TLP:AMBER

ASM-VP REPORT

ORGANO JUDICIAL

October 09, 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

8%

Discovered Hosts

13

Vulnerable Hosts

7

Executive Summary Vulnerability Severity Distribution

Scanner	Critical	High	Medium	Low	Total
Organo Judicial	2	2	11	1	16
Domain Scan: www.organojudicial.gob.pa	2	0	2	22	26

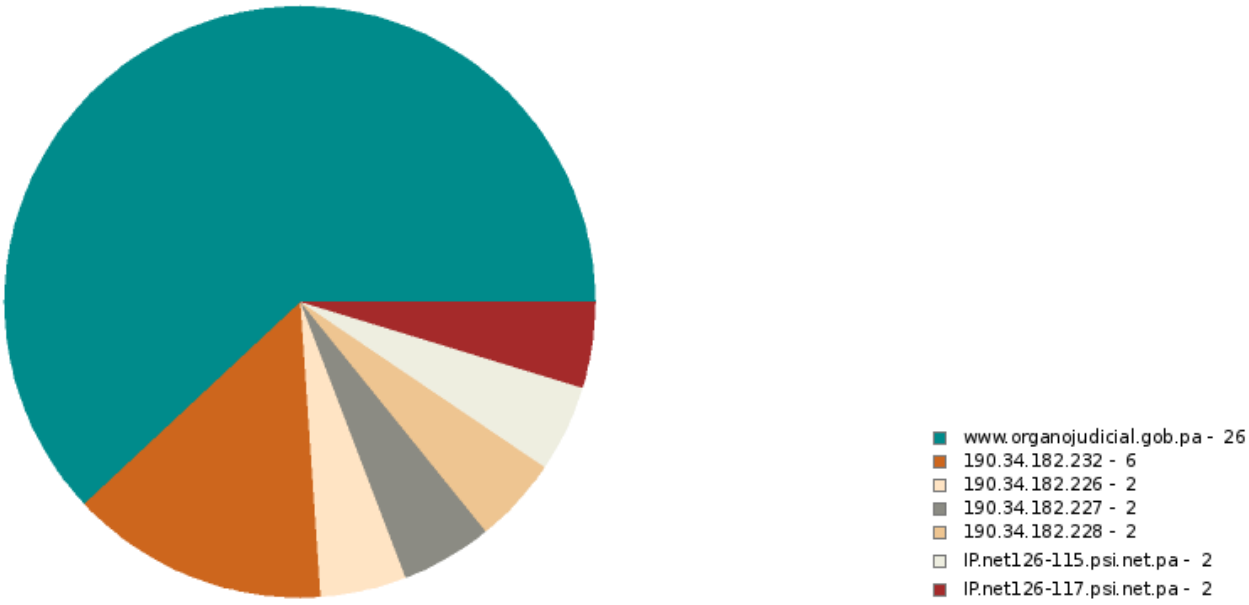
LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

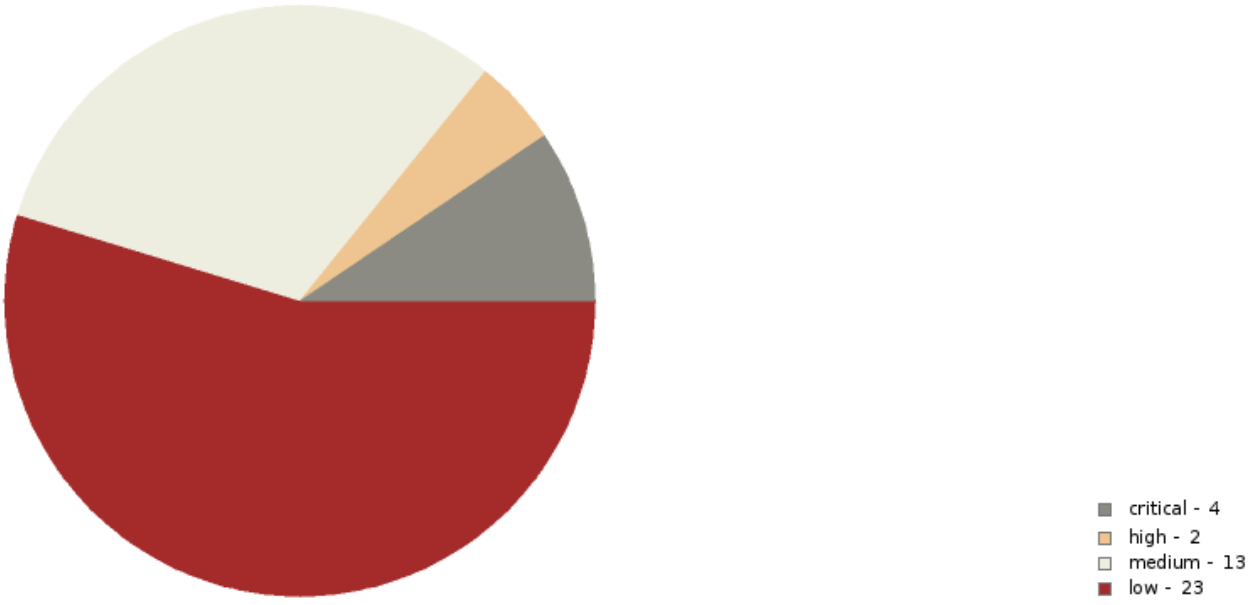
ASM-VP REPORT

Organo Judicial 10/09/2023

Most Vulnerable Host *



Vulnerability Distribution



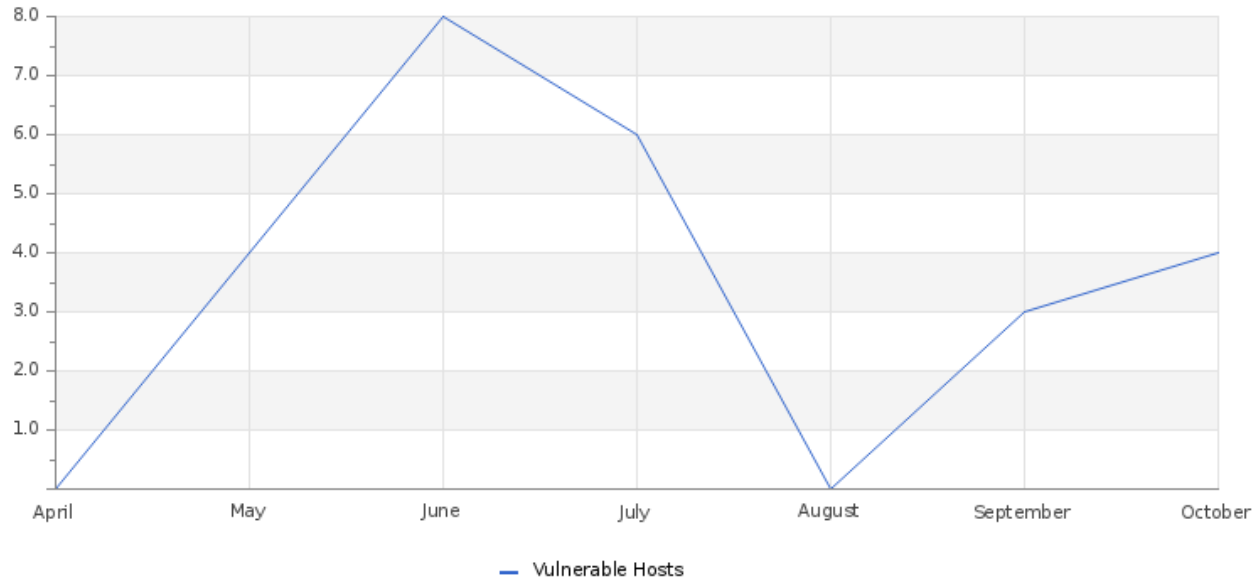
LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

Top 10 Most Common Vulnerabilities

Vulnerability
Client-side HTTP parameter pollution (reflected)
Open redirection (DOM-based)
TLS Version 1.00 Protocol Detection
TLS Version 1.10 Protocol Deprecated
Cookie without HttpOnly flag set
Cross-site scripting (reflected)
TLS cookie without secure flag set
Strict transport security not enforced
Vulnerable JavaScript dependency
CGI Generic SQL Injection Detection (potential, 2nd order, 2nd pass)

History

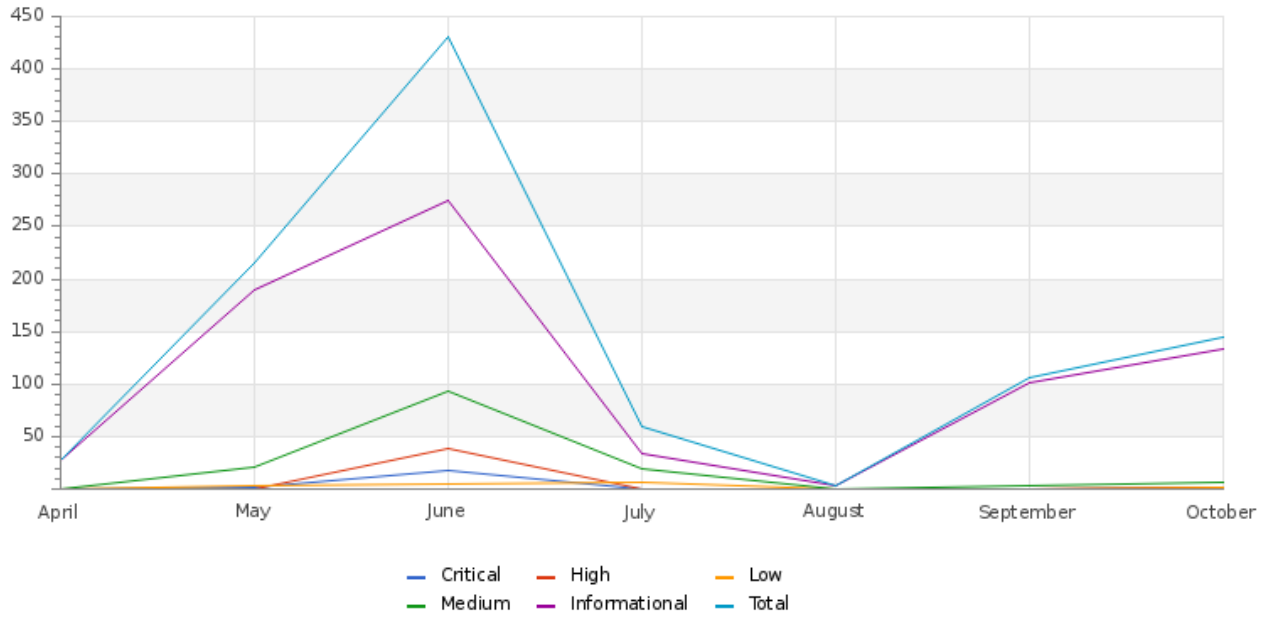
Vulnerable Host History



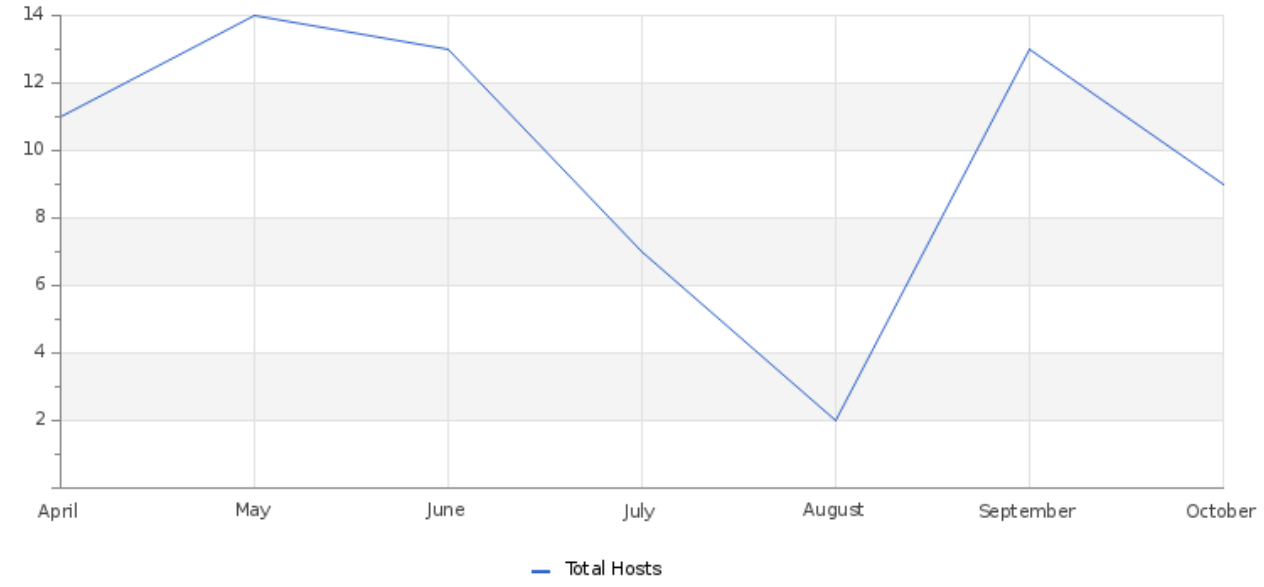
ASM-VP REPORT

Organo Judicial 10/09/2023

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
190.34.182.228	2	2
IP.net126-115.psi.net.pa	2	2

Open Port Monitoring

Open Ports

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
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
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
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

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

Vulnerability

MSS-BAS Email

Cymulate Score

1%

MSS-BAS Web

Cymulate Score

53%

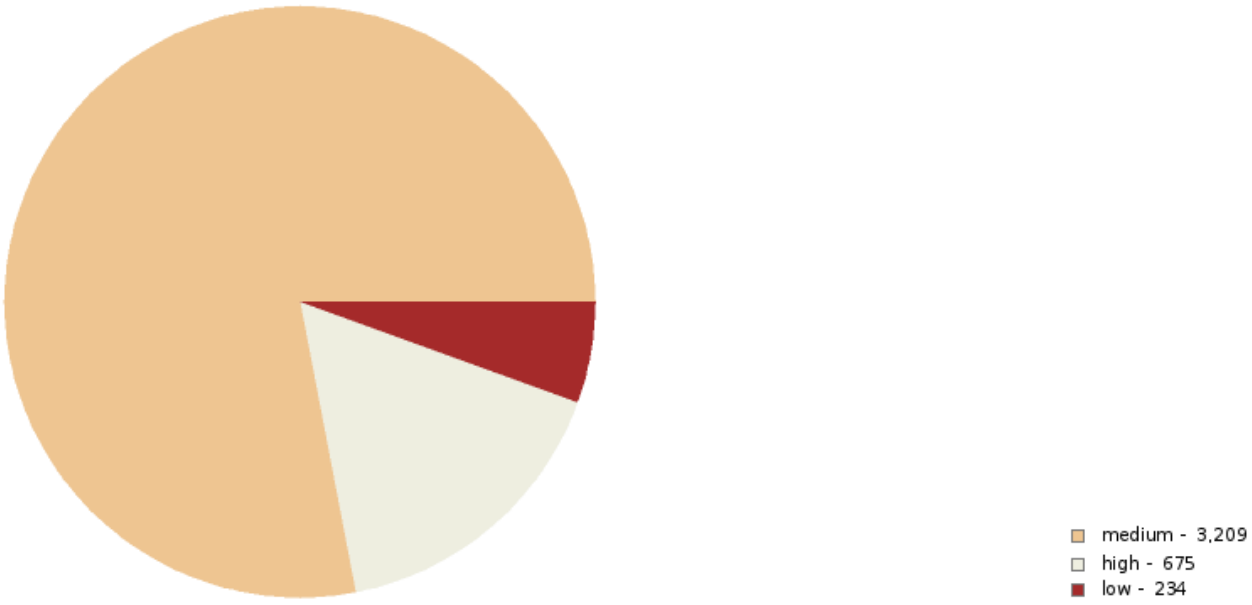
Simulation Summary

Penetrated : 5,439 / Total Tests: 23,316

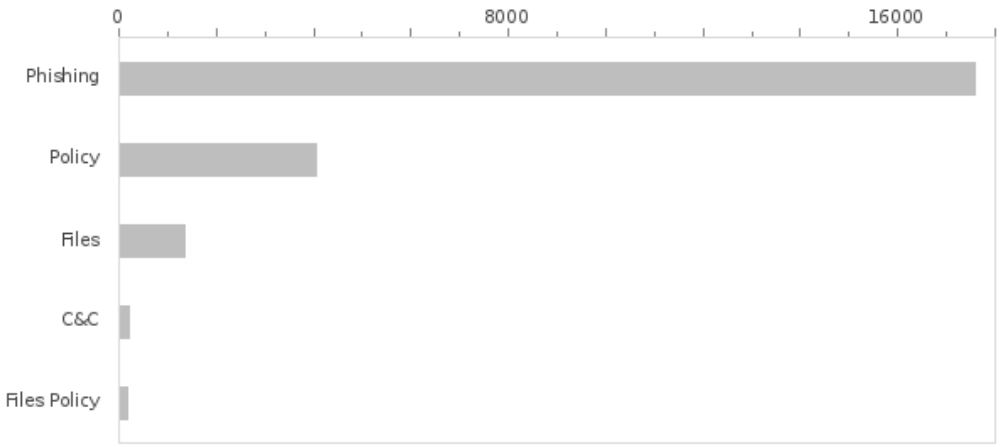
ASM-VP REPORT

Organo Judicial 10/09/2023

Penetrations by Severity



Browsing Sent

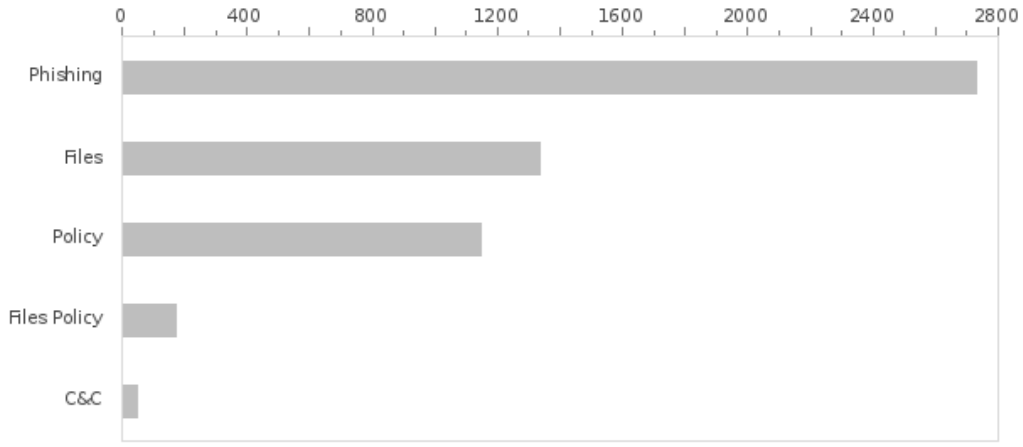


LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

ASM-VP REPORT

Organo Judicial 10/09/2023

Browsing Penetrated



Percent Penetrated

23%

Simulations Sent/Penetrated

Category	Penetrated	Total
Phishing	2,729	17,572
Policy	1,147	4,035
Files	1,338	1,338
C&C	51	197
Files Policy	174	174

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

Security Validation

MSS-BAS EDR

Cymulate Score

5%

Simulation Summary

Penetrated : 71 / Sent : 1,389

Ransomware based code execution

Penetrated : 1 / Total Tests: 343

Malware based execution

Not detected : 68 / Total: 898

Trojan based code execution

penetrated : 0 / Total tests : 50

Ransomware Scenarios blocked

99%

Malware Signatures blocked

92%

ASM-VP REPORT

Organo Judicial 10/09/2023

Trojan Scenarios blocked

100%

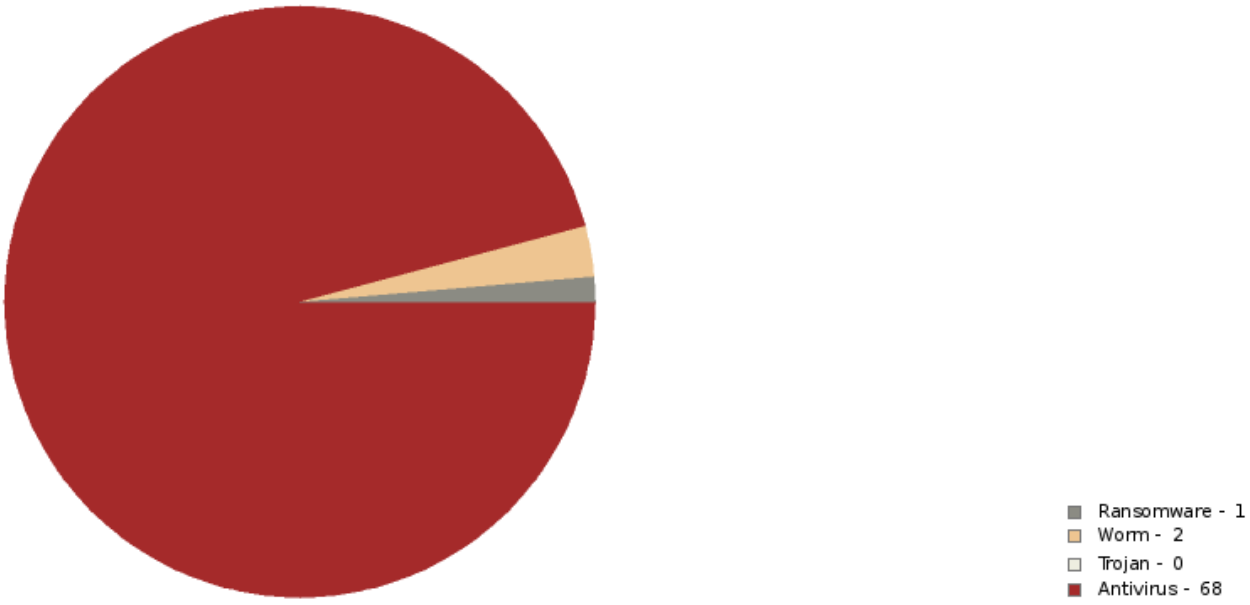
Worm based code execution

penetrated : 2 / Total tests : 98

Worm Scenarios blocked

98%

Distribution Of Attack Types Penetrated



Percent Penetrated

5%

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

TLP:AMBER

GLESEC
COMPLETELY PERCEPTI

ASM-VP REPORT

Organo Judicial 10/09/2023

Simulations Sent/Penetrated

Category	Penetrated	Total
Antivirus	68	898
Ransomware	1	343
Worm	2	98
Trojan	0	50

MSS-BAS IMTHREAT

Cymulate Score

46%

Percent Penetrated

51%

Simulation Summary

Penetrated: 258 / Total: 505

Immediate Threats Campaigns

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-10-08	India Cert Alert - NoEscape Ransomware	9d346518330eeefbf288aeca_edr7b2b6243bc158415c7fee3f2c19694f0e5f7d51cXxX6Exe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-10-08	India Cert Alert - NoEscape Ransomware	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ind ia_cert_alert_-_noescape_ransomware_af3c36c7-693e-49c7-b531-d7ff96f44142/16d9e96945_browsing7a76874e7452e687a7b6843c65ef75d1a4404d369074ad389f6c38XxX8Sh.sh?X-Am z-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20231008%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20231008T133029Z&X-Amz-Expires=600&X-Amz-Signature=2737602cc0b0deb936e4c72fcaac34233bfbb39d5b35900b5bd44c7fe3aad12e&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-10-08	India Cert Alert - NoEscape Ransomware	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ind ia_cert_alert_-_noescape_ransomware_af3c36c7-693e-49c7-b531-d7ff96f44142/aa5a48_browsing7db37ce176e17c7abbb2b1d460ba926344e46737f2f64b65bf5a4a3e58XxX7Sh.sh?X-Am z-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20231008%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20231008T133029Z&X-Amz-Expires=600&X-Amz-Signature=478f9bf7cdd561bd8f021665b970957d1bbc713b46de0e31fdae7c9fb948dfba&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 10/09/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-10-08	India Cert Alert - NoEscape Ransomware	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ind ia_cert_alert_-_noescape_ransomware_af3c36c7-693e-49c7-b531-d7ff96f44142/0_brows ing7c70968c66c93b6d6c9a90255e1c81a3b385632c83f53f69534b3f55212ced9XxX5Dll.dll?X- Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Crede ntial=AKIAJPJC2Q3D5GWFTK3Q%2F20231008%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date =20231008T133028Z&X-Amz-Expires=600&X-Amz-Signature=8ec92c187c18e0f3c52ec782ed6d b32897299150c50976704f990aedd14bb068&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-10-08	India Cert Alert - NoEscape Ransomware	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ind ia_cert_alert_-_noescape_ransomware_af3c36c7-693e-49c7-b531-d7ff96f44142/21162bb d_browsing796ad2bf9954265276bfebea8741596e8fe9d86070245d9b5f9db6daXxX4Elf.elf?X- Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Crede ntial=AKIAJPJC2Q3D5GWFTK3Q%2F20231008%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date =20231008T133021Z&X-Amz-Expires=600&X-Amz-Signature=427b8c7297ec705aee99288f65d1 d0dbf746aa85f6afb0f7798ab5977367045b&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-10-08	India Cert Alert - NoEscape Ransomware	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ind ia_cert_alert_-_noescape_ransomware_af3c36c7-693e-49c7-b531-d7ff96f44142/68ff985 5262b_browsing7a9c27e349c5e3bf68b2fc9f9ca32a9d2b844f2265dccd2bc0d8XxX3Exe.exe?X- Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Crede ntial=AKIAJPJC2Q3D5GWFTK3Q%2F20231008%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date =20231008T133019Z&X-Amz-Expires=600&X-Amz-Signature=1e4a37fbf4cbdc782fd7692038fb a46585625c4c704e8b46aebd57fd3aba4516&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-10-08	India Cert Alert - NoEscape Ransomware	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ind ia_cert_alert_-_noescape_ransomware_af3c36c7-693e-49c7-b531-d7ff96f44142/68e5caa 3f0fd4adc595b1163bf0dd30ca621c5d_browsing7a6ad0a20dfa1968346daa3c8XxX1Dll.dll?X- Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Crede ntial=AKIAJPJC2Q3D5GWFTK3Q%2F20231008%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date =20231008T133014Z&X-Amz-Expires=600&X-Amz-Signature=a06086c82010772b788ac3962857 47b071595bb9c5327368c8105755c2f92418&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-10-08	RedLine Stealer A new variant surfaces Deploying using Batch Script	19_edr7b50f15375335928e08c5cc5b6f50cd93864655237b8db85556d4057f3b988XxX226Exe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-10-08	RedLine Stealer A new variant surfaces Deploying using Batch Script	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/red line_stealer_a_new_variant_surfaces_deploying_using_batch_script_5d22d50f-f2d1-4 f00-b9e5-11cbdf78f5ab/e0f0449aae4dc11_browsing7e34517e8c83fd49faf2b379dc4f2fd35f f291dd5003864e2XxX232Zip.zip?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha2 56=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20231008%2Feu-west-1 %2Fs3%2Faws4_request&X-Amz-Date=20231008T102637Z&X-Amz-Expires=600&X-Amz-Signatu re=dc65fe3b9ded92273d3c225e162bc8b226babe09707bdb8dbffc8962ec5ce077&X-Amz-Signed Headers=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-10-08	RedLine Stealer A new variant surfaces Deploying using Batch Script	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/red line_stealer_a_new_variant_surfaces_deploying_using_batch_script_5d22d50f-f2d1-4 f00-b9e5-11cbdf78f5ab/83db86d_browsing7872e467513f186adcc02f5408e50b6a3d3aa14cbf 7dd5d1fb6affb34XxX227Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha2 56=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20231008%2Feu-west-1 %2Fs3%2Faws4_request&X-Amz-Date=20231008T102635Z&X-Amz-Expires=600&X-Amz-Signatu re=5a79d71112e13219a16c1722a29ad37e12d267c11ace1dcf8debc19f1b34da86&X-Amz-Signed Headers=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-10-05	Energy Industry Targeted With GuLoader	hxxp://91.234.99.51	Web Gateway	88E1000GMSYS	Offline/Removed
2023-10-05	Energy Industry Targeted With GuLoader	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ene rgy_industry_targeted_with_guloader_9b1a41ef-e5d9-4519-b4e4-ed0da20a8605/0c86253 01_browsing7d45f1cf09b474135ab9a603584f4c6d1d8d22b9cbce7be46dfb019XxX41Exe.exe?X - Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Cred ential=AKIAJPJC2Q3D5GWFTK3Q%2F20231005%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Dat e=20231005T065625Z&X-Amz-Expires=600&X-Amz-Signature=9f29a27a1734ba78299505fc354 f09d11ca04f145b04d50c317ae8a7949f3b92&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-10-05	Energy Industry Targeted With GuLoader	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ene rgy_industry_targeted_with_guloader_9b1a41ef-e5d9-4519-b4e4-ed0da20a8605/50f_bro wsing7d8503f51e02f52c3f666ad902900b2b90809df612c96e88cd51466416c0bXxX39Rtf.rtf?X -Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Cred ential=AKIAJPJC2Q3D5GWFTK3Q%2F20231005%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Dat e=20231005T065624Z&X-Amz-Expires=600&X-Amz-Signature=28a0ef34173dd3cc2fd7651df47 81ebff1e65d42f83b265d58dd2fefc86ad1a7&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-10-05	Energy Industry Targeted With GuLoader	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ene rgy_industry_targeted_with_guloader_9b1a41ef-e5d9-4519-b4e4-ed0da20a8605/ec5be_b rowsing7c50c187de9346e381fe229eb22a3383dfd70bbac3568051af0ee25016cXxX37Exe.exe?X - Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Cred ential=AKIAJPJC2Q3D5GWFTK3Q%2F20231005%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Dat e=20231005T065623Z&X-Amz-Expires=600&X-Amz-Signature=62011c14e2fa98148f511c5ab42 88706b16accfbb29a54f918b77f1c07399461&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-10-05	Typosquatting Campaign Delivers r77 Rootkit via npm	2e28a2fa3904b5b1014e93ab8812_edr74a9df5f8355fbab4b4424923f65ae4577dXxX2Exe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-10-05	Typosquatting Campaign Delivers r77 Rootkit via npm	82bfffb12f0094e01824df2b4c28e1_edr72b6486cf006cd52af83a7cb4f524cd56eXxX3Exe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-10-04	Ransomware attack to IFX Colombia	8,189c_edr708706eb7302d7598aeee8cd6bdb048bf1a6dbe29c59e50f0a39fd53973XxX2Elf.elf	Endpoint Security	88E1000GMSYS	Blocked

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

TLP:AMBER

GLESEC
COMPLETELY PERCEPTI

ASM-VP REPORT

Organo Judicial 10/09/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-10-04	Ransomware attack to IFX Colombia	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ransomware_attack_to_ifx_colombia_12485343-33f2-4a3a-bff4-ca464ec53084/bfc9b956818efe008c2dbf621244b6dc3de8319e89b9fa83c9e412ce_browsing70f82f2cXxX1Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20231004%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20231004T120356Z&X-Amz-Expires=600&X-Amz-Signature=2e44639d0c01a8efe53b5ba08323d91c157269794cdcb747787a510c5b87b9d5&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-10-04	A cryptor a stealer and a banking trojan	f65ba83c6db36_edr72614119dca0ea2b948100f2d984e642c674a84d9d3498481cfXxX2Exe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-10-04	A cryptor a stealer and a banking trojan	7,823_edr7d50938445902a3789f5fa35a4a32ebd313a7411748caaadaa093e8fef01XxX13Zip.zip	Endpoint Security	88E1000GMSYS	Penetrated
2023-10-04	A cryptor a stealer and a banking trojan	df_edr7dcf326ecce83b70b303a705acf70fd49022f076af463b6d805c47e741dae5XxX16Zip.zip	Endpoint Security	88E1000GMSYS	Penetrated
2023-10-04	A cryptor a stealer and a banking trojan	ecaa162123144551c1d3a9ffcba450aee141b5ac91ca992c14c38cff46_edr7563a1XxX14Zip.zip	Endpoint Security	88E1000GMSYS	Penetrated
2023-10-04	A cryptor a stealer and a banking trojan	1e9bbfa21c6482b9a3c63aa4b31ea408_edr7b971465225297596a1cb717d14f53f4XxX12Zip.zip	Endpoint Security	88E1000GMSYS	Penetrated
2023-10-04	A cryptor a stealer and a banking trojan	78_edr73dddec4a46e7ad104de9b6bd68f590575b7680a1d20b9fe1329d1ad95348fXxX3Exe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-10-04	A cryptor a stealer and a banking trojan	9b_edr742a890aff9c7a2b54b620fe5e1fcfa553648695d79c892564de09b850c92bXxX6Exe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-10-04	A cryptor a stealer and a banking trojan	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/a_cryptor_a_stealer_and_a_banking_trojan_672d5337-a358-4402-8a0f-303abe671523/c65381edfb8c208a_browsing7a84d7930f449dfb2aa2b3cf99124e8dc5f614188c025c5bXxX20Exe.exe ?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20231004%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20231004T073146Z&X-Amz-Expires=600&X-Amz-Signature=826078d85c8633456528146af0a632400499782 72d5d31a26e2f737c259ee8b4&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-10-04	A cryptor a stealer and a banking trojan	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/a_cryptor_a_stealer_and_a_banking_trojan_672d5337-a358-4402-8a0f-303abe671523/ed8e1c8f1e2b91d2a321d0a6ff3c45_browsing7dc6acbf63eb856cdadcea7d3a3368217bXxX19Exe.exe ?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20231004%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20231004T073144Z&X-Amz-Expires=600&X-Amz-Signature=bb1d5794e7bf2382697eea233ed6f78499619de2e04256c0502eaa2606fc2d81&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-10-04	A cryptor a stealer and a banking trojan	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/a_cryptor_a_stealer_and_a_banking_trojan_672d5337-a358-4402-8a0f-303abe671523/fccbb81ad665cc1dc5b5de_browsing77d3bbc9516fca5acfa7031f4d0b56b691deef4c01XxX18Zip.zip ?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20231004%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20231004T073133Z&X-Amz-Expires=600&X-Amz-Signature=2103619a161074c6ad1e2a878d48e976a9587c97cba8e1d1f787470a1b4327f9&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-10-04	A cryptor a stealer and a banking trojan	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/a_cryptor_a_stealer_and_a_banking_trojan_672d5337-a358-4402-8a0f-303abe671523/c15eafbe8ed2fd_browsing7db38a8771d56541a7c17c632c41bab85de2176ce630eae591XxX17Zip.zip ?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20231004%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20231004T073124Z&X-Amz-Expires=600&X-Amz-Signature=9a10e9aef9bcd3f0ccb07f3e26c39eda44139c0e575b6ad95564d331a7063c27&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-10-04	A cryptor a stealer and a banking trojan	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/a_cryptor_a_stealer_and_a_banking_trojan_672d5337-a358-4402-8a0f-303abe671523/80863bcd05413ab49db2005390121e6852_browsing70b487d275bfe76b3893f89f402aa9XxX15Zip.zip ?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20231004%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20231004T073119Z&X-Amz-Expires=600&X-Amz-Signature=c2529aad28b286151eecf662d7d40c2dce58d261b4094d472184d24032cbb6af&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-10-04	A cryptor a stealer and a banking trojan	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/a_cryptor_a_stealer_and_a_banking_trojan_672d5337-a358-4402-8a0f-303abe671523/6024_browsing7d4ddd08204818b60ade4bfc32d6c31756c574a5fe2cd521381385a0f868XxX7Exe.exe? X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20231004%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20231004T073109Z&X-Amz-Expires=600&X-Amz-Signature=4fa06d65da636a167af5e01b5e1dc14f3115045324b4cbca26cfca798e61ceee&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-10-04	Cyberespionage Events Targeting Southeast Asian Government Linked To Stately Taurus aka Mustang Panda	b000a0095a8fda3822_edr7103f253b6d79134b862a83df50315d7d9c5b537fd994bXxX79Exe.exe	Endpoint Security	88E1000GMSYS	Penetrated
2023-10-04	Cyberespionage Events Targeting Southeast Asian Government Linked To Stately Taurus aka Mustang Panda	12,534f_edr7014b3338d8f9f86ff1bbeacf8c80ad03f1d0d19077ff0e406c58b5133XxX81Exe.exe	Endpoint Security	88E1000GMSYS	Blocked

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

TLP:AMBER

ASM-VP REPORT

Organo Judicial 10/09/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-10-04	Cyberespionage Events Targeting Southeast Asian Government Linked To Stately Taurus aka Mustang Panda	31eb1de_edr7e840a342fd468e558e5ab627bcb4c542a8fe01aec4d5ba01d539a0fcXxX83Exe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-10-04	Cyberespionage Events Targeting Southeast Asian Government Linked To Stately Taurus aka Mustang Panda	4a8b_edr7cfb2e33aa079ba51166591c7a210ad8b3c7c7f242fccf8cb2e71e8e40d5XxX69Exe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-10-04	Cyberespionage Events Targeting Southeast Asian Government Linked To Stately Taurus aka Mustang Panda	66b_edr7983831cbb952ceeb1ffff608880f1805f1df0b062cef4c17b258b7f478ceXxX85Dll.dll	Endpoint Security	88E1000GMSYS	Blocked
2023-10-04	Cyberespionage Events Targeting Southeast Asian Government Linked To Stately Taurus aka Mustang Panda	hxxp://207.246.89.250	Web Gateway	88E1000GMSYS	Offline/Removed
2023-10-04	Cyberespionage Events Targeting Southeast Asian Government Linked To Stately Taurus aka Mustang Panda	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/cyberespionage_events_targeting_southeast_asian_government_linked_to_stately_taurus_aka_mustang_panda_6ca18d24-7f85-466a-b6f5-7d3b21b5e34d/8129bd45466c26_browsing76b248c08bb0efcd9ccc8b684abf3435e290fcf4739c0a439fXxX77Dll.dll?X-Amz-Algorithm=AW S4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20231004%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20231004T072457Z&X-Amz-Expires=600&X-Amz-Signature=9323dde2e978834989186acfa846bd9b1bd9016c4853e3c1827fe8cd788b9741&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-10-04	Cyberespionage Events Targeting Southeast Asian Government Linked To Stately Taurus aka Mustang Panda	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/cyberespionage_events_targeting_southeast_asian_government_linked_to_stately_taurus_aka_mustang_panda_6ca18d24-7f85-466a-b6f5-7d3b21b5e34d/18_browsing74b20e3e802406c594341699c5863a2c07c4c79cf762888ee28142af83547fXxX73Dll.dll?X-Amz-Algorithm=AW S4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20231004%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20231004T072457Z&X-Amz-Expires=600&X-Amz-Signature=b11fe0a3a12658bc22d0014afe1248ae9fb8c68d798cc9f5a07ec3d618295020&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-10-04	Cyberespionage Events Targeting Southeast Asian Government Linked To Stately Taurus aka Mustang Panda	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/cyberespionage_events_targeting_southeast_asian_government_linked_to_stately_taurus_aka_mustang_panda_6ca18d24-7f85-466a-b6f5-7d3b21b5e34d/3c2fe308c0a563e06263bbacf_browsing793bbe9b2259d795fcc36b953793a7e499e7f71XxX71Exe.exe?X-Amz-Algorithm=AW S4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20231004%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20231004T072457Z&X-Amz-Expires=600&X-Amz-Signature=c88fb3072bf9e252de06909d781efad27a9b182a469c1eb037c063f83c1073ed&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-10-04	Cyberespionage Events Targeting Southeast Asian Government Linked To Stately Taurus aka Mustang Panda	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/cyberespionage_events_targeting_southeast_asian_government_linked_to_stately_taurus_aka_mustang_panda_6ca18d24-7f85-466a-b6f5-7d3b21b5e34d/64ab1c1b19682026900d060b969ab3c3ab860988_browsing733b7e7bf3ba78a4ea0340b9XxX67Exe.exe?X-Amz-Algorithm=AW S4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20231004%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20231004T072455Z&X-Amz-Expires=600&X-Amz-Signature=f2ac1bb51e8d0c5c9859204ad3f751a45e54cc5e718307bbe4f4ec2425f1db6c&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-10-04	Cyberespionage Events Targeting Southeast Asian Government Linked To Stately Taurus aka Mustang Panda	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/cyberespionage_events_targeting_southeast_asian_government_linked_to_stately_taurus_aka_mustang_panda_6ca18d24-7f85-466a-b6f5-7d3b21b5e34d/011fe99_browsing74f07cb12ba30e69e7a84e5cb489ce14a81bced59a11031fc0c3681b7XxX65Dll.dll?X-Amz-Algorithm=AW S4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20231004%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20231004T072453Z&X-Amz-Expires=600&X-Amz-Signature=29b81fe2685f1701befed5fe50d24ce7ec22df6378ccd1b38fe3cd27ebbb802d&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-10-04	Cyberespionage Events Targeting Southeast Asian Government Linked To Stately Taurus aka Mustang Panda	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/cyberespionage_events_targeting_southeast_asian_government_linked_to_stately_taurus_aka_mustang_panda_6ca18d24-7f85-466a-b6f5-7d3b21b5e34d/8445aa54adf4d666e65084909a_browsing7b989a190ec6eca2844546c2e99a8cfb832fadXxX63Exe.exe?X-Amz-Algorithm=AW S4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20231004%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20231004T072445Z&X-Amz-Expires=600&X-Amz-Signature=1e48fc08ea5a177521b894aea0cd90a4fb74e15bc55bfa8df9cb172403227e74&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-10-03	Vulnerable Openfire Messaging Servers Under Attack CVE-2023-32315	5d2530b809fd069f9_edr7b30a5938d471dd2145341b5793a70656aad6045445cf6dXxX7Elf.elf	Endpoint Security	88E1000GMSYS	Blocked
2023-10-03	Vulnerable Openfire Messaging Servers Under Attack CVE-2023-32315	a3f_edr72a73e146834b43dab8833e0a9cfee6d08843a4c23fdf425295e53517afceXxX9Elf.elf	Endpoint Security	88E1000GMSYS	Blocked

TLP:AMBER

GLESEC
COMPLETELY PERCEPTI

ASM-VP REPORT

Organo Judicial 10/09/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-10-03	Vulnerable Openfire Messaging Servers Under Attack CVE-2023-32315	hxxp://185.17.0.226	Web Gateway	88E1000GMSYS	Blocked
2023-10-03	Vulnerable Openfire Messaging Servers Under Attack CVE-2023-32315	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/vulnerable_openfire_messaging_servers_under_attack_cve-2023-32315_5cd8affb-c4fb-4521-a16f-085aa726470b/5aba6a_browsing705e3c0cdaee966b5cd940cca0f97acb632ffd4f25ab805c69a3d9e352XxX5Jar.jar?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20231003%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20231003T094743Z&X-Amz-Expires=600&X-Amz-Signature=50423024ab966dd32b4ba86528daa3f806036beb7cd595f256fbce7e491c8061&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-10-03	Vulnerable Openfire Messaging Servers Under Attack CVE-2023-32315	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/vulnerable_openfire_messaging_servers_under_attack_cve-2023-32315_5cd8affb-c4fb-4521-a16f-085aa726470b/ee_browsing7c12fc58ca5d79e549f411ee1021a0980b396af6417e6445102117cdf600baXxX3Jar.jar?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20231003%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20231003T094742Z&X-Amz-Expires=600&X-Amz-Signature=a959cfbb82ff9720c8a15faa8d5572f935c1e63b7570506042e3bc8fe252185e&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-10-03	Vulnerable Openfire Messaging Servers Under Attack CVE-2023-32315	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/vulnerable_openfire_messaging_servers_under_attack_cve-2023-32315_5cd8affb-c4fb-4521-a16f-085aa726470b/48a88aef82d96cc2209cdba8b93662df5a2b6a_browsing7c609dd76667993cd06c337867XxX1Jar.jar?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20231003%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20231003T094742Z&X-Amz-Expires=600&X-Amz-Signature=c79354ce3d2e40c746289a7f6cd0c42bbabd5b3eda0e3106d5bece9e141f3cb8&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-10-08	India Cert Alert - NoEscape Ransomware	68e5caa3f0fd4adc595b1163bf0dd30ca621c5d_edr7a6ad0a20dfa1968346daa3c8XxX1Dll.dll	Endpoint Security	88E1000GMSYS	Blocked
2023-10-08	India Cert Alert - NoEscape Ransomware	68ff9855262b_edr7a9c27e349c5e3bf68b2fc9f9ca32a9d2b844f2265dccd2bc0d8XxX3Exe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-10-08	India Cert Alert - NoEscape Ransomware	0_edr7c70968c66c93b6d6c9a90255e1c81a3b385632c83f53f69534b3f55212ced9XxX5Dll.dll	Endpoint Security	88E1000GMSYS	Blocked
2023-10-08	India Cert Alert - NoEscape Ransomware	21,162bbd_edr796ad2bf9954265276bfebea8741596e8fe9d86070245d9b5f9db6daXxX4Elf.elf	Endpoint Security	88E1000GMSYS	Blocked
2023-10-08	India Cert Alert - NoEscape Ransomware	16d9e96945_edr7a76874e7452e687a7b6843c65ef75d1a4404d369074ad389f6c38XxX8Sh.sh	Endpoint Security	88E1000GMSYS	Blocked
2023-10-08	India Cert Alert - NoEscape Ransomware	aa5a48_edr7db37ce176e17c7abbb2b1d460ba926344e46737f2f64b65bf5a4a3e58XxX7Sh.sh	Endpoint Security	88E1000GMSYS	Blocked
2023-10-08	India Cert Alert - NoEscape Ransomware	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ind ia_cert_alert_-_noescape_ransomware_af3c36c7-693e-49c7-b531-d7ff96f44142/9d346518330eeefbf288aeca_browsing7b2b6243bc158415c7fee3f2c19694f0e5f7d51cXxX6Exe.exe?X- Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20231008%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20231008T133028Z&X-Amz-Expires=600&X-Amz-Signature=6227579bff5ce8296e5420cf0519586d86e8a5beb2783cf9a4b333bcf0355cc9&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-10-08	RedLine Stealer A new variant surfaces Deploying using Batch Script	e0f0449aae4dc11_edr7e34517e8c83fd49faf2b379dc4f2fd35ff291dd5003864e2XxX232Zip.zi p	Endpoint Security	88E1000GMSYS	Penetrated
2023-10-08	RedLine Stealer A new variant surfaces Deploying using Batch Script	83db86d_edr7872e467513f186adcc02f5408e50b6a3d3aa14cbf7dd5d1fb6affb34XxX227Exe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-10-08	RedLine Stealer A new variant surfaces Deploying using Batch Script	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/redline_stealer_a_new_variant_surfaces_deploying_using_batch_script_5d22d50f-f2d1-4f00-b9e5-11cbdf78f5ab/19_browsing7b50f15375335928e08c5cc5b6f50cd93864655237b8db85556d4057f3b988XxX226Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20231008%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20231008T102632Z&X-Amz-Expires=600&X-Amz-Signature=a3afbd127c4aab5889aad16e49fe6eed75c23b8ec2ed2453e3cc8ba0fe10e08e&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-10-05	Energy Industry Targeted With GuLoader	ec5be_edr7c50c187de9346e381fe229eb22a3383dfd70bbac3568051af0ee25016cXxX37Exe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-10-05	Energy Industry Targeted With GuLoader	0c8625301_edr7d45f1cf09b474135ab9a603584f4c6d1d8d22b9cbce7be46dfb019XxX41Exe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-10-05	Energy Industry Targeted With GuLoader	50f_edr7d8503f51e02f52c3f666ad902900b2b90809df612c96e88cd51466416c0bXxX39Rtf.rtf	Endpoint Security	88E1000GMSYS	Blocked

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

TLP:AMBER

GLESEC
COMPLETELY PERCEPTI

ASM-VP REPORT

Organo Judicial 10/09/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-10-05	Typosquatting Campaign Delivers r77 Rootkit via npm	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/typosquatting_campaign_delivers_r77_rootkit_via_npm_1fc52882-70d7-446b-87c1-7fd4633ad014/82bfffb12f0094e01824df2b4c28e1_browsing72b6486cf006cd52af83a7cb4f524cd56eXxX3Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20231005%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20231005T065355Z&X-Amz-Expires=600&X-Amz-Signature=2a6f4b58dcd2102dfc9859d6d1b144e464a59b89051d0b3cfe895ab0161b14ce&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-10-05	Typosquatting Campaign Delivers r77 Rootkit via npm	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/typosquatting_campaign_delivers_r77_rootkit_via_npm_1fc52882-70d7-446b-87c1-7fd4633ad014/02e28a2fa3904b5b1014e93ab8812_browsing74a9df5f8355fbab4b4424923f65ae4577dXxX2Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20231005%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20231005T065352Z&X-Amz-Expires=600&X-Amz-Signature=861551f5bdd7d1a9a2911094f22242d22e01603240b8eefa1710094da55ddcb9&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-10-04	Ransomware attack to IFX Colombia	bfc9b956818efe008c2dbf621244b6dc3de8319e89b9fa83c9e412ce_edr70f82f2cXxX1Exe.exe	Endpoint Security	88E1000GMSYS	Penetrated
2023-10-04	Ransomware attack to IFX Colombia	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ransomware_attack_to_ifx_colombia_12485343-33f2-4a3a-bff4-ca464ec53084/8189c_browsing708706eb7302d7598aeee8cd6bdb048bf1a6dbe29c59e50f0a39fd53973XxX2Elf.elf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20231004%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20231004T120400Z&X-Amz-Expires=600&X-Amz-Signature=0afb9c50ca73f1942c199043fb0fe213712797961960644b66b4f0988e9f87a4&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-10-04	A cryptor a stealer and a banking trojan	c15eafbe8ed2fd_edr7db38a8771d56541a7c17c632c41bab85de2176ce630eae591XxX17Zip.zip	Endpoint Security	88E1000GMSYS	Penetrated
2023-10-04	A cryptor a stealer and a banking trojan	fccbb81ad665cc1dc5b5de_edr77d3bbc9516fca5acfa7031f4d0b56b691deef4c01XxX18Zip.zip	Endpoint Security	88E1000GMSYS	Penetrated
2023-10-04	A cryptor a stealer and a banking trojan	80,863bcd05413ab49db2005390121e6852_edr70b487d275bfe76b3893f89f402aa9XxX15Zip.zip	Endpoint Security	88E1000GMSYS	Penetrated
2023-10-04	A cryptor a stealer and a banking trojan	c65381edfb8c208a_edr7a84d7930f449dfb2aa2b3cf99124e8dc5f614188c025c5bXxX20Exe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-10-04	A cryptor a stealer and a banking trojan	ed8e1c8f1e2b91d2a321d0a6ff3c45_edr7dc6acbf63eb856cdadcea7d3a3368217bXxX19Exe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-10-04	A cryptor a stealer and a banking trojan	6,024_edr7d4ddd08204818b60ade4bfc32d6c31756c574a5fe2cd521381385a0f868XxX7Exe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-10-04	A cryptor a stealer and a banking trojan	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/a_cryptor_a_stealer_and_a_banking_trojan_672d5337-a358-4402-8a0f-303abe671523/df_browsing7dcf326ecce83b70b303a705acf70fd49022f076af463b6d805c47e741dae5XxX16Zip.zip ?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20231004%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20231004T073121Z&X-Amz-Expires=600&X-Amz-Signature=3907f82d65e47254a5689cb2c8a21ca971f6b1a0fc7852911da84e1d6dc21c78&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-10-04	A cryptor a stealer and a banking trojan	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/a_cryptor_a_stealer_and_a_banking_trojan_672d5337-a358-4402-8a0f-303abe671523/ecaa162123144551c1d3a9ffcba450aee141b5ac91ca992c14c38cff46_browsing7563a1XxX14Zip.zip ?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20231004%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20231004T073115Z&X-Amz-Expires=600&X-Amz-Signature=3a0b977190701 30fafa5530569bc3e87cb6d382a7e3a3f8c0bf9ae763198ac50&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-10-04	A cryptor a stealer and a banking trojan	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/a_cryptor_a_stealer_and_a_banking_trojan_672d5337-a358-4402-8a0f-303abe671523/7823_browsing7d50938445902a3789f5fa35a4a32ebd313a7411748caaadaa093e8fef01XxX13Zip.zip ?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20231004%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20231004T073113Z&X-Amz-Expires=600&X-Amz-Signature=0939edd4b3f92f27b14e439cae5a3a561b2ae6afe9e0765494832d5be8863de9&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-10-04	A cryptor a stealer and a banking trojan	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/a_cryptor_a_stealer_and_a_banking_trojan_672d5337-a358-4402-8a0f-303abe671523/1e9bbfa21c6482b9a3c63aa4b31ea408_browsing7b971465225297596a1cb717d14f53f4XxX12Zip.zip ?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20231004%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20231004T073109Z&X-Amz-Expires=600&X-Amz-Signature=354dd802aa110d8e23722c66bb00db2f3e0bd03f3c48a8700c1603b7d85a956a&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-10-04	A cryptor a stealer and a banking trojan	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/a_cryptor_a_stealer_and_a_banking_trojan_672d5337-a358-4402-8a0f-303abe671523/9b_browsing742a890aff9c7a2b54b620fe5e1fcfa553648695d79c892564de09b850c92bXxX6Exe.exe? X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20231004%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20231004T073108Z&X-Amz-Expires=600&X-Amz-Signature=557b249bf8d5b5f51d01c354debc3e762ce0b9ca83f30da8c4510d516b664f83&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-10-04	A cryptor a stealer and a banking trojan	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/a_cryptor_a_stealer_and_a_banking_trojan_672d5337-a358-4402-8a0f-303abe671523/78_browsing73dddec4a46e7ad104de9b6bd68f590575b7680a1d20b9fe1329d1ad95348fXxX3Exe.exe? X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20231004%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20231004T073101Z&X-Amz-Expires=600&X-Amz-Signature=274ad390ff9948881d693b4137e0aff05e8d0f6fd4d64fc42f97b38a00f8d106&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated

TLP:AMBER

GLESEC
COMPLETELY PERCEPTI

ASM-VP REPORT

Organo Judicial 10/09/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-10-04	A cryptor a stealer and a banking trojan	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/a_cryptor_a_stealer_and_a_banking_trojan_672d5337-a358-4402-8a0f-303abe671523/f65ba83c6db36_browsing72614119dca0ea2b948100f2d984e642c674a84d9d3498481cfXxX2Exe.exe? X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20231004%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20231004T073058Z&X-Amz-Expires=600&X-Amz-Signature=62b8780e3ca597cebec1b16eabc24cdf0f78617a01ec7d8e87f9e47990a0b7ae&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-10-04	Cyberespionage Events Targeting Southeast Asian Government Linked To Stately Taurus aka Mustang Panda	8,445aa54adf4d666e65084909a_edr7b989a190ec6eca2844546c2e99a8cfb832fadXxX63Exe.exe	Endpoint Security	88E1000GMSYS	Penetrated
2023-10-04	Cyberespionage Events Targeting Southeast Asian Government Linked To Stately Taurus aka Mustang Panda	64ab1c1b19682026900d060b969ab3c3ab860988_edr733b7e7bf3ba78a4ea0340b9XxX67Exe.exe	Endpoint Security	88E1000GMSYS	Penetrated
2023-10-04	Cyberespionage Events Targeting Southeast Asian Government Linked To Stately Taurus aka Mustang Panda	3c2fe308c0a563e06263bbacf_edr793bbe9b2259d795fcc36b953793a7e499e7f71XxX71Exe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-10-04	Cyberespionage Events Targeting Southeast Asian Government Linked To Stately Taurus aka Mustang Panda	11fe99_edr74f07cb12ba30e69e7a84e5cb489ce14a81bced59a11031fc0c3681b7XxX65Dll.dll	Endpoint Security	88E1000GMSYS	Blocked
2023-10-04	Cyberespionage Events Targeting Southeast Asian Government Linked To Stately Taurus aka Mustang Panda	8,129bd45466c26_edr76b248c08bb0efcd9ccc8b684abf3435e290fcf4739c0a439fXxX77Dll.dll	Endpoint Security	88E1000GMSYS	Blocked
2023-10-04	Cyberespionage Events Targeting Southeast Asian Government Linked To Stately Taurus aka Mustang Panda	18_edr74b20e3e802406c594341699c5863a2c07c4c79cf762888ee28142af83547fXxX73Dll.dll	Endpoint Security	88E1000GMSYS	Blocked
2023-10-04	Cyberespionage Events Targeting Southeast Asian Government Linked To Stately Taurus aka Mustang Panda	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/cyberespionage_events_targeting_southeast_asian_government_linked_to_stately_taurus_aka_mustang_panda_6ca18d24-7f85-466a-b6f5-7d3b21b5e34d/66b_browsing7983831cbb952ceeb1ffff608880f1805f1df0b062cef4c17b258b7f478ceXxX85Dll.dll?X-Amz-Algorithm=AW S4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20231004%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20231004T072512Z&X-Amz-Expires=600&X-Amz-Signature=bc2dc18ef5dc7604100ce09abb7a2b2aa19802081ee306d744f04a0808bea920&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-10-04	Cyberespionage Events Targeting Southeast Asian Government Linked To Stately Taurus aka Mustang Panda	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/cyberespionage_events_targeting_southeast_asian_government_linked_to_stately_taurus_aka_mustang_panda_6ca18d24-7f85-466a-b6f5-7d3b21b5e34d/31eb1de_browsing7e840a342fd468e558e5ab627bcb4c542a8fe01aec4d5ba01d539a0fcXxX83Exe.exe?X-Amz-Algorithm=AW S4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20231004%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20231004T072506Z&X-Amz-Expires=600&X-Amz-Signature=c5f7e8a8e12448850789e9eeb38acd8e7cafa17edf4c6c0791ee730eea95b478&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-10-04	Cyberespionage Events Targeting Southeast Asian Government Linked To Stately Taurus aka Mustang Panda	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/cyberespionage_events_targeting_southeast_asian_government_linked_to_stately_taurus_aka_mustang_panda_6ca18d24-7f85-466a-b6f5-7d3b21b5e34d/12534f_browsing7014b3338d8f9f86ff1bbeacf8c80ad03f1d0d19077ff0e406c58b5133XxX81Exe.exe?X-Amz-Algorithm=AW S4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20231004%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20231004T072504Z&X-Amz-Expires=600&X-Amz-Signature=d18bf92d8e39b3b9d43c973b03bbf021f1b58372385853c56eb1fdd57875cd5f&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-10-04	Cyberespionage Events Targeting Southeast Asian Government Linked To Stately Taurus aka Mustang Panda	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/cyberespionage_events_targeting_southeast_asian_government_linked_to_stately_taurus_aka_mustang_panda_6ca18d24-7f85-466a-b6f5-7d3b21b5e34d/b000a0095a8fda3822_browsing7103f253b6d79134b862a83df50315d7d9c5b537fd994bXxX79Exe.exe?X-Amz-Algorithm=AW S4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20231004%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20231004T072458Z&X-Amz-Expires=600&X-Amz-Signature=1e0d78ef6a692ce6172f99a917a32e95aab298c649968bbd735427fedd7261f7&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-10-04	Cyberespionage Events Targeting Southeast Asian Government Linked To Stately Taurus aka Mustang Panda	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/cyberespionage_events_targeting_southeast_asian_government_linked_to_stately_taurus_aka_mustang_panda_6ca18d24-7f85-466a-b6f5-7d3b21b5e34d/4a8b_browsing7cfb2e33aa079ba51166591c7a210ad8b3c7c7f242fccf8cb2e71e8e40d5XxX69Exe.exe?X-Amz-Algorithm=AW S4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20231004%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20231004T072456Z&X-Amz-Expires=600&X-Amz-Signature=d2421d0ad988f29b021ddad1878ae677cd2191f7be47e866c51a17d1f819b0d5&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 10/09/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-10-03	Vulnerable Openfire Messaging Servers Under Attack CVE-2023-32315	48a88aef82d96cc2209cdba8b93662df5a2b6a_edr7c609dd76667993cd06c337867XxX1Jar.jar	Endpoint Security	88E1000GMSYS	Penetrated
2023-10-03	Vulnerable Openfire Messaging Servers Under Attack CVE-2023-32315	ee_edr7c12fc58ca5d79e549f411ee1021a0980b396af6417e6445102117cdf600baXxX3Jar.jar	Endpoint Security	88E1000GMSYS	Penetrated
2023-10-03	Vulnerable Openfire Messaging Servers Under Attack CVE-2023-32315	5aba6a_edr705e3c0cdaee966b5cd940cca0f97acb632ffd4f25ab805c69a3d9e352XxX5Jar.jar	Endpoint Security	88E1000GMSYS	Penetrated
2023-10-03	Vulnerable Openfire Messaging Servers Under Attack CVE-2023-32315	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/vulnerable_openfire_messaging_servers_under_attack_cve-2023-32315_5cd8affb-c4fb-4521-a16f-085aa726470b/a3f_browsing72a73e146834b43dab8833e0a9cfee6d08843a4c23fdf425295e53517afceXxX9Elf.elf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20231003%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20231003T094741Z&X-Amz-Expires=600&X-Amz-Signature=b4910b76b34ae0c615ea68979239daf5562d3e0a6113a04e80e663629bf4d683&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-10-03	Vulnerable Openfire Messaging Servers Under Attack CVE-2023-32315	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/vulnerable_openfire_messaging_servers_under_attack_cve-2023-32315_5cd8affb-c4fb-4521-a16f-085aa726470b/5d2530b809fd069f9_browsing7b30a5938d471dd2145341b5793a70656aad6045445cf6dXxX7Elf.elf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20231003%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20231003T094735Z&X-Amz-Expires=600&X-Amz-Signature=c70555c5752bb20d61abc6c0fef47994e7b4fc0d871242f465c414f8b8c7fa1a&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-20	Cert IL Alert - Medical institutions in Israel are under attack	hxxp://34.197.32.16	Web Gateway	88E1000GMSYS	Offline/Removed
2023-09-20	Cert IL Alert - Medical institutions in Israel are under attack	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/cer t_il_alert_-_medical_institutions_in_israel_are_under_attack_8cba78f4-a71b-428c-ad44-526029c4d686/Freeworldbgjfcaaaeg1_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230920%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230920T110625Z&X-Amz-Expires=600&X-Amz-Signature=b345e46a3e46debae838a8d64e39643cfcfbf6ae654f7dbc161030e64781389e&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-20	Cert IL Alert - Medical institutions in Israel are under attack	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/cer t_il_alert_-_medical_institutions_in_israel_are_under_attack_8cba78f4-a71b-428c-ad44-526029c4d686/Freeworldbgjfcaaaeg2_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230920%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230920T110620Z&X-Amz-Expires=600&X-Amz-Signature=4a17f79042a009d6ad807b7027050f358b6b368a1b3b91fcac74b3b067ff1abb&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-20	ShroudedSnooper Targets Telecommunications Firms In The Middle East With Custom Backdoors	e1ad1_edr73e49eee1194f2a55afa681cef7c3b8f6c26572f474dec7a42e9f0cdc9dXxX69Exe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-09-20	ShroudedSnooper Targets Telecommunications Firms In The Middle East With Custom Backdoors	7,495c1ea421063845eb8f4599a1c1_edr7c105f700ca0671ca874c5aa5aef3764c1cXxX71Exe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-09-20	ShroudedSnooper Targets Telecommunications Firms In The Middle East With Custom Backdoors	c5b4542d61af_edr74cf7454d7f1c8d96218d709de38f94ccfa7c16b15f726dc08c0XxX77Dll.dll	Endpoint Security	88E1000GMSYS	Blocked
2023-09-20	ShroudedSnooper Targets Telecommunications Firms In The Middle East With Custom Backdoors	911_edr7bd328e37be121fb497596a2d0619a0eaca44752a1854523b8af46a5b0cebXxX73Dll.dll	Endpoint Security	88E1000GMSYS	Blocked
2023-09-20	ShroudedSnooper Targets Telecommunications Firms In The Middle East With Custom Backdoors	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/shroudedsnooper_targets_telecommunications_firms_in_the_middle_east_with_custom_backdoors_4b05b247-3c9e-469a-a7b7-ea9d4bac8ef6/38_browsing75ed58c0d42e05c83843b32ed33d6ba5e94e18ffe8fb1bf34fd7dedf3f82a7XxX79Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230920%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230920T105004Z&X-Amz-Expires=600&X-Amz-Signature=8fd0634373468ee2e940b69b56676e950ef6533f938debb5af933d693b1df6f4&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 10/09/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-09-20	ShroudedSnooper Targets Telecommunications Firms In The Middle East With Custom Backdoors	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/shroudedsnooper_targets_telecommunications_firms_in_the_middle_east_with_custom_backdoors_4b05b247-3c9e-469a-a7b7-ea9d4bac8ef6/1146b1f38e420936b_browsing7c5f6b22212f3aa93515f3738c861f499ed1047865549cbXxX75Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230920%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230920T105003Z&X-Amz-Expires=600&X-Amz-Signature=2ba0ed68e710885ce7ad50988e89938b2b45f053f9fd3290ec75fa839b860c97&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-19	PSA Ongoing Webex malvertising campaign drops BatLoader	hxxp://206.71.149.46	Web Gateway	88E1000GMSYS	Offline/Removed
2023-09-19	PSA Ongoing Webex malvertising campaign drops BatLoader	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/psa_ongoing_webex_malvertising_campaign_drops_batloader_bdb3cf59-9cd0-4a62-9ddc-2b0986179b5d/7a1245584c0a12186aa_browsing7228c75a319ca7f57e7b0db55c1bd9b8d7f9b397bfac8XxX11Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230919%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230919T080917Z&X-Amz-Expires=600&X-Amz-Signature=7f5e00fc184ac22da82aa60519fff8b1b79e48b58b54c5784817ca2cf4159510&X-Amz-SignedHeaders=host& x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-19	EV Certificates Abused To Deliver RedLine Vidar And Knight Ransomware	a6258d_edr70bc0b5d5c87368c5024d3f23585790b14227b8c59333413082524a956XxX6Exe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-09-19	EV Certificates Abused To Deliver RedLine Vidar And Knight Ransomware	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ev_certificates_abused_to_deliver_redline_vidar_and_knight_ransomware_bce1d28b-06b4-4b1e-bc88-6c40a4549b92/9123e42cdd3421e8f2_browsing76ac711988fb8a8929172fa76674ec4de230e6d528d09aXxX4Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230919%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230919T062221Z&X-Amz-Expires=600&X-Amz-Signature=af6d0f98163a0c5331738e3848b792516de82c363d7ffaea6c52cdcc1fef438f&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-15	Nazar: Spirits of the Past	Naz5_edrDll.dll	Endpoint Security	88E1000GMSYS	Blocked
2023-09-15	Nazar: Spirits of the Past	Naz3_edrDll.dll	Endpoint Security	88E1000GMSYS	Penetrated
2023-09-15	Nazar: Spirits of the Past	Naz1_edrDll.dll	Endpoint Security	88E1000GMSYS	Penetrated
2023-09-15	Nazar: Spirits of the Past	Naz2_edrExe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-09-15	Nazar: Spirits of the Past	Naz1_edrExe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-09-15	Nazar: Spirits of the Past	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/narspiritsofthepast/Naz4_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-C ontent-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230915% 2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230915T121152Z&X-Amz-Expires=600&X- Amz-Signature=5201b49ce45df7eb865cbcebde6150ff1097072b7c206d35fc2b7ee8424736e9&X -Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-15	Nazar: Spirits of the Past	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/narspiritsofthepast/Naz3_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-C ontent-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230915% 2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230915T121152Z&X-Amz-Expires=600&X- Amz-Signature=d25c8571378e0ce069cb186a69e23e2a8064ed7e10055936847e45216fd4e73f&X -Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-15	Nazar: Spirits of the Past	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/narspiritsofthepast/Naz4_browsingDll.dll?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-C ontent-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230915% 2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230915T121150Z&X-Amz-Expires=600&X- Amz-Signature=288db881b8d3de792d8cd764ac351bc90e3eb52802a821a5885ddc76b5edbe8a&X -Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-15	Nazar: Spirits of the Past	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/narspiritsofthepast/Naz2_browsingDll.dll?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-C ontent-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230915% 2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230915T121150Z&X-Amz-Expires=600&X- Amz-Signature=877770e6e7edcb2d8ffaabf7b600c82b6b064b2f8b7b6fc6daa81c0e6419f5bd&X -Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-15	New Ransomware Spotted - White Rabbit and It's Evasion Tactics	Whiterabbit1_edrDll.dll	Endpoint Security	88E1000GMSYS	Blocked
2023-09-15	New Ransomware Spotted - White Rabbit and It's Evasion Tactics	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/new_ransomware_spotted_-_white_rabbit_and_it%27s_evasion_tactics_30ad417d-8d75-4a7f -8dab-ab2aeff0f3fb/Whiterabbit2_browsingDll.dll?X-Amz-Algorithm=AWS4-HMAC-SHA256 &X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F2 0230915%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230915T092122Z&X-Amz-Expire s=600&X-Amz-Signature=5aa9e7b29bb5bcd82aca539cca3f02cacb7f5fc6d7bd0676aaffcc242c 4ecacb&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-15	8Base Ransomware - A Heavy Hitting Player	Eightbasebgiiacggfh4_edrExe.exe	Endpoint Security	88E1000GMSYS	Blocked

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

TLP:AMBER

ASM-VP REPORT

Organo Judicial 10/09/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-09-15	8Base Ransomware - A Heavy Hitting Player	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/8base_ransomware_-_a_heavy_hitting_player_a5893f49-67e5-45ef-a151-6ce0c11c6ff8/Eightbasebgiiacggfh1_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230915%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230915T005528Z&X-Amz-Expires=600&X-Amz-Signature=2bda1e374e75e7d71965e01ab8a4fd9eec2333c3adeec0dd999ef8ecf65537df&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-15	8Base Ransomware - A Heavy Hitting Player	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/8base_ransomware_-_a_heavy_hitting_player_a5893f49-67e5-45ef-a151-6ce0c11c6ff8/Eightbasebgiiacggfh2_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230915%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230915T005527Z&X-Amz-Expires=600&X-Amz-Signature=0fc2eedaf8859c55bec44c367761e5272c2158b72d33bc69891997eaf37b7020&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-15	8Base Ransomware - A Heavy Hitting Player	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/8base_ransomware_-_a_heavy_hitting_player_a5893f49-67e5-45ef-a151-6ce0c11c6ff8/Eightbasebgiiacggfh3_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230915%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230915T005526Z&X-Amz-Expires=600&X-Amz-Signature=69373529f483d651d1f9fe9c085c80cff9c666bb0714769bcf1fc9b9c27543de&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-14	DarkGate Loader Malware Delivered via Microsoft Teams	9,904d65e59f3fbbbf38932ae_edr7bff9681ac73b0e30b8651ec567f7032a94234fXxX210Zip.zip	Endpoint Security	88E1000GMSYS	Blocked
2023-09-14	DarkGate Loader Malware Delivered via Microsoft Teams	1bcde4d4613f046b63e9_edr70aa10ea2662d8aa7d326857128b59cb88484cce9a2dXxX212Au3.au3	Endpoint Security	88E1000GMSYS	Blocked
2023-09-14	DarkGate Loader Malware Delivered via Microsoft Teams	4c21_edr711de81bb5584d35e744394eed2f36fef0d93474dfc5685665a9e159eef1XxX213Vbs.vbs	Endpoint Security	88E1000GMSYS	Blocked
2023-09-14	DarkGate Loader Malware Delivered via Microsoft Teams	bcd4494_edr70626f4f34a15be00812f850c5e032723e35776fb4b9be6c7be6c8913XxX214Lnk.In k	Endpoint Security	88E1000GMSYS	Blocked
2023-09-14	DarkGate Loader Malware Delivered via Microsoft Teams	0c59f568da43_edr731e3212b6461978e960644be386212cc448a715dbf3f489d758XxX211Zip.zip	Endpoint Security	88E1000GMSYS	Blocked
2023-09-14	DarkGate Loader Malware Delivered via Microsoft Teams	hxxp://5.188.87.58:2351/msiwbzadczl	Web Gateway	88E1000GMSYS	Offline/Removed
2023-10-03	Budworm APT Uses Updated Custom Tool In Attacks On Government And Telecoms	f15_edr7090fd3ccd4220298c06ce8734361b724d80459592b10ac632acc624f455eXxX56Exe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-10-03	Budworm APT Uses Updated Custom Tool In Attacks On Government And Telecoms	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/budworm_apt_uses_updated_custom_tool_in_attacks_on_government_and_telecoms_30722f75-0938-4cff-8f1c-d5d507f063a3/c3405d9c9d593d_browsing75d773c0615254e69d0362954384058ee970a3ec0944519c37XxX62Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20231003%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20231003T094515Z&X-Amz-Expires=600&X-Amz-Signature=ba920b7037b955e7eaa667949f845f2f7cbc676ba7fb55ab807b624fe674b199&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-10-03	ZenRAT Malware Brings More Chaos Than Calm	60,098db9f251bca8d40bf6b19e3defa1b81ff3bdc138_edr76766988429a2e922a06XxX1Exe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-10-03	ZenRAT Malware Brings More Chaos Than Calm	e318b2c1693bc_edr771dfe9a66ee2cebcc2b426b01547bb0164d09d025467cb9ee3XxX7Exe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-10-03	ZenRAT Malware Brings More Chaos Than Calm	83_edr78c6faf198f4182c55f85c494052a5288a6d7823de89914986b2352076bb12XxX2Exe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-10-03	ZenRAT Malware Brings More Chaos Than Calm	d_edr7d59f7db946c7e77fed4b927b48ab015e5f3ea8e858d330930e9f7ac1276536XxX5Exe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-10-03	ZenRAT Malware Brings More Chaos Than Calm	hxxps://obsproject.com	Web Gateway	88E1000GMSYS	Offline/Removed
2023-10-03	ZenRAT Malware Brings More Chaos Than Calm	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/zenrat_malware_brings_more_chaos_than_calm_74ba0f2a-89d8-4f81-af99-4ce7cda10e1e/f_browsing7573ad27ff407e84d3ebf173cbeaaa6aba62eb74b4b2b934bc0433df3d9e066XxX8Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20231003%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20231003T094227Z&X-Amz-Expires=600&X-Amz-Signature=7a08a4568f982c8d090d085c6a519a71053c7a692bb7d27aaf93753e735c862f&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated

TLP:AMBER

GLESEC
COMPLETELY PERCEPTI

ASM-VP REPORT

Organo Judicial 10/09/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-10-03	ZenRAT Malware Brings More Chaos Than Calm	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/zen rat_malware_brings_more_chaos_than_calm_74ba0f2a-89d8-4f81-af99-4ce7cda10e1e/e0c 06_browsing7fc8e10a662c42926f6cdadfa5c6b8c90d5dff3f0e9f381210180d47d37XxX6Exe.ex e?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-C redential=AKIAJPJC2Q3D5GWFTK3Q%2F20231003%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20231003T094223Z&X-Amz-Expires=600&X-Amz-Signature=84912d612aa93dd9033ea810 8e7349d86b33a3ed475b101d29be57ffcd5a2cb1&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-10-03	ZenRAT Malware Brings More Chaos Than Calm	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/zen rat_malware_brings_more_chaos_than_calm_74ba0f2a-89d8-4f81-af99-4ce7cda10e1e/ba3 6d9d6e53_browsing7a1c1ecdf1ace9f170a3a13c19e77f582a5cae5c928a341c1be8dXxX4Exe.ex e?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-C redential=AKIAJPJC2Q3D5GWFTK3Q%2F20231003%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20231003T094221Z&X-Amz-Expires=600&X-Amz-Signature=1a17624680fa8db1c9f49e21 b480e9bff758a1a7ef8c1aaca27cc4dd6caa2bf4&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-10-03	ZenRAT Malware Brings More Chaos Than Calm	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/zen rat_malware_brings_more_chaos_than_calm_74ba0f2a-89d8-4f81-af99-4ce7cda10e1e/986 aa8e20962b289_browsing71b3a5335ef46cf96c102fa828ae7486c2ac2137a0690b76XxX3Exe.ex e?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-C redential=AKIAJPJC2Q3D5GWFTK3Q%2F20231003%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20231003T094216Z&X-Amz-Expires=600&X-Amz-Signature=c7cd32db317cc712fcb67b88 efcac23123df483ae911249e31695e0446287c92&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-10-03	BunnyLoader the newest Malware-as-a-Service	90e6ebc8_edr79283382d8b62679351ee7e1aaf7e79c23dd1e462e840838feaa5e69XxX2Exe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-10-03	BunnyLoader the newest Malware-as-a-Service	454bd68088f1_edr7718527b300134cae3eed1c7db3ba7ed9e08d291ef7729229a79XxX3Exe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-10-03	BunnyLoader the newest Malware-as-a-Service	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/bun nyloader_the_newest_malware-as-a-service_84b5fe3f-55cf-49cb-8659-234fd347544b/9b 8efc369c_browsing7ff541f885c605c462c7d5a16acfbdfef3b28adc4e5418e890142fXxX1Exe.e xe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20231003%2Feu-west-1%2Fs3%2Faws4_request&X-Amz - Date=20231003T093937Z&X-Amz-Expires=600&X-Amz-Signature=7ba93e4000ab6a4454dabd4 9d6eb7825a2a4824916bc4f8cf1fc35df5d5e394d&X-Amz-SignedHeaders=host&x-id=GetObjec t	Web Gateway	88E1000GMSYS	Penetrated
2023-09-28	Stealth Falcon Preying Over Middle Eastern Skies with Deadglyph	56_edr71b3a89c0e88a9bfb0bd5bc434fa5245578becfdeb284f4796f65eecbd6f15XxX14Dll.dll	Endpoint Security	88E1000GMSYS	Blocked
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	4da5_edr7027ffe7e32c891334d6834923bc17e4174c53ace4ff69de6410c24d84cbXxX154Dll.dll	Endpoint Security	88E1000GMSYS	Penetrated
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	b6d26c5b2b2300fa8bf_edr784919638ba849805896cf969c5c330668b350907c148XxX163Pdf.pd f	Endpoint Security	88E1000GMSYS	Penetrated
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	a42dd6bea439b_edr79db90067b84464e755488b784c3ee2e64ef169b9dcdd92b069XxX119Dll.dl l	Endpoint Security	88E1000GMSYS	Blocked
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	60d96d8d3a09f822ded0a3c84194a5d88ed62a9_edr79cbb6378545b45b04353bb37XxX127Dll.dll	Endpoint Security	88E1000GMSYS	Blocked
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	79a1402bc_edr77aa2702dc5dca660ca0d1bf08a2923e0a1018da70e7d7c31d9417fXxX128Iso.iso	Endpoint Security	88E1000GMSYS	Blocked
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	7fc9e830_edr756e23aa4b050f4ceaeb2a83cd71cfc0145392a0bc03037af373066bXxX130Dll.dll	Endpoint Security	88E1000GMSYS	Blocked
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	46c8289301129c0833529495f4f3_edr748b5adff78e18f1427654cb3b597352873eXxX171Pdf.pdf	Endpoint Security	88E1000GMSYS	Penetrated
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	4_edr7e8f705febc94c832307dbf3e6d9c65164099230f4d438f7fe4851d701b580bXxX129Html.html	Endpoint Security	88E1000GMSYS	Blocked

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

TLP:AMBER

GLESEC
COMPLETELY PERCEPTI

ASM-VP REPORT

Organo Judicial 10/09/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	d_edr7bda5e39327fe12b0c1f42c8e27787f177a352f8eebafbe35d3e790724eceffXxX131Dll.dl l	Endpoint Security	88E1000GMSYS	Blocked
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	a8ae10b43cbf4e3344e0184b33a699b19a29866bc1e41201ace1a995e8ca3149_edrXxX132Lnk.ln k	Endpoint Security	88E1000GMSYS	Blocked
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	48_edr75a9c4af3044db281c5dc02e5386c77f331e3b92e5ae79ff9961d8cd1f7c4fXxX134Svg.svg	Endpoint Security	88E1000GMSYS	Blocked
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	ae_edr79aa17e6f3cc8e816e32335738b61b343e78c20abb8ae044adfeac5d97bf70XxX151Dll.dl l	Endpoint Security	88E1000GMSYS	Blocked
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	948c62e8d953038b6a0030136cb82f55a8251db2c165ca0_edr7c01a7568f4644240XxX213Iso.iso	Endpoint Security	88E1000GMSYS	Penetrated
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	19,442,634bc2e0bfa6d08b_edr7be333a351b932a517a1002c0e1c49fea8381372a6eXxX211Pdf.pdf	Endpoint Security	88E1000GMSYS	Penetrated
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	302c0d553c9e_edr7f2561864d79022b780a53ec0a5927e8962d883b88dde249d044XxX155Pdf.pdf	Endpoint Security	88E1000GMSYS	Blocked
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	e22bc_edr75bb87e19554cd0f98c98b22a07368c2b23adacc41fe2cd68c20957d60aXxX183Lnk.ln k	Endpoint Security	88E1000GMSYS	Blocked
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	0e22e6a1dc529008d6228_edr7cfddaed53c7f4cc698feec144f00c92594dc76d036XxX198Lnk.lnk	Endpoint Security	88E1000GMSYS	Blocked
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	3a_edr76182529c4fd5276091ed8ff4c4dcc89e4abc5981348a066c4eb34a9956947XxX201Lnk.lnk	Endpoint Security	88E1000GMSYS	Blocked
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	1_edr7cf399a9c5b2dbd55ebd6b5a4695a2f6aca6464abc7140f3c0e7a750c6117bdXxX199Html.html	Endpoint Security	88E1000GMSYS	Blocked
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	459cc8a6eca9aae2abc4de0b93b9e0a6c439a86b0e3_edr737b4e02f9e98f039c85bXxX214Zip.zip	Endpoint Security	88E1000GMSYS	Blocked
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	5d4bf026fad409_edr79541efd2419ec0b042c8cf83bc1a61cbcc069efe0069ccd27XxX208Zip.zip	Endpoint Security	88E1000GMSYS	Blocked
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/backchannel_diplomacy_apt29s_rapidly_evolving_diplomatic_phishing_operations_2c27ca45-2f26-4cad-810d-8f6daf97e038/2589_browsing700d01c8a60a4f2d8188e31712821c7085a4715785e2871ac517c81477e3XxX212Lnk.lnk?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230928%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230928T111439Z&X-Amz-Expires=600&X-Amz-Signature=62415ef51fc4d2ca637474d2d2c47e920bca2ccfc18934c8a252d74787c1ccc8&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/backchannel_diplomacy_apt29s_rapidly_evolving_diplomatic_phishing_operations_2c27ca45-2f26-4cad-810d-8f6daf97e038/02ce4_browsing7bd766f7489c6326c30351eb9b365f9997de1b2f92924d130fa07e0d82cXxX210Lnk.lnk?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230928%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230928T111439Z&X-Amz-Expires=600&X-Amz-Signature=fc6ad52e1cef037ad019f7fa9475ba59e7192e98cb2f54ba9c12675705349545&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 10/09/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/backchannel_diplomacy_apt29s_rapidly_evolving_diplomatic_phishing_operations_2c27ca45-2f26-4cad-810d-8f6daf97e038/62a903a4b5cd2_browsing7d739950e71ab74061e815af4830a29df6dcbf8c1a34abc87cbXxX209Lnk.lnk?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230928%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230928T111438Z&X-Amz-Expires=600&X-Amz-Signature=7619f704a93ded8b3bb16c4a3fd6e51cce62778ea6f3364aae18dffee26d597f&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/backchannel_diplomacy_apt29s_rapidly_evolving_diplomatic_phishing_operations_2c27ca45-2f26-4cad-810d-8f6daf97e038/cd4956e4c1a3f_browsing7c8c008c4658bb9eba7169aa874c55c12fc748b0ccfe0f4a59aXxX203Html.html?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230928%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230928T111437Z&X-Amz-Expires=600&X-Amz-Signature=d81aa4583c62b5ba12a1e6470db061eb638abefb4a534a0c153f5dd9d197ac1b&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/backchannel_diplomacy_apt29s_rapidly_evolving_diplomatic_phishing_operations_2c27ca45-2f26-4cad-810d-8f6daf97e038/452_browsing7057000a4b06f000983b5b61cc85c10f03691fa17d5c51a9fd0b24280662dXxX200Html.html?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230928%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230928T111433Z&X-Amz-Expires=600&X-Amz-Signature=8cb98148880c725b6537ee97105faeea13f7299fd0d7937c856d81c0a9714470&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/backchannel_diplomacy_apt29s_rapidly_evolving_diplomatic_phishing_operations_2c27ca45-2f26-4cad-810d-8f6daf97e038/6f3_browsing7579d445639c7dfebb4927fe7f6ea70d25d1127f9d9b5078f8ccd4da36127XxX194Lnk.lnk?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230928%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230928T111425Z&X-Amz-Expires=600&X-Amz-Signature=00cfbf48048b221088a7e4628d7ee161959ba609183961f3f54ff3ec7e03e2f2&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/backchannel_diplomacy_apt29s_rapidly_evolving_diplomatic_phishing_operations_2c27ca45-2f26-4cad-810d-8f6daf97e038/62ce8e1489a8b8_browsing7539792c07179faf1db1b46caa39b55902a4d82dcec44d72aeXxX193Pdf.pdf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230928%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230928T111424Z&X-Amz-Expires=600&X-Amz-Signature=2467aeb1d146e6aa7541d8ede140f02a7e1fda3c9a58f6d72ad14df1ca99b089&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/backchannel_diplomacy_apt29s_rapidly_evolving_diplomatic_phishing_operations_2c27ca45-2f26-4cad-810d-8f6daf97e038/c520912_browsing7e65b0465c8a707ca127b067aa8756c1138bd0d3636f71bfbe8fd9bdaXxX191Lnk.lnk?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230928%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230928T111424Z&X-Amz-Expires=600&X-Amz-Signature=6557424fd19f6ac358be018225871fa32e7481af0e03983622094ce161e17204&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/backchannel_diplomacy_apt29s_rapidly_evolving_diplomatic_phishing_operations_2c27ca45-2f26-4cad-810d-8f6daf97e038/640a08b52623cd8_browsing702de066f1f9a6923b18283fc2656137cd9c584da1e07775cXxX188Lnk.lnk?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230928%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230928T111424Z&X-Amz-Expires=600&X-Amz-Signature=e26f9ab164454544b193eda33fe1703ef61b496bf2812b4732c8122c21f69e44&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/backchannel_diplomacy_apt29s_rapidly_evolving_diplomatic_phishing_operations_2c27ca45-2f26-4cad-810d-8f6daf97e038/2a54121a0_browsing73f291de3a2e2a0616bd6739b588a1b69318ff4340826a3ab673e8cXxX187Dll.dll?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230928%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230928T111423Z&X-Amz-Expires=600&X-Amz-Signature=52eb5cb3422ee556147ab1188cc11ee6bd407ae28abdc4cb0fc7a4fc4da80ae3&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/backchannel_diplomacy_apt29s_rapidly_evolving_diplomatic_phishing_operations_2c27ca45-2f26-4cad-810d-8f6daf97e038/ece45b0ed8_browsing7b6e956022a5e20582701b7f22c699d89c44144adde252515b0a66XxX178Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230928%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230928T111422Z&X-Amz-Expires=600&X-Amz-Signature=f2acd0a9b9bc5e9e546891415dae9a6d90695a0208e20935546c8990e0c35474&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/backchannel_diplomacy_apt29s_rapidly_evolving_diplomatic_phishing_operations_2c27ca45-2f26-4cad-810d-8f6daf97e038/61fc12f8d9e54fa16233e4_browsing73cdd5a66af4c03944568b7fbeefb5231d6da30215XxX169Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230928%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230928T111420Z&X-Amz-Expires=600&X-Amz-Signature=d020b8830dfcf8dbfda2f2016b444dd217e089ddd3dade25788e60e5e1e28477&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 10/09/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/backchannel_diplomacy_apt29s_rapidly_evolving_diplomatic_phishing_operations_2c27ca45-2f26-4cad-810d-8f6daf97e038/92a5be2893_browsing743435b79e94aa64a74233a2240fd790ca948e1cb046da5b4072f1XxX167Html.html?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230928%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230928T111409Z&X-Amz-Expires=600&X-Amz-Signature=e214c19e58ce47962eb373aa10a7398637449c310f3e72e297e707e8259eaf12&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/backchannel_diplomacy_apt29s_rapidly_evolving_diplomatic_phishing_operations_2c27ca45-2f26-4cad-810d-8f6daf97e038/0e_browsing7072742314e25bab71c94b9738be45d9bc7e7ecb34fac57059805a0458d9d9XxX159Html.html?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230928%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230928T111403Z&X-Amz-Expires=600&X-Amz-Signature=77930172aeb07e252f7e2633f90d41029724a40dbf7721aa28ca04e3ce8fd453&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/backchannel_diplomacy_apt29s_rapidly_evolving_diplomatic_phishing_operations_2c27ca45-2f26-4cad-810d-8f6daf97e038/044c42_browsing788cfe2b14b5bd3ff6e51f3b1e10983be1a3641165f10a1a3c8d9b2eb0XxX158Html.html?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230928%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230928T111402Z&X-Amz-Expires=600&X-Amz-Signature=842bdca647985c6863392756701fb08b6bc84fba67edb3a4899c892cc9653eba&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/backchannel_diplomacy_apt29s_rapidly_evolving_diplomatic_phishing_operations_2c27ca45-2f26-4cad-810d-8f6daf97e038/38f8b8036ed2a0b5abb8fbf264ee6fd2b82dcd91_browsing7f60d9f1d8f18d07c26b1534XxX141Dll.dll?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230928%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230928T111400Z&X-Amz-Expires=600&X-Amz-Signature=ef8917845f98c8e2cec0fdf6d88374e662195c2d398eb18841bb1a462b012f82&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/backchannel_diplomacy_apt29s_rapidly_evolving_diplomatic_phishing_operations_2c27ca45-2f26-4cad-810d-8f6daf97e038/af1922c665e9be6b29a5e3d0d3ac5916ae1fc_browsing74ac2fe9931e5273f3c4043f395XxX133Iso.iso?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230928%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230928T111357Z&X-Amz-Expires=600&X-Amz-Signature=7c5462cf691eab28c8f0fae3c4c4c433037a471fac046e86f0d6fbbbc3827a65&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/backchannel_diplomacy_apt29s_rapidly_evolving_diplomatic_phishing_operations_2c27ca45-2f26-4cad-810d-8f6daf97e038/0dd55a234be8e3e0_browsing7b0eb19f47abe594295889564ce6a9f6e8cc4d3997018839XxX126Zip.zip?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230928%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230928T111337Z&X-Amz-Expires=600&X-Amz-Signature=fe16e49024ea519a22892340acf95dab83748a3951f3483aef9574000f526e2d&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/backchannel_diplomacy_apt29s_rapidly_evolving_diplomatic_phishing_operations_2c27ca45-2f26-4cad-810d-8f6daf97e038/311e9c8cf6d0b2950_browsing74ffefaa9f277cb1f806343be262c59f88fbdf6fe242517XxX125Docx.docx?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230928%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230928T111336Z&X-Amz-Expires=600&X-Amz-Signature=8fb3b9f6339d5c0a4d027294492be779a52e00ab3409902b9a7e995b92b70aeb&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/backchannel_diplomacy_apt29s_rapidly_evolving_diplomatic_phishing_operations_2c27ca45-2f26-4cad-810d-8f6daf97e038/18cc4c15_browsing77a5b3793ecc1e14db2883ffc6bf7c9792cf22d953c1482ffc124f5aXxX122Dll.dll?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230928%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230928T111336Z&X-Amz-Expires=600&X-Amz-Signature=9e33e6c44314ece9a3298bc1881ae47d3dfb73d9c4a743c0448845673ab85d1f&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/backchannel_diplomacy_apt29s_rapidly_evolving_diplomatic_phishing_operations_2c27ca45-2f26-4cad-810d-8f6daf97e038/c03292fca415b51d08da32e2f_browsing7226f66382eb391e19d53e3d81e3e3ba73aa8c1XxX118Iso.iso?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230928%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230928T111325Z&X-Amz-Expires=600&X-Amz-Signature=e9af3d571cfbd07fe0aabdb780c7583fdcb89955aec39d38a02f17013288d15f&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-28	A multi-ransomware cybercriminal group	90cdcf54bbaeb9c5c4afc9b_edr74b48b13e293746ee8858c033fc9d365fd4074018XxX239Dll.dll	Endpoint Security	88E1000GMSYS	Penetrated
2023-09-28	A multi-ransomware cybercriminal group	3cc_edr739bb1882fc9dbb056f39ebe4965771aeca0ceb44e85da39d1ba7dade693fXxX242Exe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-09-28	A multi-ransomware cybercriminal group	43c3b5dbc18ebbc55c12_edr7d197255446d5f3e074fdac37f3e901b718acbe7c833XxX247Exe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-09-28	A multi-ransomware cybercriminal group	hxxp://psychologymax.com	Web Gateway	88E1000GMSYS	Blocked

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

TLP:AMBER

GLESEC
COMPLETELY PERCEPTI

ASM-VP REPORT

Organo Judicial 10/09/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-09-28	A multi-ransomware cybercriminal group	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/a_m ulti-ransomware_cybercriminal_group_756a8cbd-3ebf-476b-907c-f0321ede760f/4f4864a 1d5f19a3c5552d80483526f341349_browsing7835549dce8c61fef116b666fa09XxX246Dll.dll? X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Cre dential=AKIAJPJC2Q3D5GWFTK3Q%2F20230928%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Da te=20230928T110914Z&X-Amz-Expires=600&X-Amz-Signature=4174e8f4080fbad5b9750dfe68 98aadc662dc35d0ecff341a0a59bfe5133994f&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-28	A multi-ransomware cybercriminal group	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/a_m ulti-ransomware_cybercriminal_group_756a8cbd-3ebf-476b-907c-f0321ede760f/606bd_b rowsing75ed9d2d6107ea7ee67063d1761a99f2fb5e932c8344d11395d24587dd6XxX243Exe.exe? X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Cre dential=AKIAJPJC2Q3D5GWFTK3Q%2F20230928%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Da te=20230928T110909Z&X-Amz-Expires=600&X-Amz-Signature=74e4deb0447d6f5b5a97036a0b 2dd43eb0ba79cb0df040748085303073 4fcaca&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-28	A multi-ransomware cybercriminal group	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/a_m ulti-ransomware_cybercriminal_group_756a8cbd-3ebf-476b-907c-f0321ede760f/e9_brow sing7bdf7fafb1cb2a2bf0a4e14f51e18a34f3ff2f6f7b99731e93070d50801befXxX236Exe.exe? X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Cre dential=AKIAJPJC2Q3D5GWFTK3Q%2F20230928%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Da te=20230928T110903Z&X-Amz-Expires=600&X-Amz-Signature=943e8d14160b0417d980183e09 75b331b32d4997b88460df2d4e42d2697a8ca7&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-27	GOLD MELODY Profile of an Initial Access Broker	a3d5ead160614336a013f5de4cff65a5198b1d_edr73238a5b456f558e70b503f52eXxX282Exe.ex e	Endpoint Security	88E1000GMSYS	Blocked
2023-09-27	GOLD MELODY Profile of an Initial Access Broker	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/gol d_melody_profile_of_an_initial_access_broker_143aa500-b32d-43ca-93ca-45aa9dbf76e c/05d5fa365498651bcbb8a356cd580b255cd4fd_browsing735e59f81d0c595b06ee61ad10XxX28 6Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD& X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230927%2Feu-west-1%2Fs3%2Faws4_request &X-Amz-Date=20230927T093323Z&X-Amz-Expires=600&X-Amz-Signature=fc147d67f081c9744 21e65146904bfc0f6367e960ddcdfc088fcdbb06702bd34&X-Amz-SignedHeaders=host&x-id=Ge tObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-27	GOLD MELODY Profile of an Initial Access Broker	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/gol d_melody_profile_of_an_initial_access_broker_143aa500-b32d-43ca-93ca-45aa9dbf76e c/fd544bda416f0819df01b45_browsing7d42888af64f2652fd9a907fd4cfc129a5556e97bXxX26 7Pl.pl?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230927%2Feu-west-1%2Fs3%2Faws4_request&X -Amz-Date=20230927T093321Z&X-Amz-Expires=600&X-Amz-Signature=4c8805d50bb4c1515a9 cc21f5b50a06cd2ae70f7697fec094c25b2deca62f3d6&X-Amz-SignedHeaders=host&x-id=GetO bject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-27	Gallium APT Group Suspected To Be Behind Southeast Asian Government Attacks	c1f43b_edr7cf46ba12cfc1357b17e4f5af408740af7ae70572c9cf988ac50260ce1XxX791Aspx.a spx	Endpoint Security	88E1000GMSYS	Blocked
2023-09-27	Gallium APT Group Suspected To Be Behind Southeast Asian Government Attacks	5aa035ebc3359ee851_edr7d99569c8881fcb7f48ab7e9a2f101f7e7ec23e636c79bXxX803Exe.exe	Endpoint Security	88E1000GMSYS	Penetrated
2023-09-27	Gallium APT Group Suspected To Be Behind Southeast Asian Government Attacks	225e5818dc_edr7e7b23110f64fbb718c1792ad93ba7eb893bfbee96cdb13180fbf7XxX805Exe.exe	Endpoint Security	88E1000GMSYS	Penetrated
2023-09-27	Gallium APT Group Suspected To Be Behind Southeast Asian Government Attacks	bd5dcf5911f959dd_edr79de046d151e8a4aed3b854a322135acc37e3edb3643d0e2XxX801Exe.ex e	Endpoint Security	88E1000GMSYS	Blocked
2023-09-27	Gallium APT Group Suspected To Be Behind Southeast Asian Government Attacks	c_edr74897b1e986e2876873abb3b5069bf1b103667f7f0e6b4581fbda3fd647a74aXxX807Exe.ex e	Endpoint Security	88E1000GMSYS	Blocked
2023-09-27	Gallium APT Group Suspected To Be Behind Southeast Asian Government Attacks	4cb020a66fdbc99b0bce2ae24d5684685e2b1e9219fbdfda56b3aace4e8d5f66_edrXxX797Exe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-09-27	Gallium APT Group Suspected To Be Behind Southeast Asian Government Attacks	36e661edc1ad4e44ba38d8f_edr7a6bd00c2b4bc32e9fae8b955b1b4c6355aa6abedXxX795Aspx.aspx	Endpoint Security	88E1000GMSYS	Blocked
2023-09-27	Gallium APT Group Suspected To Be Behind Southeast Asian Government Attacks	hxxp://45.117.103.86	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 10/09/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-09-27	Gallium APT Group Suspected To Be Behind Southeast Asian Government Attacks	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/gallium_apt_group_suspected_to_be_behind_southeast_asian_government_attacks_6a307a01-1160-4385-a86f-96036b7efe1d/9242846351a65655e93ed2aeaf36b535ff5b_browsing79ddf76c33d54089d9005a66265bXxX799Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230927%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230927T092745Z&X-Amz-Expires=600&X-Amz-Signature=2f13f20f79c97fe6cc6e4f165f67f73c367bbe49ef4bc6d265609bad68e1653c&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-27	Gallium APT Group Suspected To Be Behind Southeast Asian Government Attacks	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/gallium_apt_group_suspected_to_be_behind_southeast_asian_government_attacks_6a307a01-1160-4385-a86f-96036b7efe1d/009a9d1609592abe039324da2a8a69c4a305ca999920bf6bbef8392_browsing73516783aXxX793Aspx.aspx?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230927%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230927T092743Z&X-Amz-Expires=600&X-Amz-Signature=5c8d24606813e0094f044dd0954680e3d0a9cc5581e1e697b27d11dc78559af6&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-24	OilRigs Outer Space and Juicy Mix Same olrig new drill pipes	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/oilrigs_outer_space_and_juicy_mix_same_olrig_new_drill_pipes_0ab5d94d-42b2-4922-be6 0-edb7e292ed32/6013d_browsing7e0c4a54c78c846836da9e70785b3b8ca1f0b9d76fa88129baa5a4805dcXxX19Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230924%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230924T081142Z&X-Amz-Expires=600&X-Amz-Signature=0adcd54bfc9a25a104d7c98b0096fbf7d9499708d42176dfd3a5356117bb04d0&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-24	OilRigs Outer Space and Juicy Mix Same olrig new drill pipes	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/oilrigs_outer_space_and_juicy_mix_same_olrig_new_drill_pipes_0ab5d94d-42b2-4922-be6 0-edb7e292ed32/5_browsing7fd32c39c64d9f58846fa91b19c3086b66b0e733ebbc30f917a1f5063389691XxX16Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230924%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230924T081141Z&X-Amz-Expires=600&X-Amz-Signature=67e98be593dd3088e4679fe34230cffa2e01451e99b1edceae6dcd604bb5c610&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-24	OilRigs Outer Space and Juicy Mix Same olrig new drill pipes	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/oilrigs_outer_space_and_juicy_mix_same_olrig_new_drill_pipes_0ab5d94d-42b2-4922-be6 0-edb7e292ed32/8a8a_browsing7a506fd57bde314ce6154f2484f280049f2bda504d43704b9ad412d5d618XxX15Doc.doc?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230924%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230924T081139Z&X-Amz-Expires=600&X-Amz-Signature=fac25dc7819dd373ba17c7a31ebf7364cfb9ba429f40e1e55a2a0829d2dcbabb&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-24	OilRigs Outer Space and Juicy Mix Same olrig new drill pipes	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/oilrigs_outer_space_and_juicy_mix_same_olrig_new_drill_pipes_0ab5d94d-42b2-4922-be6 0-edb7e292ed32/64156f9ca51951a9bf91b5b_browsing74073d31c16873ca60492c25895c1f0f074787345XxX14Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230924%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230924T081137Z&X-Amz-Expires=600&X-Amz-Signature=a019dddf0101cb593450ee6780306e89056d86ff6a01cebc616114a77b057b52&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-21	Kmrox Ransomware	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/kmrox_ransomware_d46e036b-3c42-4936-824e-0cf2fe915272/82881ebbc_browsing7c5599d1e98006d7e97106a87983b78eeca0a7cdcdddfff981e0a87XxX1Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230921%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230921T115430Z&X-Amz-Expires=600&X-Amz-Signature=4293d1c6dff755d69d9c5fc398310a5175ddd295d0f42264c96a15efbe3f9da8&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-21	StopRansomware Snatch Ransomware CISA	28e82f28d0b9eb6a53d22983e21a9505ada925ebb61382fabebd_edr76b8c4acff7cXxX9Exe.exe	Endpoint Security	88E1000GMSYS	Penetrated
2023-09-21	StopRansomware Snatch Ransomware CISA	2,155a029a024a2ffa4eff9108ac15c_edr7db527ca1c8f89ccfd94cc3a70b77cfc57XxX15Bat.bat	Endpoint Security	88E1000GMSYS	Penetrated
2023-09-21	StopRansomware Snatch Ransomware CISA	5,950b4e2_edr7554585123d7fca44e83169375c6001201e3bf26e57d079437e70bcdXxX7Exe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-09-21	StopRansomware Snatch Ransomware CISA	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/stopransomware_snatch_ransomware_cisa_773b69b9-0bcc-40e5-84fc-c1a0daecc85d/Extra_browsingSample50Bat.bat?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230921%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230921T112703Z&X-Amz-Expires=600&X-Amz-Signature=89c0950b40791d0d9d9de3edf66e9605b24b1d4e9ccc7e1296ec38a136545af3&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-21	StopRansomware Snatch Ransomware CISA	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/stopransomware_snatch_ransomware_cisa_773b69b9-0bcc-40e5-84fc-c1a0daecc85d/b998a8c15cc19c8c31c89b30f692a40b14d_browsing7a6c09233eb976c07f19a84eccb40XxX21Bat.bat?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230921%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230921T112658Z&X-Amz-Expires=600&X-Amz-Signature=83abd88d4428d81166ae4bcb18a642c2083ea342c6f320de0e37dad87c7cbe8d&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 10/09/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-09-21	StopRansomware Snatch Ransomware CISA	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/stopransomware_snatch_ransomware_cisa_773b69b9-0bcc-40e5-84fc-c1a0daecc85d/a80c_browsing7fe1f88cf24ad4c55910a9f2189f1eedad25d7d0fd53dbfe6bdd68912a84XxX20Bat.bat?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230921%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230921T112657Z&X-Amz-Expires=600&X-Amz-Signature=83385f8616b9a229bd90b7cb3bcc7d97003803a293c63617c3c20cf68198c53e&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-21	StopRansomware Snatch Ransomware CISA	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/stopransomware_snatch_ransomware_cisa_773b69b9-0bcc-40e5-84fc-c1a0daecc85d/6c9d8c5_browsing77dddf9cc480f330617e263a6ee4461651b4dec1f7215bda77df911e7XxX18Bat.bat?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230921%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230921T112657Z&X-Amz-Expires=600&X-Amz-Signature=839e1cb41746ccc9d7d6b881d4fae69820c3469d260646507a90ff8dea4398f6&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-21	StopRansomware Snatch Ransomware CISA	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/stopransomware_snatch_ransomware_cisa_773b69b9-0bcc-40e5-84fc-c1a0daecc85d/25142_browsing7c578eaa814f07037fbe6e388b3bc86ed3800d7887c9d24e7b94176e30dXxX16Bat.bat?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230921%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230921T112656Z&X-Amz-Expires=600&X-Amz-Signature=4a76179273842371746eb7c504e2bb78b4195d1b988be9b8425da315aadedfab1&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-21	StopRansomware Snatch Ransomware CISA	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/stopransomware_snatch_ransomware_cisa_773b69b9-0bcc-40e5-84fc-c1a0daecc85d/510e9fa38a08d446189c34fe6125295f410b36f00aceb65e_browsing7b4508e9d7c4e1d1XxX13Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230921%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230921T112649Z&X-Amz-Expires=600&X-Amz-Signature=ebbbcd7e0212fbdbefa03c1ac8beff7214ad1676a6b9ff434dd9f3e87c5f22a0&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-21	StopRansomware Snatch Ransomware CISA	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/stopransomware_snatch_ransomware_cisa_773b69b9-0bcc-40e5-84fc-c1a0daecc85d/a201f_browsing7f81277e28c0bdd680427b979aee70e42e8a98c67f11e7c83d02f8fe7aeXxX11Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230921%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230921T112648Z&X-Amz-Expires=600&X-Amz-Signature=49e7a45f9ec4f6ac513ef6eb7f75e6aed735f6ad8cb20fac4b2ee3a76f471244&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-21	StopRansomware Snatch Ransomware CISA	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/stopransomware_snatch_ransomware_cisa_773b69b9-0bcc-40e5-84fc-c1a0daecc85d/0965cb8ee38adedd9ba06bdad9220a35890c2df0e4c_browsing78d0559cd6da653bf740fXxX5Bat.bat?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230921%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230921T112635Z&X-Amz-Expires=600&X-Amz-Signature=43106175a95f16206c32a6d163526e4bb1949e3777701a849570aaafe415ddc6&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-21	Cert IL Alert - Medical institutions in Israel are under attack - v2	2f8a32618e3a0c63350ae6fb2c4cd334e3_edr770d395eafe622988a62688dc76cf9XxX1Exe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-09-21	Cert IL Alert - Medical institutions in Israel are under attack - v2	d34c981c4e6504c2ae9065a1bc324a1_edr706890c263f7f6704e8327bede1bc4370XxX2Exe.exe	Endpoint Security	88E1000GMSYS	Penetrated
2023-09-14	Ransomware GandCrab poses as Super Mario	3,849,381,059d9e8bbcc59c253d2cbe1c92f_edr7e1f1992b752d396e349892f2bb0e7XxX1Xls.xls	Endpoint Security	88E1000GMSYS	Blocked
2023-09-14	Ransomware GandCrab poses as Super Mario	93dd4d_edr7baf1e89d024c59dbffce1c4cbc85774a1b7bcc8914452dc8aa8a79a78XxX6Unkn.unkn	Endpoint Security	88E1000GMSYS	Penetrated
2023-09-14	Ransomware GandCrab poses as Super Mario	630b6f15c_edr770716268c539c5558152168004657beee740e73ee9966d6de1753fXxX4Exe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-09-14	Ransomware GandCrab poses as Super Mario	ec2a_edr7e8da04bc4e60652d6f7cc2d41ec68ff900d39fc244cc3b5a29c42acb7a4XxX3Exe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-09-14	Ransomware GandCrab poses as Super Mario	0c8c2_edr7f06a0acb976b8f12ff6749497d4ce1f7a98c2a161b0a9eb956e6955362XxX2Png.png	Endpoint Security	88E1000GMSYS	Blocked
2023-09-14	Ransomware GandCrab poses as Super Mario	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ransomware_gandcrab_poses_as_super_mario_a7882dde-c326-4ab6-a9c9-e583adbf360b/f30454bcc_browsing7f1bc1f328b9b546f5906887fd0278c40d90ab75b8631ef18ed3b7fXxX5Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230914%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230914T083225Z&X-Amz-Expires=600&X-Amz-Signature=8392190c56e64b7b1a17e8621d797afbbc693a02fe9efd48c8249c0b01cbbcdd&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-12	Analysis of Cuba ransomware gang activity and tooling	Analysisbgjeejbidb83_edrDll.dll	Endpoint Security	88E1000GMSYS	Blocked
2023-09-12	Analysis of Cuba ransomware gang activity and tooling	Analysisbgjeejbidb81_edrExe.exe	Endpoint Security	88E1000GMSYS	Blocked

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

TLP:AMBER

GLESEC
COMPLETELY PERCEPTI

ASM-VP REPORT

Organo Judicial 10/09/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-09-12	Analysis of Cuba ransomware gang activity and tooling	Analysisbgjeejbidb82_edrExe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-09-12	Analysis of Cuba ransomware gang activity and tooling	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/analysis_of_cuba_ransomware_gang_activity_and_tooling_1d95ea70-5cb0-47cd-b0d6-96a82fa88cf9/Analysisbgjeejbidb80_browsingPs1.ps1?X-Amz-Algorithm=AWS4-HMAC-SHA256&X- Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230912%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230912T122228Z&X-Amz-Expires=600&X-Amz-Signature=d2da643c9a61a79b9cee53ac9f320862b6dffe46fed45bb0a83667f990bfe19c&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-12	New Agent Tesla Variant Being Spread by Crafted Excel Document	Newbgjeacdgbc35_edrExe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-09-12	New Agent Tesla Variant Being Spread by Crafted Excel Document	Newbgjeacdgbc38_edrXls.xls	Endpoint Security	88E1000GMSYS	Blocked
2023-09-12	New Agent Tesla Variant Being Spread by Crafted Excel Document	hxxps://23.95.128.195	Web Gateway	88E1000GMSYS	Penetrated
2023-09-10	Mac users targeted in new malvertising campaign delivering Atomic Stealer	hxxps://app-downloads.org	Web Gateway	88E1000GMSYS	Offline/Removed
2023-09-10	Mac users targeted in new malvertising campaign delivering Atomic Stealer	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/mac_users_targeted_in_new_malvertising_campaign_delivering_atomic_stealer_372edf24-a29d-4a8b-92c6-482baa0d0f8b/Macbgjebbhdei59_browsingMacho.macho?X-Amz-Algorithm= AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230910%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230910T122903Z&X-Amz-Expires=600&X-Amz-Signature=6d06b097f62c98eb1db7c0e7526063552d58e12d29a5e18925af687d08e9b5b4&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-10	APT37 Distributes Backdoor Via Malicious LNK	Apt3_edr7bgjebdbddg9Bat.bat	Endpoint Security	88E1000GMSYS	Blocked
2023-09-10	APT37 Distributes Backdoor Via Malicious LNK	hxxp://bian0151.cafe24.com/admin/board/1.html	Web Gateway	88E1000GMSYS	Blocked
2023-09-10	APT37 Distributes Backdoor Via Malicious LNK	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/apt37_distributes_backdoor_via_malicious_lnk_ee3688ed-d478-43de-9666-a047cb0a5445/Apt3_browsing7bgjebdbddg7Lnk.lnk?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230910%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230910T122638Z&X-Amz-Expires=600&X-Amz-Signature=ec960f64924a94360ce5a24a8a76b823aa518dd8e83a5f13cfd27428365097a2&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-10	APT37 Distributes Backdoor Via Malicious LNK	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/apt37_distributes_backdoor_via_malicious_lnk_ee3688ed-d478-43de-9666-a047cb0a5445/Apt3_browsing7bgjebdbddg5Html.html?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content -Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230910%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230910T122636Z&X-Amz-Expires=600&X-Amz-Signature=e13f3ec173e6e4542f62d657f5e67f343af33bb933a0d48d9ea7a8df6b0e0790&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-10	Multiple Nation-State Threat Actors Exploit CVE-2022-47966 and CVE-2022-42475	Multiplebgjebbgije2_edrExe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-09-10	Multiple Nation-State Threat Actors Exploit CVE-2022-47966 and CVE-2022-42475	hxxp://179.60.147.4	Web Gateway	88E1000GMSYS	Offline/Removed
2023-09-10	Multiple Nation-State Threat Actors Exploit CVE-2022-47966 and CVE-2022-42475	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/multiple_nation-state_threat_actors_exploit_cve-2022-47966_and_cve-2022-42475_0eb2b3c2-ba42-463c-8922-732350ccc3c2/Multiplebgjebbgije4_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230910%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230910T075450Z&X-Amz-Expires=600&X-Amz-Signature=29a2c05bd6cb9bdba1c9c365d6fd272cc96b61cc624c2092af452f54b39d5935&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-10-03	Budworm APT Uses Updated Custom Tool In Attacks On Government And Telecoms	c3405d9c9d593d_edr75d773c0615254e69d0362954384058ee970a3ec0944519c37XxX62Exe.exe	Endpoint Security	88E1000GMSYS	Blocked

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

TLP:AMBER

GLESEC
COMPLETELY PERCEPTI

ASM-VP REPORT

Organo Judicial 10/09/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-10-03	Budworm APT Uses Updated Custom Tool In Attacks On Government And Telecoms	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/budworm_apt_uses_updated_custom_tool_in_attacks_on_government_and_telecoms_30722f75-0938-4cff-8f1c-d5d507f063a3/f15_browsing7090fd3ccd4220298c06ce8734361b724d80459592b10ac632acc624f455eXxX56Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20231003%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20231003T094505Z&X-Amz-Expires=600&X-Amz-Signature=bb2acebd32a6927ae0efe71a4ca7aa51c2c6be6f8c02f11163cb60a58ade97e5&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-10-03	ZenRAT Malware Brings More Chaos Than Calm	ba36d9d6e53_edr7a1c1ecdf1ace9f170a3a13c19e77f582a5cae5c928a341c1be8dXxX4Exe.exe	Endpoint Security	88E1000GMSYS	Penetrated
2023-10-03	ZenRAT Malware Brings More Chaos Than Calm	986aa8e20962b289_edr71b3a5335ef46cf96c102fa828ae7486c2ac2137a0690b76XxX3Exe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-10-03	ZenRAT Malware Brings More Chaos Than Calm	e0c06_edr7fc8e10a662c42926f6cdadfa5c6b8c90d5dff3f0e9f381210180d47d37XxX6Exe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-10-03	ZenRAT Malware Brings More Chaos Than Calm	f_edr7573ad27ff407e84d3ebf173cbeaaa6aba62eb74b4b2b934bc0433df3d9e066XxX8Exe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-10-03	ZenRAT Malware Brings More Chaos Than Calm	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/zenrat_malware_brings_more_chaos_than_calm_74ba0f2a-89d8-4f81-af99-4ce7cda10e1e/e318b2c1693bc_browsing771dfe9a66ee2cebcc2b426b01547bb0164d09d025467cb9ee3XxX7Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20231003%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20231003T094224Z&X-Amz-Expires=600&X-Amz-Signature=0112d7fa758245f770d727c28481638da688238b681a923d143cd705b8d45e41&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-10-03	ZenRAT Malware Brings More Chaos Than Calm	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/zenrat_malware_brings_more_chaos_than_calm_74ba0f2a-89d8-4f81-af99-4ce7cda10e1e/d_browsing7d59f7db946c7e77fed4b927b48ab015e5f3ea8e858d330930e9f7ac1276536XxX5Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20231003%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20231003T094222Z&X-Amz-Expires=600&X-Amz-Signature=cba9e0fe5a340b576e8f5c9db517ac4e763d52b6d7d018c24a63de794c2a7be7&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-10-03	ZenRAT Malware Brings More Chaos Than Calm	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/zenrat_malware_brings_more_chaos_than_calm_74ba0f2a-89d8-4f81-af99-4ce7cda10e1e/83_browsing78c6faf198f4182c55f85c494052a5288a6d7823de89914986b2352076bb12XxX2Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20231003%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20231003T094214Z&X-Amz-Expires=600&X-Amz-Signature=4cc1ad4d80812a586fe1ebbc68cf849029e2051ccaac71b3252cf83f714ec541&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-10-03	ZenRAT Malware Brings More Chaos Than Calm	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/zenrat_malware_brings_more_chaos_than_calm_74ba0f2a-89d8-4f81-af99-4ce7cda10e1e/60098db9f251bca8d40bf6b19e3defa1b81ff3bdc138_browsing76766988429a2e922a06XxX1Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20231003%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20231003T094212Z&X-Amz-Expires=600&X-Amz-Signature=c80270b3680e71e02a818080af037273919982d4273b951e791b6f2667f0bd25&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-10-03	BunnyLoader the newest Malware-as-a-Service	9b8efc369c_edr7ff541f885c605c462c7d5a16acfbdfef3b28adc4e5418e890142fXxX1Exe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-10-03	BunnyLoader the newest Malware-as-a-Service	hxxp://37.139.129.145	Web Gateway	88E1000GMSYS	Offline/Removed
2023-10-03	BunnyLoader the newest Malware-as-a-Service	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/bunnyloader_the_newest_malware-as-a-service_84b5fe3f-55cf-49cb-8659-234fd347544b/454bd68088f1_browsing7718527b300134cae3eed1c7db3ba7ed9e08d291ef7729229a79XxX3Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20231003%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20231003T093941Z&X-Amz-Expires=600&X-Amz-Signature=a7370cfca7015b21f57aa46282a7f220f857c061026f00a9aba593319aa1d711&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-10-03	BunnyLoader the newest Malware-as-a-Service	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/bunnyloader_the_newest_malware-as-a-service_84b5fe3f-55cf-49cb-8659-234fd347544b/90e6ebc8_browsing79283382d8b62679351ee7e1aaf7e79c23dd1e462e840838feaa5e69XxX2Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20231003%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20231003T093940Z&X-Amz-Expires=600&X-Amz-Signature=880dc96d834c39e9cc279262b6f2d8c54ba9f02f38155a385b615cc23df7e697&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-28	Stealth Falcon Preying Over Middle Eastern Skies with Deadglyph	hxxp://45.14.227.55	Web Gateway	88E1000GMSYS	Offline/Removed
2023-09-28	Stealth Falcon Preying Over Middle Eastern Skies with Deadglyph	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/stealth_falcon_preying_over_middle_eastern_skies_with_deadglyph_4806bcf6-a437-424f-b07b-56ce09a352fe/56_browsing71b3a89c0e88a9bfb0bd5bc434fa5245578becfdeb284f4796f65eecbd6f15XxX14Dll.dll?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230928%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230928T111919Z&X-Amz-Expires=600&X-Amz-Signature=f013a658328d4b981fe490cfe4ca1d011a9bf6d184d20b584b102e9dc2d16127&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated

TLP:AMBER

GLESEC
COMPLETELY PERCEPTI

ASM-VP REPORT

Organo Judicial 10/09/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	c03292fca415b51d08da32e2f_edr7226f66382eb391e19d53e3d81e3e3ba73aa8c1XxX118Iso.is o	Endpoint Security	88E1000GMSYS	Blocked
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	18cc4c15_edr77a5b3793ecc1e14db2883ffc6bf7c9792cf22d953c1482ffc124f5aXxX122Dll.dll	Endpoint Security	88E1000GMSYS	Penetrated
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	311e9c8cf6d0b2950_edr74ffefaa9f277cb1f806343be262c59f88fbdf6fe242517XxX125Docx.docx	Endpoint Security	88E1000GMSYS	Blocked
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	61fc12f8d9e54fa16233e4_edr73cdd5a66af4c03944568b7fbeefb5231d6da30215XxX169Exe.exe	Endpoint Security	88E1000GMSYS	Penetrated
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	0dd55a234be8e3e0_edr7b0eb19f47abe594295889564ce6a9f6e8cc4d3997018839XxX126Zip.zip	Endpoint Security	88E1000GMSYS	Blocked
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	af1922c665e9be6b29a5e3d0d3ac5916ae1fc_edr74ac2fe9931e5273f3c4043f395XxX133Iso.is o	Endpoint Security	88E1000GMSYS	Blocked
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	2a54121a0_edr73f291de3a2e2a0616bd6739b588a1b69318ff4340826a3ab673e8cXxX187Dll.dll	Endpoint Security	88E1000GMSYS	Penetrated
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	38f8b8036ed2a0b5abb8fbf264ee6fd2b82dcd91_edr7f60d9f1d8f18d07c26b1534XxX141Dll.dll	Endpoint Security	88E1000GMSYS	Blocked
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	452_edr7057000a4b06f000983b5b61cc85c10f03691fa17d5c51a9fd0b24280662dXxX200Html.html	Endpoint Security	88E1000GMSYS	Penetrated
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	44c42_edr788cfe2b14b5bd3ff6e51f3b1e10983be1a3641165f10a1a3c8d9b2eb0XxX158Html.html	Endpoint Security	88E1000GMSYS	Blocked
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	0e_edr7072742314e25bab71c94b9738be45d9bc7e7ecb34fac57059805a0458d9d9XxX159Html.html	Endpoint Security	88E1000GMSYS	Blocked
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	92a5be2893_edr743435b79e94aa64a74233a2240fd790ca948e1cb046da5b4072f1XxX167Html.html	Endpoint Security	88E1000GMSYS	Blocked
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	640a08b52623cd8_edr702de066f1f9a6923b18283fc2656137cd9c584da1e07775cXxX188Lnk.lnk	Endpoint Security	88E1000GMSYS	Blocked
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	ece45b0ed8_edr7b6e956022a5e20582701b7f22c699d89c44144adde252515b0a66XxX178Exe.ex e	Endpoint Security	88E1000GMSYS	Blocked
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	c520912_edr7e65b0465c8a707ca127b067aa8756c1138bd0d3636f71bfbe8fd9bdaXxX191Lnk.ln k	Endpoint Security	88E1000GMSYS	Blocked
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	62ce8e1489a8b8_edr7539792c07179faf1db1b46caa39b55902a4d82dcec44d72aeXxX193Pdf.pdf	Endpoint Security	88E1000GMSYS	Blocked

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

TLP:AMBER

GLESEC
COMPLETELY PERCEPTI

ASM-VP REPORT

Organo Judicial 10/09/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	6f3_edr7579d445639c7dfebb4927fe7f6ea70d25d1127f9d9b5078f8ccd4da36127XxX194Lnk.lnk	Endpoint Security	88E1000GMSYS	Blocked
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	2,589_edr700d01c8a60a4f2d8188e31712821c7085a4715785e2871ac517c81477e3XxX212Lnk.lnk	Endpoint Security	88E1000GMSYS	Blocked
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	2ce4_edr7bd766f7489c6326c30351eb9b365f9997de1b2f92924d130fa07e0d82cXxX210Lnk.lnk	Endpoint Security	88E1000GMSYS	Blocked
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	cd4956e4c1a3f_edr7c8c008c4658bb9eba7169aa874c55c12fc748b0ccfe0f4a59aXxX203Html.h tml	Endpoint Security	88E1000GMSYS	Blocked
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	62a903a4b5cd2_edr7d739950e71ab74061e815af4830a29df6dcbf8c1a34abc87cbXxX209Lnk.lnk	Endpoint Security	88E1000GMSYS	Blocked
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	hxxp://kitaeri.com	Web Gateway	88E1000GMSYS	Offline/Removed
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/backchannel_diplomacy_apt29s_rapidly_evolving_diplomatic_phishing_operations_2c27ca45-2f26-4cad-810d-8f6daf97e038/459cc8a6eca9aae2abc4de0b93b9e0a6c439a86b0e3_browsing737b4e02f9e98f039c85bXxX214Zip.zip?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Con tent-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230928%2F eu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230928T111448Z&X-Amz-Expires=600&X-Am z-Signature=2447434293f875f10d9c10a6809e393128d63d73ee5afc20f4fc94f4885a4225&X-A mz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/backchannel_diplomacy_apt29s_rapidly_evolving_diplomatic_phishing_operations_2c27ca45-2f26-4cad-810d-8f6daf97e038/948c62e8d953038b6a0030136cb82f55a8251db2c165ca0_browsing7c01a7568f4644240XxX213Iso.iso?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Con tent-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230928%2F eu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230928T111445Z&X-Amz-Expires=600&X-Am z-Signature=7d2495fad8a6120f39c51abb34005ea0a585e9a37c076e1d3f60751fe78e9222&X-A mz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/backchannel_diplomacy_apt29s_rapidly_evolving_diplomatic_phishing_operations_2c27ca45-2f26-4cad-810d-8f6daf97e038/19442634bc2e0bfa6d08b_browsing7be333a351b932a517a1002c0e1c49fea8381372a6eXxX211Pdf.pdf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Con tent-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230928%2F eu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230928T111439Z&X-Amz-Expires=600&X-Am z-Signature=983c989ba9ad9c182f3618816532b54192adaa6bab55b50e2fb60cbadd398182&X-A mz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/backchannel_diplomacy_apt29s_rapidly_evolving_diplomatic_phishing_operations_2c27ca45-2f26-4cad-810d-8f6daf97e038/5d4bf026fad409_browsing79541efd2419ec0b042c8cf83bc1a61cbcc069efe0069ccd27XxX208Zip.zip?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Con tent-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230928%2F eu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230928T111438Z&X-Amz-Expires=600&X-Am z-Signature=16c1a10c52951c7e55233fcbaac5d8c8724754d307c7c59ce5d2f36c9a15d8a6&X-A mz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/backchannel_diplomacy_apt29s_rapidly_evolving_diplomatic_phishing_operations_2c27ca45-2f26-4cad-810d-8f6daf97e038/3a_browsing76182529c4fd5276091ed8ff4c4dcc89e4abc5981348a066c4eb34a9956947XxX201Lnk.lnk?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Con tent-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230928%2F eu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230928T111436Z&X-Amz-Expires=600&X-Am z-Signature=8540de3f3e5bd9f926521ae238de48ea6596fbab623363e6b44032b9f2f501df&X-A mz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/backchannel_diplomacy_apt29s_rapidly_evolving_diplomatic_phishing_operations_2c27ca45-2f26-4cad-810d-8f6daf97e038/1_browsing7cf399a9c5b2dbd55ebd6b5a4695a2f6aca6464abc7140f3c0e7a750c6117bdXxX199Html.html?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230928%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230928T111431Z&X-Amz-Expires=600&X-Amz-Signature=2ce3633ff8cbc843f2959b61c164891678fad8d993718b82cd8ca328de5ed4c7&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 10/09/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/backchannel_diplomacy_apt29s_rapidly_evolving_diplomatic_phishing_operations_2c27ca45-2f26-4cad-810d-8f6daf97e038/0e22e6a1dc529008d6228_browsing7cfddaed53c7f4cc698feec144f00c92594dc76d036XxX198Lnk.lnk?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230928%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230928T111430Z&X-Amz-Expires=600&X-Amz-Signature=f612be7ab68c493a9b1cf098d05c876a72789a7e2395dfae6a6d61efcc11e6ac&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/backchannel_diplomacy_apt29s_rapidly_evolving_diplomatic_phishing_operations_2c27ca45-2f26-4cad-810d-8f6daf97e038/e22bc_browsing75bb87e19554cd0f98c98b22a07368c2b23adacc41fe2cd68c20957d60aXxX183Lnk.lnk?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230928%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230928T111423Z&X-Amz-Expires=600&X-Amz-Signature=cd1daf925493bc6d58730c9331a7a7c734aa13723b6dc1f068ecf517c3fce43c&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/backchannel_diplomacy_apt29s_rapidly_evolving_diplomatic_phishing_operations_2c27ca45-2f26-4cad-810d-8f6daf97e038/46c8289301129c0833529495f4f3_browsing748b5adff78e18f1427654cb3b597352873eXxX171Pdf.pdf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230928%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230928T111422Z&X-Amz-Expires=600&X-Amz-Signature=cc4213581e636db8ec9f208cb1ef6074f131713ff76a0239ca92cb6da21eb0a5&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/backchannel_diplomacy_apt29s_rapidly_evolving_diplomatic_phishing_operations_2c27ca45-2f26-4cad-810d-8f6daf97e038/b6d26c5b2b2300fa8bf_browsing784919638ba849805896cf969c5c330668b350907c148XxX163Pdf.pdf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230928%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230928T111403Z&X-Amz-Expires=600&X-Amz-Signature=8a70329f0582c458c1e0bb877df27165034e69d12ed296bbc5bb006b27317f19&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/backchannel_diplomacy_apt29s_rapidly_evolving_diplomatic_phishing_operations_2c27ca45-2f26-4cad-810d-8f6daf97e038/302c0d553c9e_browsing7f2561864d79022b780a53ec0a5927e8962d883b88dde249d044XxX155Pdf.pdf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230928%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230928T111401Z&X-Amz-Expires=600&X-Amz-Signature=cf93189533a36fe1067046682dc54e4f29b9b932fc26f39a7c349632401e92d8&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/backchannel_diplomacy_apt29s_rapidly_evolving_diplomatic_phishing_operations_2c27ca45-2f26-4cad-810d-8f6daf97e038/4da5_browsing7027ffe7e32c891334d6834923bc17e4174c53ace4ff69de6410c24d84cbXxX154Dll.dll?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230928%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230928T111401Z&X-Amz-Expires=600&X-Amz-Signature=11878adb9fcd21b9f2f0d7f01301d382d4981d9687a1cf02b702b799496a1e37&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/backchannel_diplomacy_apt29s_rapidly_evolving_diplomatic_phishing_operations_2c27ca45-2f26-4cad-810d-8f6daf97e038/ae_browsing79aa17e6f3cc8e816e32335738b61b343e78c20abb8ae044adfeac5d97bf70XxX151Dll.dll?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230928%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230928T111401Z&X-Amz-Expires=600&X-Amz-Signature=f95301f6c0e89b35171a2ef081b7db8aee6fa87fe3bc936fa76465f002d712d0&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/backchannel_diplomacy_apt29s_rapidly_evolving_diplomatic_phishing_operations_2c27ca45-2f26-4cad-810d-8f6daf97e038/48_browsing75a9c4af3044db281c5dc02e5386c77f331e3b92e5ae79ff9961d8cd1f7c4fXxX134Svg.svg?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230928%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230928T111358Z&X-Amz-Expires=600&X-Amz-Signature=20933e77c3123303f023d703daf790dce28aea7033c3f0c886ea2d8daa470e61&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/backchannel_diplomacy_apt29s_rapidly_evolving_diplomatic_phishing_operations_2c27ca45-2f26-4cad-810d-8f6daf97e038/a8ae10b43cbf4e3344e0184b33a699b19a29866bc1e41201ace1a995e8ca3149_browsingXxX132Lnk.lnk?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230928%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230928T111357Z&X-Amz-Expires=600&X-Amz-Signature=2282695be7704b9ed56cc481334cacd487a5f7a530d4c49b69358f25cd554e85&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/backchannel_diplomacy_apt29s_rapidly_evolving_diplomatic_phishing_operations_2c27ca45-2f26-4cad-810d-8f6daf97e038/d_browsing7bda5e39327fe12b0c1f42c8e27787f177a352f8eebafbe35d3e790724eceffXxX131Dll.dll?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230928%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230928T111351Z&X-Amz-Expires=600&X-Amz-Signature=e54f83125a25fd70e9509905617e1465de2a988c9c941d6f69bb8be4332add70&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 10/09/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/backchannel_diplomacy_apt29s_rapidly_evolving_diplomatic_phishing_operations_2c27ca45-2f26-4cad-810d-8f6daf97e038/7fc9e830_browsing756e23aa4b050f4ceaeb2a83cd71cfc0145392a0bc03037af373066bXxX130Dll.dll?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230928%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230928T111351Z&X-Amz-Expires=600&X-Amz-Signature=033f1da131436e2445daa7cc65f52e616eedc7b9082a2474c7d5bce7cb5a5ece&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/backchannel_diplomacy_apt29s_rapidly_evolving_diplomatic_phishing_operations_2c27ca45-2f26-4cad-810d-8f6daf97e038/4_browsing7e8f705febc94c832307dbf3e6d9c65164099230f4d438f7fe4851d701b580bXxX129Html.html?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230928%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230928T111343Z&X-Amz-Expires=600&X-Amz-Signature=abc4b6a8232409e7c6e499fb00806732e74361573ff03965461b5f0b3c189950&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/backchannel_diplomacy_apt29s_rapidly_evolving_diplomatic_phishing_operations_2c27ca45-2f26-4cad-810d-8f6daf97e038/79a1402bc_browsing77aa2702dc5dca660ca0d1bf08a2923e0a1018da70e7d7c31d9417fXxX128Iso.iso?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230928%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230928T111338Z&X-Amz-Expires=600&X-Amz-Signature=5e36300735a0b5187e0655408f7289d97931e4b746fb44c45402eab32c2a6e2f&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/backchannel_diplomacy_apt29s_rapidly_evolving_diplomatic_phishing_operations_2c27ca45-2f26-4cad-810d-8f6daf97e038/60d96d8d3a09f822ded0a3c84194a5d88ed62a9_browsing79cbb6378545b45b04353bb37XxX127Dll.dll?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230928%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230928T111338Z&X-Amz-Expires=600&X-Amz-Signature=c27203195ef17019ea05b0f78401b2b0215685e9c0c405bb4d465e7aa14bbcde&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-28	Backchannel Diplomacy APT29s Rapidly Evolving Diplomatic Phishing Operations	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/backchannel_diplomacy_apt29s_rapidly_evolving_diplomatic_phishing_operations_2c27ca45-2f26-4cad-810d-8f6daf97e038/a42dd6bea439b_browsing79db90067b84464e755488b784c3ee2e64ef169b9dcdd92b069XxX119Dll.dll?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230928%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230928T111336Z&X-Amz-Expires=600&X-Amz-Signature=b9f5b353c461854a6c7ad016a7077aa34eb4fcdc1f86197acbad63341012a1f6&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-28	A multi-ransomware cybercriminal group	e9_edr7bdf7fafb1cb2a2bf0a4e14f51e18a34f3ff2f6f7b99731e93070d50801befXxX236Exe.ex e	Endpoint Security	88E1000GMSYS	Blocked
2023-09-28	A multi-ransomware cybercriminal group	4f4864a1d5f19a3c5552d80483526f341349_edr7835549dce8c61fef116b666fa09XxX246Dll.dll	Endpoint Security	88E1000GMSYS	Penetrated
2023-09-28	A multi-ransomware cybercriminal group	606bd_edr75ed9d2d6107ea7ee67063d1761a99f2fb5e932c8344d11395d24587dd6XxX243Exe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-09-28	A multi-ransomware cybercriminal group	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/a_multi-ransomware_cybercriminal_group_756a8cbd-3ebf-476b-907c-f0321ede760f/43c3b5dbc18ebbc55c12_browsing7d197255446d5f3e074fdac37f3e901b718acbe7c833XxX247Exe.exe? X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230928%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230928T110915Z&X-Amz-Expires=600&X-Amz-Signature=e26cd43b17f2b7c3566508f539fceb6a9997230ef9ee0dc30ef3f014e944a030&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-28	A multi-ransomware cybercriminal group	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/a_multi-ransomware_cybercriminal_group_756a8cbd-3ebf-476b-907c-f0321ede760f/3cc_browsing739bb1882fc9dbb056f39ebe4965771aeca0ceb44e85da39d1ba7dade693fXxX242Exe.exe? X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230928%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230928T110908Z&X-Amz-Expires=600&X-Amz-Signature=1c141987ef844c42a49b763aed7efa545ce4c438fce64c3e140c7bed89d631ee&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-28	A multi-ransomware cybercriminal group	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/a_multi-ransomware_cybercriminal_group_756a8cbd-3ebf-476b-907c-f0321ede760f/90cdcf54bbaeb9c5c4afc9b_browsing74b48b13e293746ee8858c033fc9d365fd4074018XxX239Dll.dll? X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230928%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230928T110905Z&X-Amz-Expires=600&X-Amz-Signature=9b05a67391b9f2fa67ec64d303f8835f3b8934fd29a7f9cc8a77544621c42994&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-27	GOLD MELODY Profile of an Initial Access Broker	fd544bda416f0819df01b45_edr7d42888af64f2652fd9a907fd4cfc129a5556e97bXxX267Pl.pl	Endpoint Security	88E1000GMSYS	Blocked
2023-09-27	GOLD MELODY Profile of an Initial Access Broker	5d5fa365498651bcbb8a356cd580b255cd4fd_edr735e59f81d0c595b06ee61ad10XxX286Exe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-09-27	GOLD MELODY Profile of an Initial Access Broker	hxxp://64.190.113.185	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 10/09/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-09-27	GOLD MELODY Profile of an Initial Access Broker	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/gol d_melody_profile_of_an_initial_access_broker_143aa500-b32d-43ca-93ca-45aa9dbf76e c/a3d5ead160614336a013f5de4cff65a5198b1d_browsing73238a5b456f558e70b503f52eXxX28 2Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD& X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230927%2Feu-west-1%2Fs3%2Faws4_request &X-Amz-Date=20230927T093322Z&X-Amz-Expires=600&X-Amz-Signature=214558edf33a935e4 e21167a70d95bde26a782b4dc37fb35021f74fbb991fb61&X-Amz-SignedHeaders=host&x-id=Ge tObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-27	Gallium APT Group Suspected To Be Behind Southeast Asian Government Attacks	9,242,846,351a65655e93ed2aeaf36b535ff5b_edr79ddf76c33d54089d9005a66265bXxX799Exe.exe	Endpoint Security	88E1000GMSYS	Penetrated
2023-09-27	Gallium APT Group Suspected To Be Behind Southeast Asian Government Attacks	9a9d1609592abe039324da2a8a69c4a305ca999920bf6bbef8392_edr73516783aXxX793Aspx.aspx	Endpoint Security	88E1000GMSYS	Blocked
2023-09-27	Gallium APT Group Suspected To Be Behind Southeast Asian Government Attacks	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/gal lium_apt_group_suspected_to_be_behind_southeast_asian_government_attacks_6a307a0 1-1160-4385-a86f-96036b7efe1d/c_browsing74897b1e986e2876873abb3b5069bf1b103667f7 f0e6b4581fbda3fd647a74aXxX807Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Cont ent-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230927%2Fe u-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230927T092752Z&X-Amz-Expires=600&X-Amz - Signature=0a36b6958e76631369bb870b47fcc695d93da0f15dd88798deffb80f6cf72048&X-Am z-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-27	Gallium APT Group Suspected To Be Behind Southeast Asian Government Attacks	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/gal lium_apt_group_suspected_to_be_behind_southeast_asian_government_attacks_6a307a0 1-1160-4385-a86f-96036b7efe1d/225e5818dc_browsing7e7b23110f64fbb718c1792ad93ba7e b893bfbee96cdb13180fbf7XxX805Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Cont ent-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230927%2Fe u-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230927T092751Z&X-Amz-Expires=600&X-Amz - Signature=db575a069c66f9d2f82ed646d457c31383405d0cfea378881026d349cd983185&X-Am z-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-27	Gallium APT Group Suspected To Be Behind Southeast Asian Government Attacks	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/gal lium_apt_group_suspected_to_be_behind_southeast_asian_government_attacks_6a307a0 1-1160-4385-a86f-96036b7efe1d/5aa035ebc3359ee851_browsing7d99569c8881fcb7f48ab7e 9a2f101f7e7ec23e636c79bXxX803Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Cont ent-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230927%2Fe u-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230927T092746Z&X-Amz-Expires=600&X-Amz - Signature=38b8dbf835518efa89beb2c5e62b13d86245a1a906f0a0fce4f177f606f1504b&X-Am z-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-27	Gallium APT Group Suspected To Be Behind Southeast Asian Government Attacks	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/gal lium_apt_group_suspected_to_be_behind_southeast_asian_government_attacks_6a307a0 1-1160-4385-a86f-96036b7efe1d/bd5dcf5911f959dd_browsing79de046d151e8a4aed3b854a3 22135acc37e3edb3643d0e2XxX801Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Cont ent-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230927%2Fe u-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230927T092746Z&X-Amz-Expires=600&X-Amz - Signature=f88f7cfab6a342fe144e6990aabfc6e669699a3bcb484b14ba98cf7e17b35802&X-Am z-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-27	Gallium APT Group Suspected To Be Behind Southeast Asian Government Attacks	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/gal lium_apt_group_suspected_to_be_behind_southeast_asian_government_attacks_6a307a0 1-1160-4385-a86f-96036b7efe1d/4cb020a66fdbc99b0bce2ae24d5684685e2b1e9219fbdfda56 b3aace4e8d5f66_browsingXxX797Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Cont ent-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230927%2Fe u-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230927T092744Z&X-Amz-Expires=600&X-Amz - Signature=b1d6d9e314b9a409ad5ffd79c34b57dd62b9c9f07f8351baf831d3c11f3e505c&X-Am z-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-27	Gallium APT Group Suspected To Be Behind Southeast Asian Government Attacks	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/gal lium_apt_group_suspected_to_be_behind_southeast_asian_government_attacks_6a307a0 1-1160-4385-a86f-96036b7efe1d/36e661edc1ad4e44ba38d8f_browsing7a6bd00c2b4bc32e9f ae8b955b1b4c6355aa6abedXxX795Aspx.aspx?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Co ntent-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230927%2 Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230927T092743Z&X-Amz-Expires=600&X-A mz-Signature=baf8797c208ccadfbd4cad97f7635064200da11f2642bb71b3bfb1083c11d292&X- Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-27	Gallium APT Group Suspected To Be Behind Southeast Asian Government Attacks	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/gal lium_apt_group_suspected_to_be_behind_southeast_asian_government_attacks_6a307a0 1-1160-4385-a86f-96036b7efe1d/c1f43b_browsing7cf46ba12cfc1357b17e4f5af408740af7a e70572c9cf988ac50260ce1XxX791Aspx.aspx?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Co ntent-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230927%2 Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230927T092741Z&X-Amz-Expires=600&X-A mz-Signature=4706a09a5104721cff8c5ed7ef92e6092d0fea475be7e068a42c1144a6a3415d&X- Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-24	OilRigs Outer Space and Juicy Mix Same olrig new drill pipes	64,156f9ca51951a9bf91b5b_edr74073d31c16873ca60492c25895c1f0f074787345XxX14Exe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-09-24	OilRigs Outer Space and Juicy Mix Same olrig new drill pipes	8a8a_edr7a506fd57bde314ce6154f2484f280049f2bda504d43704b9ad412d5d618XxX15Doc.doc	Endpoint Security	88E1000GMSYS	Blocked

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

TLP:AMBER

GLESEC
COMPLETELY PERCEPTI

ASM-VP REPORT

Organo Judicial 10/09/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-09-24	OilRigs Outer Space and Juicy Mix Same olrig new drill pipes	6,013d_edr7e0c4a54c78c846836da9e70785b3b8ca1f0b9d76fa88129baa5a4805dcXxX19Exe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-09-24	OilRigs Outer Space and Juicy Mix Same olrig new drill pipes	5_edr7fd32c39c64d9f58846fa91b19c3086b66b0e733ebbc30f917a1f5063389691XxX16Exe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-09-21	Kmrox Ransomware	82,881ebbc_edr7c5599d1e98006d7e97106a87983b78eeca0a7cdcdddfff981e0a87XxX1Exe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-09-21	StopRansomware Snatch Ransomware CISA	965cb8ee38adedd9ba06bdad9220a35890c2df0e4c_edr78d0559cd6da653bf740fXxX5Bat.bat	Endpoint Security	88E1000GMSYS	Penetrated
2023-09-21	StopRansomware Snatch Ransomware CISA	510e9fa38a08d446189c34fe6125295f410b36f00aceb65e_edr7b4508e9d7c4e1d1XxX13Exe.exe	Endpoint Security	88E1000GMSYS	Penetrated
2023-09-21	StopRansomware Snatch Ransomware CISA	25,142_edr7c578eaa814f07037fbe6e388b3bc86ed3800d7887c9d24e7b94176e30dXxX16Bat.bat	Endpoint Security	88E1000GMSYS	Penetrated
2023-09-21	StopRansomware Snatch Ransomware CISA	6c9d8c5_edr77dddf9cc480f330617e263a6ee4461651b4dec1f7215bda77df911e7XxX18Bat.bat	Endpoint Security	88E1000GMSYS	Penetrated
2023-09-21	StopRansomware Snatch Ransomware CISA	Extra_edrSample50Bat.bat	Endpoint Security	88E1000GMSYS	Penetrated
2023-09-21	StopRansomware Snatch Ransomware CISA	b998a8c15cc19c8c31c89b30f692a40b14d_edr7a6c09233eb976c07f19a84eccb40XxX21Bat.bat	Endpoint Security	88E1000GMSYS	Penetrated
2023-09-21	StopRansomware Snatch Ransomware CISA	a80c_edr7fe1f88cf24ad4c55910a9f2189f1eedad25d7d0fd53dbfe6bdd68912a84XxX20Bat.bat	Endpoint Security	88E1000GMSYS	Penetrated
2023-09-21	StopRansomware Snatch Ransomware CISA	a201f_edr7f81277e28c0bdd680427b979aee70e42e8a98c67f11e7c83d02f8fe7aeXxX11Exe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-09-21	StopRansomware Snatch Ransomware CISA	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/stopransomware_snatch_ransomware_cisa_773b69b9-0bcc-40e5-84fc-c1a0daecc85d/2155a029a024a2ffa4eff9108ac15c_browsing7db527ca1c8f89ccfd94cc3a70b77cfc57XxX15Bat.bat?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230921%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230921T112656Z&X-Amz-Expires=600&X-Amz-Signature=de21f04313f50f511302692c29392f193f1195ca0e0bde842ae9bf9d614a0b49&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-21	StopRansomware Snatch Ransomware CISA	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/stopransomware_snatch_ransomware_cisa_773b69b9-0bcc-40e5-84fc-c1a0daecc85d/28e82f28d0b9eb6a53d22983e21a9505ada925ebb61382fabebd_browsing76b8c4acff7cXxX9Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230921%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230921T112644Z&X-Amz-Expires=600&X-Amz-Signature=5b26d1951b025c404a92d8fe914a0312997f7fe8218ca2456fca45c9ababc305&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-21	StopRansomware Snatch Ransomware CISA	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/stopransomware_snatch_ransomware_cisa_773b69b9-0bcc-40e5-84fc-c1a0daecc85d/5950b4e2_browsing7554585123d7fca44e83169375c6001201e3bf26e57d079437e70bcdXxX7Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230921%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230921T112636Z&X-Amz-Expires=600&X-Amz-Signature=757b08e503446515c5707cbf9e7fef098e40aafb151b7118c7781475c0168776&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-21	Cert IL Alert - Medical institutions in Israel are under attack - v2	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/cert_il_alert_-_medical_institutions_in_israel_are_under_attack_46905b20-ed73-4bcc-a2e1-51a616849b56/d34c981c4e6504c2ae9065a1bc324a1_browsing706890c263f7f6704e8327bede1bc4370XxX2Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230921%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230921T105537Z&X-Amz-Expires=600&X-Amz-Signature=661d31e5ec1585ac274fd6a4b49f0235784dc07a386c2f53c3a829b1a968c8a5&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-21	Cert IL Alert - Medical institutions in Israel are under attack - v2	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/cert_il_alert_-_medical_institutions_in_israel_are_under_attack_46905b20-ed73-4bcc-a2e1-51a616849b56/2f8a32618e3a0c63350ae6fb2c4cd334e3_browsing770d395eafe622988a62688dc76cf9XxX1Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230921%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230921T105531Z&X-Amz-Expires=600&X-Amz-Signature=87f71e3751fe7047f81bf8722eba1a54c8fdf047a189189906fbd7672b149b7b&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-20	Cert IL Alert - Medical institutions in Israel are under attack	Freeworldbgjfcaaaeg1_edrExe.exe	Endpoint Security	88E1000GMSYS	Penetrated
2023-09-20	Cert IL Alert - Medical institutions in Israel are under attack	Freeworldbgjfcaaaeg2_edrExe.exe	Endpoint Security	88E1000GMSYS	Blocked

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

TLP:AMBER

GLESEC
COMPLETELY PERCEPTI

ASM-VP REPORT

Organo Judicial 10/09/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-09-20	ShroudedSnooper Targets Telecommunications Firms In The Middle East With Custom Backdoors	38_edr75ed58c0d42e05c83843b32ed33d6ba5e94e18ffe8fb1bf34fd7dedf3f82a7XxX79Exe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-09-20	ShroudedSnooper Targets Telecommunications Firms In The Middle East With Custom Backdoors	1,146b1f38e420936b_edr7c5f6b22212f3aa93515f3738c861f499ed1047865549cbXxX75Exe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-09-20	ShroudedSnooper Targets Telecommunications Firms In The Middle East With Custom Backdoors	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/shroudedsnooper_targets_telecommunications_firms_in_the_middle_east_with_custom_backdoors_4b05b247-3c9e-469a-a7b7-ea9d4bac8ef6/c5b4542d61af_browsing74cf7454d7f1c8d96218d709de38f94ccfa7c16b15f726dc08c0XxX77Dll.dll?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230920%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230920T105004Z&X-Amz-Expires=600&X-Amz-Signature=39dcbb3643f351b4262a3652c1c864b80731b92d37dca25f36a954d30d5f3afa&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-20	ShroudedSnooper Targets Telecommunications Firms In The Middle East With Custom Backdoors	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/shroudedsnooper_targets_telecommunications_firms_in_the_middle_east_with_custom_backdoors_4b05b247-3c9e-469a-a7b7-ea9d4bac8ef6/911_browsing7bd328e37be121fb497596a2d0619a0eaca44752a1854523b8af46a5b0cebXxX73Dll.dll?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230920%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230920T105003Z&X-Amz-Expires=600&X-Amz-Signature=ef664896db60b115211bcc942692b3dd694fa2cd1dd7020cfc0bb4b6d1c45f5b&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-20	ShroudedSnooper Targets Telecommunications Firms In The Middle East With Custom Backdoors	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/shroudedsnooper_targets_telecommunications_firms_in_the_middle_east_with_custom_backdoors_4b05b247-3c9e-469a-a7b7-ea9d4bac8ef6/7495c1ea421063845eb8f4599a1c1_browsing7c105f700ca0671ca874c5aa5aef3764c1cXxX71Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230920%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230920T105002Z&X-Amz-Expires=600&X-Amz-Signature=1eb5f9219c980732ea0fcf8609554658774943847839c4b25a5cd4a49e7d9cd8&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-20	ShroudedSnooper Targets Telecommunications Firms In The Middle East With Custom Backdoors	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/shroudedsnooper_targets_telecommunications_firms_in_the_middle_east_with_custom_backdoors_4b05b247-3c9e-469a-a7b7-ea9d4bac8ef6/e1ad1_browsing73e49eee1194f2a55afa681cef7c3b8f6c26572f474dec7a42e9f0cdc9dXxX69Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230920%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230920T105001Z&X-Amz-Expires=600&X-Amz-Signature=149b13237343a220b354a6063a0aec53a57da44ebaac0ba4e409988ff117c28d&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-19	PSA Ongoing Webex malvertising campaign drops BatLoader	7a1245584c0a12186aa_edr7228c75a319ca7f57e7b0db55c1bd9b8d7f9b397bfac8XxX11Exe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-09-19	EV Certificates Abused To Deliver RedLine Vidar And Knight Ransomware	9,123e42cdd3421e8f2_edr76ac711988fb8a8929172fa76674ec4de230e6d528d09aXxX4Exe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-09-19	EV Certificates Abused To Deliver RedLine Vidar And Knight Ransomware	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ev_certificates_abused_to_deliver_redline_vidar_and_knight_ransomware_bce1d28b-06b4-4b1e-bc88-6c40a4549b92/a6258d_browsing70bc0b5d5c87368c5024d3f23585790b14227b8c59333413082524a956XxX6Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230919%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230919T062225Z&X-Amz-Expires=600&X-Amz-Signature=1b9698ca742f9a88db1dc1c733151fed5df4718f09b50c31b8ea5649e90e36a2&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-15	Nazar: Spirits of the Past	Naz4_edrExe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-09-15	Nazar: Spirits of the Past	Naz3_edrExe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-09-15	Nazar: Spirits of the Past	Naz4_edrDll.dll	Endpoint Security	88E1000GMSYS	Blocked
2023-09-15	Nazar: Spirits of the Past	Naz2_edrDll.dll	Endpoint Security	88E1000GMSYS	Blocked
2023-09-15	Nazar: Spirits of the Past	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/nazarspiritsofthepast/Naz2_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-C ontent-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230915% 2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230915T121154Z&X-Amz-Expires=600&X- Amz-Signature=22293ea8c9f2415b7cd6c249c53ebeb00b9a59460403f53d23022c96f14e631b&X -Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-15	Nazar: Spirits of the Past	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/nazarspiritsofthepast/Naz3_browsingDll.dll?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-C ontent-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230915% 2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230915T121151Z&X-Amz-Expires=600&X- Amz-Signature=04f5d28521041e432d9cbc779c10ed7dea654358f5b33362276b5fbca57fbb62&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 10/09/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-09-15	Nazar: Spirits of the Past	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/naz arspiritsofthepast/Naz1_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-C ontent-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230915% 2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230915T121148Z&X-Amz-Expires=600&X- Amz-Signature=ab3173af0a47bef8be8b4489daf320f53238c27970b6f2561ce517cf07cbcc9d&X -Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-15	Nazar: Spirits of the Past	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/naz arspiritsofthepast/Naz1_browsingDll.dll?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-C ontent-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230915% 2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230915T121147Z&X-Amz-Expires=600&X- Amz-Signature=158df5494f7c049bb9e1fda31ce13b209a357a5d6a3c9bb0a4d2ca603bcdcb77&X -Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-15	Nazar: Spirits of the Past	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/naz arspiritsofthepast/Naz5_browsingDll.dll?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-C ontent-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230915% 2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230915T121141Z&X-Amz-Expires=600&X- Amz-Signature=dae47066b2dd4c5376a0bd2d1f72bfa2326ccd28d852292e7199debad35bd7ad&X -Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-15	New Ransomware Spotted - White Rabbit and It's Evasion Tactics	Whiterabbit2_edrDll.dll	Endpoint Security	88E1000GMSYS	Blocked
2023-09-15	New Ransomware Spotted - White Rabbit and It's Evasion Tactics	hxxps://104-168-132-128.nip.io	Web Gateway	88E1000GMSYS	Offline/Removed
2023-09-15	New Ransomware Spotted - White Rabbit and It's Evasion Tactics	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/new _ransomware_spotted_-_white_rabbit_and_it%27s_evasion_tactics_30ad417d-8d75-4a7f -8dab-ab2aeff0f3fb/Whiterabbit1_browsingDll.dll?X-Amz-Algorithm=AWS4-HMAC-SHA256 &X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F2 0230915%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230915T092124Z&X-Amz-Expire s=600&X-Amz-Signature=120e1402c921600728cf64a740cd9196ba7bb54d274c2601c75e0e9a67 e07560&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-15	8Base Ransomware - A Heavy Hitting Player	Eightbasebgiiacggfh1_edrExe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-09-15	8Base Ransomware - A Heavy Hitting Player	Eightbasebgiiacggfh3_edrExe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-09-15	8Base Ransomware - A Heavy Hitting Player	Eightbasebgiiacggfh2_edrExe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-09-15	8Base Ransomware - A Heavy Hitting Player	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/8ba se_ransomware_-_a_heavy_hitting_player_a5893f49-67e5-45ef-a151-6ce0c11c6ff8/Eigh tbasebgiiacggfh4_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230915%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230915T005515Z&X-Amz-Expires=600&X-Amz-Signature=a5756dc3e4d62755a91765b2576f6581dd3acbad096a01fe108ad17412999011&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Blocked
2023-09-14	DarkGate Loader Malware Delivered via Microsoft Teams	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/dar kgate_loader_malware_delivered_via_microsoft_teams_485ec643-39a1-477b-b544-d0247 d9421f3/bcd4494_browsing70626f4f34a15be00812f850c5e032723e35776fb4b9be6c7be6c891 3XxX214Lnk.lnk?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PA YLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230914%2Feu-west-1%2Fs3%2Faws4_r equest&X-Amz-Date=20230914T115412Z&X-Amz-Expires=600&X-Amz-Signature=dbe4a08554a 036ca294ac4f4b4e66d8e8f2dbacb97ab64763a2bdd5eccc3fc21&X-Amz-SignedHeaders=host&x - id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-14	DarkGate Loader Malware Delivered via Microsoft Teams	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/dar kgate_loader_malware_delivered_via_microsoft_teams_485ec643-39a1-477b-b544-d0247 d9421f3/4c21_browsing711de81bb5584d35e744394eed2f36fef0d93474dfc5685665a9e159eef 1XxX213Vbs.vbs?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PA YLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230914%2Feu-west-1%2Fs3%2Faws4_r equest&X-Amz-Date=20230914T115412Z&X-Amz-Expires=600&X-Amz-Signature=9ab0d0b3fbe 0114733ab894f538750a1678a5239af57ef18509594b7e2bb6fce&X-Amz-SignedHeaders=host&x - id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-14	DarkGate Loader Malware Delivered via Microsoft Teams	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/dar kgate_loader_malware_delivered_via_microsoft_teams_485ec643-39a1-477b-b544-d0247 d9421f3/1bcde4d4613f046b63e9_browsing70aa10ea2662d8aa7d326857128b59cb88484cce9a2 dXxX212Au3.au3?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PA YLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230914%2Feu-west-1%2Fs3%2Faws4_r equest&X-Amz-Date=20230914T115406Z&X-Amz-Expires=600&X-Amz-Signature=37c72b3bbe1 e4b7651d63c4147b336a12adcf25edf9ea3acfc50d361c78384c5&X-Amz-SignedHeaders=host&x - id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-14	DarkGate Loader Malware Delivered via Microsoft Teams	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/dar kgate_loader_malware_delivered_via_microsoft_teams_485ec643-39a1-477b-b544-d0247 d9421f3/0c59f568da43_browsing731e3212b6461978e960644be386212cc448a715dbf3f489d75 8XxX211Zip.zip?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PA YLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230914%2Feu-west-1%2Fs3%2Faws4_r equest&X-Amz-Date=20230914T115405Z&X-Amz-Expires=600&X-Amz-Signature=11efe483e24 6f6064c191aa73df36f374ebc0e83f33285719802c86820e22d59&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 10/09/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-09-14	DarkGate Loader Malware Delivered via Microsoft Teams	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/darkgate_loader_malware_delivered_via_microsoft_teams_485ec643-39a1-477b-b544-d0247d9421f3/09904d65e59f3fbbbf38932ae_browsing7bff9681ac73b0e30b8651ec567f7032a94234fXxX210Zip.zip?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230914%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230914T115404Z&X-Amz-Expires=600&X-Amz-Signature=29689673090d75527dcc20c8048655203a75750dbade8818b7fb3f9789a45151&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-14	Ransomware GandCrab poses as Super Mario	f30454bcc_edr7f1bc1f328b9b546f5906887fd0278c40d90ab75b8631ef18ed3b7fXxX5Exe.exe	Endpoint Security	88E1000GMSYS	Penetrated
2023-09-14	Ransomware GandCrab poses as Super Mario	hxxp://185.158.248.142	Web Gateway	88E1000GMSYS	Penetrated
2023-09-14	Ransomware GandCrab poses as Super Mario	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ransomware_gandcrab_poses_as_super_mario_a7882dde-c326-4ab6-a9c9-e583adbf360b/93dd4d_browsing7baf1e89d024c59dbffce1c4cbc85774a1b7bcc8914452dc8aa8a79a78XxX6Unkn.unk n?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230914%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230914T083226Z&X-Amz-Expires=600&X-Amz-Signature=3dcadd7b8dbb3611f71a41df7151d5a6a498ad4ef8763e26db970e728817510e&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-14	Ransomware GandCrab poses as Super Mario	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ransomware_gandcrab_poses_as_super_mario_a7882dde-c326-4ab6-a9c9-e583adbf360b/630b6f15c_browsing770716268c539c555815216800 4657beee740e73ee9966d6de1753fXxX4Exe.exe? X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230914%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230914T083222Z&X-Amz-Expires=600&X-Amz-Signature=48053d3221bb4f7d3f00e66b6521f0be42fbf0dba8ca9db3d51b86b9911a7aab&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-14	Ransomware GandCrab poses as Super Mario	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ransomware_gandcrab_poses_as_super_mario_a7882dde-c326-4ab6-a9c9-e583adbf360b/ec2a_browsing7e8da04bc4e60652d6f7cc2d41ec68ff900d39fc244cc3b5a29c42acb7a4XxX3Exe.exe? X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230914%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230914T083218Z&X-Amz-Expires=600&X-Amz-Signature=131ae8fd0214887cf4bad4f57585d012d5c737bc3eb3c74cebf4bda342dc761c&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-14	Ransomware GandCrab poses as Super Mario	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ransomware_gandcrab_poses_as_super_mario_a7882dde-c326-4ab6-a9c9-e583adbf360b/0c8c2_browsing7f06a0acb976b8f12ff6749497d4ce1f7a98c2a161b0a9eb956e6955362XxX2Png.png? X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230914%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230914T083217Z&X-Amz-Expires=600&X-Amz-Signature=3a1238ec33a36bb556a7883d74cb239d3187cd775c63dfc4d4378dca4d1bf4a2&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-14	Ransomware GandCrab poses as Super Mario	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/ransomware_gandcrab_poses_as_super_mario_a7882dde-c326-4ab6-a9c9-e583adbf360b/3849381059d9e8bbcc59c253d2cbe1c92f_browsing7e1f1992b752d396e349892f2bb0e7XxX1Xls.xls? X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230914%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230914T083214Z&X-Amz-Expires=600&X-Amz-Signature=088b28f20ba40deeb034485c58d29e4ae143ed1491fa609067b0c994ad9acebe&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-12	Analysis of Cuba ransomware gang activity and tooling	Analysisbgjeejbidb80_edrPs1.ps1	Endpoint Security	88E1000GMSYS	Blocked
2023-09-12	Analysis of Cuba ransomware gang activity and tooling	hxxp://217.79.243.148	Web Gateway	88E1000GMSYS	Offline/Removed
2023-09-12	Analysis of Cuba ransomware gang activity and tooling	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/analysis_of_cuba_ransomware_gang_activity_and_tooling_1d95ea70-5cb0-47cd-b0d6-96a82fa88cf9/Analysisbgjeejbidb83_browsingDll.dll?X-Amz-Algorithm=AWS4-HMAC-SHA256&X- Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230912%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230912T122234Z&X-Amz-Expires=600&X-Amz-Signature=11c13b2a8e6f225651aa7256ef68c3f45fb7933c5c03b54dc316197b6aec0c9d&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-12	Analysis of Cuba ransomware gang activity and tooling	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/analysis_of_cuba_ransomware_gang_activity_and_tooling_1d95ea70-5cb0-47cd-b0d6-96a82fa88cf9/Analysisbgjeejbidb82_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X- Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230912%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230912T122232Z&X-Amz-Expires=600&X-Amz-Signature=960d77f71cca95f64b6c853c5fb67e504e04e422a1e14b0fb6976f9114ac7c1a&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-12	Analysis of Cuba ransomware gang activity and tooling	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/analysis_of_cuba_ransomware_gang_activity_and_tooling_1d95ea70-5cb0-47cd-b0d6-96a82fa88cf9/Analysisbgjeejbidb81_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X- Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230912%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230912T122230Z&X-Amz-Expires=600&X-Amz-Signature=ad9b40df8ff1a707984021315a27281b75ad8ed8ff47e343751d68a7d653d805&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated

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

TLP:AMBER

ASM-VP REPORT

Organo Judicial 10/09/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-09-12	New Agent Tesla Variant Being Spread by Crafted Excel Document	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/new_agent_tesla_variant_being_spread_by_crafted_excel_document_a70e19dc-8084-4d29-a124-46eeb0a4fe8e/Newbgjeacdgbc38_browsingXls.xls?X-Amz-Algorithm=AWS4-HMAC-SHA25 6&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230912%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230912T080122Z&X-Amz-Expires=600&X-Amz-Signature=60ac79ba10f55470a00be00ea2ee98c8fa2dd9e4d9a3b8459977b15268746df1&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-12	New Agent Tesla Variant Being Spread by Crafted Excel Document	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/new_agent_tesla_variant_being_spread_by_crafted_excel_document_a70e19dc-8084-4d29-a124-46eeb0a4fe8e/Newbgjeacdgbc35_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA25 6&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230912%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230912T080119Z&X-Amz-Expires=600&X-Amz-Signature=121191ec0b6bd60f7e86390d7935bd4f7fc246344d206b30834f65c2b410856e&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-10	Mac users targeted in new malvertising campaign delivering Atomic Stealer	Macbgjebbhdei59_edrMacho.macho	Endpoint Security	88E1000GMSYS	Penetrated
2023-09-10	APT37 Distributes Backdoor Via Malicious LNK	Apt3_edr7bgjebdbddg5Html.html	Endpoint Security	88E1000GMSYS	Blocked
2023-09-10	APT37 Distributes Backdoor Via Malicious LNK	Apt3_edr7bgjebdbddg7Lnk.lnk	Endpoint Security	88E1000GMSYS	Blocked
2023-09-10	APT37 Distributes Backdoor Via Malicious LNK	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/apt37_distributes_backdoor_via_malicious_lnk_ee3688ed-d478-43de-9666-a047cb0a5445/Apt3_browsing7bgjebdbddg9Bat.bat?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230910%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230910T122655Z&X-Amz-Expires=600&X-Amz-Signature=941280c239fe7a923e8ed4fe66a0524c88c89561cdddce2fd2c0db7dbb3d9932&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated
2023-09-10	Multiple Nation-State Threat Actors Exploit CVE-2022-47966 and CVE-2022-42475	Multiplebgjebbgije4_edrExe.exe	Endpoint Security	88E1000GMSYS	Blocked
2023-09-10	Multiple Nation-State Threat Actors Exploit CVE-2022-47966 and CVE-2022-42475	hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/multiple_nation-state_threat_actors_exploit_cve-2022-47966_and_cve-2022-42475_0eb2b 3c2-ba42-463c-8922-732350ccc3c2/Multiplebgjebbgije2_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230910%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230910T075448Z&X-Amz-Expires=600&X-Amz-Signature=dbeef7e37304fc0d51180b26651807766d234847fff65f8bfbee9c3e4b92633c&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	88E1000GMSYS	Penetrated

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

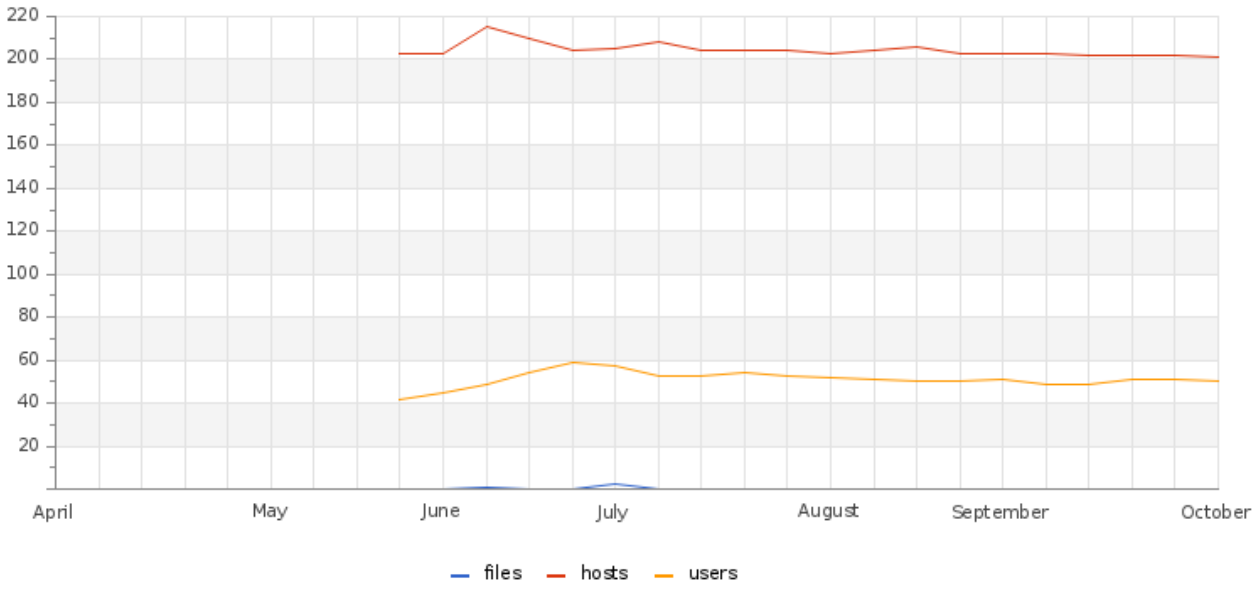
Threats

MSS-EDR

Average Threat - User Defined

77

Threat Score



Brute Force Detection by Ratio - User Defined

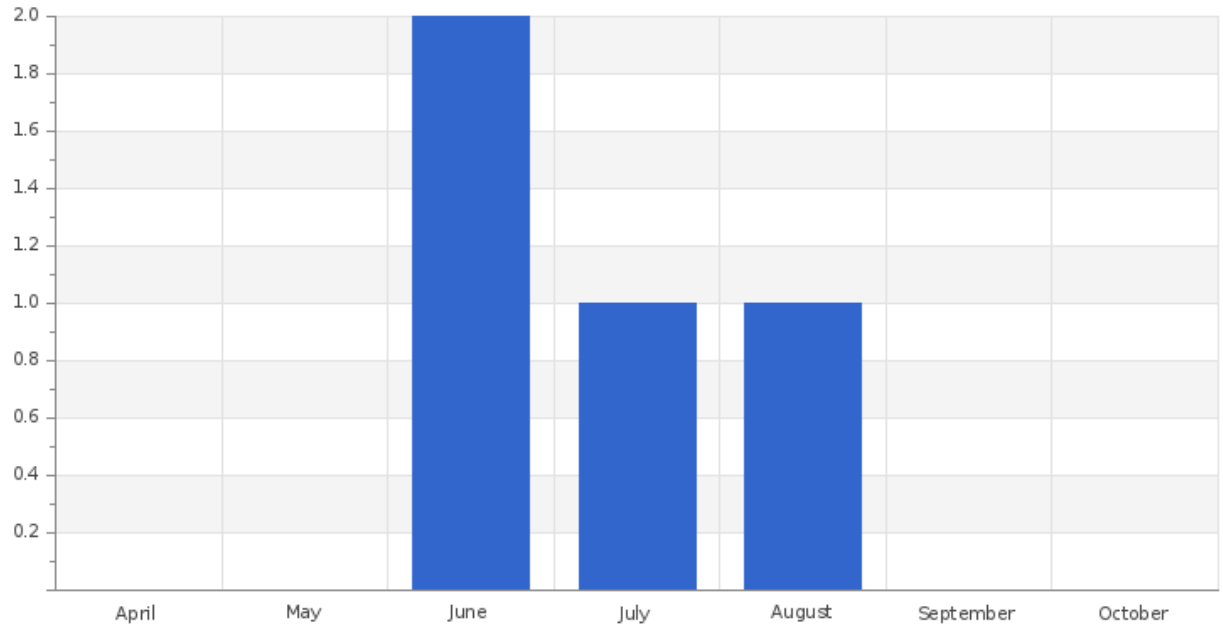
Host \ User Name	Ratio (Bad : Good)	Probability
88e0o21cq\administrador	39 : 141	0.28
88e0o20cq\administrador	1 : 76	0.01
88e0o21a5\administrador	1 : 1,365	0.00

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

ASM-VP REPORT

Organo Judicial 10/09/2023

Events



Total Hosts - User Defined

85

MSS-DDOS

Total Attacks over 24 hours

314,455

Critical Attacks over 24 hours

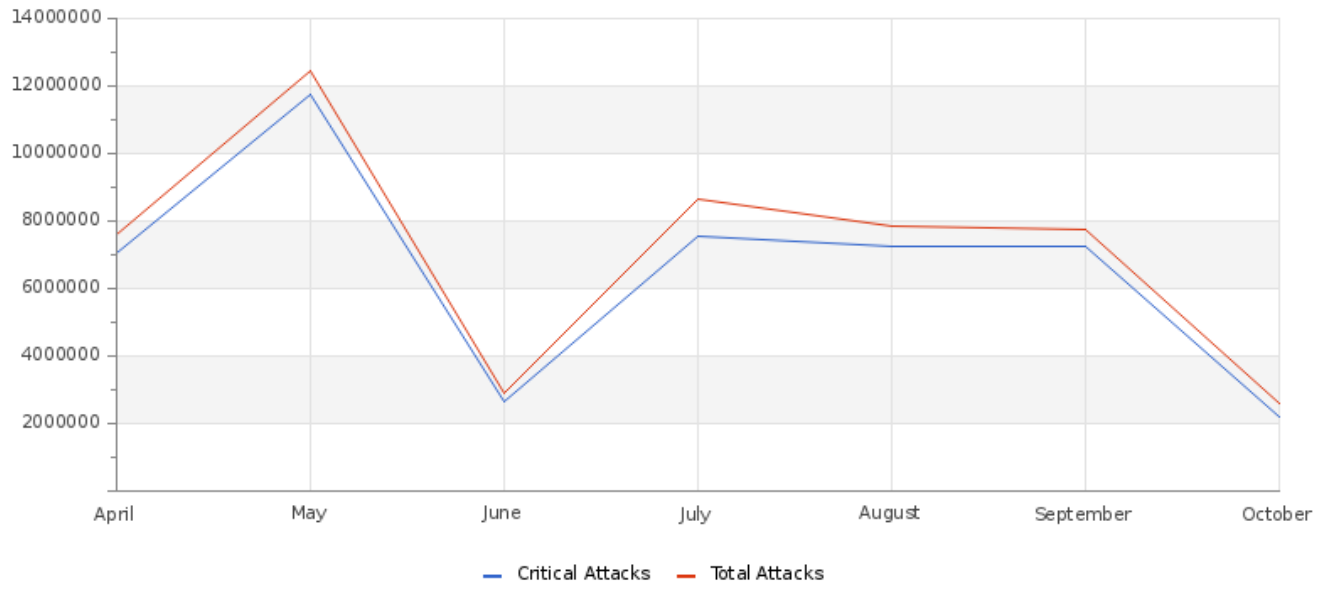
261,627

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

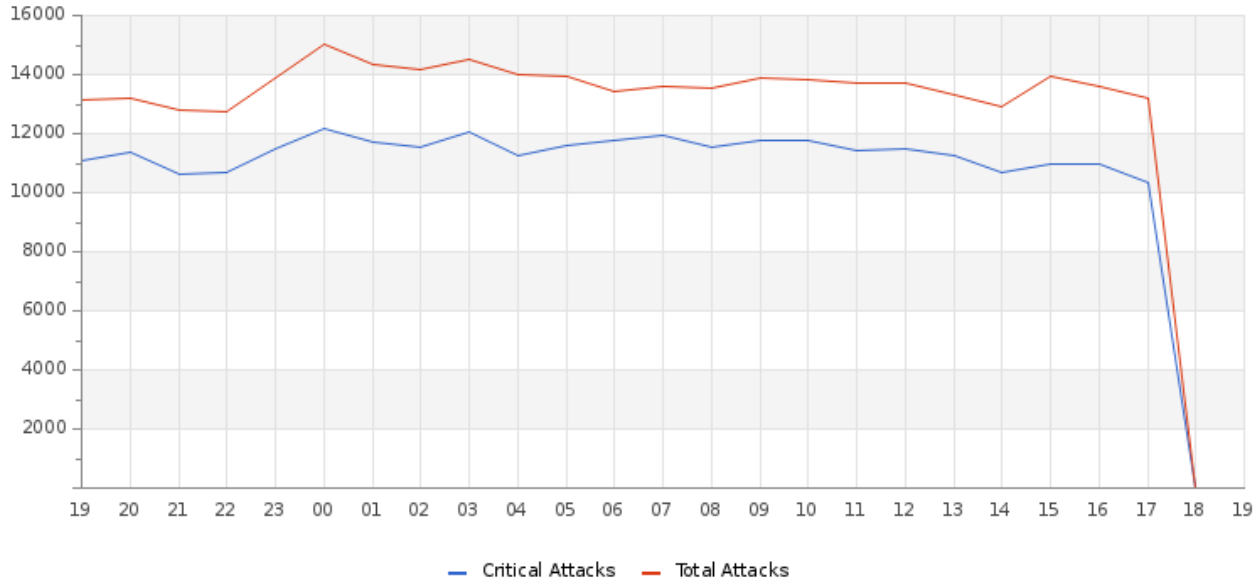
ASM-VP REPORT

Organo Judicial 10/09/2023

Total & Critical Attacks Per Month In Last 6 Months



Executive Summary - Critical and Total Attacks In Past 24 Hours

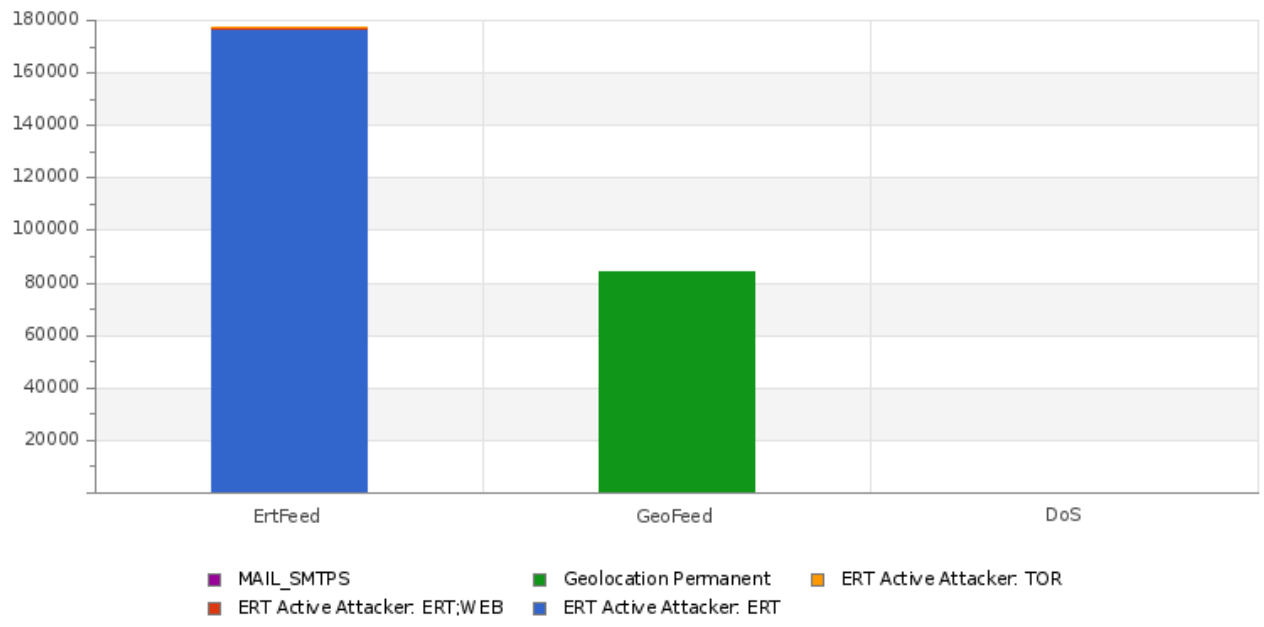


LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

ASM-VP REPORT

Organo Judicial 10/09/2023

Critical Attacks Blocked



Executive Summary - Most Common Attack Durations

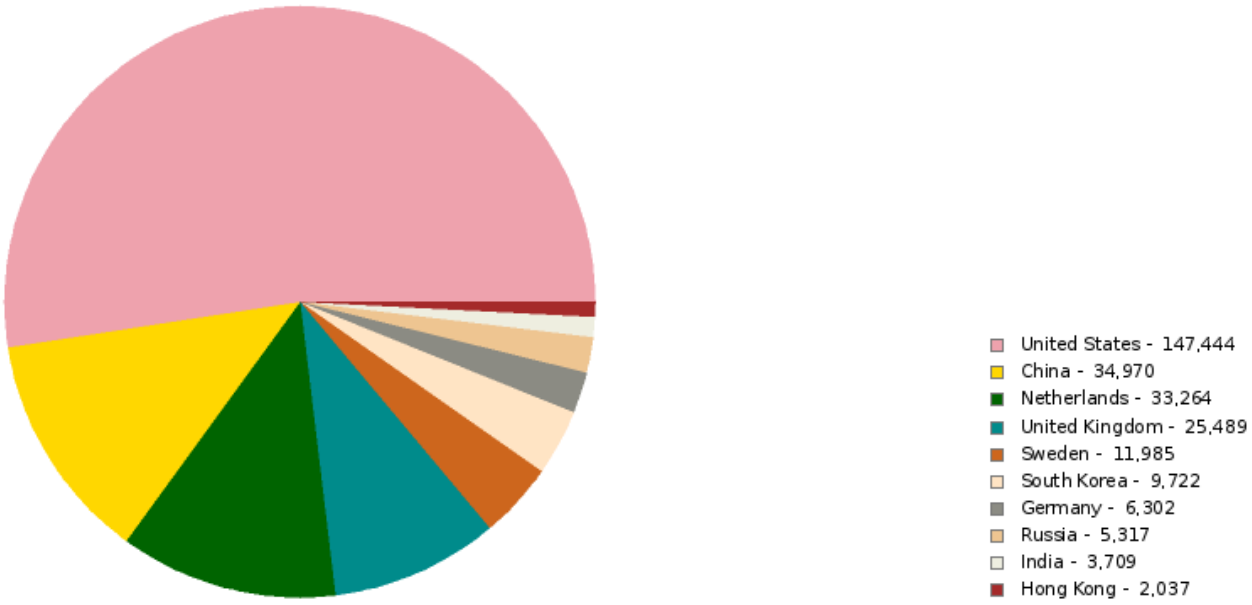
range	Access	Anomalies	Anti-Scanning	ErtFeed	GeoFeed
Less Than A Minute	0	2	4	38,930	0
One to Five Minutes	0	0	1	1,477	0
Thirty to Sixty Minutes	45	44	0	0	92
Ten to Thirty Minutes	1	7	0	0	46
Five to Ten Minutes	0	1	0	4	0

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

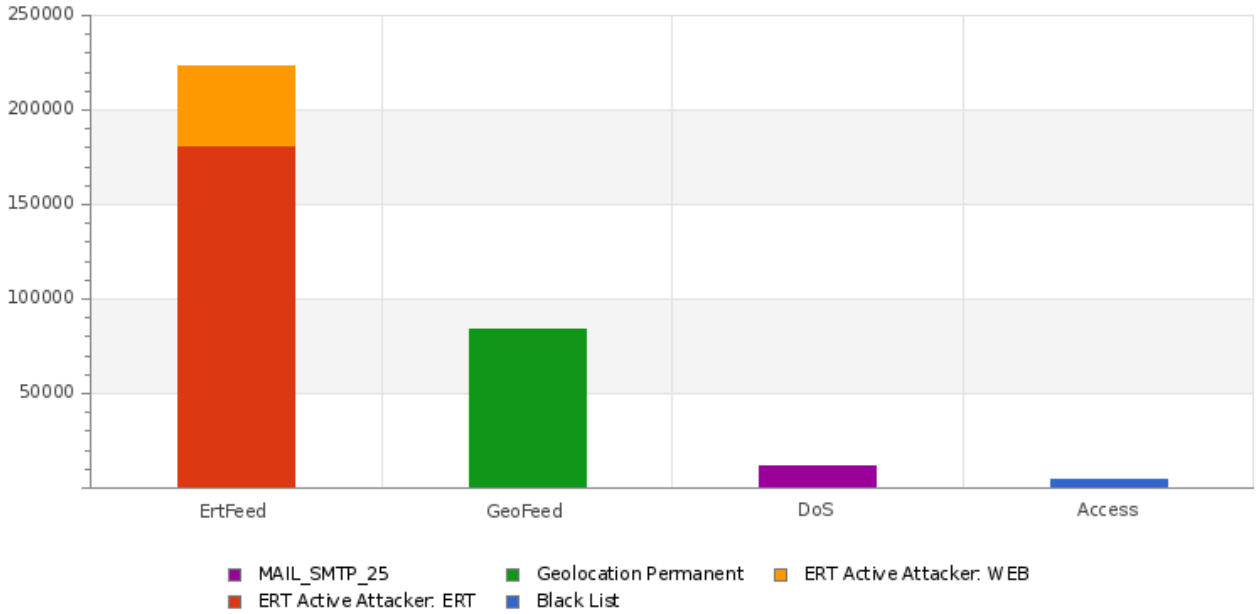
ASM-VP REPORT

Organo Judicial 10/09/2023

Executive Summary - Top Attacking Countries



Types of Blocked Attacks

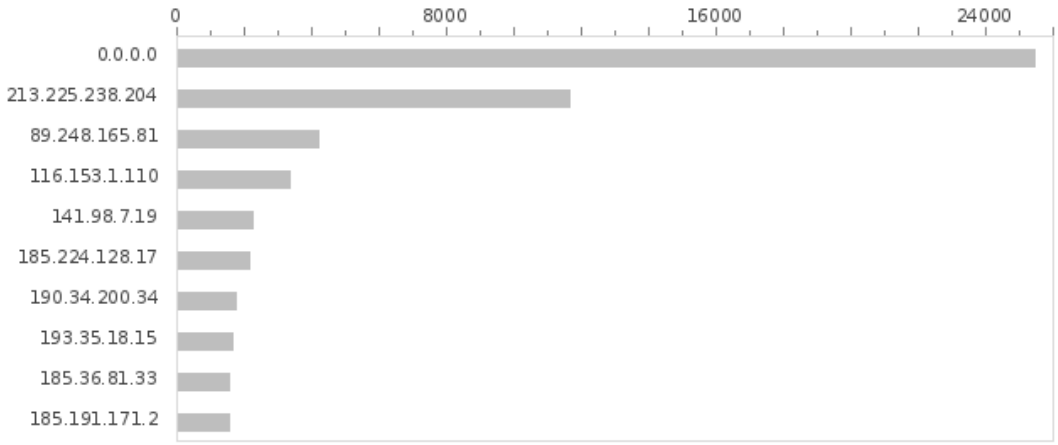


LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

ASM-VP REPORT

Organo Judicial 10/09/2023

Top Attack Sources



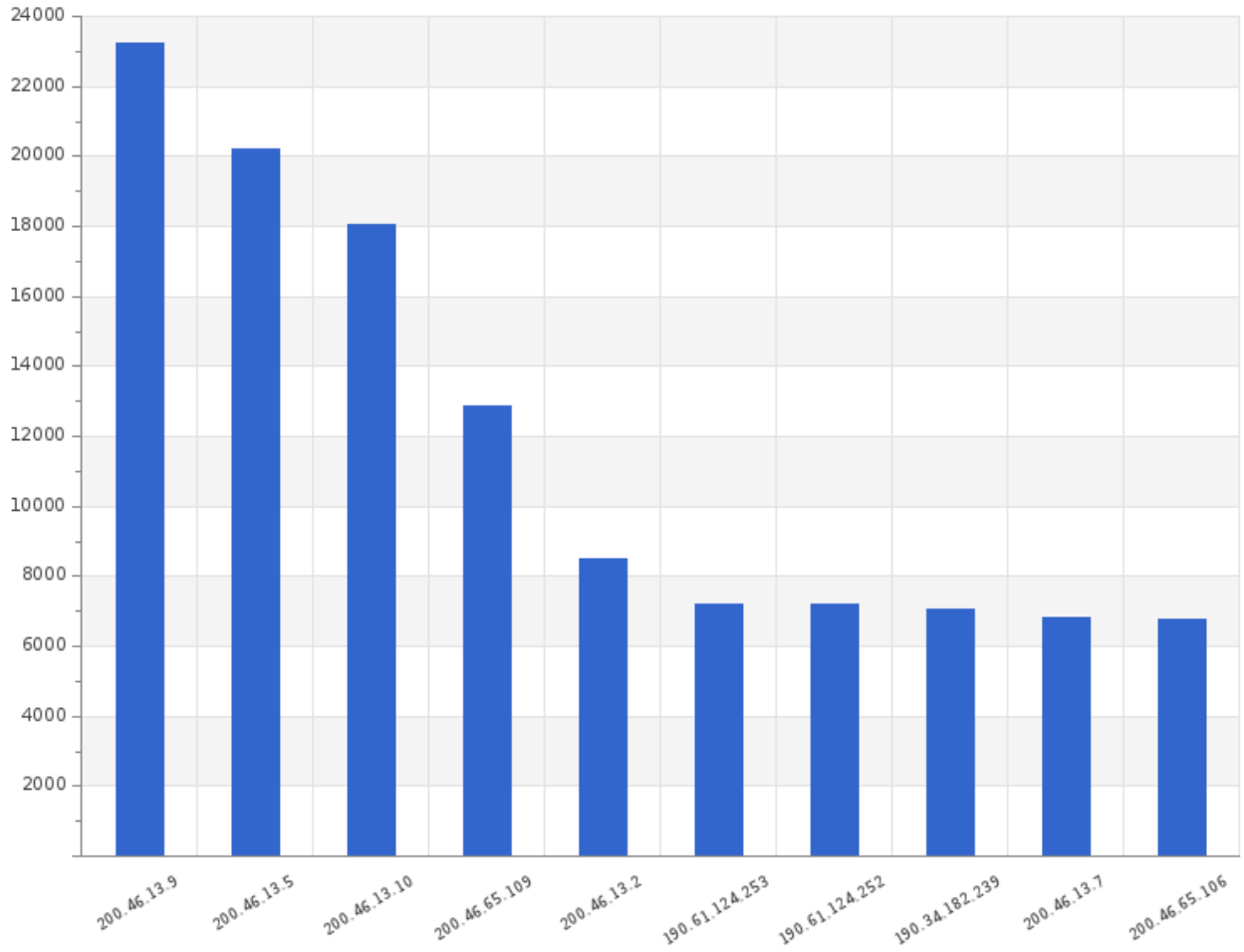
Top Assets Protected

LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

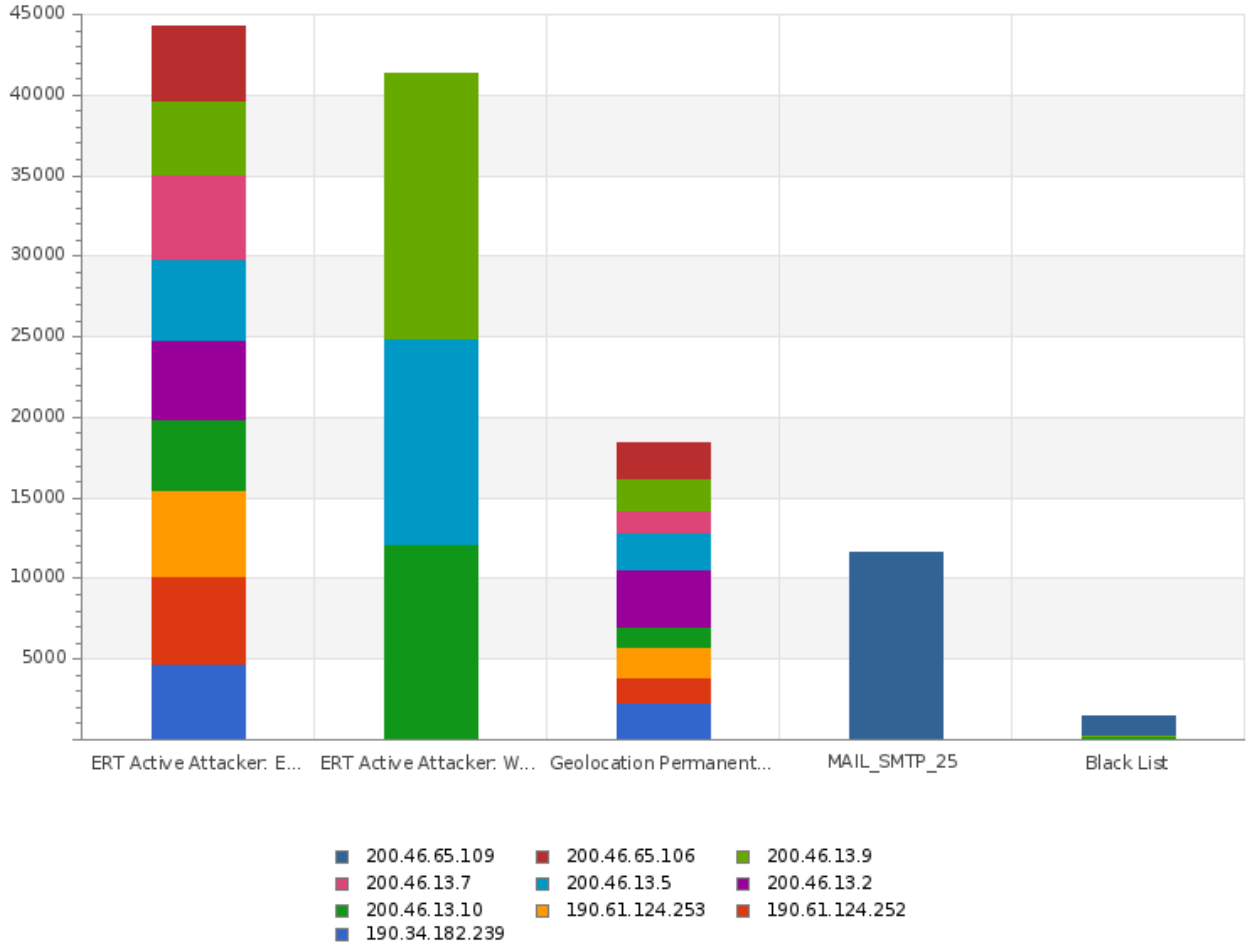
ASM-VP REPORT

Organo Judicial 10/09/2023



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

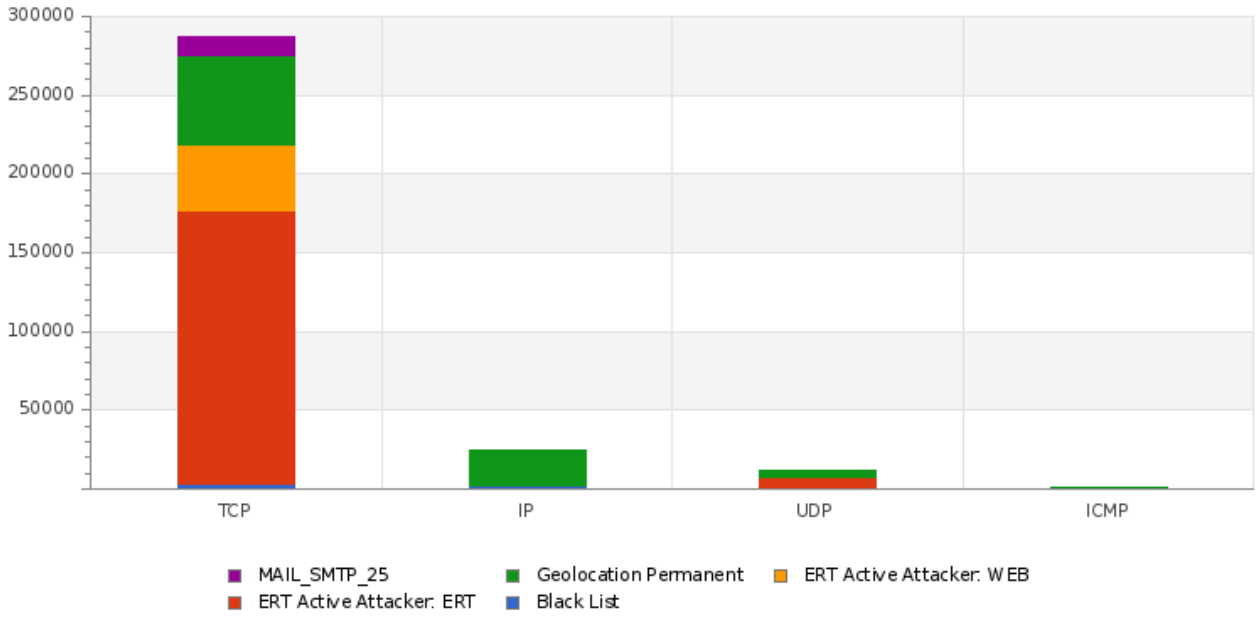
Top Attack Type Per Protected Asset



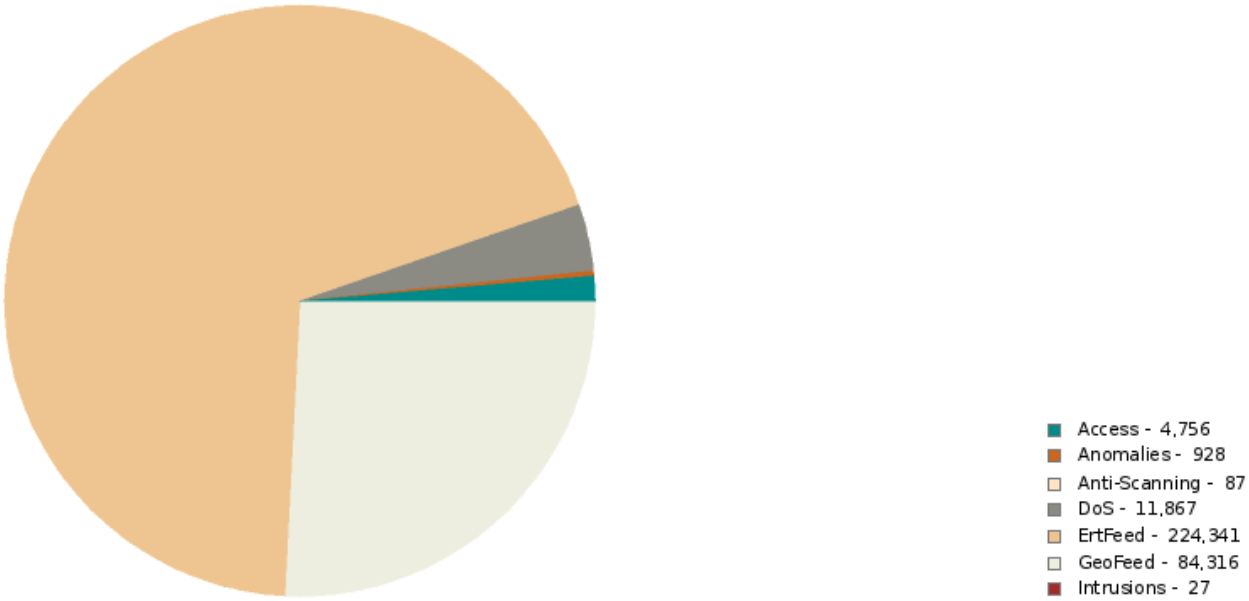
ASM-VP REPORT

Organo Judicial 10/09/2023

Top Blocked DDOS Types



Executive Summary - Types of Blocked Attacks



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

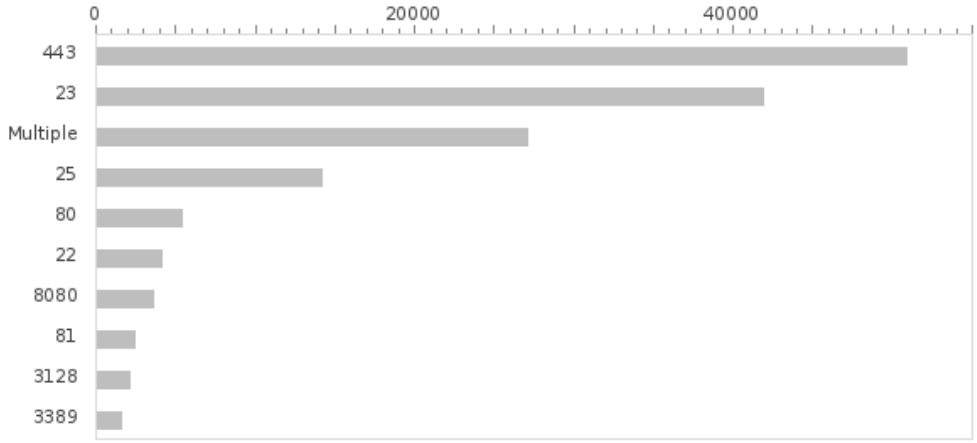
ASM-VP REPORT

Organo Judicial 10/09/2023

Executive Summary - Total Bandwidth/Packet Count by Attack Type

Category	MB/s	KB/s
ErtFeed	7.64	7,827.51
GeoFeed	3.70	3,792.41
DoS	0.51	521.19
Access	0.18	186.77
Anomalies	0.08	83.17
Anti-Scanning	0.04	40.07
Intrusions	0.00	0.00
--Total Bandwidth--	12.15	12,451.12

Executive Summary - Attacks Blocked by Destination Port



MSS-BOT

Bot Hits

591

Signatures

68

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

ASM-VP REPORT

Organo Judicial 10/09/2023

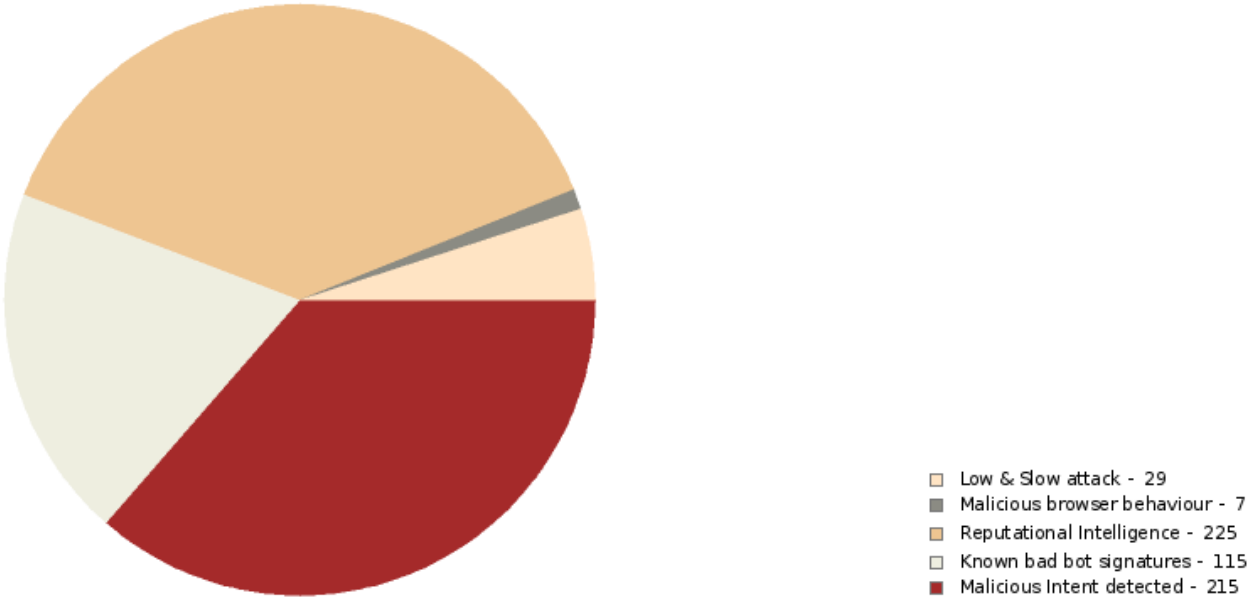
Transactions

591

Impacted Paths

237

Bot Classification

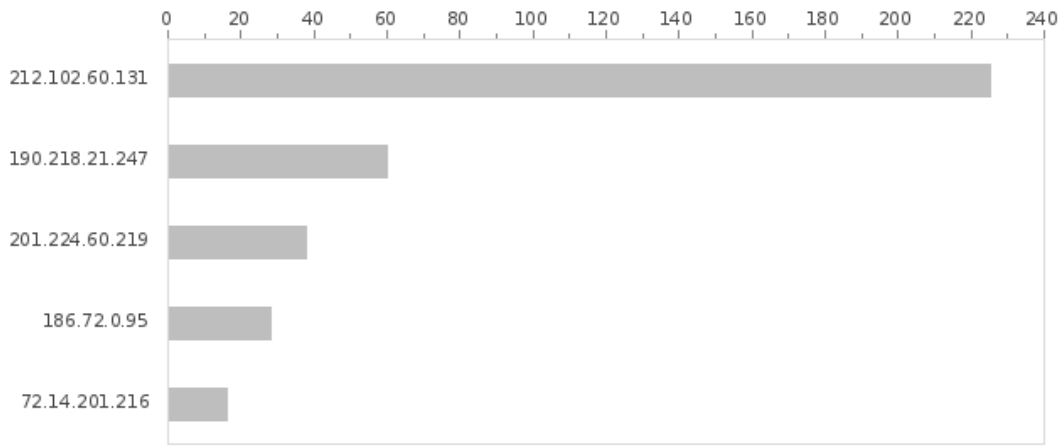


LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

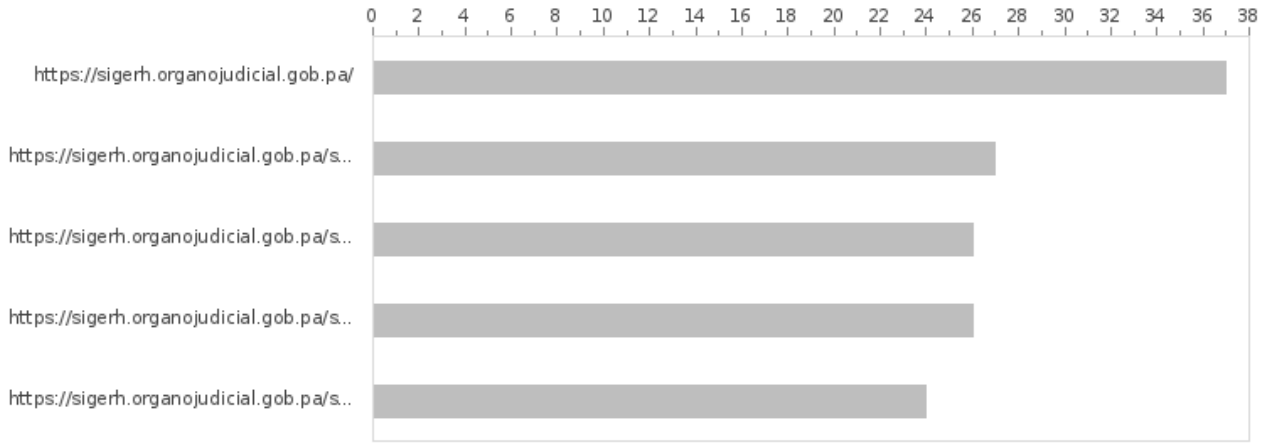
ASM-VP REPORT

Organo Judicial 10/09/2023

Top Bad Bot IPs



Top Impacted Paths



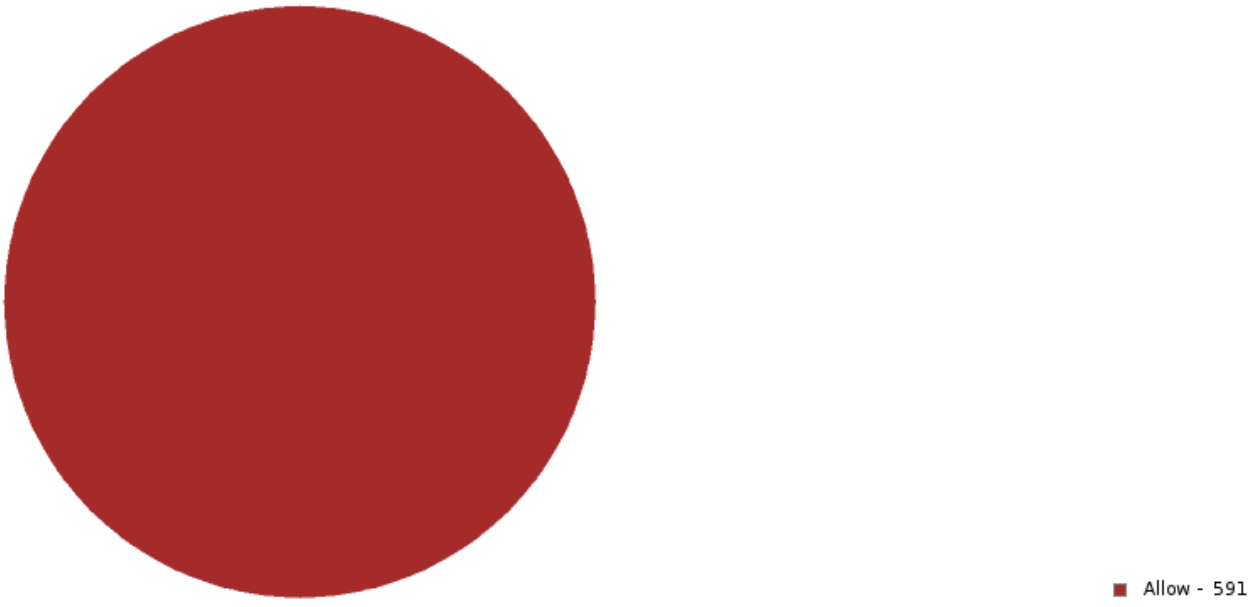
LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

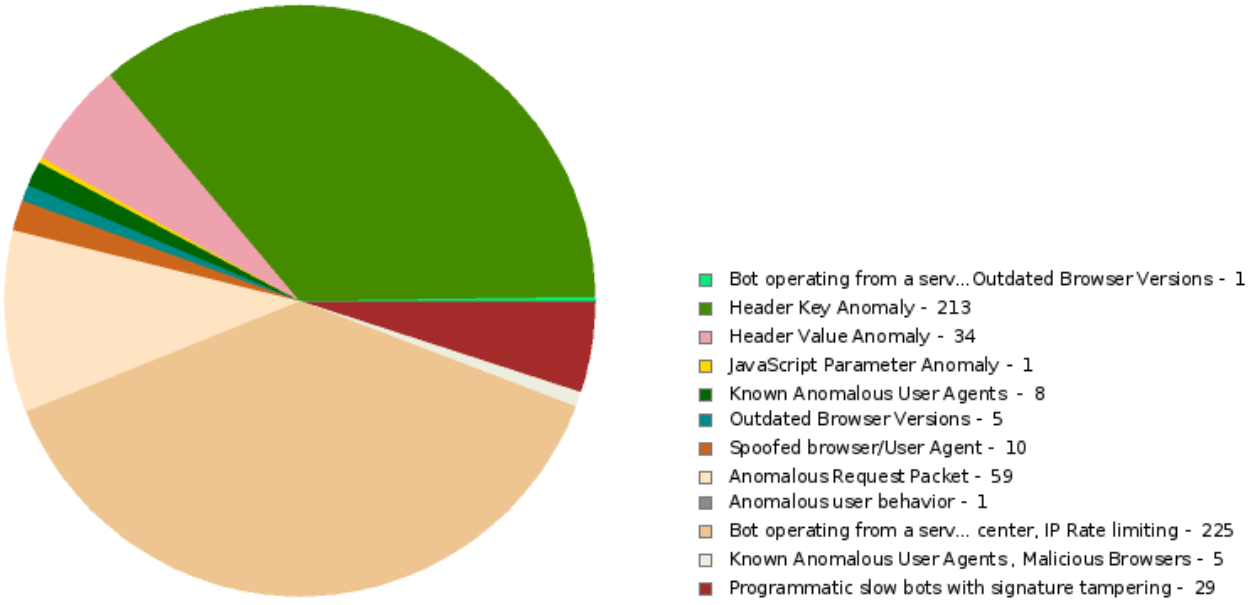
ASM-VP REPORT

Organo Judicial 10/09/2023

Bot Action



Bot Violation



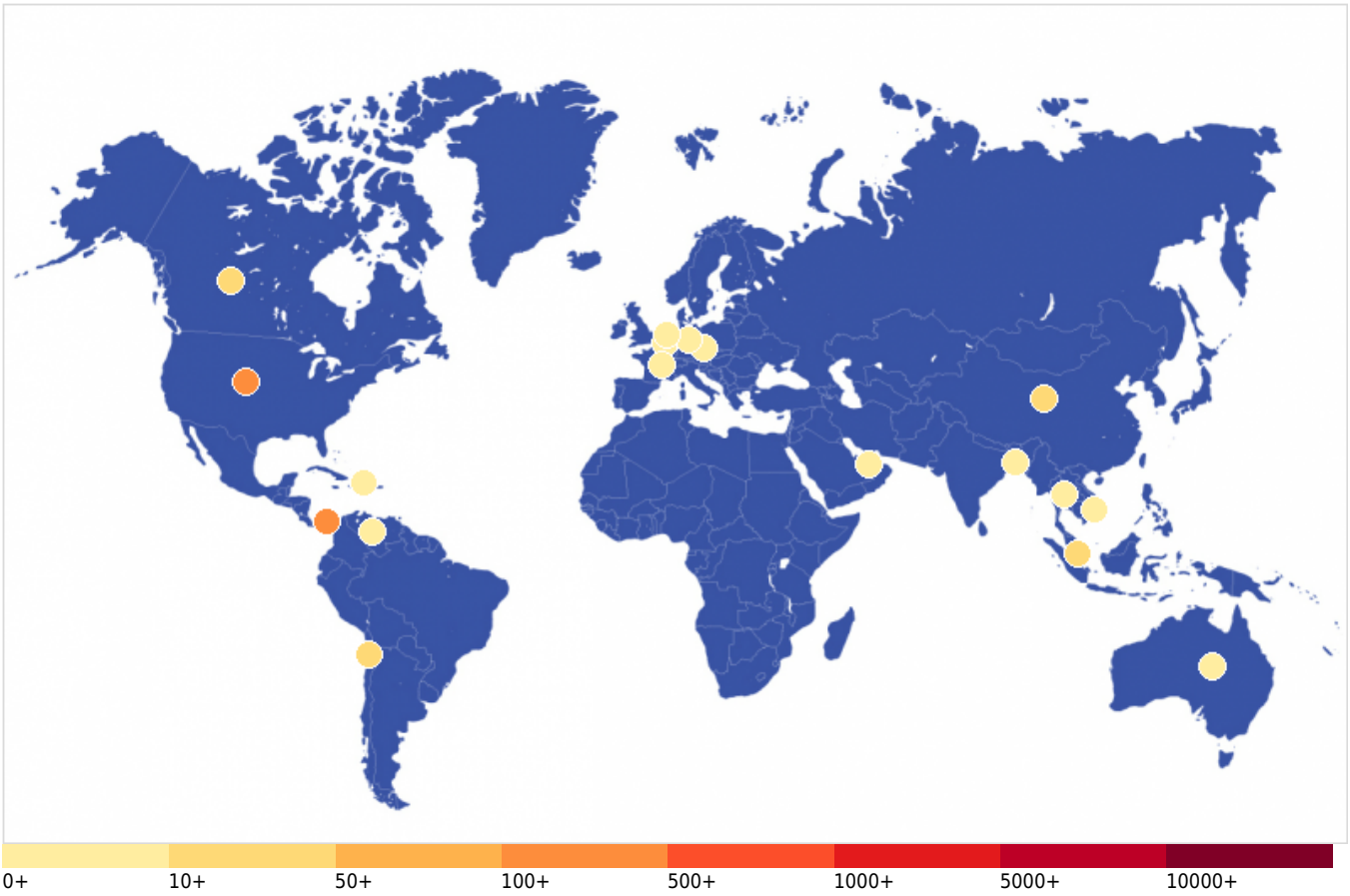
LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

TLP:AMBER

ASM-VP REPORT

Organo Judicial 10/09/2023

Bot Activity Map



Bangladesh - 1
Belgium - 1
Chile - 13
China - 30
Czechia - 4
France - 5
Germany - 3
Thailand - 1
United Arab Emirates - 1
United States - 281
Venezuela - 1
Australia - 8
Canada - 16
Dominican Republic - 1
Netherlands - 5
Panama - 206
Singapore - 13
Vietnam - 1

Top User Agents

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

ASM-VP REPORT

Organo Judicial 10/09/2023

Peak Times By Bot Classification

Peak Time	Category	Count
14/09/2023 3:00:00 AM	Known bad bot signatures	7
15/09/2023 5:00:00 AM	Malicious Intent detected	38
19/09/2023 1:00:00 AM	Malicious Intent detected	38
14/09/2023 18:00:00 PM	Low & Slow attack	8
17/09/2023 22:00:00 PM	Malicious browser behaviour	5
6/10/2023 3:00:00 AM	Reputational Intelligence	225

LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

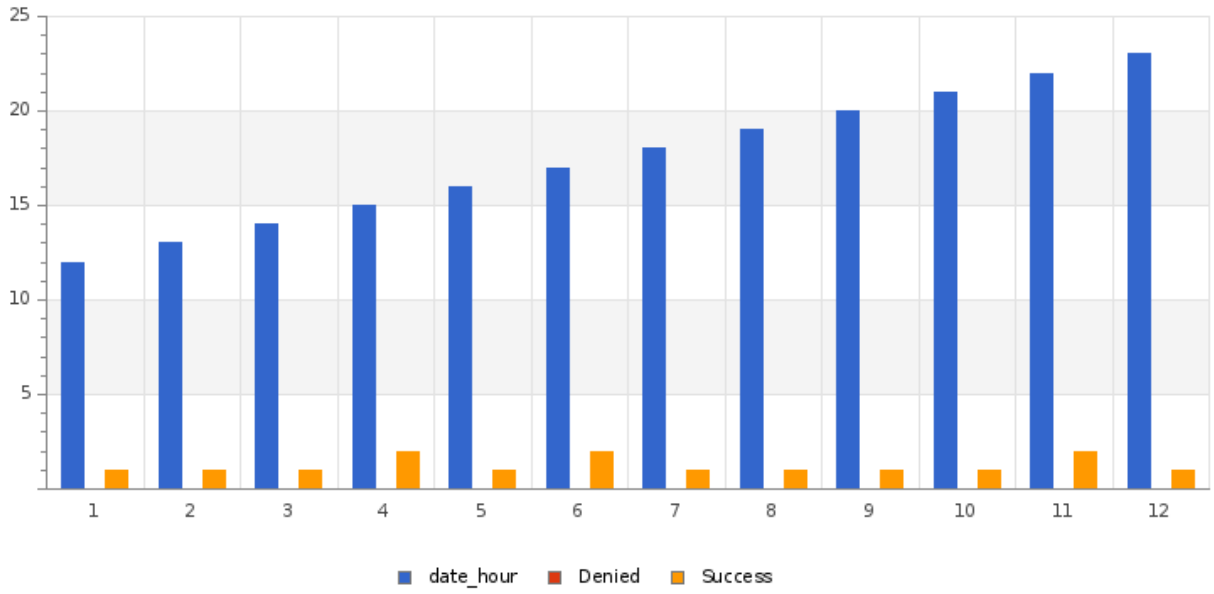
Trusted Access

MSS-TAS

Total Users *

15

Average Authentications by Hour of the Day



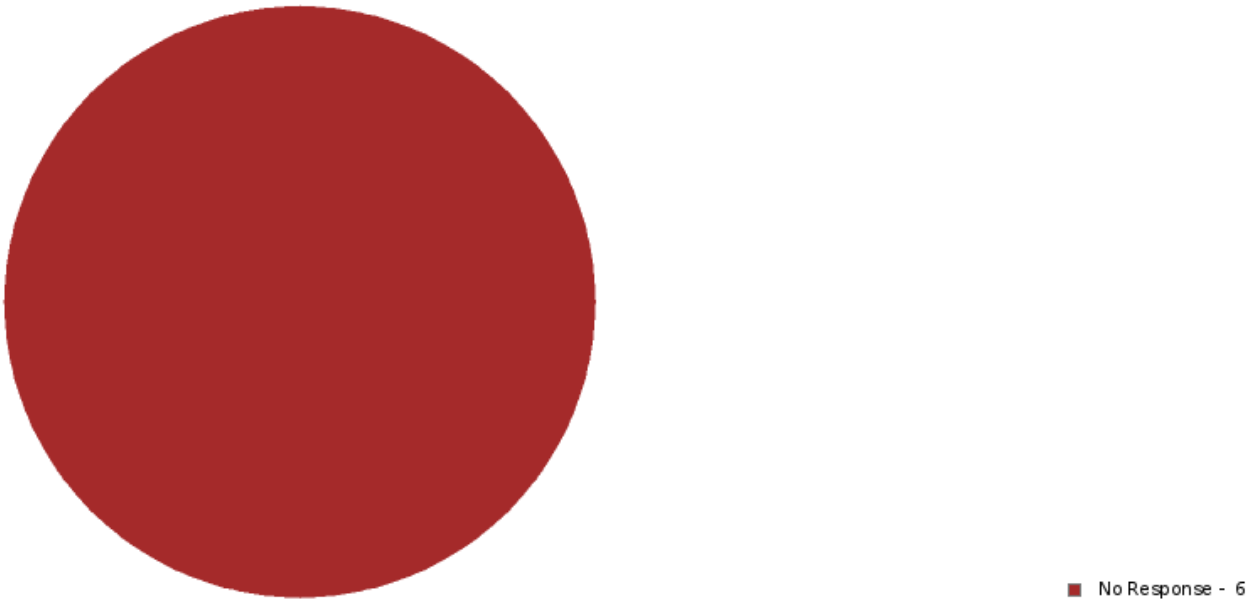
LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

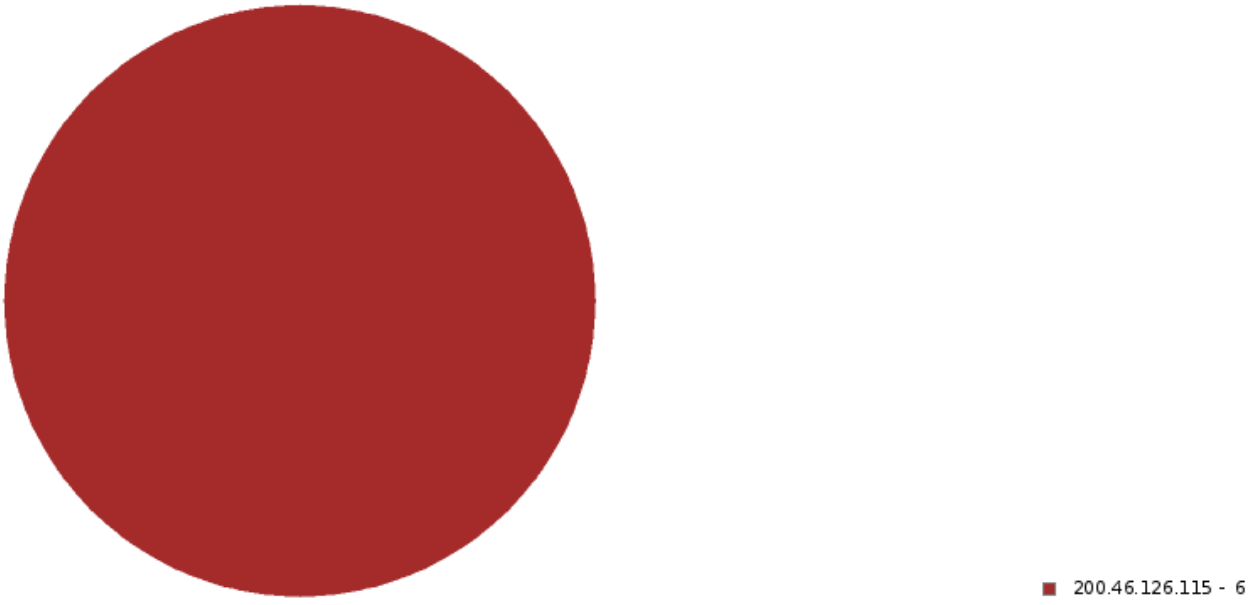
ASM-VP REPORT

Organo Judicial 10/09/2023

Top of Failed Authentications *



Top Authentications Failed by IPs *



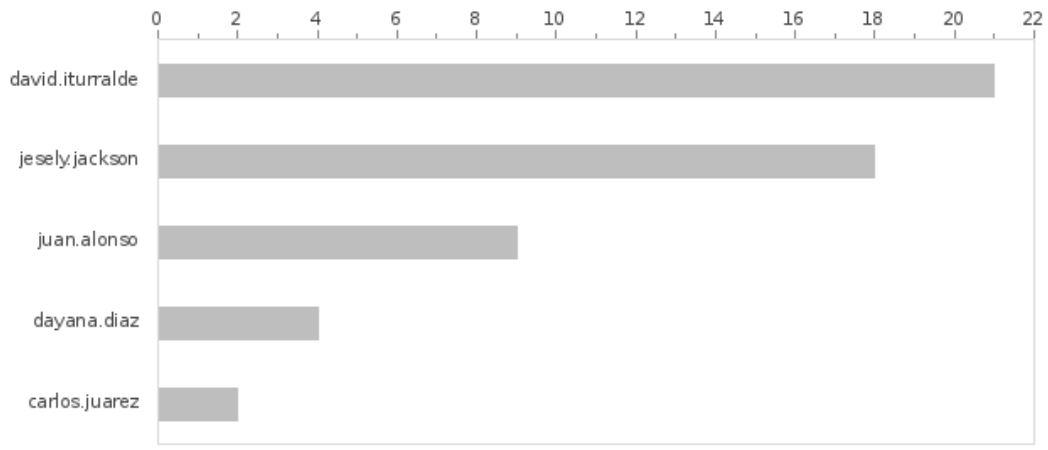
LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

ASM-VP REPORT

Organo Judicial 10/09/2023

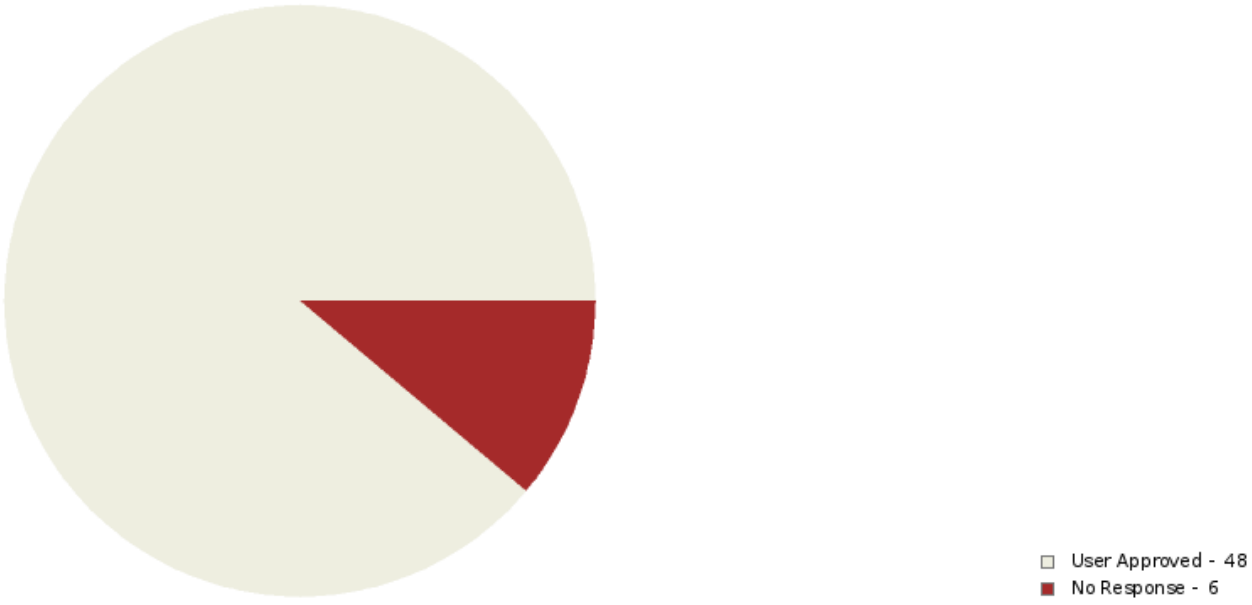
Top Authenticated Users *



Most Active Applications *

app	Denied	Success	Total
Skywatch	5	44	49
Cymulate	1	4	5

Authentication Status in the Last 24 Hours *



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

ASM-VP REPORT

Organo Judicial 10/09/2023

Users with failed authentications *

user	Time	src_ip
jesely.jackson	Wed Sep 27 13:09:24 2,023 UTC	200.46.126.115
jesely.jackson	Tue Sep 26 15:19:26 2,023 UTC	200.46.126.115
jesely.jackson	Mon Sep 18 12:11:49 2,023 UTC	200.46.126.115
juan.alonso	Thu Sep 14 21:05:55 2,023 UTC	200.46.126.115
david.iturralde	Mon Sep 11 13:04:37 2,023 UTC	200.46.126.115
david.iturralde	Tue Sep 12 13:53:33 2,023 UTC	200.46.126.115

Authentications left as No response by Users *

Username	IP Address	Time
juan.alonso	200.46.126.115	Thu Sep 14 21:05:55 2,023 UTC
jesely.jackson	200.46.126.115	Wed Sep 27 13:09:24 2,023 UTC
jesely.jackson	200.46.126.115	Tue Sep 26 15:19:26 2,023 UTC
jesely.jackson	200.46.126.115	Mon Sep 18 12:11:49 2,023 UTC
david.iturralde	200.46.126.115	Mon Sep 11 13:04:37 2,023 UTC
david.iturralde	200.46.126.115	Tue Sep 12 13:53:33 2,023 UTC

Call timed out by Users *

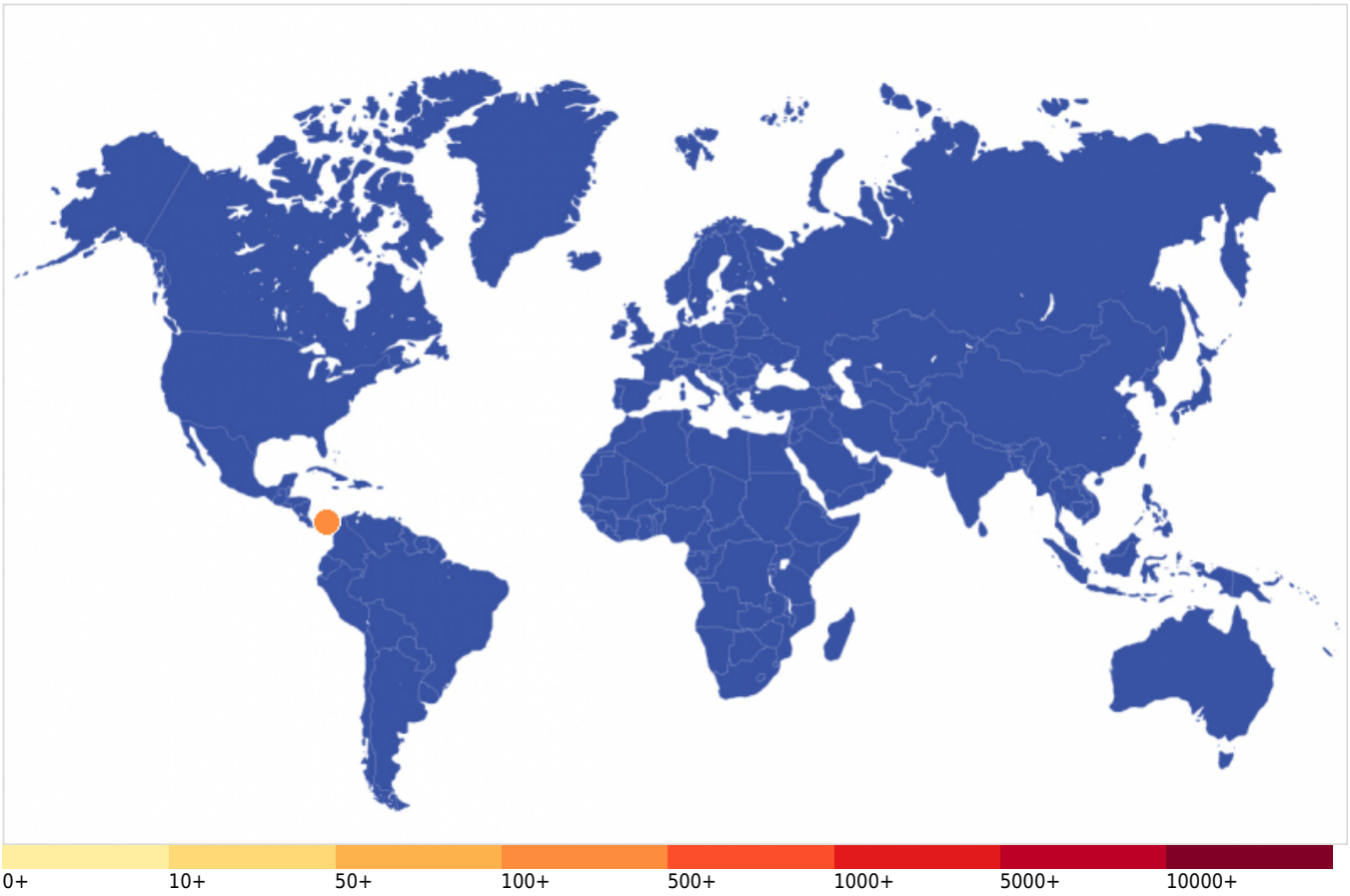
Username	Time	IP Address
juan.alonso	Thu Sep 14 21:05:55 2,023 UTC	200.46.126.115
jesely.jackson	Wed Sep 27 13:09:24 2,023 UTC	200.46.126.115
jesely.jackson	Tue Sep 26 15:19:26 2,023 UTC	200.46.126.115
jesely.jackson	Mon Sep 18 12:11:49 2,023 UTC	200.46.126.115
david.iturralde	Mon Sep 11 13:04:37 2,023 UTC	200.46.126.115
david.iturralde	Tue Sep 12 13:53:33 2,023 UTC	200.46.126.115

Most Successful Authenticated Countries *

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

ASM-VP REPORT

Organo Judicial 10/09/2023

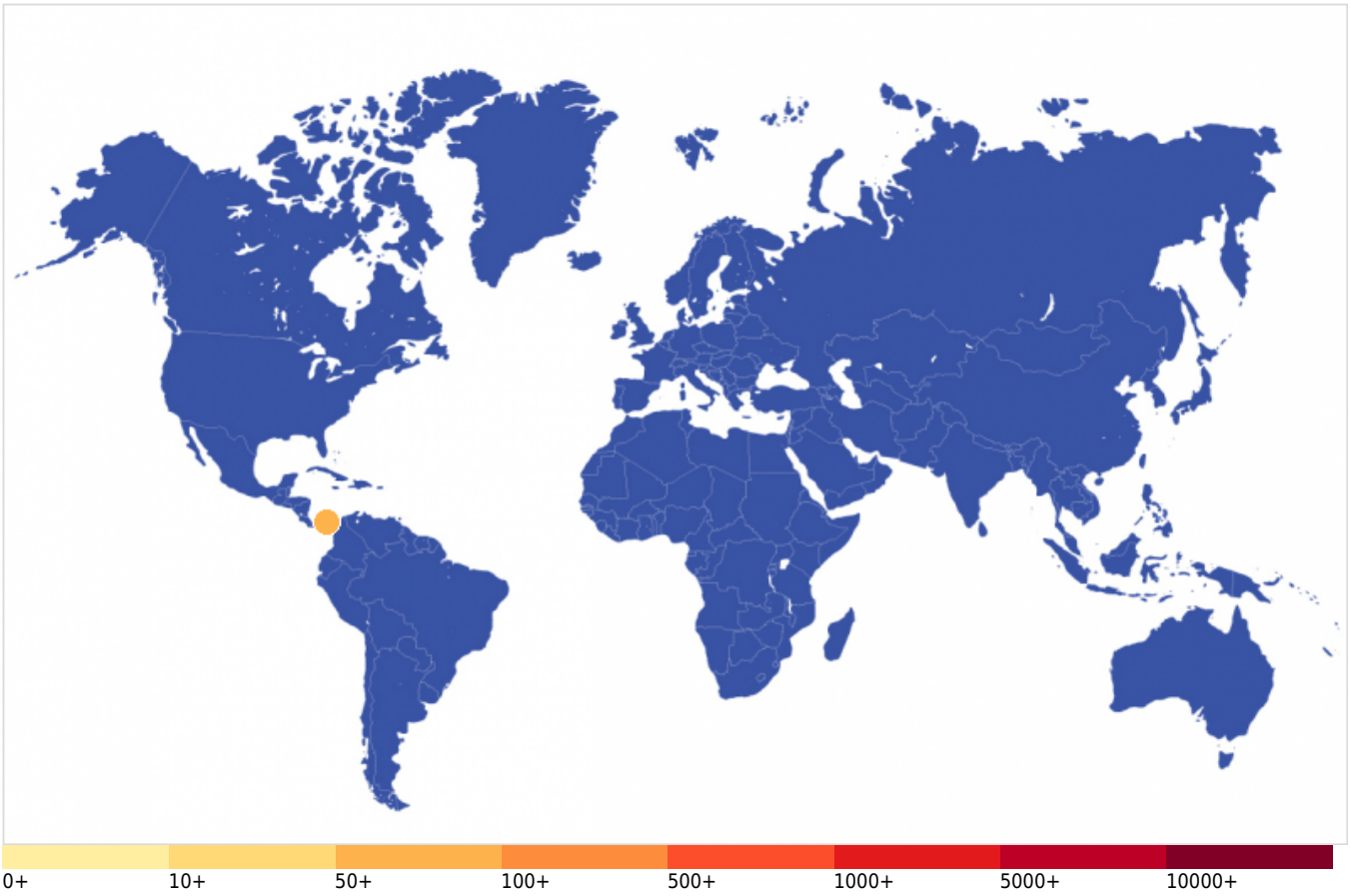


Countries with Most Failed Authentications *

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

ASM-VP REPORT

Organo Judicial 10/09/2023

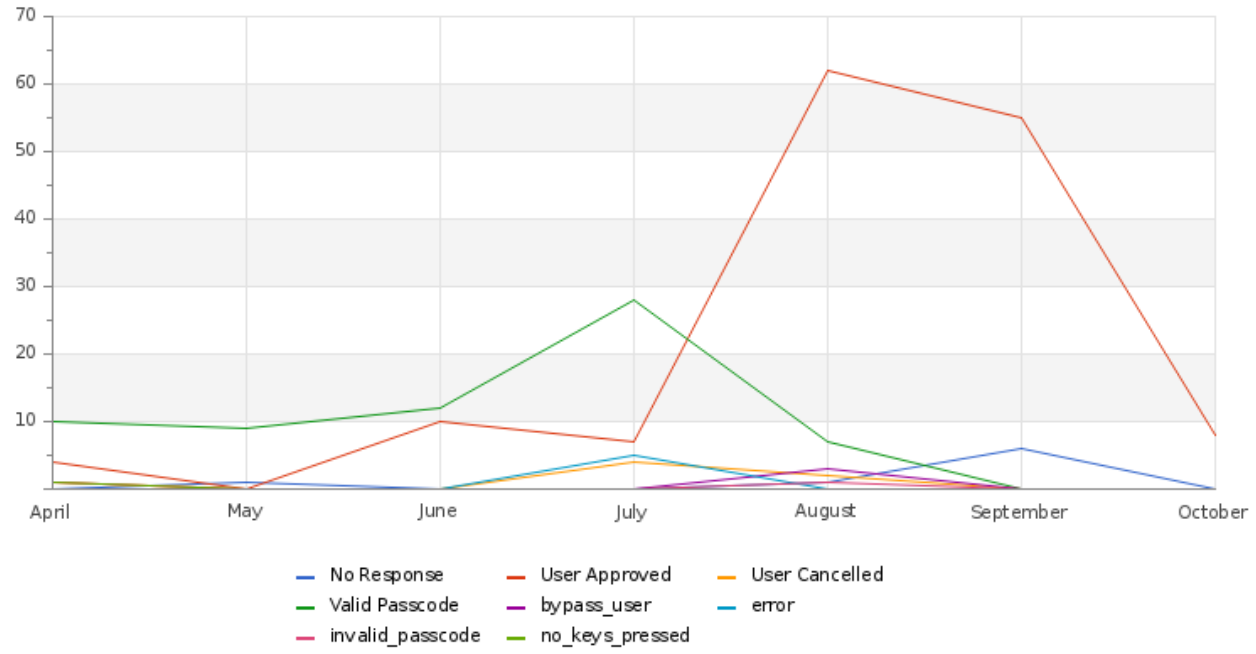


LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

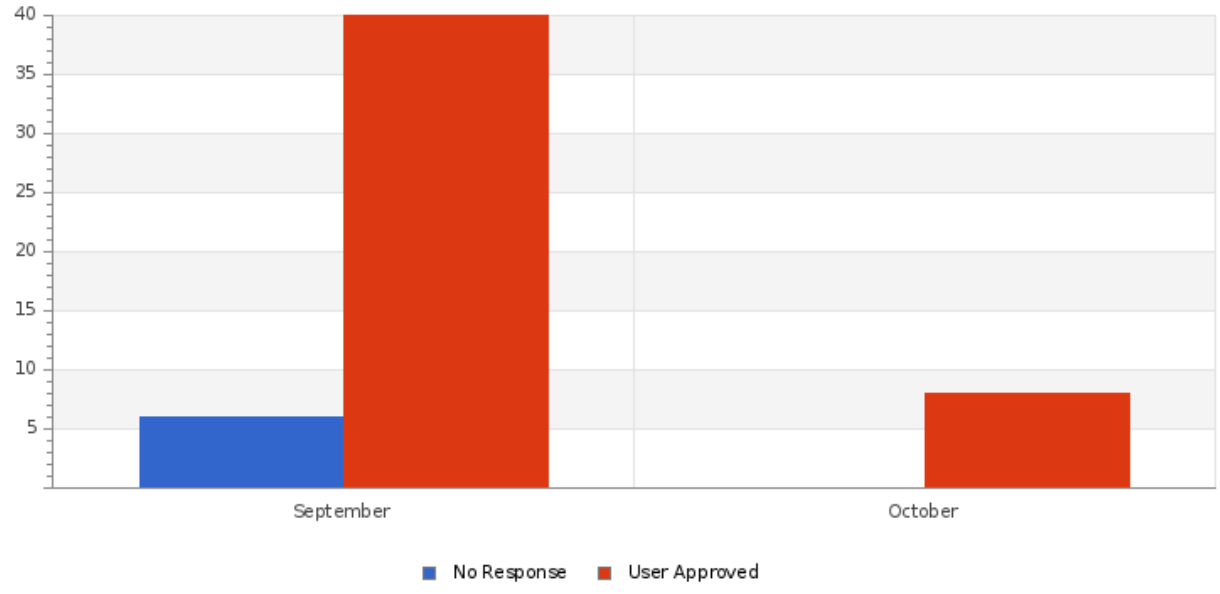
ASM-VP REPORT

Organo Judicial 10/09/2023

Trusted Access In Last 6 Months



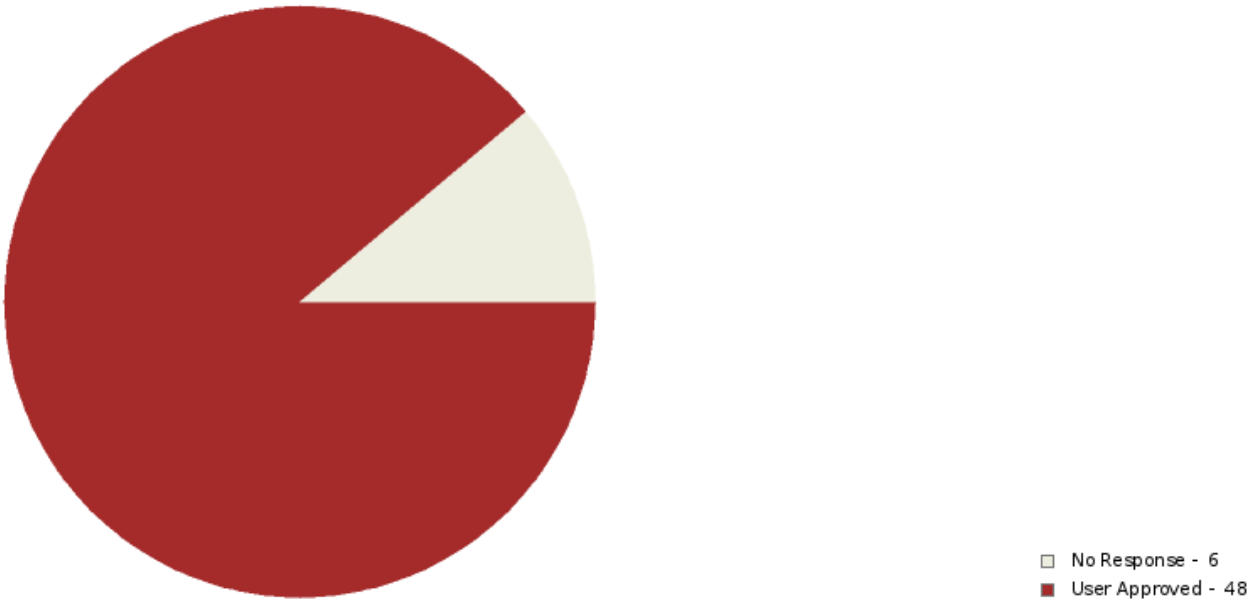
Successful and Failed Authentications *



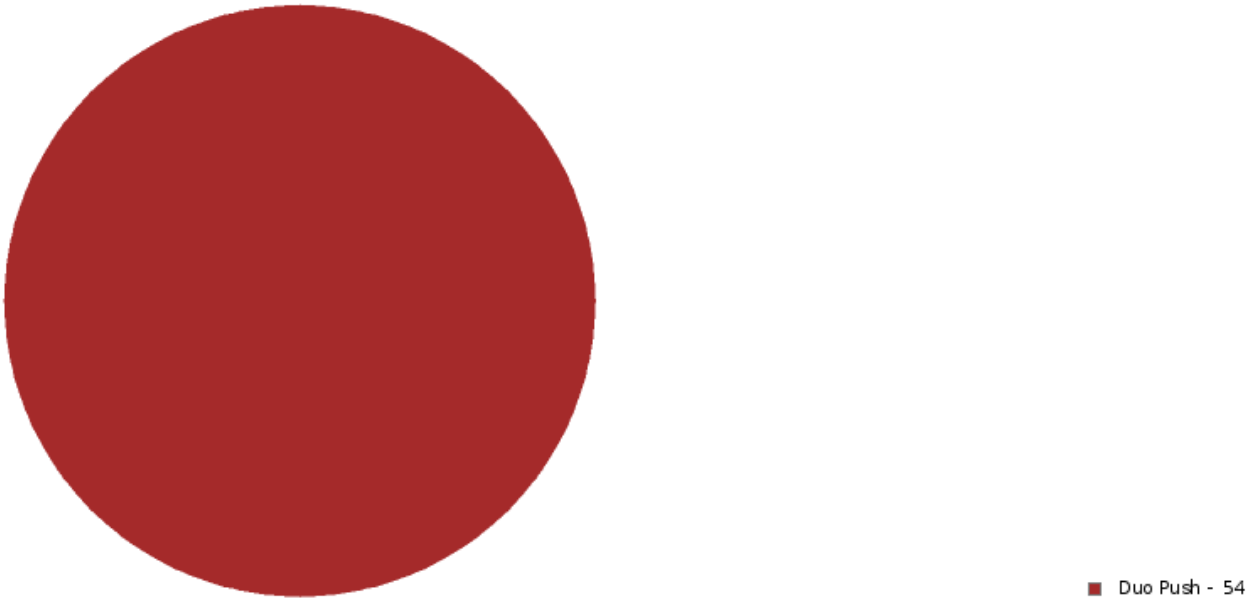
ASM-VP REPORT

Organo Judicial 10/09/2023

Successful Authentications *

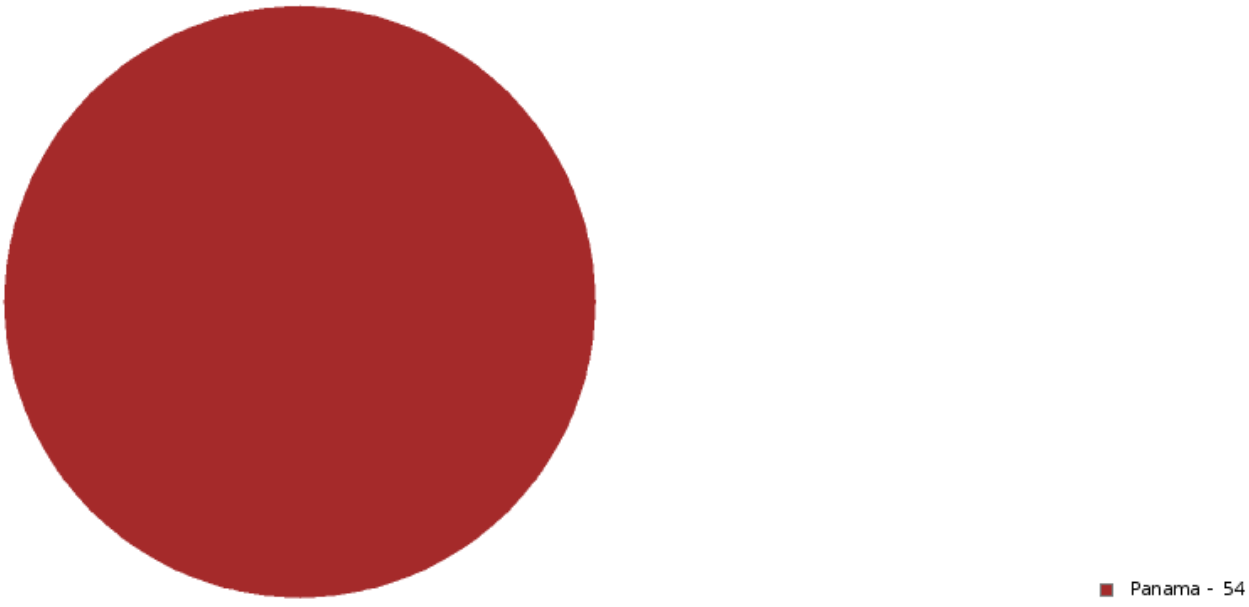


Successful Authentications by Factor *



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.**

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