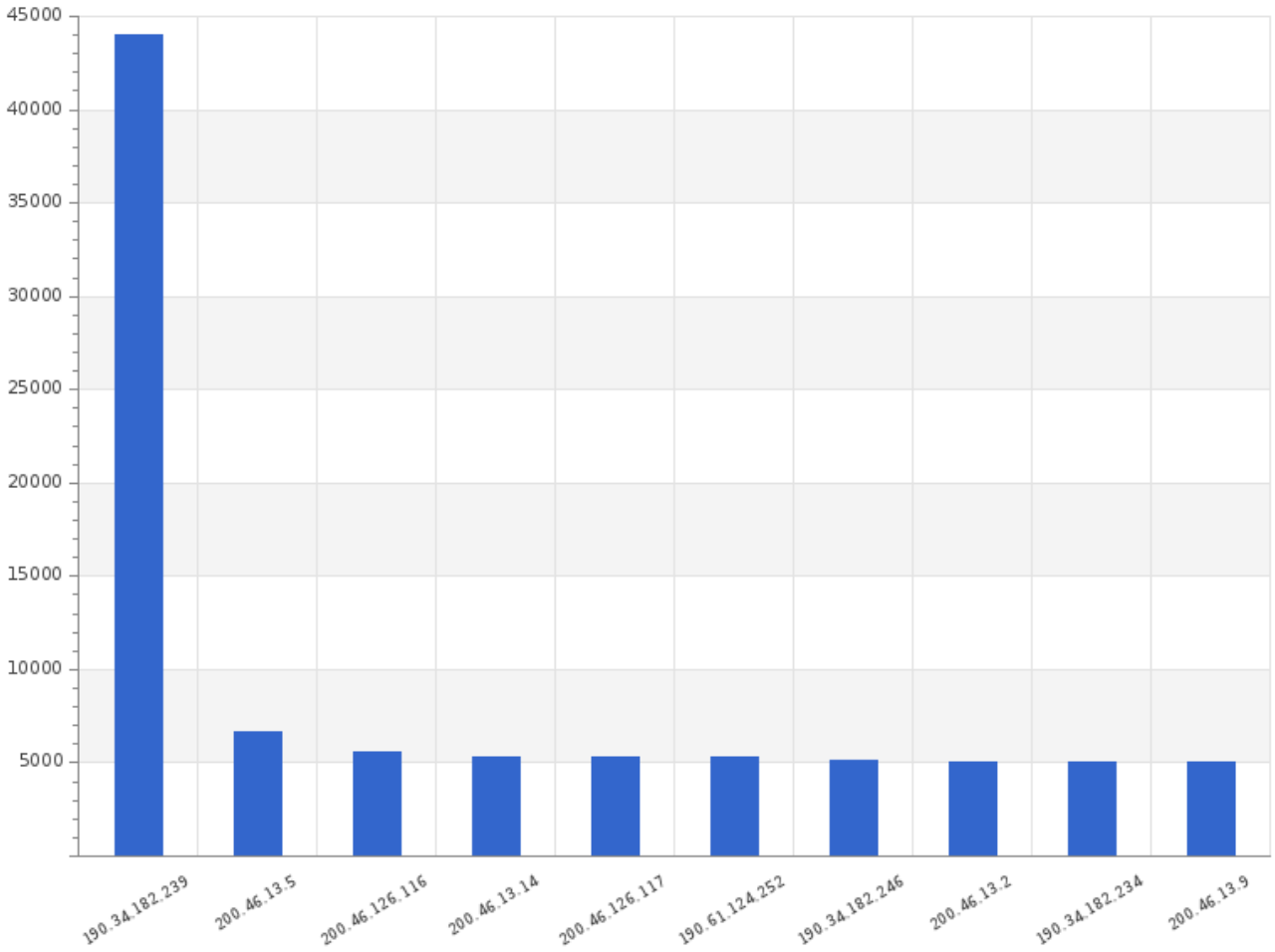
Top Assets Protected

LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

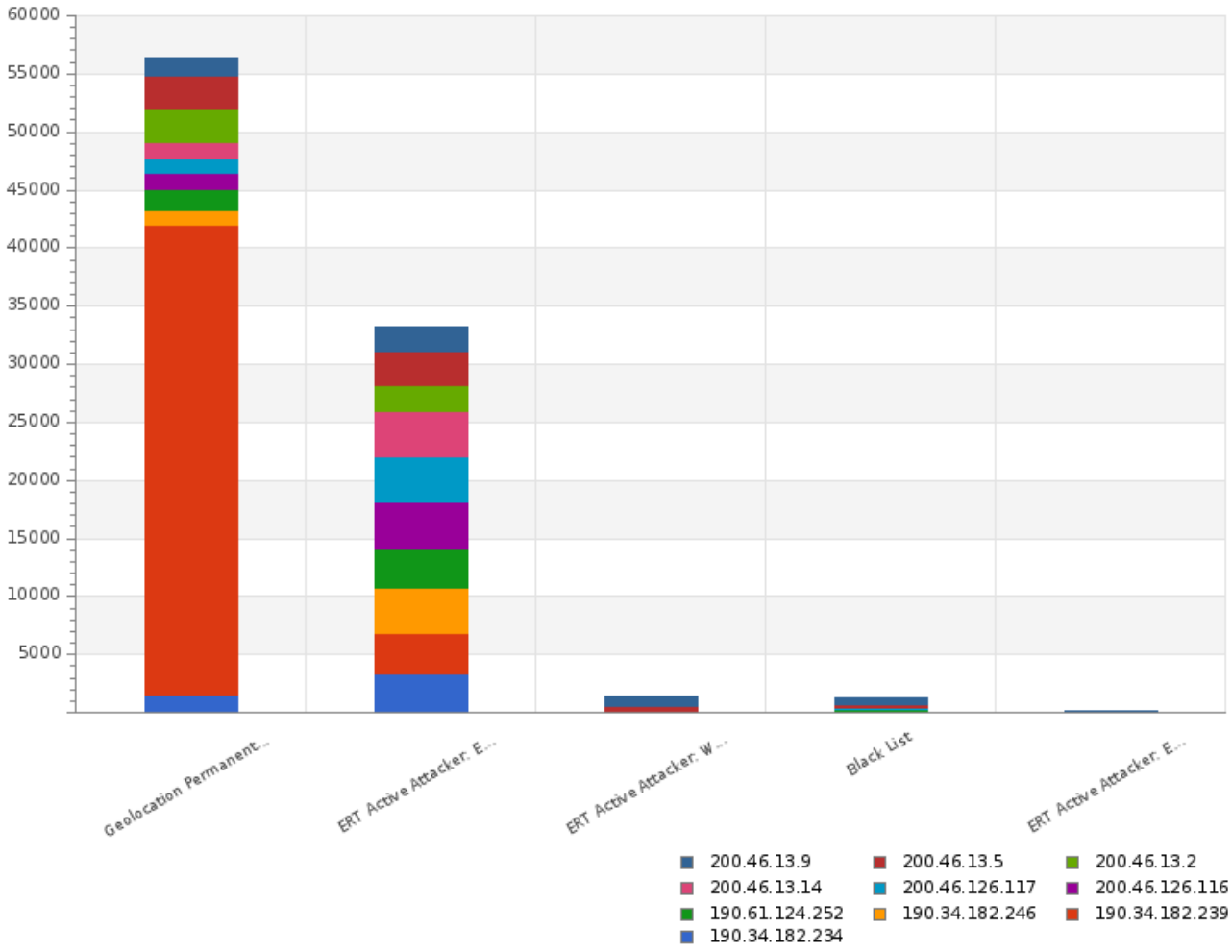
ASM-VP REPORT

Organo Judicial 07/26/2023



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

Top Attack Type Per Protected Asset

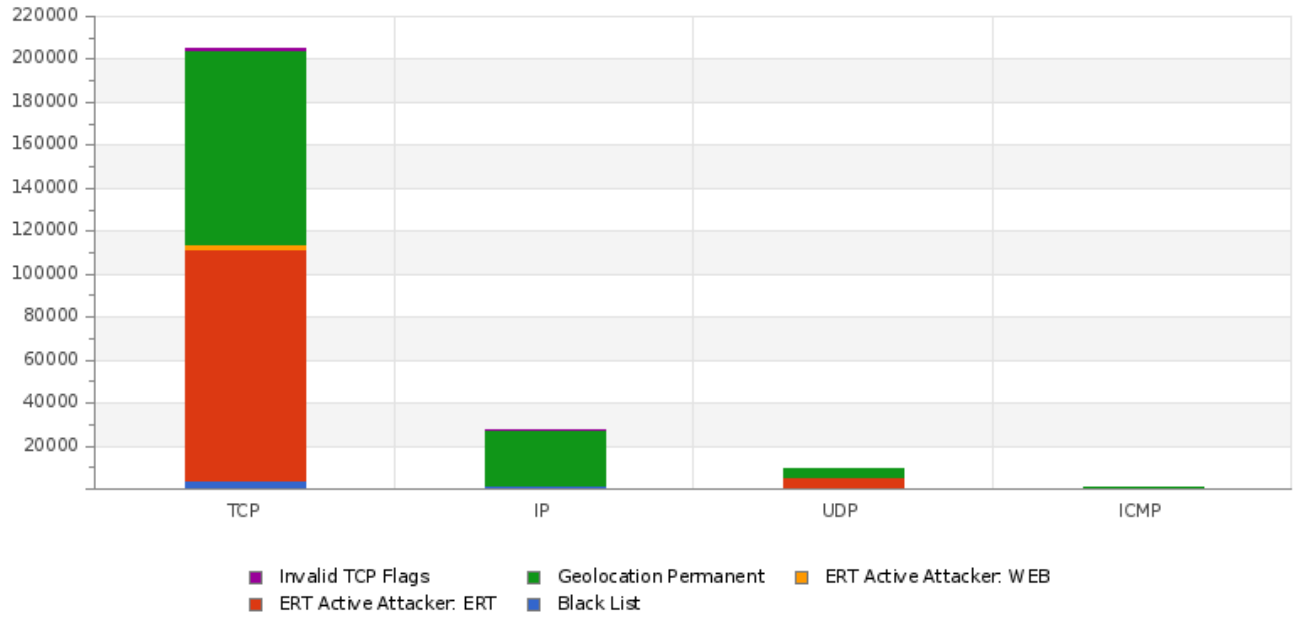


LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

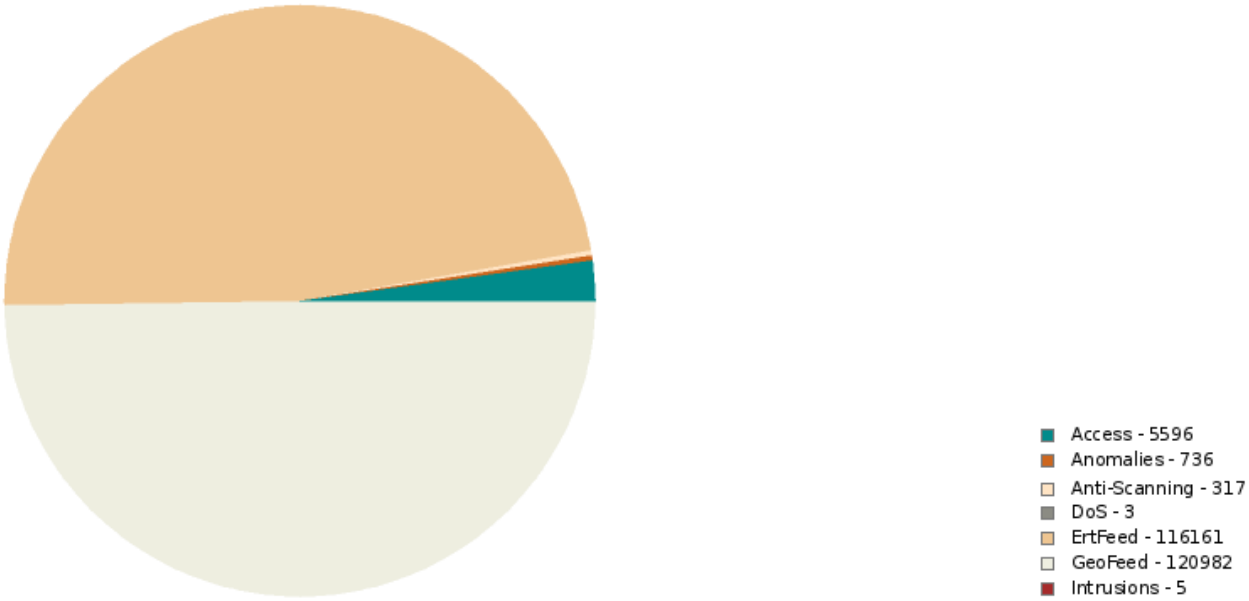
ASM-VP REPORT

Organo Judicial 07/26/2023

Top Blocked DDOS Types



Executive Summary - Types of Blocked Attacks



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

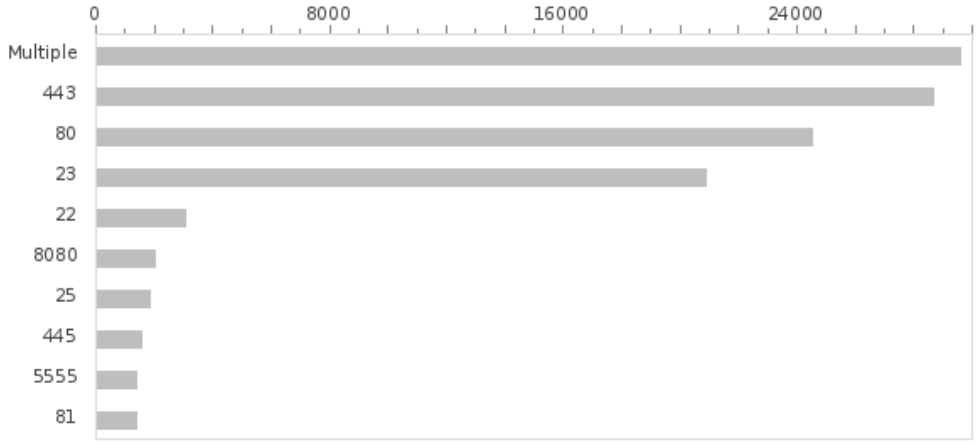
ASM-VP REPORT

Organo Judicial 07/26/2023

Executive Summary - Total Bandwidth/Packet Count by Attack Type

Category	MB/s	KB/s
GeoFeed	5.21	5337.93
ErtFeed	3.59	3677.90
Access	0.26	264.00
Anomalies	0.13	133.24
Anti-Scanning	0.02	23.65
DoS	0.00	0.07
Intrusions	0.00	0.00
--Total Bandwidth--	9.21	9436.79

Executive Summary - Attacks Blocked by Destination Port



MSS-BOT

Bot Hits

1172

Signatures

45

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

ASM-VP REPORT

Organo Judicial 07/26/2023

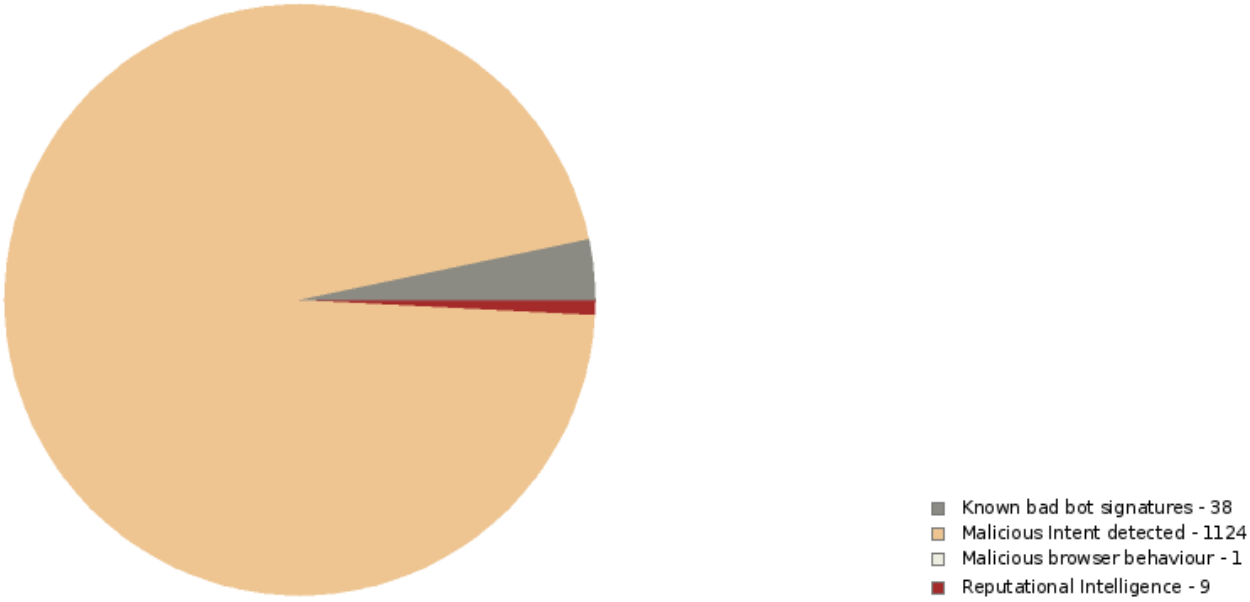
Transactions

1171

Impacted Paths

75

Bot Classification



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

ASM-VP REPORT

Organo Judicial 07/26/2023

Top Bad Bot IPs

Top Impacted Paths

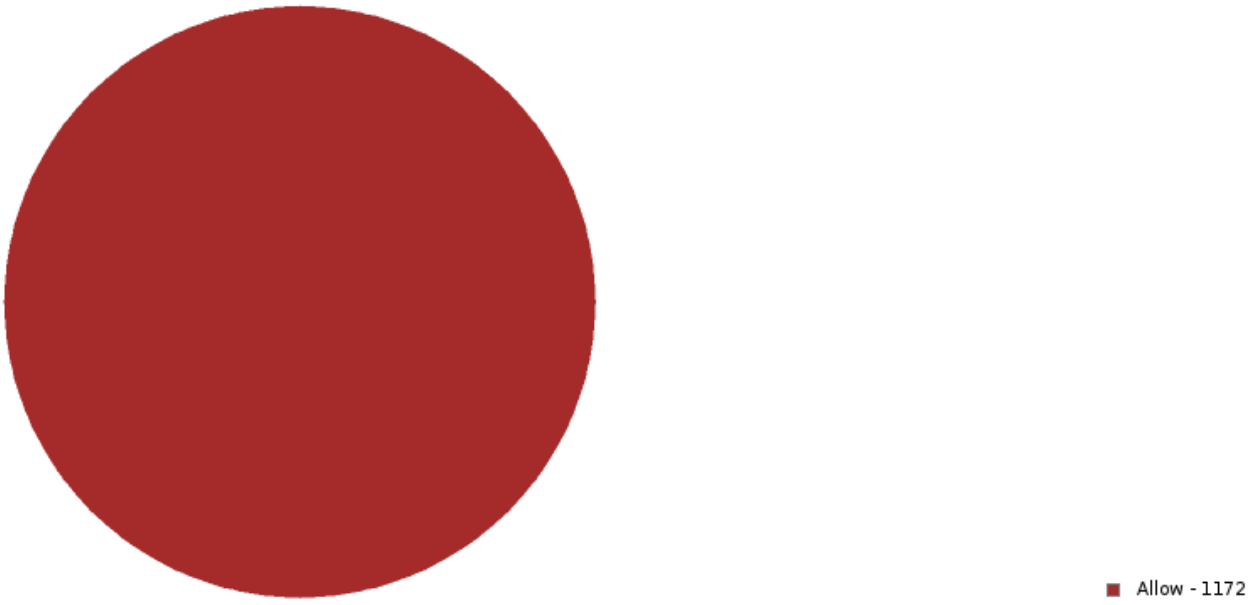
LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

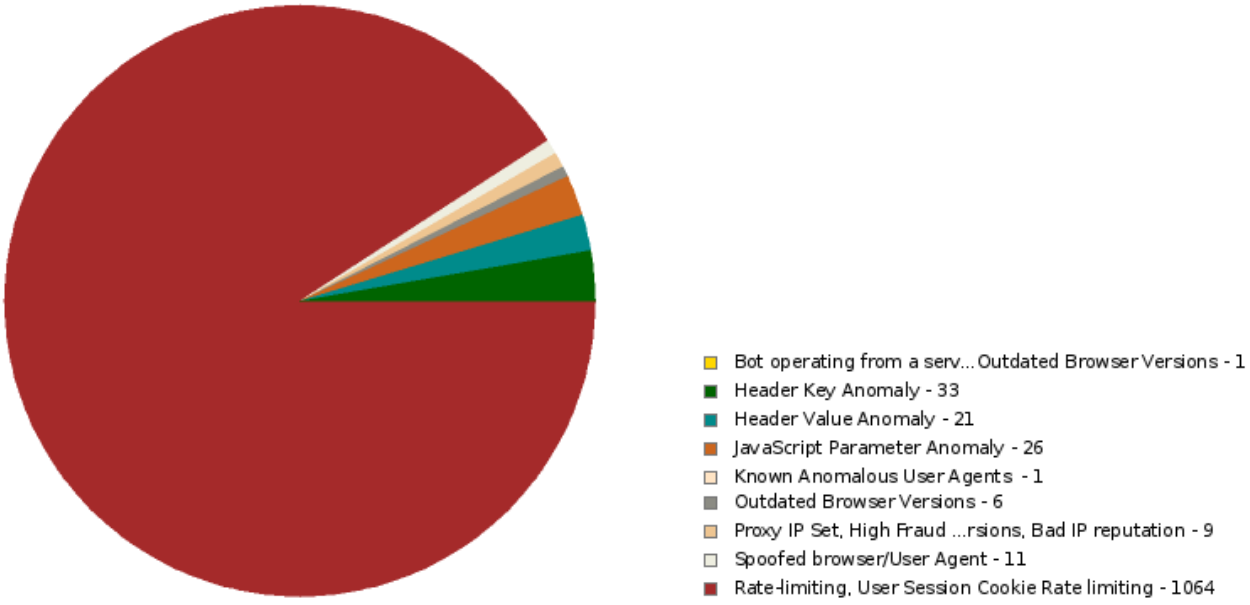
ASM-VP REPORT

Organo Judicial 07/26/2023

Bot Action



Bot Violation

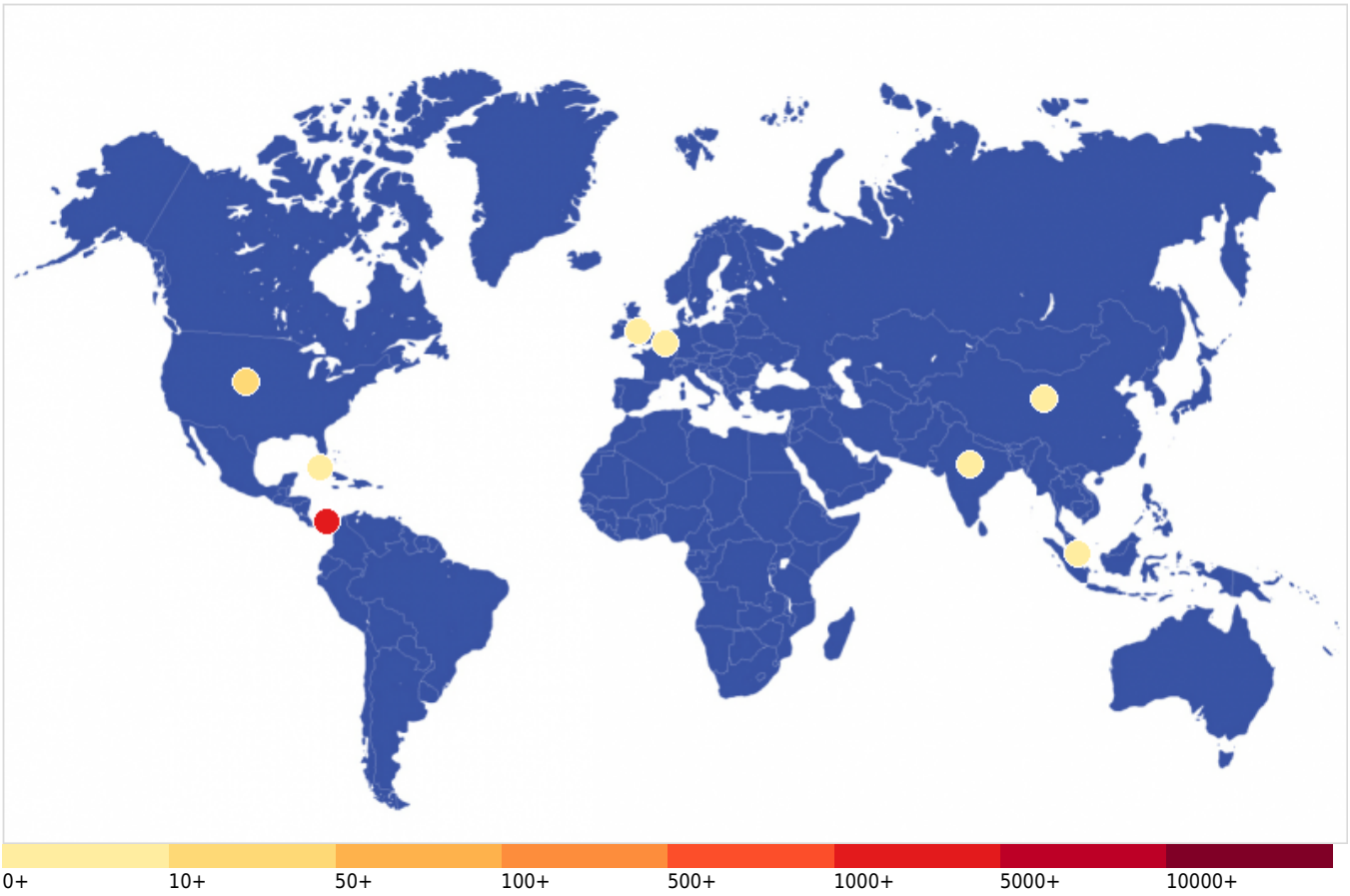


TLP:AMBER

ASM-VP REPORT

Organo Judicial 07/26/2023

Bot Activity Map



Belgium - 1
United States - 27

China - 9
Panama - 1123

Cuba - 2
Singapore - 5

India - 2
United Kingdom - 3

Top User Agents

Peak Times By Bot Classification

Peak Time	Category	Count
16/07/2023 1:00:00 AM	Reputational Intelligence	9
20/07/2023 22:00:00 PM	Malicious browser behaviour	1
13/07/2023 1:00:00 AM	Malicious Intent detected	1059
24/07/2023 6:00:00 AM	Known bad bot signatures	4

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

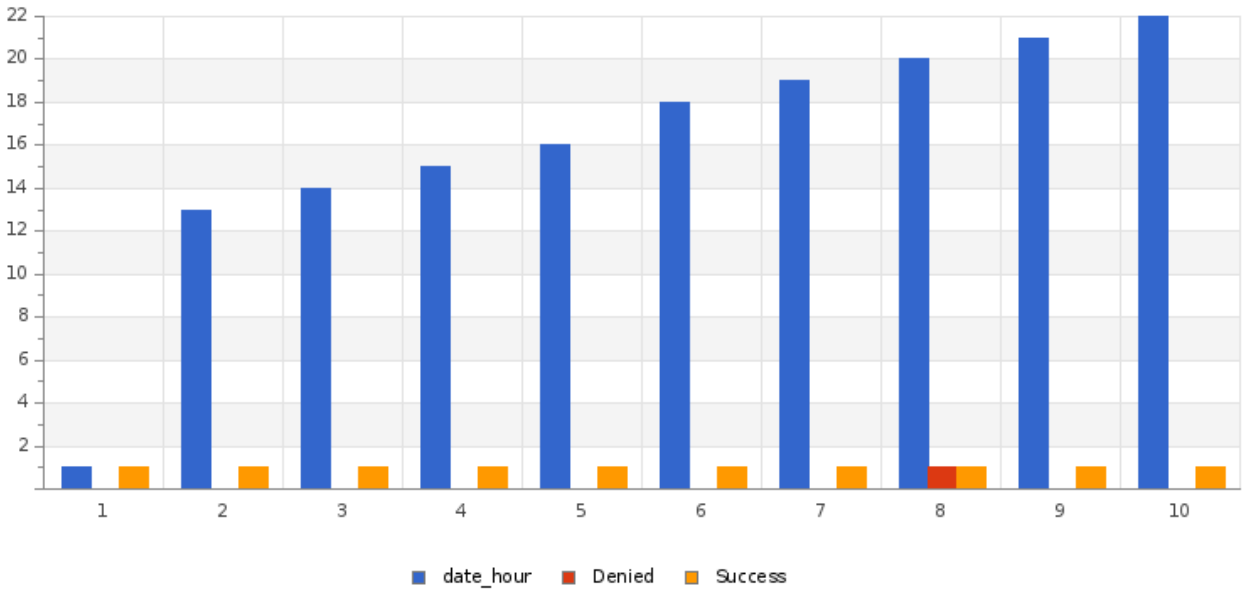
Trusted Access

MSS-TAS

Total Users *

7

Average Authentications by Hour of the Day

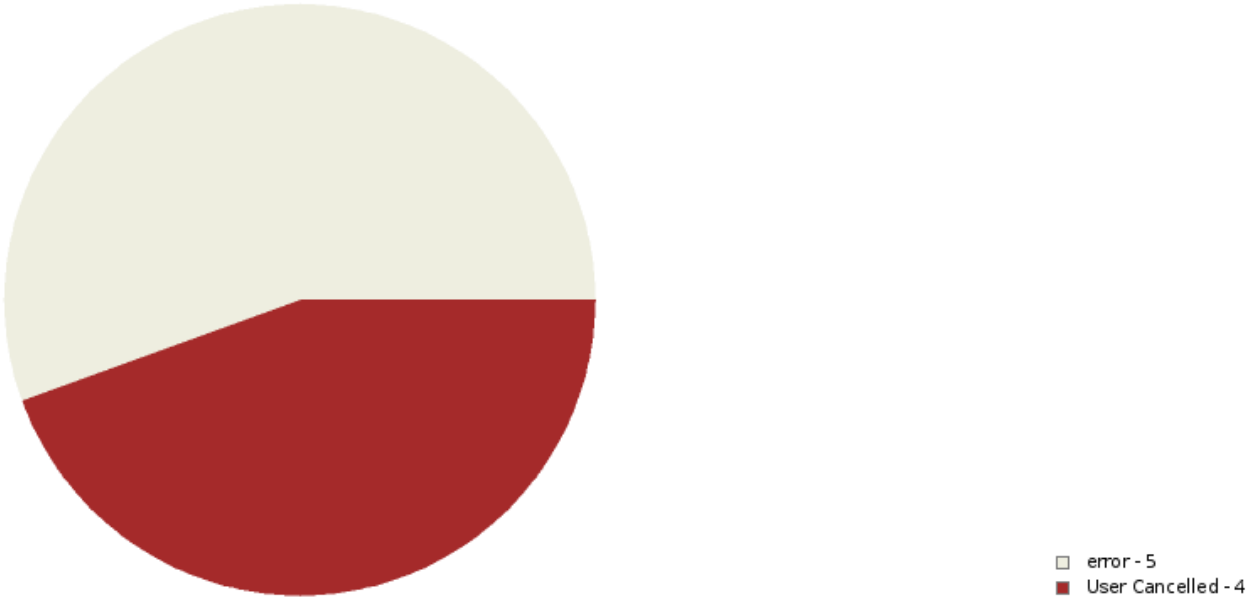


LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

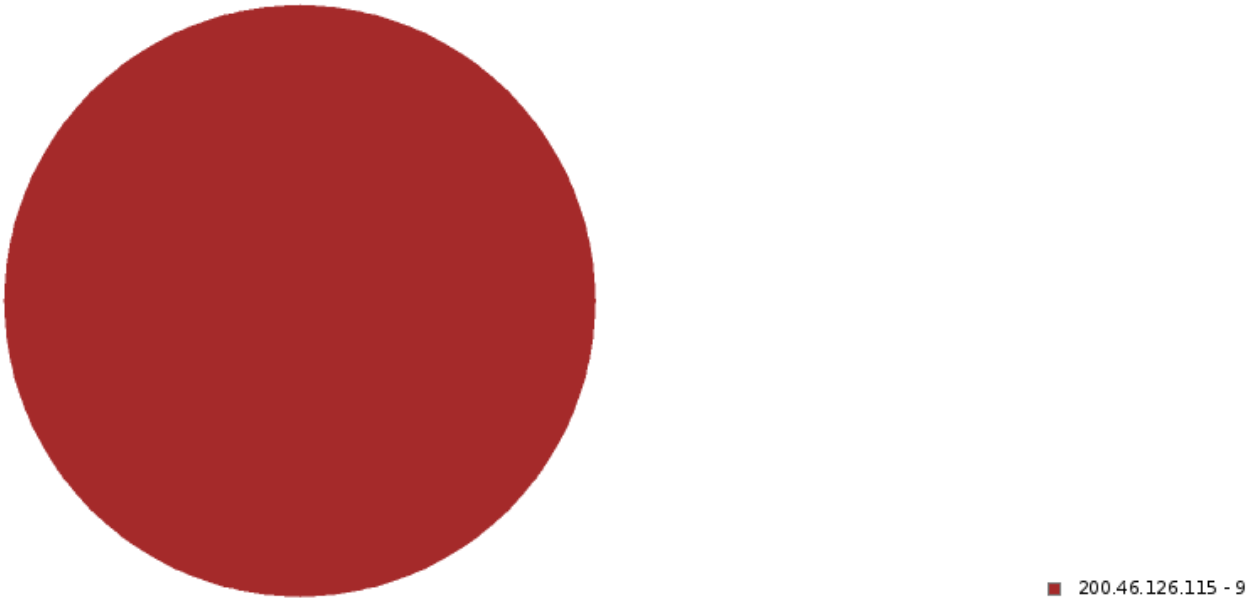
ASM-VP REPORT

Organo Judicial 07/26/2023

Top of Failed Authentications *



Top Authentications Failed by IPs *

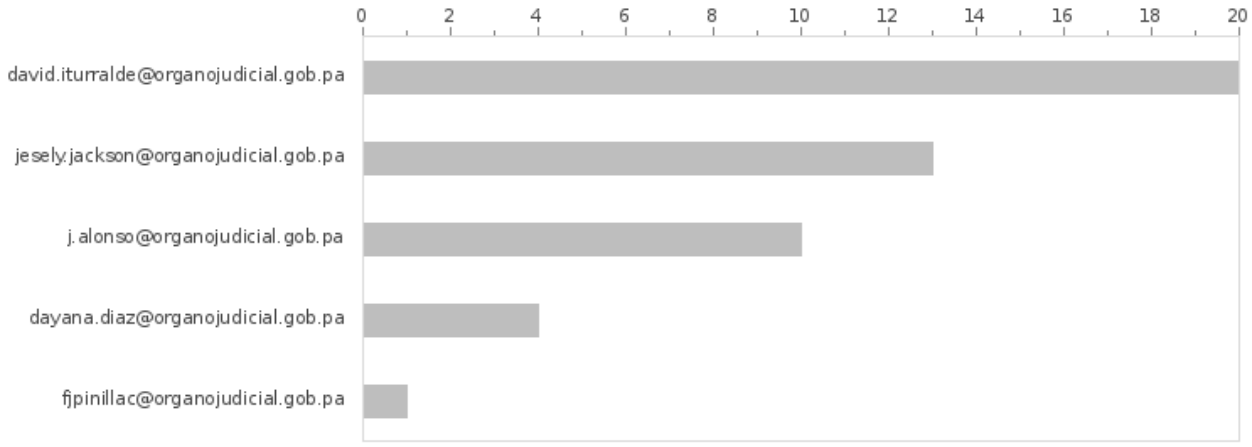


LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

ASM-VP REPORT

Organo Judicial 07/26/2023

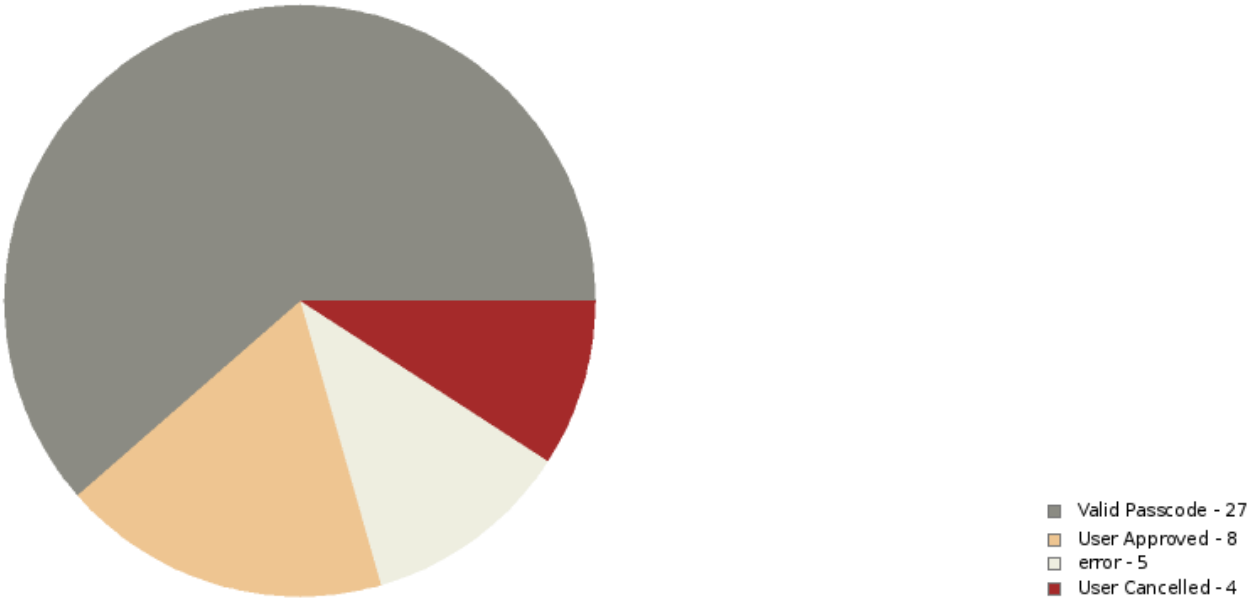
Top Authenticated Users *



Most Active Applications *

app	Denied	Success	Total
GMP	9	39	48

Authentication Status in the Last 24 Hours *



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

ASM-VP REPORT

Organo Judicial 07/26/2023

Users with failed authentications *

user	Time	src_ip
jesely.jackson@organojudicial.gob.pa	Tue Jul 18 20:35:12 2,023 UTC	200.46.126.115
jesely.jackson@organojudicial.gob.pa	Tue Jul 18 20:35:42 2,023 UTC	200.46.126.115
jesely.jackson@organojudicial.gob.pa	Tue Jul 18 20:36:32 2,023 UTC	200.46.126.115
jesely.jackson@organojudicial.gob.pa	Tue Jul 18 20:37:57 2,023 UTC	200.46.126.115
jesely.jackson@organojudicial.gob.pa	Wed Jul 19 13:53:26 2,023 UTC	200.46.126.115
david.iturralde@organojudicial.gob.pa	Fri Jul 14 19:59:18 2,023 UTC	200.46.126.115
jesely.jackson@organojudicial.gob.pa	Mon Jul 24 13:34:07 2,023 UTC	200.46.126.115
jesely.jackson@organojudicial.gob.pa	Mon Jul 24 13:34:41 2,023 UTC	200.46.126.115
jesely.jackson@organojudicial.gob.pa	Mon Jul 24 13:35:18 2,023 UTC	200.46.126.115

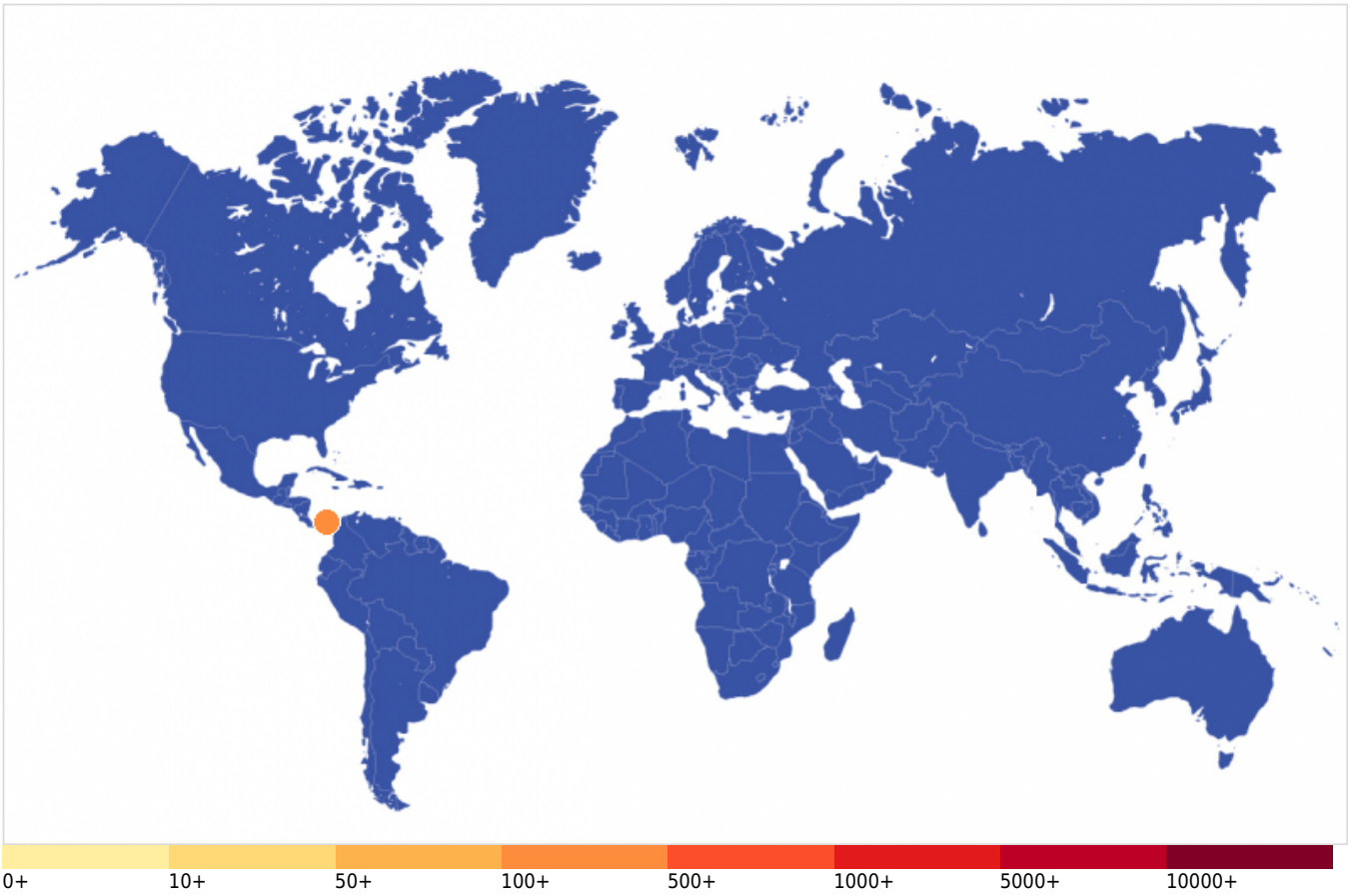
Authentications Cancelled by the Users *

Username	Time	IP Address
jesely.jackson@organojudicial.gob.pa	Tue Jul 18 20:35:12 2,023 UTC	200.46.126.115
jesely.jackson@organojudicial.gob.pa	Tue Jul 18 20:35:42 2,023 UTC	200.46.126.115
jesely.jackson@organojudicial.gob.pa	Tue Jul 18 20:36:32 2,023 UTC	200.46.126.115
jesely.jackson@organojudicial.gob.pa	Mon Jul 24 13:34:07 2,023 UTC	200.46.126.115

Most Successful Authenticated Countries *

ASM-VP REPORT

Organo Judicial 07/26/2023

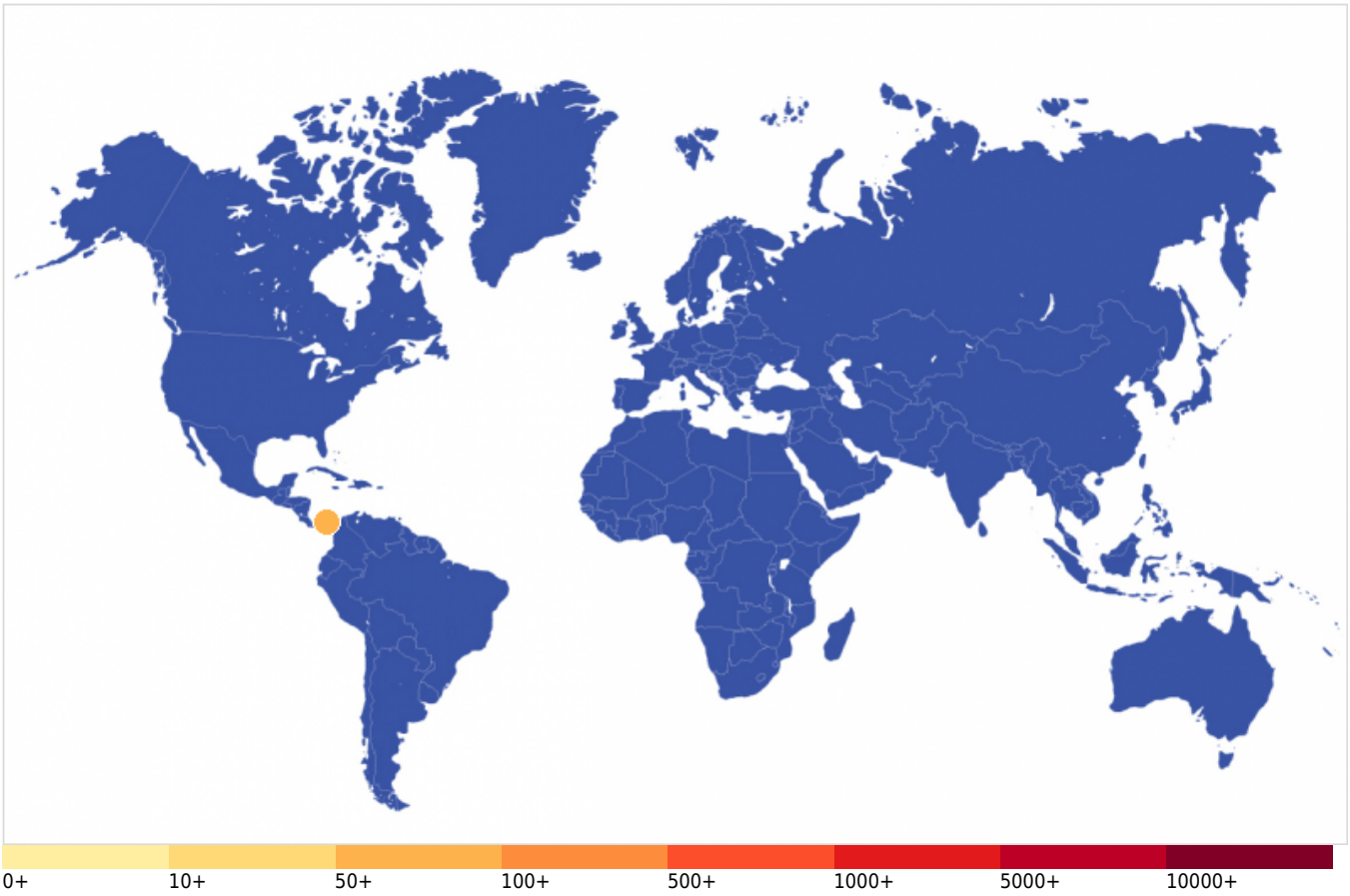


Countries with Most Failed Authentications *

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

ASM-VP REPORT

Organo Judicial 07/26/2023

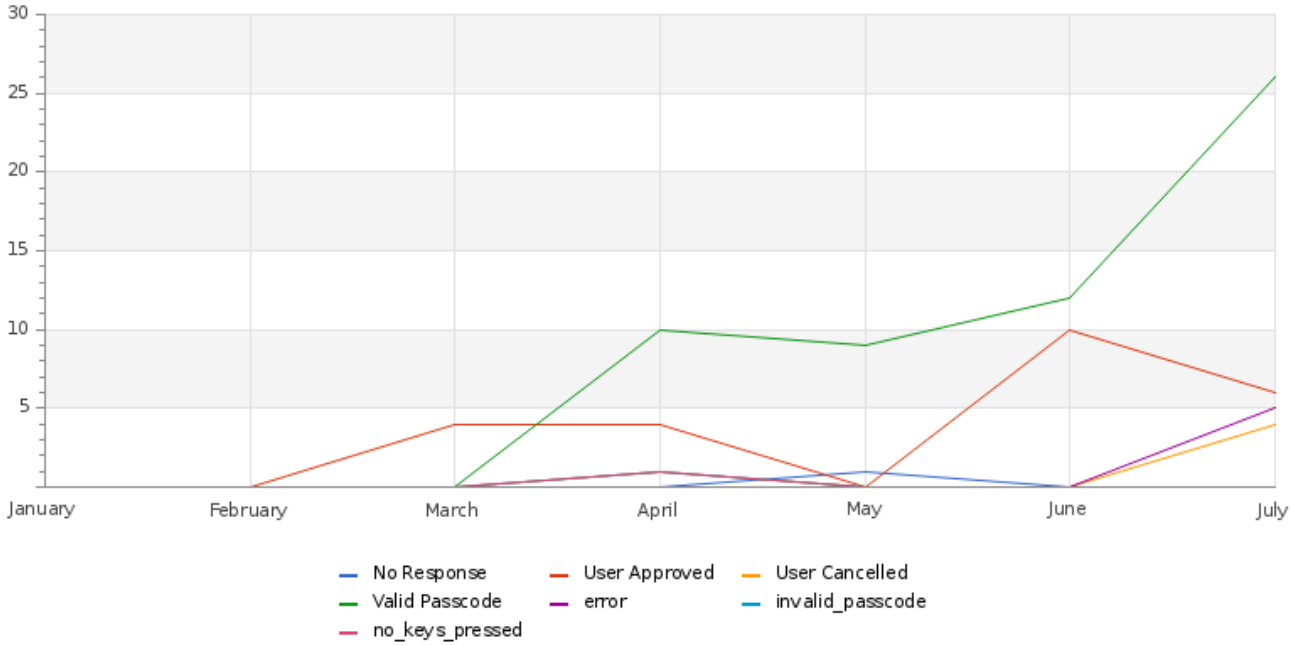


LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

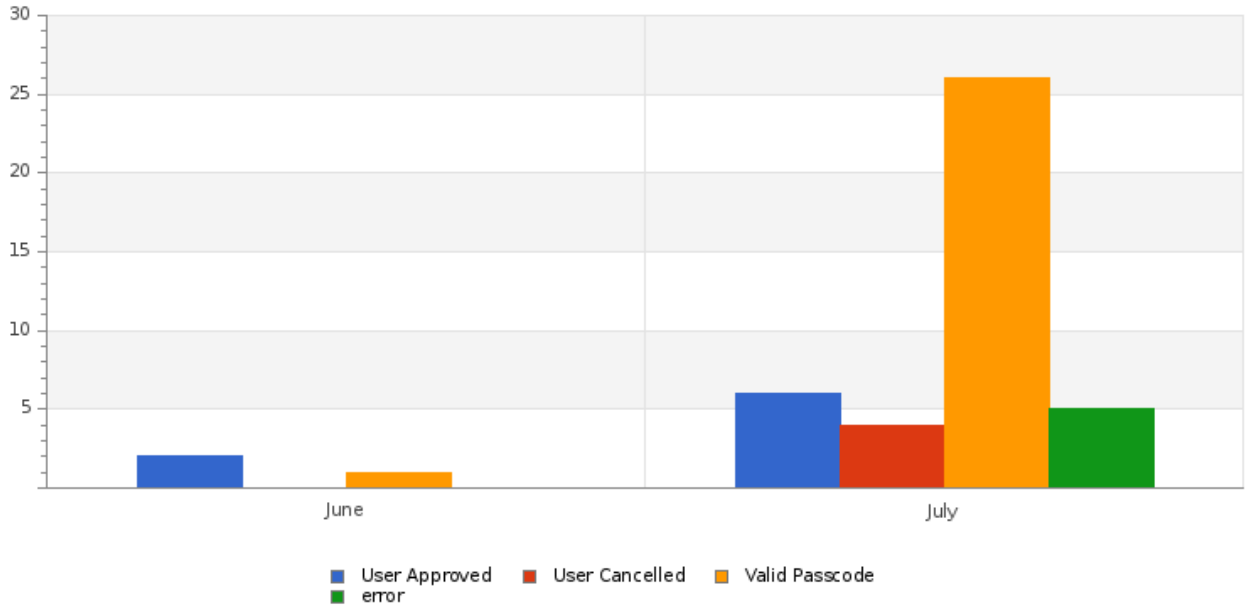
ASM-VP REPORT

Organo Judicial 07/26/2023

Trusted Access In Last 6 Months



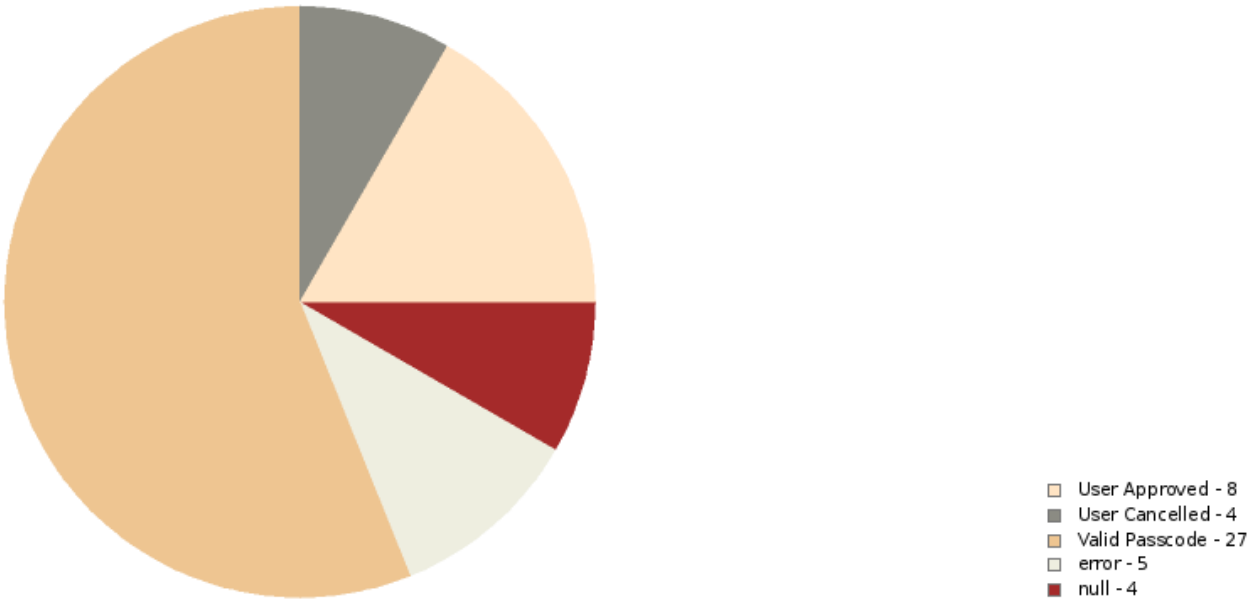
Successful and Failed Authentications *



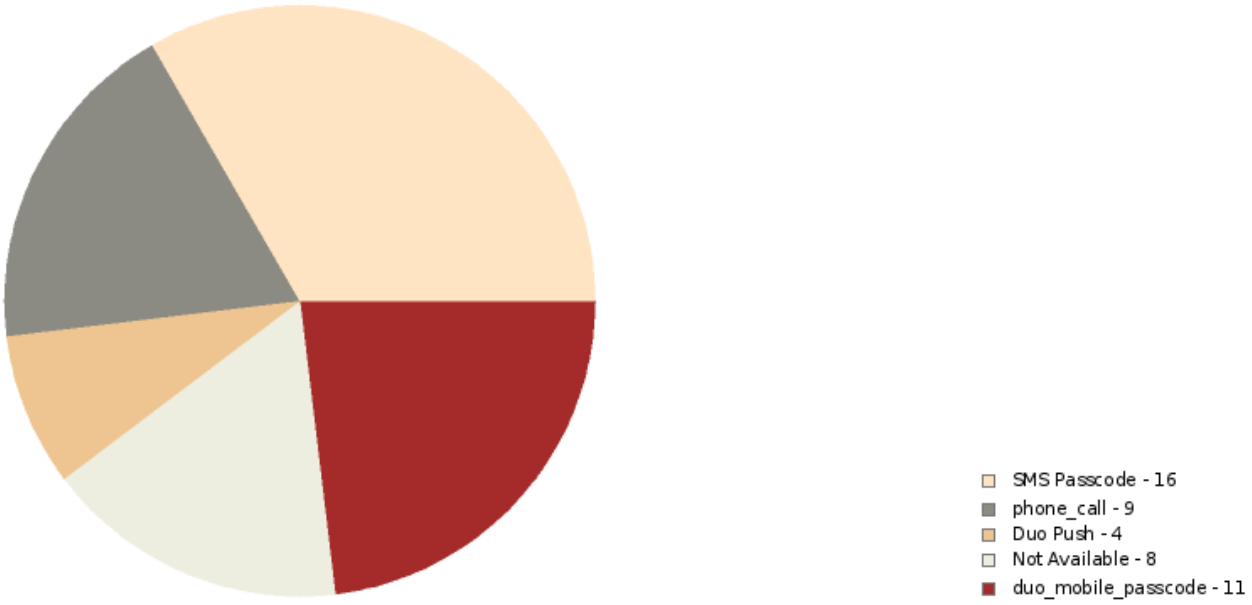
ASM-VP REPORT

Organo Judicial 07/26/2023

Successful Authentications *



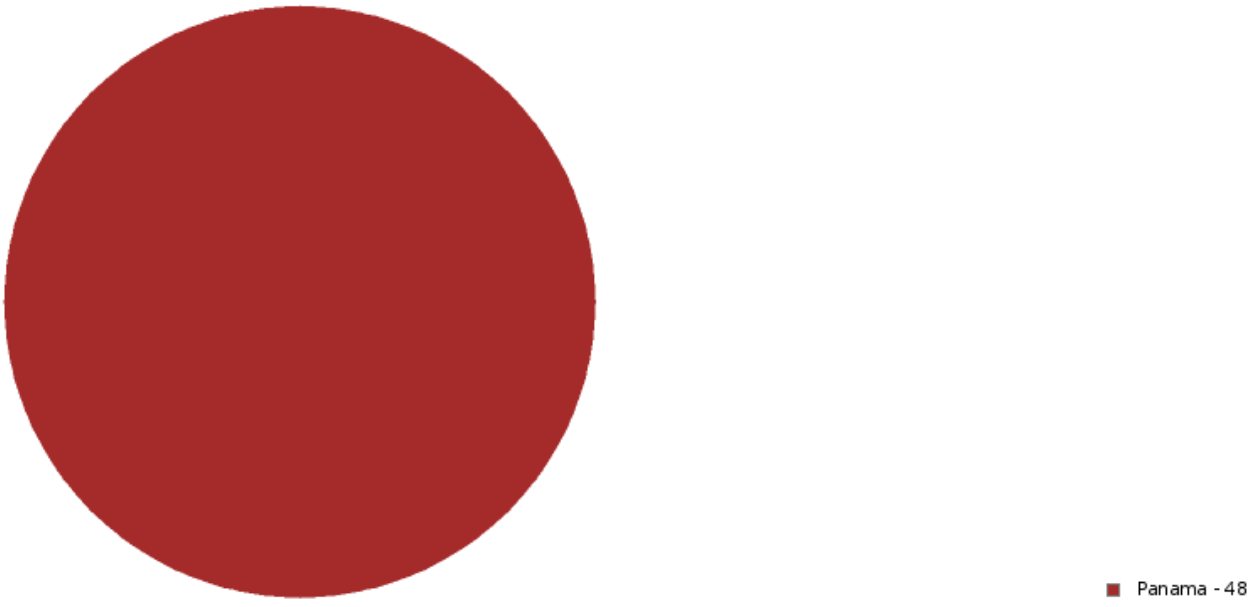
Successful Authentications by Factor *



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