TLP:AMBER

ASM-VP REPORT

ACME FINANCIAL SERVICES

August 11, 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

18%

Discovered Hosts

81

Vulnerable Hosts

42

Executive Summary Vulnerability Severity Distribution

Scanner	critical	high	medium	low
ACME	25	127	169	39
ACME	2	1	4	1
Domain Scan: acme-55.com	6	0	4	265

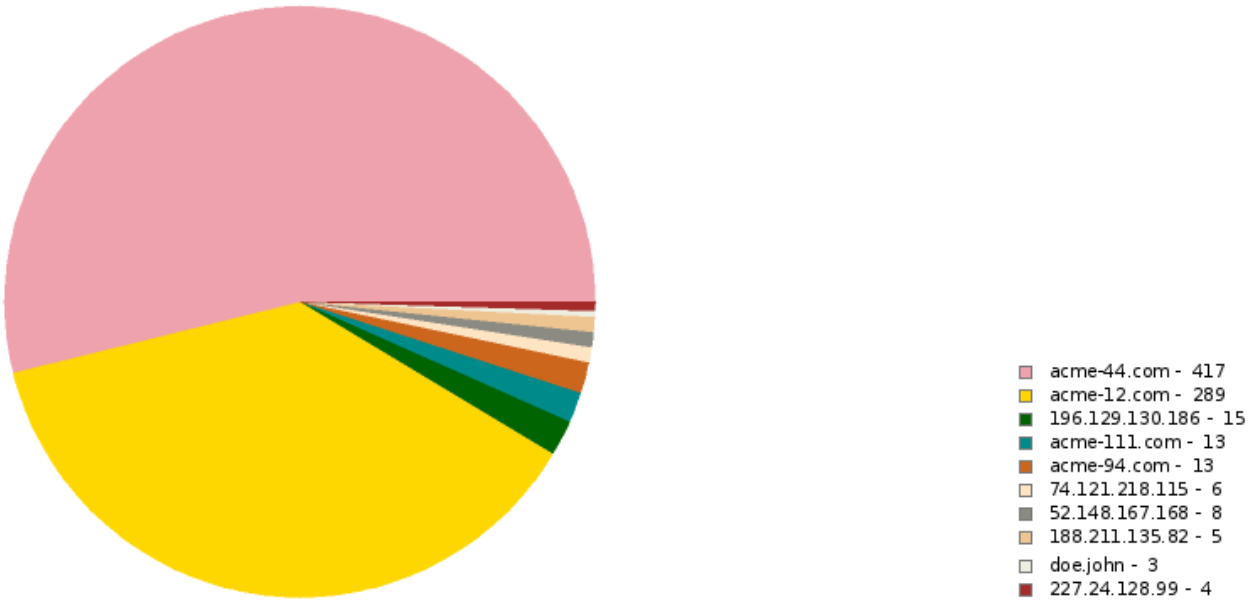
LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

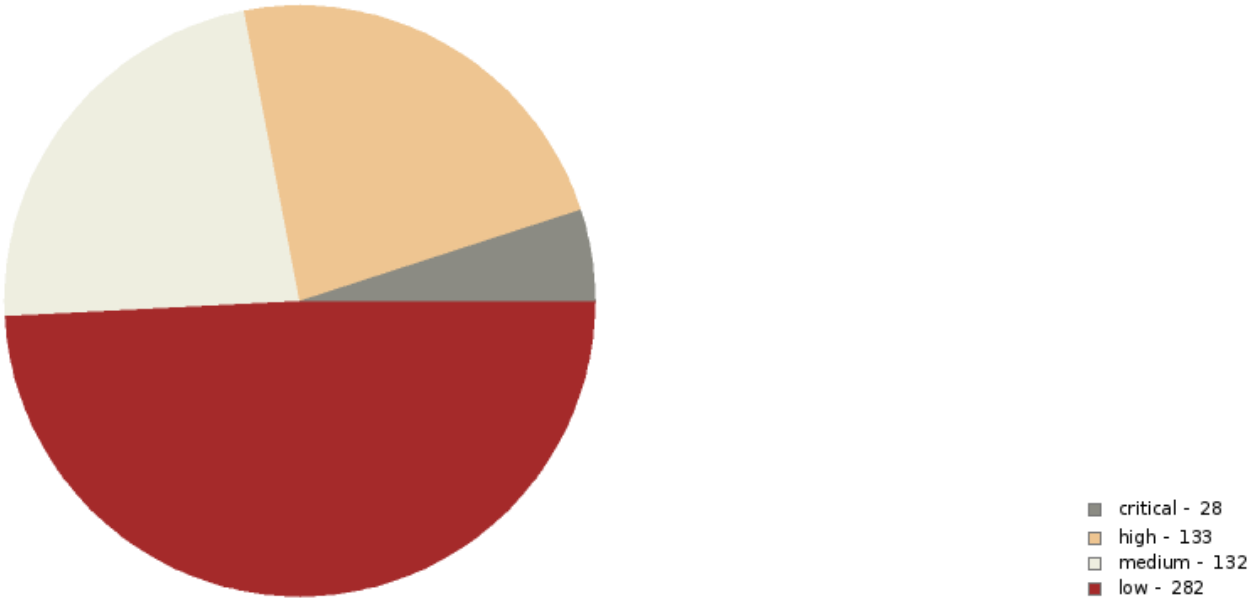
ASM-VP REPORT

ACME FINANCIAL SERVICES 08/11/2023

Most Vulnerable Host *



Vulnerability Distribution



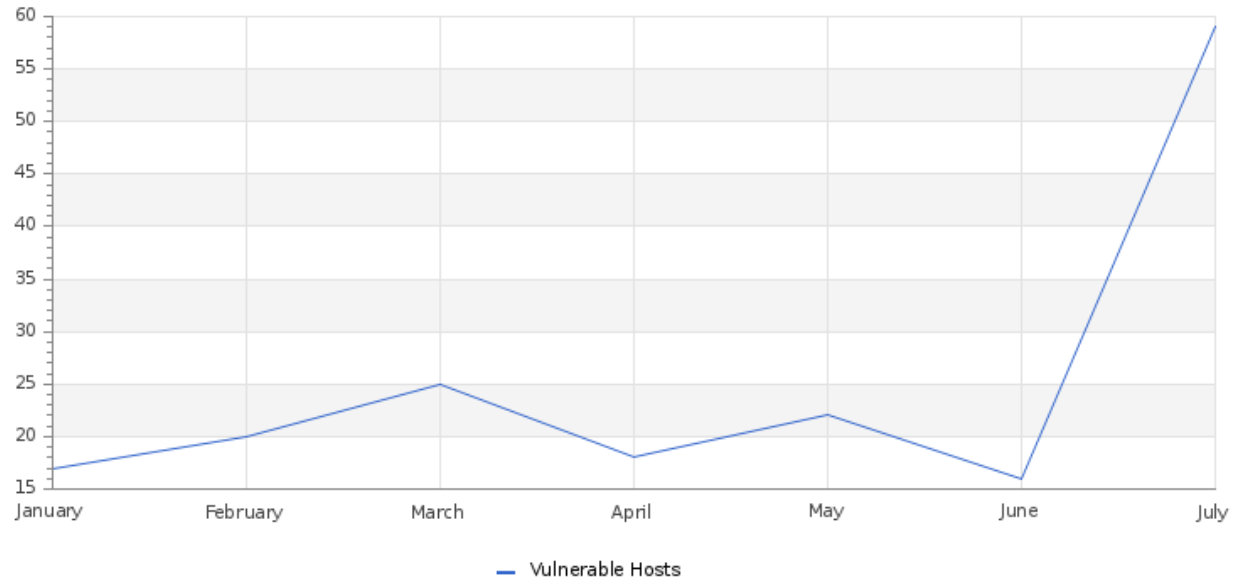
LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

Top 10 Most Common Vulnerabilities

Vulnerability
Cookie manipulation (DOM-based)
Client-side JSON injection (DOM-based)
ACME
Cross-site scripting (DOM-based)
SSL Self-Signed Certificate
Microsoft Windows Unquoted Service Path Enumeration
Web Server Allows Password Auto-Completion
Splunk Enterprise and Universal Forwarder < 9.00 Improper Certificate Validation
TLS Version 1.10 Protocol Deprecated
Client-side HTTP parameter pollution (reflected)

History

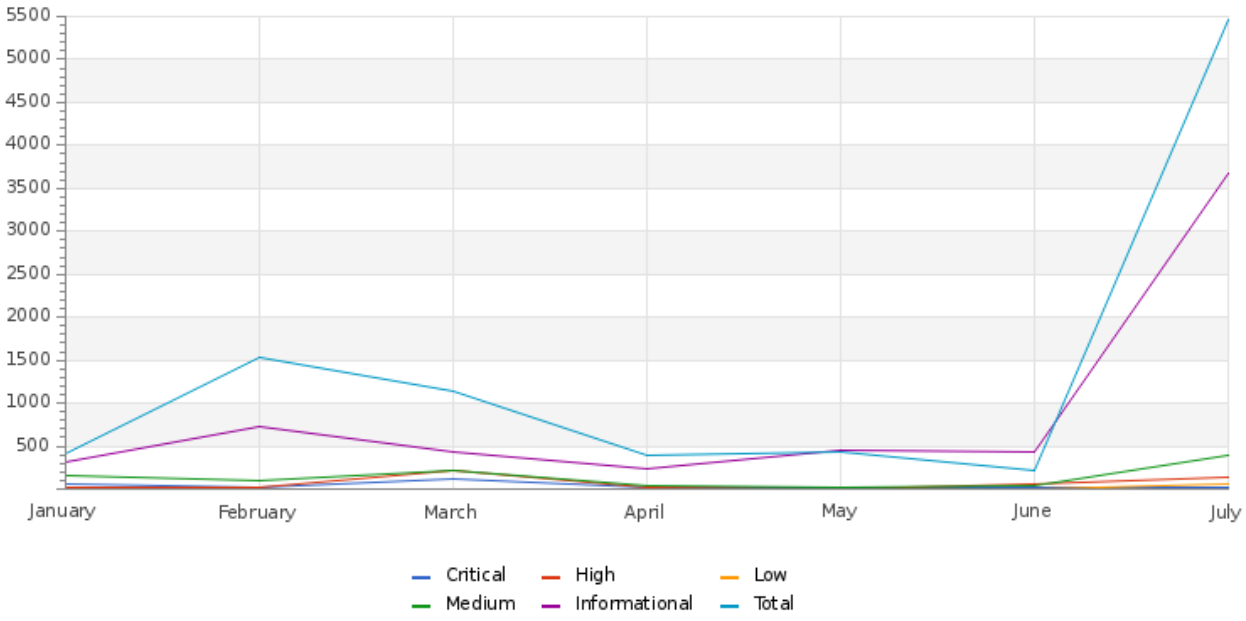
Vulnerable Host History



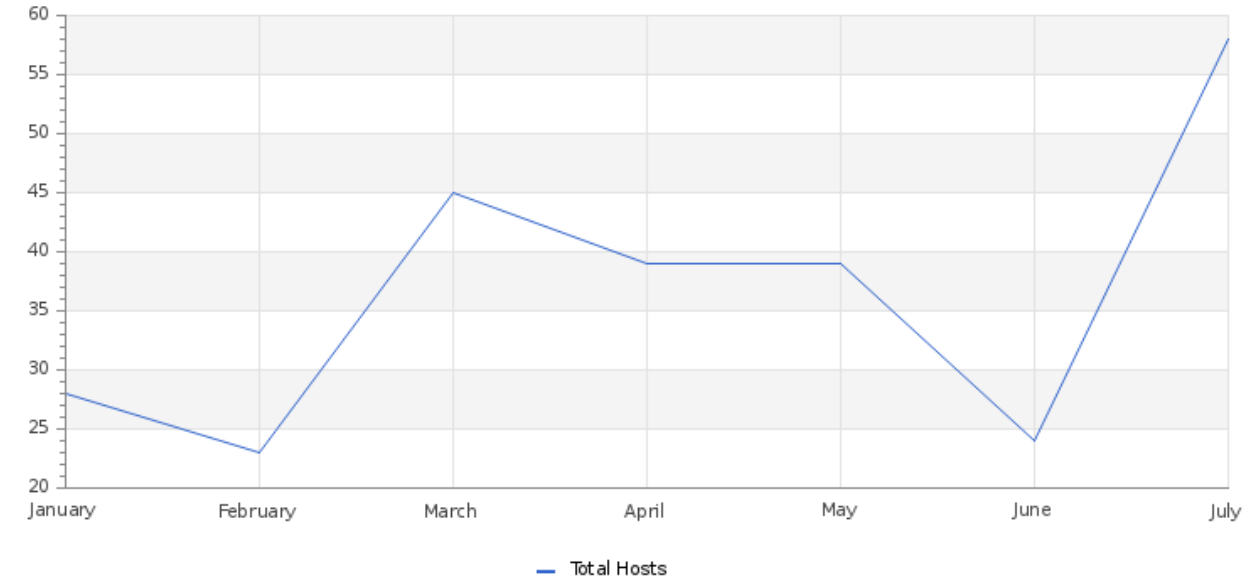
ASM-VP REPORT

ACME FINANCIAL SERVICES 08/11/2023

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
227.24.128.99	6	9
13.236.116.216	4	1
74.121.218.115	6	4
164.187.16.103	4	3
52.148.167.168	11	3
189.197.236.230	11	5
218.45.79.143	4	3
120.153.178.71	2	2
167.131.226.205	2	6
126.180.97.79	1	2
34.194.170.3	4	4
9.187.179.136	2	3
196.129.130.186	13	18
134.187.236.153	6	6
acme-16.com	9	23
doe.john	11	3
xdoe	14	7
acme-94.com	7	16
acme-69.com	3	6
acme-70.com	25	3
acme-74.com	5	2
acme-19.com	12	7
acme-20.com	8	8
acme-7.com	2	3
tdoe	3	1
acme-13.com	10	7

Open Port Monitoring

Open Ports

ip	hostname	port	status	protocol	service
127.157.200.137	acme-12.com	157	open	tcp	www

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

ASM-VP REPORT

ACME FINANCIAL SERVICES 08/11/2023

ip	hostname	port	status	protocol	service
127.157.200.137	acme-12.com	384	open	tcp	www
3.242.15.196	acme-106.com	123	open	tcp	www
3.242.15.196	acme-106.com	424	open	tcp	www
225.145.182.235	acme-85.com	101	open	tcp	www
225.145.182.235	acme-85.com	244	open	tcp	www
31.19.219.174	acme-94.com	147	open	tcp	www
31.19.219.174	acme-94.com	170	open	udp	No Service Detected
31.19.219.174	acme-94.com	255	open	tcp	epmap
31.19.219.174	acme-94.com	262	open	udp	No Service Detected
31.19.219.174	acme-94.com	190	open	udp	No Service Detected
31.19.219.174	acme-94.com	267	open	tcp	smb
31.19.219.174	acme-94.com	838	open	tcp	www
31.19.219.174	acme-94.com	655	open	tcp	cifs
31.19.219.174	acme-94.com	768	open	udp	No Service Detected
31.19.219.174	acme-94.com	3776	open	udp	No Service Detected
31.19.219.174	acme-94.com	5932	open	tcp	No Service Detected
31.19.219.174	acme-94.com	3947	open	tcp	www
31.19.219.174	acme-94.com	4583	open	udp	No Service Detected
31.19.219.174	acme-94.com	4212	open	tcp	No Service Detected
31.19.219.174	acme-94.com	4743	open	tcp	www
31.19.219.174	acme-94.com	4515	open	tcp	dce
31.19.219.174	acme-94.com	4077	open	tcp	dce
31.19.219.174	acme-94.com	11152	open	tcp	No Service Detected
31.19.219.174	acme-94.com	6546	open	tcp	dce
31.19.219.174	acme-94.com	4206	open	tcp	No Service Detected
31.19.219.174	acme-94.com	31448	open	tcp	www
31.19.219.174	acme-94.com	58247	open	tcp	www
31.19.219.174	acme-94.com	66512	open	tcp	dce
31.19.219.174	acme-94.com	87720	open	tcp	dce
31.19.219.174	acme-94.com	76935	open	tcp	dce
31.19.219.174	acme-94.com	45766	open	tcp	dce
31.19.219.174	acme-94.com	55071	open	tcp	dce
31.19.219.174	acme-94.com	41051	open	tcp	dce
31.19.219.174	acme-94.com	62128	open	tcp	dce
31.19.219.174	acme-94.com	38685	open	tcp	dce

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

ASM-VP REPORT

ACME FINANCIAL SERVICES 08/11/2023

ip	hostname	port	status	protocol	service
67.198.39.12	acme-16.com	89	open	tcp	www
67.198.39.12	acme-16.com	69	open	udp	No Service Detected
67.198.39.12	acme-16.com	185	open	tcp	epmap
67.198.39.12	acme-16.com	256	open	udp	netbios
67.198.39.12	acme-16.com	144	open	udp	No Service Detected
67.198.39.12	acme-16.com	105	open	tcp	smb
67.198.39.12	acme-16.com	841	open	tcp	No Service Detected
67.198.39.12	acme-16.com	362	open	tcp	cifs
67.198.39.12	acme-16.com	1249	open	tcp	No Service Detected
67.198.39.12	acme-16.com	5459	open	udp	No Service Detected
67.198.39.12	acme-16.com	5555	open	tcp	No Service Detected
67.198.39.12	acme-16.com	2668	open	tcp	No Service Detected
67.198.39.12	acme-16.com	9877	open	tcp	www
67.198.39.12	acme-16.com	5261	open	tcp	dce
67.198.39.12	acme-16.com	4532	open	tcp	dce
67.198.39.12	acme-16.com	4255	open	tcp	dce
67.198.39.12	acme-16.com	11309	open	tcp	dce
67.198.39.12	acme-16.com	3949	open	tcp	No Service Detected
67.198.39.12	acme-16.com	6305	open	tcp	No Service Detected
67.198.39.12	acme-16.com	11738	open	tcp	dce
67.198.39.12	acme-16.com	25317	open	tcp	No Service Detected
67.198.39.12	acme-16.com	69062	open	tcp	dce
67.198.39.12	acme-16.com	57015	open	tcp	dce
67.198.39.12	acme-16.com	29858	open	tcp	dce
67.198.39.12	acme-16.com	85276	open	tcp	dce
67.198.39.12	acme-16.com	85087	open	tcp	dce
67.198.39.12	acme-16.com	38409	open	tcp	dce
67.198.39.12	acme-16.com	77004	open	tcp	dce
67.198.39.12	acme-16.com	67750	open	tcp	dce
153.132.12.97	acme-16.com	115	open	tcp	www
153.132.12.97	acme-16.com	119	open	udp	No Service Detected
153.132.12.97	acme-16.com	244	open	tcp	epmap
153.132.12.97	acme-16.com	186	open	udp	netbios
153.132.12.97	acme-16.com	100	open	udp	No Service Detected
153.132.12.97	acme-16.com	188	open	tcp	smb

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

ip	hostname	port	status	protocol	service
153.132.12.97	acme-16.com	292	open	tcp	No Service Detected
153.132.12.97	acme-16.com	378	open	tcp	cifs
153.132.12.97	acme-16.com	2709	open	tcp	No Service Detected
153.132.12.97	acme-16.com	4703	open	udp	No Service Detected
153.132.12.97	acme-16.com	5075	open	tcp	No Service Detected
153.132.12.97	acme-16.com	5676	open	tcp	No Service Detected
153.132.12.97	acme-16.com	3862	open	tcp	www
153.132.12.97	acme-16.com	9480	open	tcp	dce
153.132.12.97	acme-16.com	11035	open	tcp	dce
153.132.12.97	acme-16.com	5930	open	tcp	dce
153.132.12.97	acme-16.com	4577	open	tcp	dce
153.132.12.97	acme-16.com	11281	open	tcp	No Service Detected
153.132.12.97	acme-16.com	9311	open	tcp	No Service Detected
153.132.12.97	acme-16.com	14484	open	tcp	dce
153.132.12.97	acme-16.com	43429	open	tcp	No Service Detected
153.132.12.97	acme-16.com	84122	open	tcp	dce
153.132.12.97	acme-16.com	39318	open	tcp	dce
153.132.12.97	acme-16.com	44577	open	tcp	dce
153.132.12.97	acme-16.com	81082	open	tcp	dce
153.132.12.97	acme-16.com	55067	open	tcp	dce
153.132.12.97	acme-16.com	64984	open	tcp	dce
153.132.12.97	acme-16.com	99068	open	tcp	dce
153.132.12.97	acme-16.com	68058	open	tcp	dce
118.237.169.45	acme-20.com	86	open	tcp	dns
118.237.169.45	acme-20.com	77	open	udp	dns
118.237.169.45	acme-20.com	105	open	udp	No Service Detected
118.237.169.45	acme-20.com	131	open	tcp	No Service Detected
118.237.169.45	acme-20.com	233	open	udp	ntp
118.237.169.45	acme-20.com	143	open	tcp	epmap

Penetration Tab

TLP:AMBER

ASM-VP REPORT

ACME FINANCIAL SERVICES 08/11/2023

Recent Scans

Scan Date	Scanned Domain	Scan Duration	Pages Scanned
2023-02-15 14:18:35	acme-6.com	12:47:51	594/594

Vulnerable Pages

2

MSS-EPCM

Devices Reporting Home

35

Top 5 Vulnerable Devices

Device	High-Severity	Medium-Severity	Low-Severity
ACME	5	13	1
DC-01	15	17	1
DC-02	17	19	1
DOCKER	0	11	0
acme-87.com	1	9	0

Top 5 Alerts

Signature	Count
ACME	3,775
Dangerous privilege granted: Log on as a Batch	2,871
Dangerous privilege granted: Log on as a Service	1,876
ACME	1,610
Users who can access Locally to the Domain Controller.	954

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

ASM-VP REPORT

ACME FINANCIAL SERVICES 08/11/2023

Hosts by Version

Version	Hosts
1.22.0609.0	35

Top 10 Weaknesses

signature	severity	count	percent
Dangerous low level privilege granted: Debug	high	29	3%
Windows Defender Credential Guard disabled	medium	27	3%
PowerShell should only allow signed policies to run	low	27	3%
Accessing Shares Anonymously	medium	27	3%
Windows Updates or WSUS are misconfigured	medium	26	3%
PowerShell logging for code execution detection	medium	26	3%
Vulnerable Service Installed	medium	25	3%
TLS Audit	medium	25	3%
Dangerous privilege granted: Deny log on Locally	medium	25	3%
Dangerous privilege granted: Allow log on Locally	medium	25	3%

MSS-BRAND

Brand

Name	Id
ACME	5

Cease and Desist Items

CurrentScore	PreviousScore	Domain
59.98	59.98	acme-105.com

ASM-VP REPORT

ACME FINANCIAL SERVICES 08/11/2023

Security Alert

Module	Url	Title	Type	Priority
Website	https://acme-106.com	acme-96.com	NewDomain	Low
Website	https://acme-106.com	acme-97.com	NewDomain	Low
Website	http://acme-106.com	acme-98.com	NewDomain	Low
Website	http://acme-106.com	acme-99.com	NewDomain	Low
Website	http://acme-106.com	acme-100.com	RelevantContentAddition	Low
Website	https://acme-106.com	acme-101.com	RelevantContentAddition	Low
Website	https://acme-106.com	acme-102.com	RelevantContentAddition	Low
Website	https://acme-106.com	acme-103.com	RelevantContentAddition	Low
Website	https://www.apollo.io	apollo.io	RelevantContentAddition	Low
Website	http://acme-106.com	acme-104.com	RelevantContentAddition	Low

Vulnerability

MSS-EPM

Total Patches Deployed

6

Total Failed Patch Deployments

4

Number of Machines Deployed To

2

Patch Scans

Scan Name	Start Date	Scan Completed
10 machines	Thu Apr 27 16:58:29 EDT 2,023	true
jdoe	Thu Apr 27 16:56:33 EDT 2,023	true
doe.jane	Thu Apr 27 16:54:37 EDT 2,023	true
8 machines	Thu Apr 27 16:32:26 EDT 2,023	true
jane.doe	Thu Apr 27 15:48:27 EDT 2,023	true
AWS_Linux	Thu Apr 27 14:10:42 EDT 2,023	true
jane.doe	Thu Apr 27 10:01:20 EDT 2,023	true

LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

ASM-VP REPORT

ACME FINANCIAL SERVICES 08/11/2023

Patch Deployments

Time Started	Bulletin ID	KB	Host
Thu Apr 27 10:25:58 EDT 2,023	MSNS23-0425-365-CURRENT	Q1632720214	115.216.52.47
Thu Apr 27 10:26:31 EDT 2,023	FF-230425	QFF11202	115.216.52.47
Thu Apr 27 10:25:30 EDT 2,023	FF-230425	QFF11202	115.216.52.47
Thu Apr 27 10:25:32 EDT 2,023	FF-230425	QFF11202	115.216.52.47
Thu Apr 27 10:25:48 EDT 2,023	FF-230425	QFF11202	115.216.52.47
Tue Apr 25 10:31:55 EDT 2,023	ZOOM-230424	QZOOM51415434	115.216.52.47
Tue Apr 25 10:32:45 EDT 2,023	ZOOM-230424	QZOOM51415434	115.216.52.47
Tue Apr 25 10:32:13 EDT 2,023	ZOOM-230424	QZOOM51415434	115.216.52.47
Tue Apr 25 10:32:05 EDT 2,023	ZOOM-230424	QZOOM51415434	115.216.52.47
Tue Apr 25 10:32:13 EDT 2,023	ZOOM-230424	QZOOM51415434	115.216.52.47
Tue Apr 25 10:31:40 EDT 2,023	ZOOM-230424	QZOOM51415434	115.216.52.47

Failed Patch Installations

Last Updated	Bulletin ID	KB	Host
Thu Apr 27 17:31:19 EDT 2,023	MSNS23-02-5023322	Q5023322	115.216.52.47
Thu Apr 27 17:27:10 EDT 2,023	MS23-02-SQL-5021126	Q5021126	115.216.52.47
Thu Apr 27 17:32:41 EDT 2,023	SPLUNKF-230214	QSPLUNKF8210	115.216.52.47
Thu Apr 27 17:23:54 EDT 2,023	CHROME-230419	QGC11205615138	115.216.52.47
Thu Apr 27 17:26:14 EDT 2,023	SPLUNKF-230214	QSPLUNKF8210	115.216.52.47
Thu Apr 27 17:17:09 EDT 2,023	FILEZ-230426	QFILEZ3640X64	115.216.52.47
Thu Apr 27 17:25:37 EDT 2,023	SQL2017RTM-CU31	Q5016884	115.216.52.47
Thu Apr 27 17:30:48 EDT 2,023	MSNS23-02-5023363	Q5023333	115.216.52.47
Thu Apr 27 17:24:07 EDT 2,023	CHROME-230419	QGC11205615138	115.216.52.47
Thu Apr 27 17:27:04 EDT 2,023	MSNS23-02-5023368	Q5023324	115.216.52.47
Thu Apr 27 10:19:41 EDT 2,023	JAVA8-230418	QJRE8U371	115.216.52.47
Thu Apr 27 10:26:31 EDT 2,023	CHROME-230419	QGC11205615138	115.216.52.47
Tue Apr 25 10:32:44 EDT 2,023	CHROME-230419	QGC11205615138	115.216.52.47
Tue Apr 25 10:31:31 EDT 2,023	ZOOM-230424	QZOOM51415434	115.216.52.47

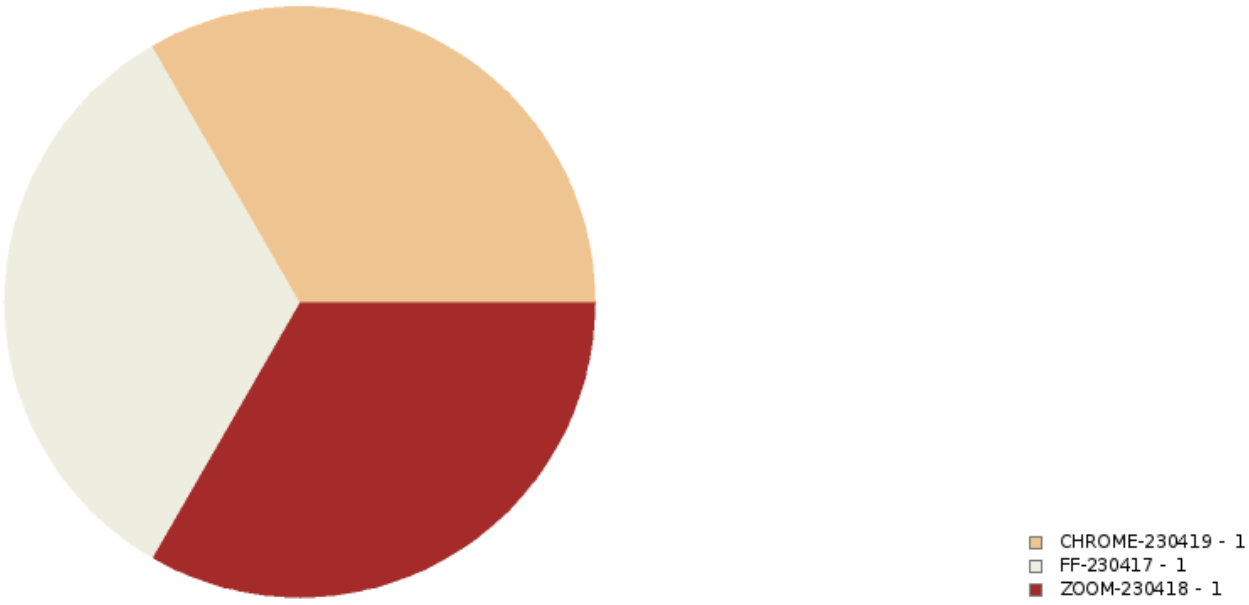
LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

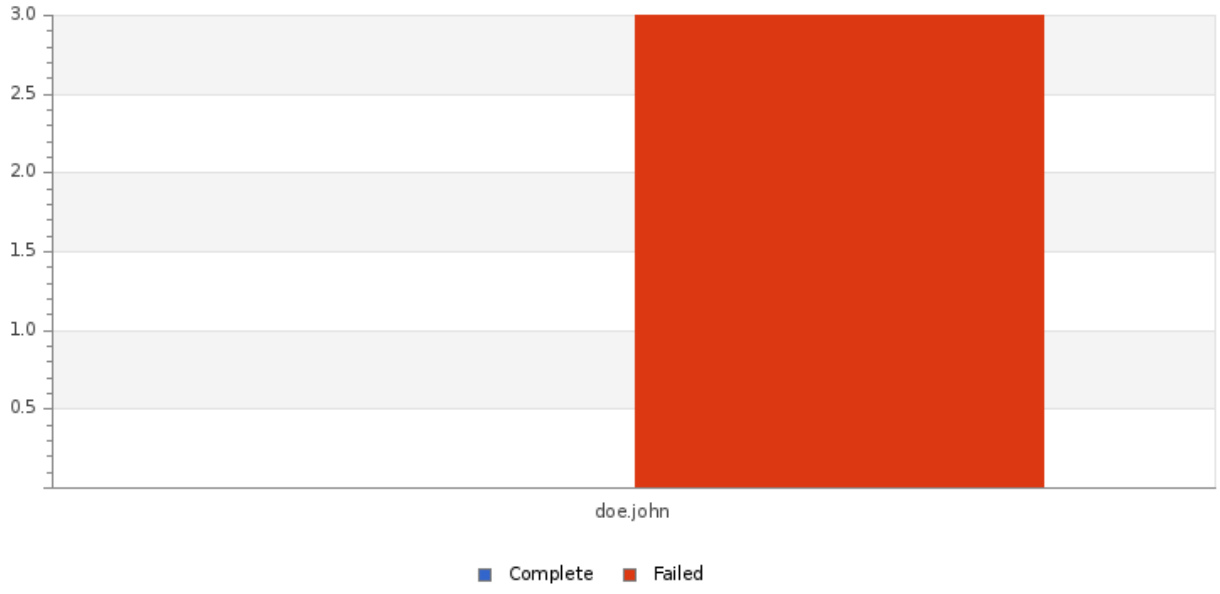
ASM-VP REPORT

ACME FINANCIAL SERVICES 08/11/2023

Top Patched Bulletins



Patch Installation Status



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

MSS-BAS Email

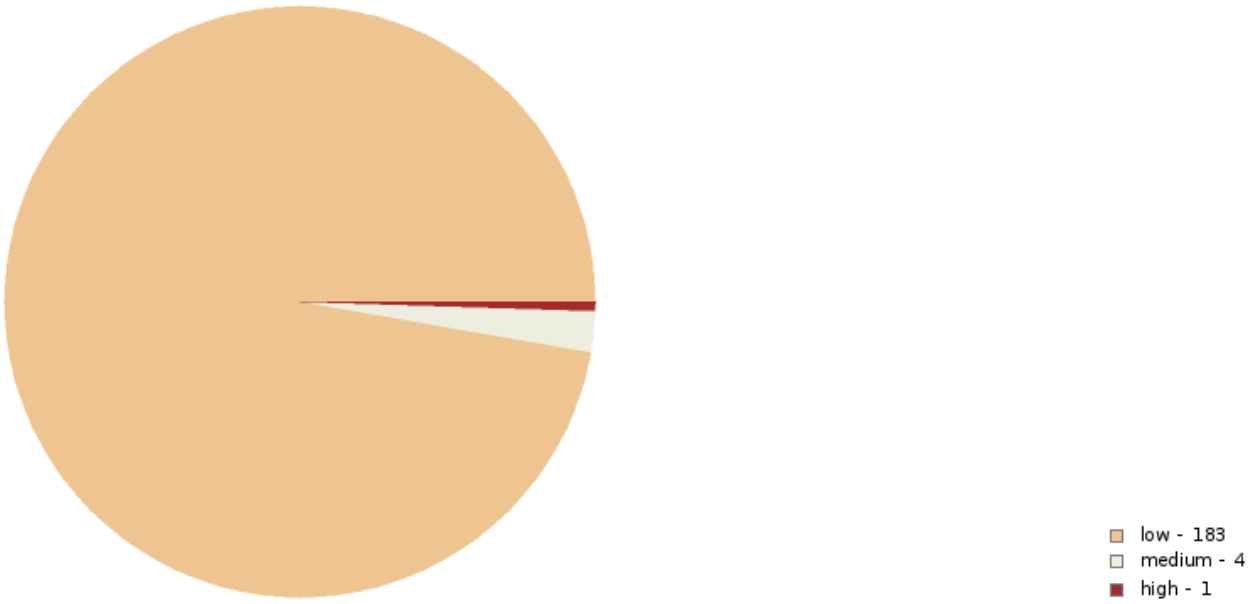
Cymulate Score

12%

Simulation Summary

Penetrated : 418 / Total Tests: 3,897

Penetrations by Severity



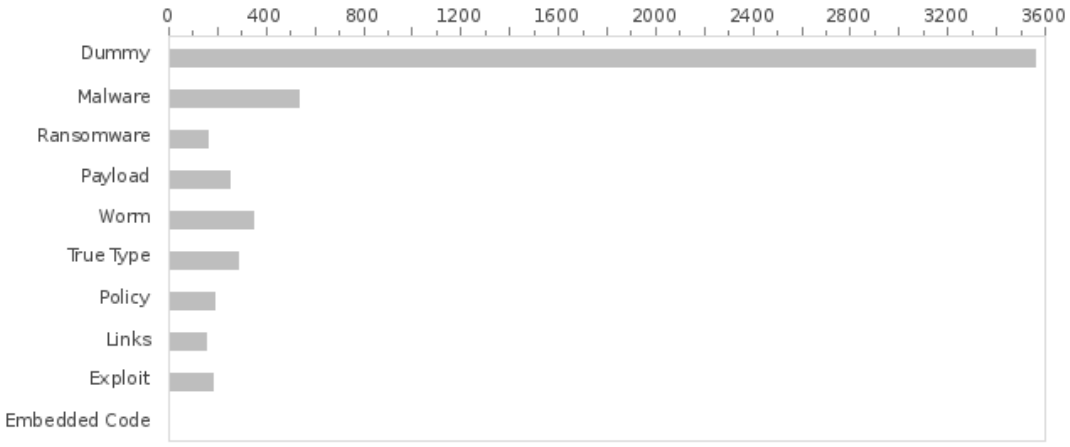
LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

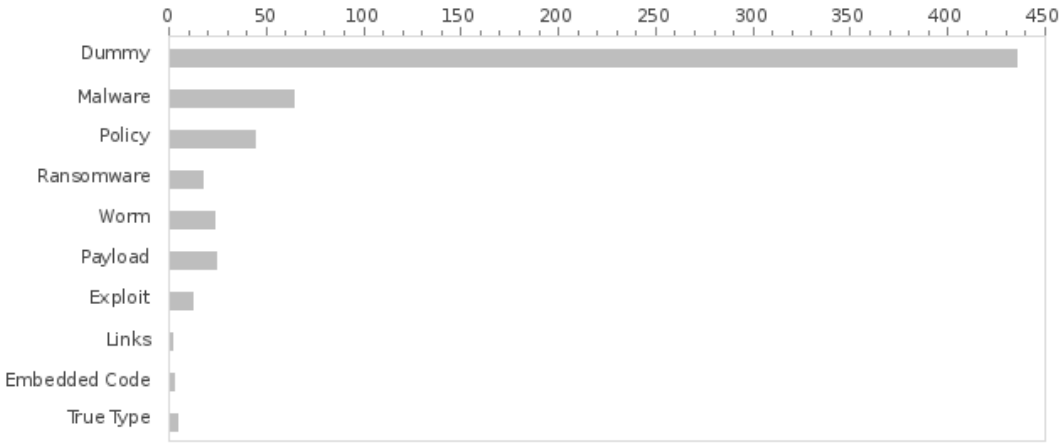
ASM-VP REPORT

ACME FINANCIAL SERVICES 08/11/2023

Emails Sent



Emails Penetrated



Percent Penetrated

20%

LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

Simulations Sent/Penetrated

Category	Penetrated	Total
Dummy	199	2,855
Malware	115	1,175
Ransomware	50	392
Payload	22	205
Worm	18	132
True Type	1	201
Policy	50	72
Links	4	174
Exploit	9	53
Embedded Code	0	6

MSS-BAS Web

Cymulate Score

52%

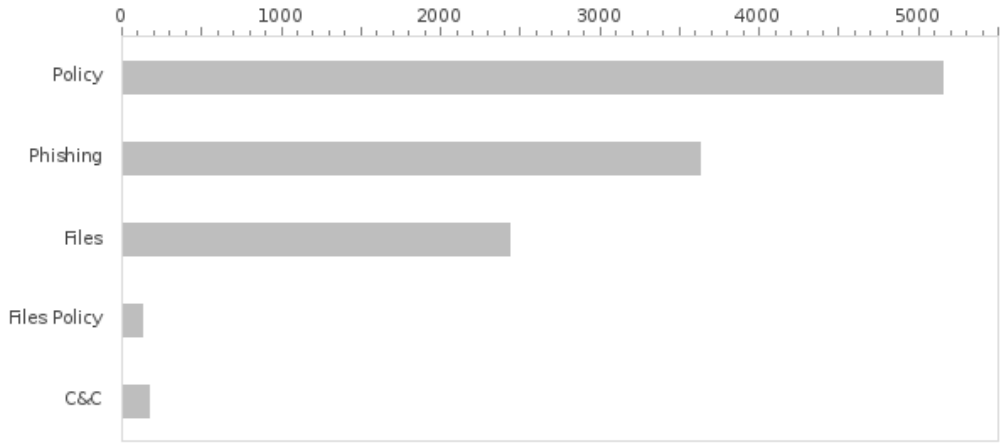
Simulation Summary

Penetrated : 1,586 / Total Tests: 7,493

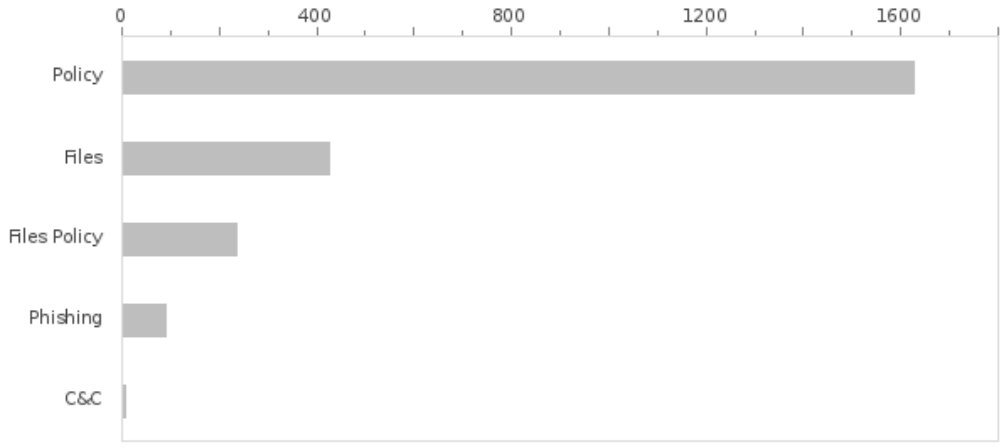
ASM-VP REPORT

ACME FINANCIAL SERVICES 08/11/2023

Browsing Sent



Browsing Penetrated



Percent Penetrated

16%

ASM-VP REPORT

ACME FINANCIAL SERVICES 08/11/2023

Simulations Sent/Penetrated

Category	Penetrated	Total
Phishing	218	13,813
Policy	1,248	5,960
Files	473	1,325
Files Policy	289	287
C&C	3	207

MSS-BAS WAF

Cymulate Score

31%

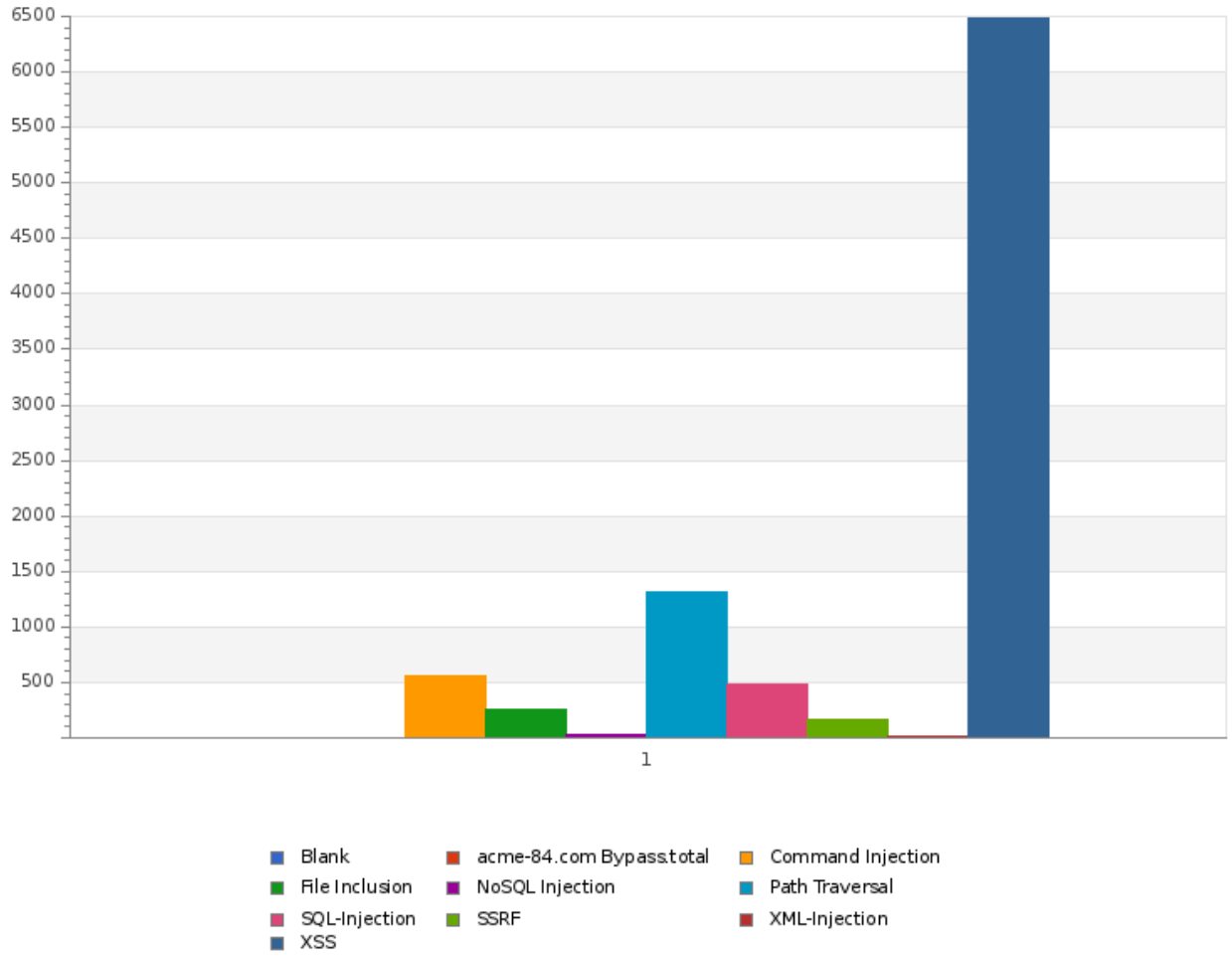
Simulation Summary

Penetrated : 718 / Total Tests: 7,670

WAF Sent

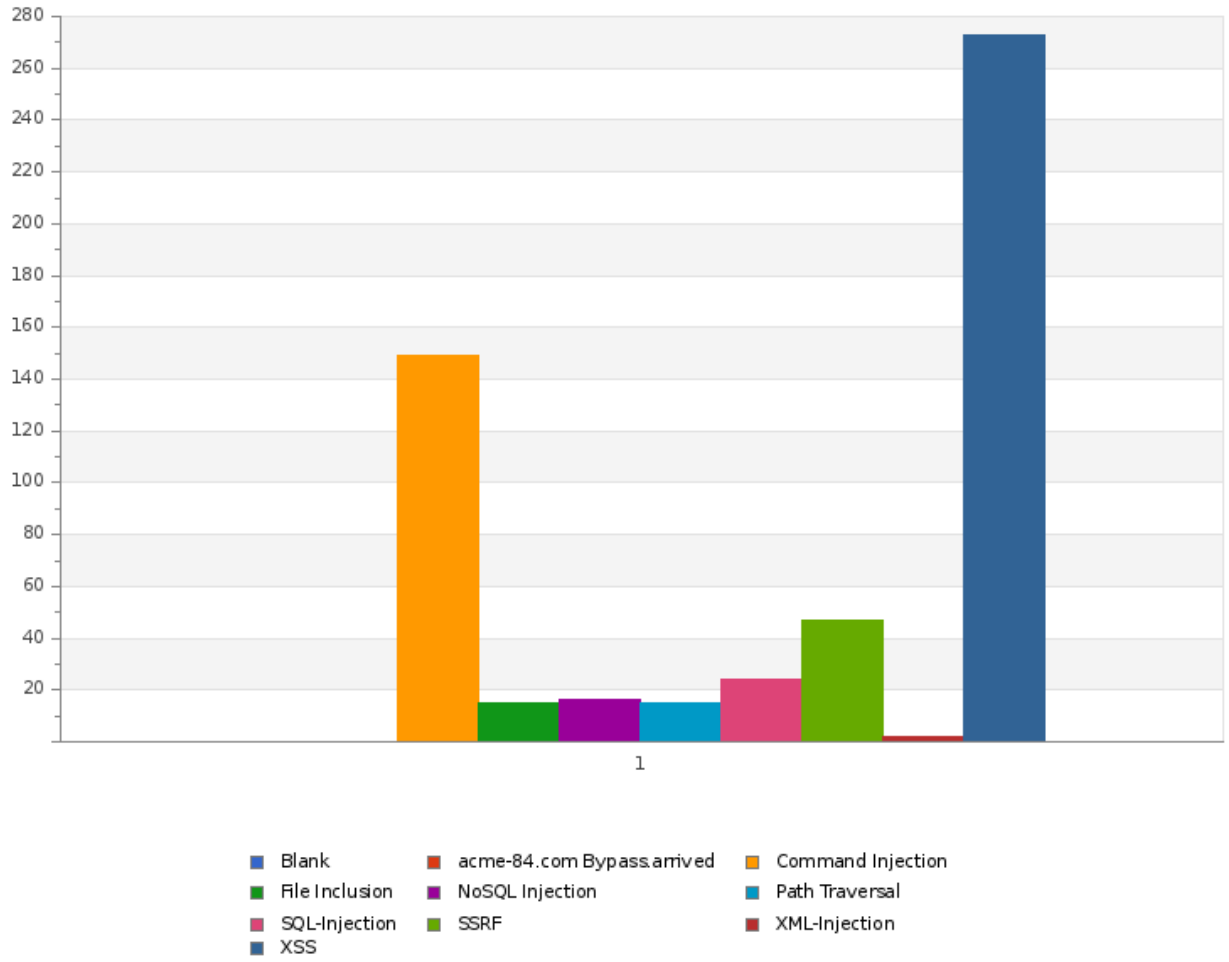
ASM-VP REPORT

ACME FINANCIAL SERVICES 08/11/2023



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

WAF Penetrated

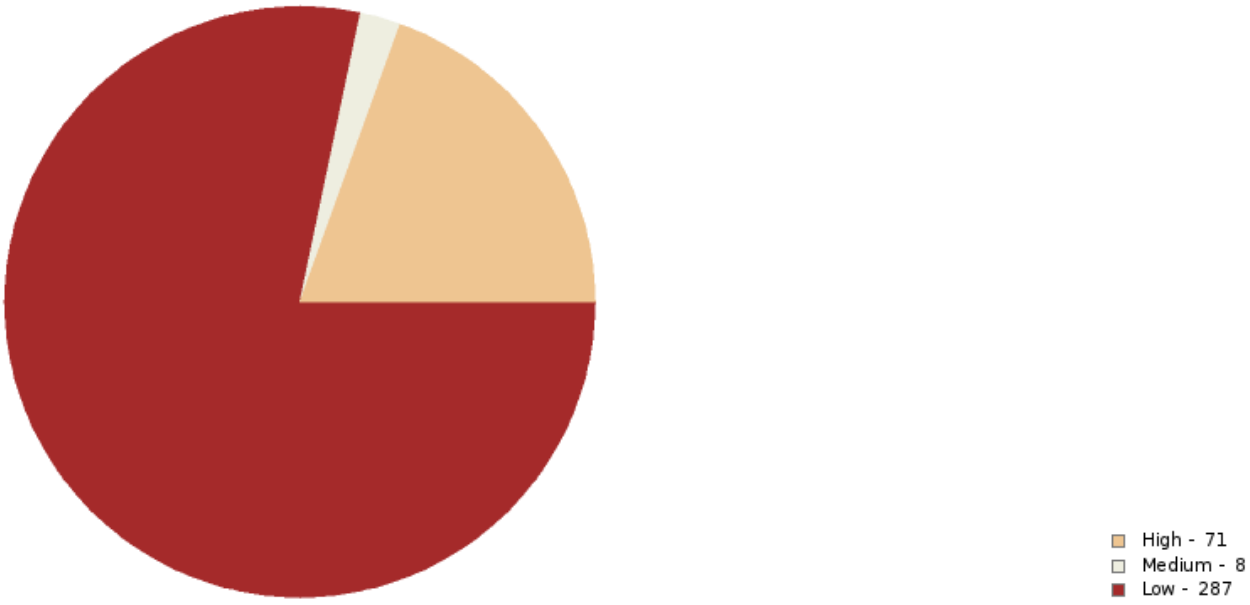


LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

ASM-VP REPORT

ACME FINANCIAL SERVICES 08/11/2023

Penetrations by Severity



Percent Penetrated

15%

Simulations Sent/Penetrated

Command Injection	File Inclusion	NoSQL Injection	Path Traversal	SQL-Injection	SSRF	WAF Bypass	XML-Injection	XSS
973	459	68	998	535	56	2	28	3,021

MSS-BAS DLP

Cymulate Score

79%

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

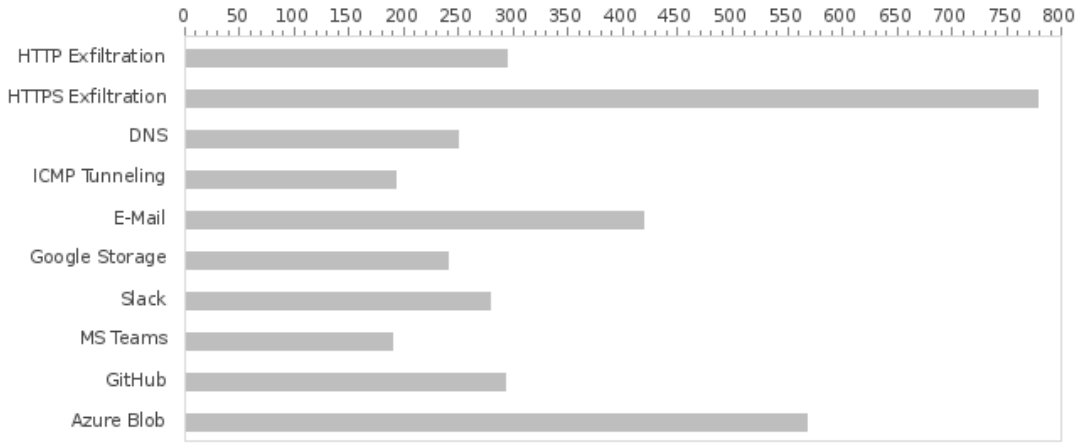
ASM-VP REPORT

ACME FINANCIAL SERVICES 08/11/2023

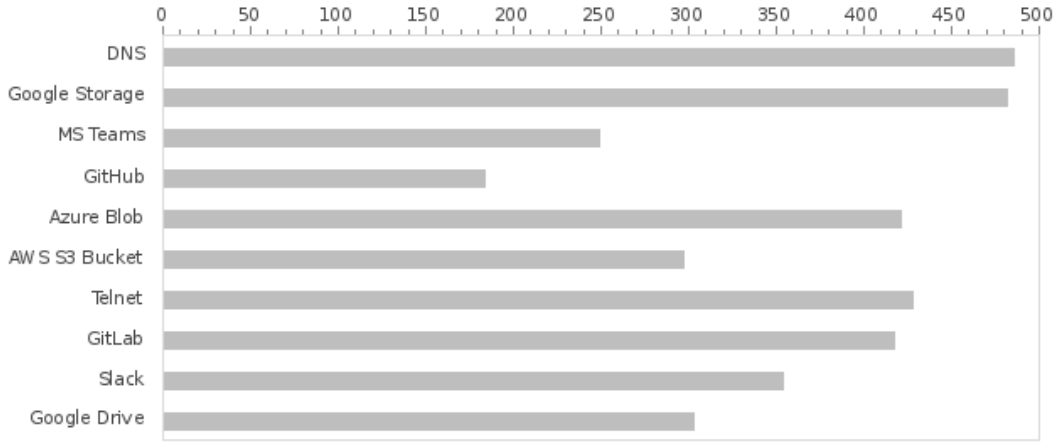
Simulation Summary

Penetrated : 2,487 / Total Tests: 4,406

Simulated Samples Sent



Simulated Samples Penetrated



Least and Most Vulnerable Categories

Least Vulnerable Classification	Most Vulnerable Classification	Least Vulnerable Phrase	Most Vulnerable Phrase
Medical	source code	AWS configuration	US Social Security Numbers

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

ASM-VP REPORT

ACME FINANCIAL SERVICES 08/11/2023

Percent Penetrated

%

Simulations Sent/Penetrated

Category	Penetrated	Total
HTTP Exfiltration	5	718
HTTPS Exfiltration	2	651
E-Mail	1	476
Removable Device	5	400
SFTP	1	235
DNS	254	302
Telnet	307	357
ICMP Tunneling	416	229
Google Storage	304	244
MS Teams	349	107
GitHub	373	385
Azure Blob	370	210
AWS S3 Bucket	325	421
GitLab	350	163
Slack	242	409
Google Drive	257	203
One Drive	353	317
DNS Tunneling	3	45
Open Ports	2	49
Gmail + Append	1	25
Browser Http	0	33
Browser Https	0	37

MSS-BAS LM

ASM-VP REPORT

ACME FINANCIAL SERVICES 08/11/2023

Lateral Movement Vector Total Score

1%

Lateral Movement Assessment Score

1%

Credentials Scraped

26

Databases Found

1

Endpoints Discovered

354

Local Admin Accounts Discovered

3

Endpoints Reached

8

Network Shares Discovered

3

ASM-VP REPORT

ACME FINANCIAL SERVICES 08/11/2023

Servers Discovered

0

Domain Admin Accounts Discovered

false

Webservers Discovered

8

Workstations Discovered

1

Security Validation

MSS-BAS Phishing

Cymulate Score

3%

Simulation Summary

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

Clicked Links

2+2

Credentials Harvested

0+0

Opened Emails

2+2

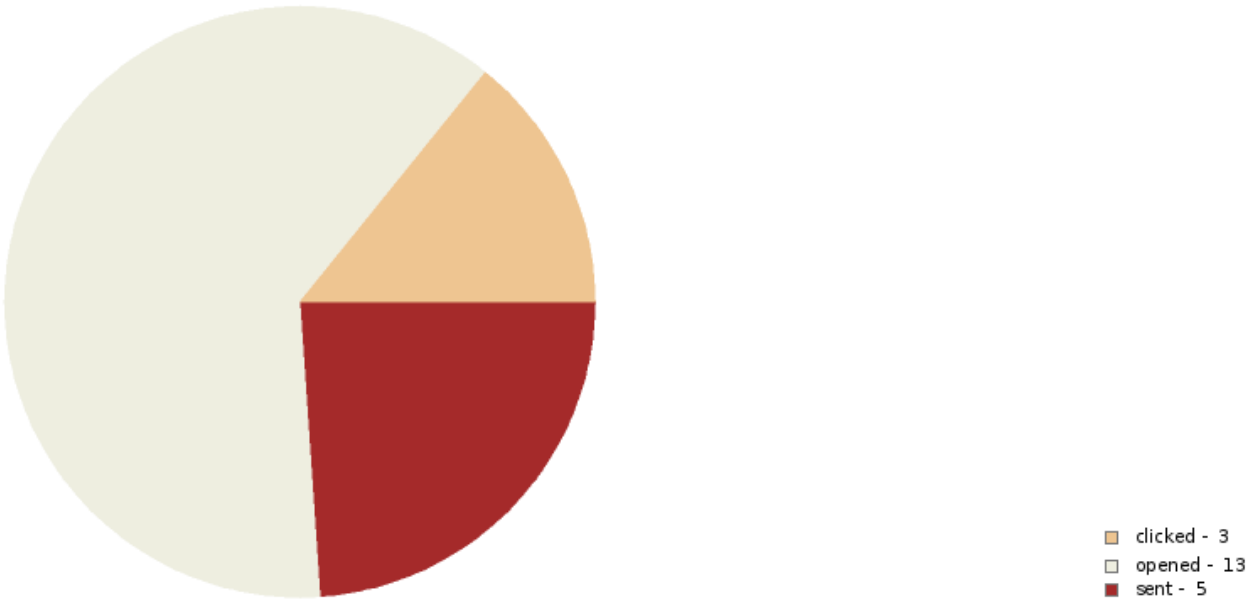
LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

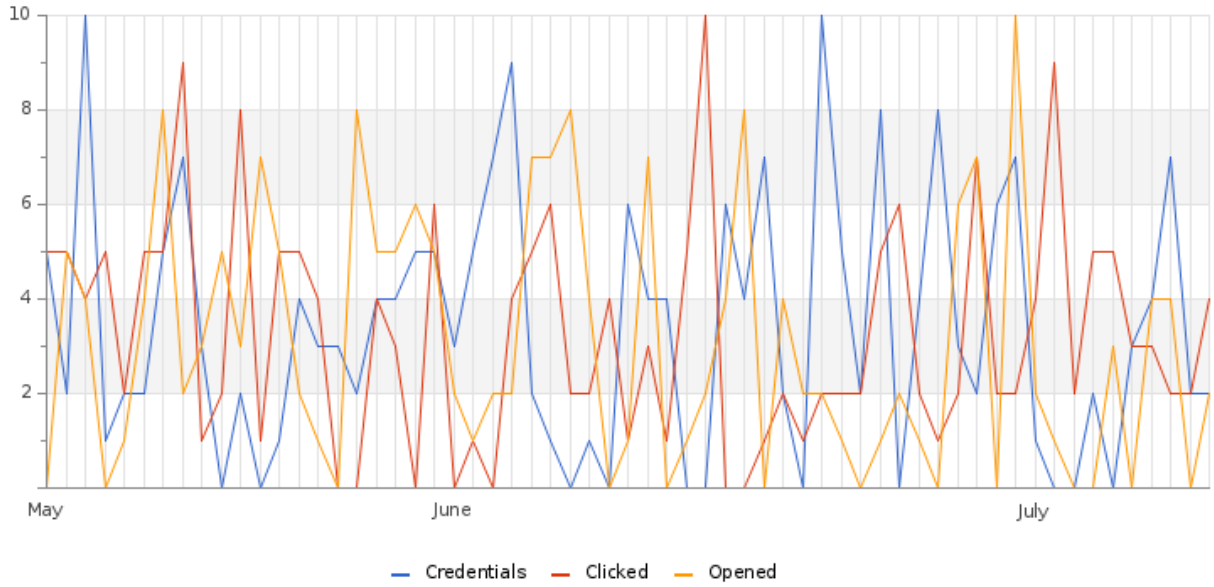
ASM-VP REPORT

ACME FINANCIAL SERVICES 08/11/2023

Phishing Sent



Phishing Penetrated



LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

ASM-VP REPORT

ACME FINANCIAL SERVICES 08/11/2023

Simulations Sent/Penetrated

Category	Penetrated	Total
Dummy	199	2,855
Malware	115	1,175
Ransomware	50	392
Payload	22	205
Worm	18	132
True Type	1	201
Policy	50	72
Links	4	174
Exploit	9	53
Embedded Code	0	6

MSS-BAS EDR

Cymulate Score

11%

Simulation Summary

Penetrated : 894 / Sent : 1,367

Ransomware based code execution

Penetrated : 0 / Total Tests: 343

Malware based execution

Not detected : 876 / Total: 876

Trojan based code execution

penetrated : 2 / Total tests : 50

Ransomware Scenarios blocked

179%

Malware Signatures blocked

145%

Trojan Scenarios blocked

96%

Worm based code execution

penetrated : 10 / Total tests : 98

Worm Scenarios blocked

129%

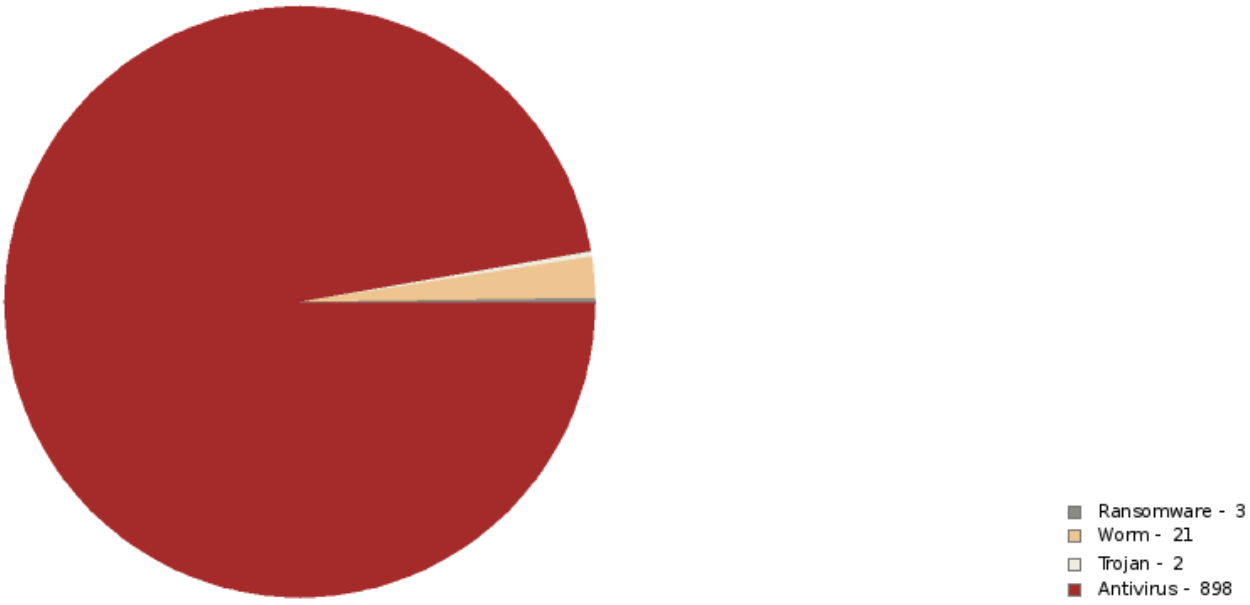
LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

ASM-VP REPORT

ACME FINANCIAL SERVICES 08/11/2023

Distribution Of Attack Types Penetrated



Percent Penetrated

80%

Simulations Sent/Penetrated

Category	Penetrated	Total
Antivirus	777	560
Ransomware	6	420
Worm	22	51
Trojan	4	86

MSS-BAS IMTHREAT

Cymulate Score

62%

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

TLP:AMBER

ASM-VP REPORT

ACME FINANCIAL SERVICES 08/11/2023

Percent Penetrated

28%

Simulation Summary

Penetrated: 415 / Total: 1,348

Immediate Threats Campaigns

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-07-09	Threat Profile UNC3944	hxxps://acme-119.com/hotfiles/manual_upload/threat_profile_unc3944_f7ba8a64-eecc -477f-a86e-0cbdccc2a0c9/Threatbgiigjfhhb85_browsingExe.exe?X-Amz-Algorithm=AWS4- HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230709T060404Z&X-Amz-Expires=600&X-Amz-Signature=d419f1db4f287cf3dcb7f843f00d484e887ac622ef93b6d16b412c39f7b48ba4&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	ACME	Penetrated
2023-07-09	Threat Profile UNC3944	hxxps://acme-119.com/hotfiles/manual_upload/threat_profile_unc3944_f7ba8a64-eecc -477f-a86e-0cbdccc2a0c9/Threatbgiigjfhhb84_browsingExe.exe?X-Amz-Algorithm=AWS4- HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230709T060404Z&X-Amz-Expires=600&X-Amz-Signature=240bf4f84a028ec564e77f7b2d5590739da7872e24559c59f8fd7f9ee3a7713a&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	ACME	Penetrated
2023-07-09	Threat Profile UNC3944	hxxps://acme-119.com/hotfiles/manual_upload/threat_profile_unc3944_f7ba8a64-eecc -477f-a86e-0cbdccc2a0c9/Threatbgiigjfhhb83_browsingExe.exe?X-Amz-Algorithm=AWS4- HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230709T060403Z&X-Amz-Expires=600&X-Amz-Signature=7ab22eb603dfa19560d87d2aae2764c98327279a7ba0bdfeaf65dc655f0de301&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	ACME	Penetrated
2023-07-09	Threat Profile UNC3944	hxxps://acme-119.com/hotfiles/manual_upload/threat_profile_unc3944_f7ba8a64-eecc -477f-a86e-0cbdccc2a0c9/Threatbgiigjfhhb82_browsingExe.exe?X-Amz-Algorithm=AWS4- HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230709T060403Z&X-Amz-Expires=600&X-Amz-Signature=bf2bcd27baad065bbd7648b02b68de8d8898853420afe55d0b8f7584c997bfe0&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	ACME	Penetrated
2023-07-09	Threat Profile UNC3944	hxxps://acme-119.com/hotfiles/manual_upload/threat_profile_unc3944_f7ba8a64-eecc -477f-a86e-0cbdccc2a0c9/Threatbgiigjfhhb80_browsingExe.exe?X-Amz-Algorithm=AWS4- HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230709T060403Z&X-Amz-Expires=600&X-Amz-Signature=a3c1603d13ee6da4e6b4bcc8e52a8a973a83a14332607eb58cb2363d79c59c9e&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	ACME	Penetrated
2023-07-09	Threat Profile UNC3944	hxxps://acme-119.com/hotfiles/manual_upload/threat_profile_unc3944_f7ba8a64-eecc -477f-a86e-0cbdccc2a0c9/Threatbgiigjfhhb_browsing79Exe.exe?X-Amz-Algorithm=AWS4- HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230709T060402Z&X-Amz-Expires=600&X-Amz-Signature=04d8005bcce0c34bd63fd9c7a947bcc86b76d3584450b477f10f34976ab4dd79&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	ACME	Penetrated
2023-07-09	Threat Profile UNC3944	hxxps://acme-119.com/hotfiles/manual_upload/threat_profile_unc3944_f7ba8a64-eecc -477f-a86e-0cbdccc2a0c9/Threatbgiigjfhhb_browsing77Exe.exe?X-Amz-Algorithm=AWS4- HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230709T060401Z&X-Amz-Expires=600&X-Amz-Signature=61ca301dc840884642fdcbbbf4abc263d8e8bd273c196ad54e01495a0e376bc0&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	ACME	Penetrated
2023-07-09	Threat Profile UNC3944	hxxps://acme-119.com/hotfiles/manual_upload/threat_profile_unc3944_f7ba8a64-eecc -477f-a86e-0cbdccc2a0c9/Threatbgiigjfhhb_browsing76Exe.exe?X-Amz-Algorithm=AWS4- HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230709T060401Z&X-Amz-Expires=600&X-Amz-Signature=d3987aea71aa2a37ac73a9b7aa6701dd20058f56fbc7a52131ad708c09433fbe&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	ACME	Penetrated
2023-07-09	Threat Profile UNC3944	hxxps://acme-119.com/hotfiles/manual_upload/threat_profile_unc3944_f7ba8a64-eecc -477f-a86e-0cbdccc2a0c9/Threatbgiigjfhhb_browsing75Exe.exe?X-Amz-Algorithm=AWS4- HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230709T060400Z&X-Amz-Expires=600&X-Amz-Signature=b8d1185b8573ee1c9f5b65a1df97999c32250a91d39444a510dc1064b04cb147&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	ACME	Penetrated

TLP:AMBER

GLESEC
COMPLETELY PERCEPTI

ASM-VP REPORT

ACME FINANCIAL SERVICES 08/11/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-07-09	Threat Profile UNC3944	hxxps://acme-119.com/hotfiles/manual_upload/threat_profile_unc3944_f7ba8a64-eecc -477f-a86e-0cbdccc2a0c9/Threatbgiigjfhhb_browsing73Exe.exe?X-Amz-Algorithm=AWS4- HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230709T060400Z&X-Amz-Expires=600&X-Amz-Signature=5115b7b57c97caefc83c65a96f38f555a1b9114bd1df438836877a1f829631bd&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	ACME	Penetrated
2023-07-09	Threat Profile UNC3944	hxxps://acme-119.com/hotfiles/manual_upload/threat_profile_unc3944_f7ba8a64-eecc -477f-a86e-0cbdccc2a0c9/Threatbgiigjfhhb_browsing72Exe.exe?X-Amz-Algorithm=AWS4- HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230709T060400Z&X-Amz-Expires=600&X-Amz-Signature=5f968a280fef66addeac8f3e64c5ec5d60a240a7ed667d8635663270c8e3b3fe&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	ACME	Penetrated
2023-07-06	PhonyC2 Framework Used By MuddyWater	Phonyc2bgiigaijja5_edrPs1.ps1	Endpoint Security	ACME	Penetrated
2023-07-11	Unleashing WhiteSnake Stealer	hxxps://acme-119.com/hotfiles/manual_upload/unleashing_whitesnake_stealer_087f2f 0a-b8cc-45d8-aa36-a6a01b9297a7/UnleashingbgijafbdcA2_browsingExe.exe?X-Amz-Algor ithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230711%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230711T100624Z&X-Amz-Expires=600&X-Amz-Signature=53df5b97eea23e8d561d457af55f1e76313e2722154b380e375b3233cd5afbd4&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	ACME	Penetrated
2023-07-11	Unleashing WhiteSnake Stealer	hxxps://acme-119.com/hotfiles/manual_upload/unleashing_whitesnake_stealer_087f2f 0a-b8cc-45d8-aa36-a6a01b9297a7/UnleashingbgijafbdcA1_browsingExe.exe?X-Amz-Algor ithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230711%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230711T100623Z&X-Amz-Expires=600&X-Amz-Signature=6a08fb2f2874841f2bab6982ca5115dd4e5fd10f870e1fde273caa13165b0988&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	ACME	Penetrated
2023-07-11	Threat Trend Report On Kimsuky	hxxps://acme-119.com/hotfiles/manual_upload/threat_trend_report_on_kimsuky_1cf69 0bf-821f-48ed-8c03-cb291a519d85/Threatbgijafbfgb38_browsingChm.chm?X-Amz-Algorit hm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJ PJC2Q3D5GWFTK3Q%2F20230711%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230711T051257Z&X-Amz-Expires=600&X-Amz-Signature=b87484f665d292db61613afe011d9435e32679ab9d79dadf4fafc1e46cf19e82&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	ACME	Penetrated
2023-07-10	Operation Brainleeches Targets Microsoft 365 Users	hxxps://acme-119.com/hotfiles/manual_upload/operation_brainleeches_targets_micro soft_365_users_acac1185-0d7f-47a2-8dfc-ddea7a245502/Operationbgiihibied11_browsi ngJs.js?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X -Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230710%2Feu-west-1%2Fs3%2Faws4_request& X-Amz-Date=20230710T102356Z&X-Amz-Expires=600&X-Amz-Signature=0a156c394f8f0ef81b203f1fe80df1391bec763157c7da173b73b4ff8776afcd&X-Amz-SignedHeaders=host&x-id=Get Object	Web Gateway	ACME	Penetrated
2023-07-10	TeamTNT Targets Cloud Native Environments	hxxps://acme-119.com/hotfiles/manual_upload/teamtnt_targets_cloud_native_environments_b865aebc-e863-4bd8-b32b-3f6ee3bd2645/Teamtntbgiigjfdih2_browsingElf.elf?X- Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230710%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230710T072454Z&X-Amz-Expires=600&X-Amz-Signature=85da2ae0c729b7cad4cfb2dbf16d01926d1f81a6066fc9333c3eed651c8719e9&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	ACME	Penetrated
2023-07-10	TeamTNT Targets Cloud Native Environments	hxxps://acme-119.com/hotfiles/manual_upload/teamtnt_targets_cloud_native_environments_b865aebc-e863-4bd8-b32b-3f6ee3bd2645/Teamtntbgiigjfdih1_browsingElf.elf?X- Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230710%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230710T072453Z&X-Amz-Expires=600&X-Amz-Signature=28c8462295d7bf4ed55ff3bf4484bce303f3f0ce90c087ff47fe87e635ff8428&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	ACME	Penetrated
2023-07-09	ACME	Truebotbgiiijfbga1_edrExe.exe	Endpoint Security	ACME	Penetrated
2023-07-09	ACME	Truebotbgiiijfbga3_edrExe.exe	Endpoint Security	ACME	Blocked
2023-07-09	ACME	Truebotbgiiijfbga4_edrExe.exe	Endpoint Security	ACME	Blocked
2023-07-09	ACME	Truebotbgiiijfbga_edr7Dll.dll	Endpoint Security	ACME	Blocked
2023-07-09	ACME	hxxp://74.144.192.43	Web Gateway	ACME	Offline/Removed
2023-07-09	ACME	hxxps://acme-119.com/hotfiles/manual_upload/us_cert_alert_-_%28aa23-187a%29_increased_truebot_activity_infects_u.s.and_canada_networks_c18bd470-6c4d-4289-a966-659944d071c9/Truebotbgiiijfbga9_browsingDll.dll?X-Amz-Algorithm=AWS4-HMAC-SHA256& X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230709T102858Z&X-Amz-Expires=600&X-Amz-Signature=4456b0ff5fbf574668f831c229514705b724fe1bef779ddb1194b9413c68ef49&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	ACME	Penetrated

ASM-VP REPORT

ACME FINANCIAL SERVICES 08/11/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-07-09	ACME	hxxps://acme-119.com/hotfiles/manual_upload/us_cert_alert_-_%28aa23-187a%29_increased_truebot_activity_infects_u.s.and_canada_networks_c18bd470-6c4d-4289-a966-659944d071c9/Truebotbgiiijfbga8_browsingDll.dll?X-Amz-Algorithm=AWS4-HMAC-SHA256& X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230709T102857Z&X-Amz-Expires=600&X-Amz-Signature=b6814e25ff1bf83285e08e5fb51ebbb4584f11852855146e59d943d243ad1d97&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	ACME	Penetrated
2023-07-09	ACME	hxxps://acme-119.com/hotfiles/manual_upload/us_cert_alert_-_%28aa23-187a%29_increased_truebot_activity_infects_u.s.and_canada_networks_c18bd470-6c4d-4289-a966-659944d071c9/Truebotbgiiijfbga6_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256& X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230709T102857Z&X-Amz-Expires=600&X-Amz-Signature=e0f33ab10835f2c67a2b3d469629c843f0953e004f1e7fec78ae02140ebc4c24&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	ACME	Penetrated
2023-07-09	ACME	hxxps://acme-119.com/hotfiles/manual_upload/us_cert_alert_-_%28aa23-187a%29_increased_truebot_activity_infects_u.s.and_canada_networks_c18bd470-6c4d-4289-a966-659944d071c9/Truebotbgiiijfbga5_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256& X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230709T102856Z&X-Amz-Expires=600&X-Amz-Signature=899d50d3a181f6bfcc0ef167ed32c7a0b6fc4cf843204d444c1e3639d73a0b5d&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	ACME	Penetrated
2023-07-09	ACME	hxxps://acme-119.com/hotfiles/manual_upload/us_cert_alert_-_%28aa23-187a%29_increased_truebot_activity_infects_u.s.and_canada_networks_c18bd470-6c4d-4289-a966-659944d071c9/Truebotbgiiijfbga2_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256& X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230709T102850Z&X-Amz-Expires=600&X-Amz-Signature=6f3544d37de557faf85779a3131095c3e0fdb26cafd64a40044d4dcdf1fc172a&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	ACME	Penetrated
2023-07-09	Buddyransome	Buddyransombgiiiijacb2_edrExe.exe	Endpoint Security	ACME	Blocked
2023-07-09	Buddyransome	hxxps://acme-119.com/hotfiles/manual_upload/buddyransome_8cb491e4-5136-4deb-8e19-2027964f5bd2/Buddyransombgiiiijacb1_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230709T080250Z&X-Amz-Expires=600&X-Amz-Signature=0ac1bd8f044640e0e3c8d676f556174fd2bfe957a07d7cf6dd5f0013517b2db5&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	ACME	Penetrated
2023-07-09	Threat Profile UNC3944	Threatbgiigjfhhb66_edrExe.exe	Endpoint Security	ACME	Blocked
2023-07-09	Threat Profile UNC3944	Threatbgiigjfhhb_edr71Exe.exe	Endpoint Security	ACME	Penetrated
2023-07-09	Threat Profile UNC3944	Threatbgiigjfhhb_acme-119.com	Endpoint Security	ACME	Blocked
2023-07-09	Threat Profile UNC3944	Threatbgiigjfhhb_edr74Exe.exe	Endpoint Security	ACME	Blocked
2023-07-09	Threat Profile UNC3944	Threatbgiigjfhhb81_edrExe.exe	Endpoint Security	ACME	Blocked
2023-07-09	Threat Profile UNC3944	Threatbgiigjfhhb_edr78Exe.exe	Endpoint Security	ACME	Blocked
2023-07-09	Threat Profile UNC3944	hxxp://72.108.75.39	Web Gateway	ACME	Offline/Removed
2023-07-06	PhonyC2 Framework Used By MuddyWater	hxxp://155.110.157.22	Web Gateway	ACME	Offline/Removed
2023-07-06	PhonyC2 Framework Used By MuddyWater	hxxps://acme-119.com/hotfiles/manual_upload/phonyc2_framework_used_by_muddywater_055285f0-d830-4652-b2b3-c438a424a18e/Phonyc2bgiigaijja10_browsingJs.js?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230706%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230706T050232Z&X-Amz-Expires=600&X-Amz-Signature=1809f9e2cb57d1fb084bceb800c59435d06d3fa6699214923adf5424b82a8118&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	ACME	Penetrated
2023-07-06	PhonyC2 Framework Used By MuddyWater	hxxps://acme-119.com/hotfiles/manual_upload/phonyc2_framework_used_by_muddywater_055285f0-d830-4652-b2b3-c438a424a18e/Phonyc2bgiigaijja9_browsingJs.js?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230706%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230706T050232Z&X-Amz-Expires=600&X-Amz-Signature=7c746f69a23068c58228de91ecccd4144422b6a7c70fb76cdd90538967de4e90&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	ACME	Penetrated

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

TLP:AMBER

ASM-VP REPORT

ACME FINANCIAL SERVICES 08/11/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
N/A	The suspected Maha grass organization uses the WarHawk backdoor variant Spyder to spy on many countries	Thebgiifccegi21_edrExe.exe	Endpoint Security	ACME	Blocked
N/A	The suspected Maha grass organization uses the WarHawk backdoor variant Spyder to spy on many countries	Thebgiifccegi14_edrExe.exe	Endpoint Security	ACME	Blocked
2023-07-05	The suspected Maha grass organization uses the WarHawk backdoor variant Spyder to spy on many countries	Thebgiifccegi18_edrExe.exe	Endpoint Security	ACME	Blocked
2023-07-05	The suspected Maha grass organization uses the WarHawk backdoor variant Spyder to spy on many countries	Thebgiifccegi10_edrExe.exe	Endpoint Security	ACME	Blocked
2023-07-05	The suspected Maha grass organization uses the WarHawk backdoor variant Spyder to spy on many countries	hxxp://236.164.210.131	Web Gateway	ACME	Offline/Removed
2023-07-05	The suspected Maha grass organization uses the WarHawk backdoor variant Spyder to spy on many countries	hxxps://acme-119.com/hotfiles/manual_upload/the_suspected_maha_grass_organization_uses_the_warhawk_backdoor_variant_spyder_to_spy_on_many_countries_b12092f9-cbef-4912-87fe-16158033afbc/Thebgiifccegi20_browsingExe.exe?X-Amz-Algorithm=AWS4-HM AC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GW FTK3Q%2F20230705%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230705T050503Z&X-Amz-Expires=600&X-Amz-Signature=b1e1ab2e159d5b31dbb4f309624c84328629268967fee6b10 bb887d8d34e2ee6&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	ACME	Penetrated
2023-07-05	The suspected Maha grass organization uses the WarHawk backdoor variant Spyder to spy on many countries	hxxps://acme-119.com/hotfiles/manual_upload/the_suspected_maha_grass_organization_uses_the_warhawk_backdoor_variant_spyder_to_spy_on_many_countries_b12092f9-cbef-4912-87fe-16158033afbc/Thebgiifccegi19_browsingExe.exe?X-Amz-Algorithm=AWS4-HM AC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GW FTK3Q%2F20230705%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230705T050503Z&X-Amz-Expires=600&X-Amz-Signature=7677e41e48bde0625b6428970b672fc833fbf984e088d4ca7 4ecbdbb8492ad93&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	ACME	Penetrated

ASM-VP REPORT

ACME FINANCIAL SERVICES 08/11/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-07-05	The suspected Maha grass organization uses the WarHawk backdoor variant Spyder to spy on many countries	hxxps://acme-119.com/hotfiles/manual_upload/the_suspected_maha_grass_organization_uses_the_warhawk_backdoor_variant_spyder_to_spy_on_many_countries_b12092f9-cbef-4912-87fe-16158033afbc/Thebgiifccegi1_browsing7Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230705%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230705T050503Z&X-Amz-Expires=600&X-Amz-Signature=f9a24c2a2c268b875f14f539a10b9cb82cca5813343f97a0350a02b254f339f4&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	ACME	Penetrated
2023-07-05	The suspected Maha grass organization uses the WarHawk backdoor variant Spyder to spy on many countries	hxxps://acme-119.com/hotfiles/manual_upload/the_suspected_maha_grass_organization_uses_the_warhawk_backdoor_variant_spyder_to_spy_on_many_countries_b12092f9-cbef-4912-87fe-16158033afbc/Thebgiifccegi13_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230705%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230705T050502Z&X-Amz-Expires=600&X-Amz-Signature=6436ed4460b786d3fb7c387bb5d7ccc263e312921e614d470163f99b014e2629&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	ACME	Penetrated
2023-07-05	The suspected Maha grass organization uses the WarHawk backdoor variant Spyder to spy on many countries	hxxps://acme-119.com/hotfiles/manual_upload/the_suspected_maha_grass_organization_uses_the_warhawk_backdoor_variant_spyder_to_spy_on_many_countries_b12092f9-cbef-4912-87fe-16158033afbc/Thebgiifccegi9_browsingExe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230705%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230705T050501Z&X-Amz-Expires=600&X-Amz-Signature=4f6752acce685add0400e15f342f729db1786819470291edb8689a0163ed561d&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	ACME	Penetrated
2023-07-04	The DPRK strikes using a new variant of RUSTBUCKET	Thebgiiecjcjg12_edr7Macho.macho	Endpoint Security	ACME	Blocked
2023-07-04	The DPRK strikes using a new variant of RUSTBUCKET	Thebgiiecjcjg132_edrMacho.macho	Endpoint Security	ACME	Blocked
2023-07-04	The DPRK strikes using a new variant of RUSTBUCKET	Thebgiiecjcjg129_edrMacho.macho	Endpoint Security	ACME	Blocked
2023-07-04	The DPRK strikes using a new variant of RUSTBUCKET	hxxps://acme-119.com/hotfiles/manual_upload/the_dprk_strikes_using_a_new_variant_of_rustbucket_5ef1bf2d-e849-470a-b237-647c9e112e12/Thebgiiecjcjg131_browsingMacho.macho?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230704%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230704T061302Z&X-Amz-Expires=600&X-Amz-Signature=de0141f38b13d33e5cce3af1d1144768303bac972b3b527390f6eeeb9b6005ec&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	ACME	Penetrated
2023-07-04	The DPRK strikes using a new variant of RUSTBUCKET	hxxps://acme-119.com/hotfiles/manual_upload/the_dprk_strikes_using_a_new_variant_of_rustbucket_5ef1bf2d-e849-470a-b237-647c9e112e12/Thebgiiecjcjg126_browsingMacho.macho?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230704%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230704T061300Z&X-Amz-Expires=600&X-Amz-Signature=7e20bfa25055746c21c9965eafd98b21eb0bb76492c3462425a5d41bfb80cc10&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	ACME	Penetrated
2023-07-04	The DPRK strikes using a new variant of RUSTBUCKET	hxxps://acme-119.com/hotfiles/manual_upload/the_dprk_strikes_using_a_new_variant_of_rustbucket_5ef1bf2d-e849-470a-b237-647c9e112e12/Thebgiiecjcjg125_browsingMacho.macho?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230704%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230704T061259Z&X-Amz-Expires=600&X-Amz-Signature=fe0f7a9a77bf9714700f032293a4f2cf498aaeb54dd6d06c3eea8893303ee1e2&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	ACME	Penetrated
2023-07-04	The DPRK strikes using a new variant of RUSTBUCKET	hxxps://acme-119.com/hotfiles/manual_upload/the_dprk_strikes_using_a_new_variant_of_rustbucket_5ef1bf2d-e849-470a-b237-647c9e112e12/Thebgiiecjcjg122_browsingMacho.macho?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230704%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230704T061257Z&X-Amz-Expires=600&X-Amz-Signature=2ad09aac098ec7d61093b3e979e4f188772a0007cf879291ccf604b76d65fc44&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	ACME	Penetrated
2023-07-03	Word Document with an Online Attached Template	hxxps://acme-119.com/hotfiles/manual_upload/word_document_with_an_online_attached_template_10c61f38-086a-4f78-980a-6d2253adcd93/Matryoshkabgiididgjd3_browsingEx e.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-A mz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230703%2Feu-west-1%2Fs3%2Faws4_request&X- Amz-Date=20230703T113604Z&X-Amz-Expires=600&X-Amz-Signature=93890d6822fc3d0cc22f5c2a2dd8ad6b2bd1ec8b5d5741fb930c27114a086f7c&X-Amz-SignedHeaders=host&x-id=GetOb ject	Web Gateway	ACME	Penetrated

ASM-VP REPORT

ACME FINANCIAL SERVICES 08/11/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-07-03	Word Document with an Online Attached Template	hxxps://acme-119.com/hotfiles/manual_upload/word_document_with_an_online_attache d_template_10c61f38-086a-4f78-980a-6d2253adcd93/Matryoshkabgiididgjd1_browsingDo cx.docx?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X -Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230703%2Feu-west-1%2Fs3%2Faws4_request& X-Amz-Date=20230703T113604Z&X-Amz-Expires=600&X-Amz-Signature=418cb4ac674054d84d 2609597119093905a329a78851377553d1ff194c5f7d66&X-Amz-SignedHeaders=host&x-id=Get Object	Web Gateway	ACME	Penetrated
2023-07-03	Word Document with an Online Attached Template	hxxps://acme-119.com/hotfiles/manual_upload/word_document_with_an_online_attache d_template_10c61f38-086a-4f78-980a-6d2253adcd93/Matryoshkabgiididgjd2_browsingRt f.rtf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-A mz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230703%2Feu-west-1%2Fs3%2Faws4_request&X- Amz-Date=20230703T113603Z&X-Amz-Expires=600&X-Amz-Signature=0db91b5ea14aa5bbbb48 0adc56bcddd3991fc6468f9e86d974575036db83a399&X-Amz-SignedHeaders=host&x-id=GetOb ject	Web Gateway	ACME	Penetrated
2023-07-03	New Qakbot (Qbot) activity	Qbotbgiidicbbd1_edrDll.dll	Endpoint Security	ACME	Blocked
2023-07-03	New Qakbot (Qbot) activity	Qbotbgiidicbbd2_edrJs.js	Endpoint Security	ACME	Penetrated
2023-07-03	New Qakbot (Qbot) activity	hxxps://acme-119.com/hotfiles/manual_upload/new_qakbot_%28qbot%29_activity_f5a2f 41e-fc87-429d-b4af-e3e89d8c012f/Qbotbgiidicbbd3_browsingZip.zip?X-Amz-Algorithm= AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC 2Q3D5GWFTK3Q%2F20230703%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230703T1115 03Z&X-Amz-Expires=600&X-Amz-Signature=f9be98830319f00386be9250148eff8e7c04b29c88 914560e147e13590889b9a&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	ACME	Penetrated
2023-07-03	Mirai Campaign Leveraging Multiple IoT Exploits	Miraibgihfhcccf2_acme-113.com	Endpoint Security	ACME	Blocked
2023-07-03	Mirai Campaign Leveraging Multiple IoT Exploits	Miraibgihfhcccf3_acme-113.com	Endpoint Security	ACME	Blocked
2023-07-03	Mirai Campaign Leveraging Multiple IoT Exploits	Miraibgihfhcccf6_acme-113.com	Endpoint Security	ACME	Blocked
2023-07-03	Mirai Campaign Leveraging Multiple IoT Exploits	Miraibgihfhcccf_acme-113.com	Endpoint Security	ACME	Blocked
2023-07-03	Mirai Campaign Leveraging Multiple IoT Exploits	Miraibgihfhcccf5_acme-113.com	Endpoint Security	ACME	Blocked
2023-07-03	Mirai Campaign Leveraging Multiple IoT Exploits	Miraibgihfhcccf12_acme-113.com	Endpoint Security	ACME	Blocked
2023-07-03	Mirai Campaign Leveraging Multiple IoT Exploits	hxxps://acme-119.com/hotfiles/manual_upload/mirai_campaign_leveraging_multiple_i ot_exploits_29e3fabb-a46e-42e6-9931-6276108ef13d/Miraibgihfhcccf13_browsingElf.e lf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230703%2Feu-west-1%2Fs3%2Faws4_request&X-Amz - Date=20230703T083511Z&X-Amz-Expires=600&X-Amz-Signature=af73c6f39c5061619c31bca 7af6e19c1e5acc64c362d36fe6bd27c648e32ac6f&X-Amz-SignedHeaders=host&x-id=GetObjec t	Web Gateway	ACME	Penetrated
2023-07-03	Mirai Campaign Leveraging Multiple IoT Exploits	hxxps://acme-119.com/hotfiles/manual_upload/mirai_campaign_leveraging_multiple_i ot_exploits_29e3fabb-a46e-42e6-9931-6276108ef13d/Miraibgihfhcccf11_browsingElf.e lf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230703%2Feu-west-1%2Fs3%2Faws4_request&X-Amz - Date=20230703T083511Z&X-Amz-Expires=600&X-Amz-Signature=57386a5b249827c8a6eccb9 d4d498efb6109f3ccca8f69762e0471137ba9d56b&X-Amz-SignedHeaders=host&x-id=GetObjec t	Web Gateway	ACME	Penetrated
2023-07-03	Mirai Campaign Leveraging Multiple IoT Exploits	hxxps://acme-119.com/hotfiles/manual_upload/mirai_campaign_leveraging_multiple_i ot_exploits_29e3fabb-a46e-42e6-9931-6276108ef13d/Miraibgihfhcccf10_browsingElf.e lf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230703%2Feu-west-1%2Fs3%2Faws4_request&X-Amz - Date=20230703T083510Z&X-Amz-Expires=600&X-Amz-Signature=ac527e12aeb4c8076c509d3 6ddf4a8bce2d08cae78309fa08e9a9ff762300da3&X-Amz-SignedHeaders=host&x-id=GetObjec t	Web Gateway	ACME	Penetrated

ASM-VP REPORT

ACME FINANCIAL SERVICES 08/11/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-07-03	Mirai Campaign Leveraging Multiple IoT Exploits	hxxps://acme-119.com/hotfiles/manual_upload/mirai_campaign_leveraging_multiple_iot_exploits_29e3fabb-a46e-42e6-9931-6276108ef13d/Miraibgihfhcccf9_browsingElf.el f?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230703%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230703T083510Z&X-Amz-Expires=600&X-Amz-Signature=94e85ff0f2d254b3999fcb38b87b153e4b952944edbfe7496cab4e883d8d02c2&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	ACME	Penetrated
2023-07-03	Mirai Campaign Leveraging Multiple IoT Exploits	hxxps://acme-119.com/hotfiles/manual_upload/mirai_campaign_leveraging_multiple_iot_exploits_29e3fabb-a46e-42e6-9931-6276108ef13d/Miraibgihfhcccf8_browsingElf.el f?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230703%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230703T083510Z&X-Amz-Expires=600&X-Amz-Signature=96b678c438e50bd8dc4401f8f377d1c8a7ffdad9af9c5cab265bcd832ac4b047&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	ACME	Penetrated
2023-07-03	Mirai Campaign Leveraging Multiple IoT Exploits	hxxps://acme-119.com/hotfiles/manual_upload/mirai_campaign_leveraging_multiple_iot_exploits_29e3fabb-a46e-42e6-9931-6276108ef13d/Miraibgihfhcccf4_browsingElf.el f?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230703%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230703T083509Z&X-Amz-Expires=600&X-Amz-Signature=f7b4fec1057883a3cdb22fc3e42e8382181460a7b0f798fc983230196242b1e2&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	ACME	Penetrated
2023-07-03	Mirai Campaign Leveraging Multiple IoT Exploits	hxxps://acme-119.com/hotfiles/manual_upload/mirai_campaign_leveraging_multiple_iot_exploits_29e3fabb-a46e-42e6-9931-6276108ef13d/Miraibgihfhcccf1_browsingElf.el f?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230703%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230703T083508Z&X-Amz-Expires=600&X-Amz-Signature=600ea0407ba1efdeb3813df1be60b0f0e7134bd01abdf7021e65d85a2c750e65&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	ACME	Penetrated
2023-07-02	Gh0stBins RAT Analysis	Gh0stbinsbgihjbhhhb1_edrExe.exe	Endpoint Security	ACME	Blocked
2023-07-02	Gh0stBins RAT Analysis	Gh0stbinsbgihjbhhhb4_edrDll.dll	Endpoint Security	ACME	Penetrated
2023-07-02	Gh0stBins RAT Analysis	Gh0stbinsbgihjbhhhb3_edrDll.dll	Endpoint Security	ACME	Penetrated
2023-07-02	Gh0stBins RAT Analysis	hxxp://127.196.212.147	Web Gateway	ACME	Offline/Removed
2023-06-29	8Base Ransomware - A Heavy Hitting Player	Eightbasebgiiacggfh4_edrExe.exe	Endpoint Security	ACME	Blocked
2023-06-29	8Base Ransomware - A Heavy Hitting Player	hxxps://acme-119.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%2F20230629%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230629T082226Z&X-Amz-Expires=600&X-Amz-Signature=9dcec3e8b59e83d537cb77d276cabdb59e70c877512dbdccddcd88865be25a21&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	ACME	Penetrated
2023-06-29	8Base Ransomware - A Heavy Hitting Player	hxxps://acme-119.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%2F20230629%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230629T082226Z&X-Amz-Expires=600&X-Amz-Signature=1539886949054fb088bdc7236d34969c0333665df892d2fdfb46b6718e32d596&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	ACME	Penetrated
2023-06-29	8Base Ransomware - A Heavy Hitting Player	hxxps://acme-119.com/hotfiles/manual_upload/8base_ransomware_-_a_heavy_hitting_player_a5893f49-67e5-45ef-a151-6ce0c11c6ff8/Eightbasebgiiacggfh3_browsingExe.exe? X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230629%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230629T082225Z&X-Amz-Expires=600&X-Amz-Signature=37e2b0cbdff87897ad8a16a7bc545c73b64e52d95db0fa7fa52037492abd5a2c&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	ACME	Penetrated
2023-06-29	Tracing The Footsteps Of Red Wolf	Tracingbgiiaaecbg1_acme-113.com	Endpoint Security	ACME	Penetrated
2023-06-29	Tracing The Footsteps Of Red Wolf	Tracingbgiiaaecbg2_acme-113.com	Endpoint Security	ACME	Penetrated
2023-06-29	Tracing The Footsteps Of Red Wolf	Tracingbgiiaaecbg3_edrDll.dll	Endpoint Security	ACME	Penetrated
2023-07-09	Threat Profile UNC3944	hxxps://acme-119.com/hotfiles/manual_upload/threat_profile_unc3944_f7ba8a64-eecc -477f-a86e-0cbdccc2a0c9/Threatbgiigjfhhb81_browsingExe.exe?X-Amz-Algorithm=AWS4- HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230709T060403Z&X-Amz-Expires=600&X-Amz-Signature=51c89997039516b1ef4e46c507a41dc96fc9977b6de5422b39c878e08d8b75e5&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	ACME	Penetrated

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

ASM-VP REPORT

ACME FINANCIAL SERVICES 08/11/2023

Timestamp	Name	Attack_Payload	Attack_Vector	Target	Status
2023-07-09	Threat Profile UNC3944	hxxps://acme-119.com/hotfiles/manual_upload/threat_profile_unc3944_f7ba8a64-eecc -477f-a86e-0cbdccc2a0c9/Threatbgiigjfhhb_browsing78Exe.exe?X-Amz-Algorithm=AWS4- HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230709T060402Z&X-Amz-Expires=600&X-Amz-Signature=d65d9b9ee86bcf0d385a724db68c61a9a7600cbf692861cc97c978634b23dd34&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	ACME	Penetrated
2023-07-09	Threat Profile UNC3944	hxxps://acme-119.com/hotfiles/manual_upload/threat_profile_unc3944_f7ba8a64-eecc -477f-a86e-0cbdccc2a0c9/Threatbgiigjfhhb_browsing74Exe.exe?X-Amz-Algorithm=AWS4- HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230709T060400Z&X-Amz-Expires=600&X-Amz-Signature=a4d1ba25bfcad8929d171c92f4ab1ebda755151a1ab25ce086e919b8b0fe4308&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	ACME	Penetrated
2023-07-09	Threat Profile UNC3944	hxxps://acme-119.com/hotfiles/manual_upload/threat_profile_unc3944_f7ba8a64-eecc -477f-a86e-0cbdccc2a0c9/Threatbgiigjfhhb_browsing71Exe.exe?X-Amz-Algorithm=AWS4- HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230709T060359Z&X-Amz-Expires=600&X-Amz-Signature=46edce813d31907f553cff6ea8b66f9b8b8263e75936ec3df2e561861f548ba2&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	ACME	Penetrated
2023-07-09	Threat Profile UNC3944	hxxps://acme-119.com/hotfiles/manual_upload/threat_profile_unc3944_f7ba8a64-eecc -477f-a86e-0cbdccc2a0c9/Threatbgiigjfhhb_browsing70Elf.elf?X-Amz-Algorithm=AWS4- HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230709T060357Z&X-Amz-Expires=600&X-Amz-Signature=fd5d66208fff5440be1313d55ca2f32d059888741148bce6ba3b00938b3c60a8&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	ACME	Penetrated
2023-07-09	Threat Profile UNC3944	hxxps://acme-119.com/hotfiles/manual_upload/threat_profile_unc3944_f7ba8a64-eecc -477f-a86e-0cbdccc2a0c9/Threatbgiigjfhhb66_browsingExe.exe?X-Amz-Algorithm=AWS4- HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20230709%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230709T060356Z&X-Amz-Expires=600&X-Amz-Signature=7cad70acf6449f90bcda4ede5da888d28a2aba774c549a2e982fb8ff4f235c1e&X-Amz-SignedHeaders=host&x-id=GetObject	Web Gateway	ACME	Penetrated
2023-07-06	PhonyC2 Framework Used By MuddyWater	Phonyc2bgiigaijja10_edrJs.js	Endpoint Security	ACME	Penetrated
2023-07-06	PhonyC2 Framework Used By MuddyWater	Phonyc2bgiigaijja9_edrJs.js	Endpoint Security	ACME	Penetrated
2023-07-11	Unleashing WhiteSnake Stealer	UnleashingbgijafbdcaI_edrExe.exe	Endpoint Security	ACME	Blocked
2023-07-11	Unleashing WhiteSnake Stealer	UnleashingbgijafbdcaI2_edrExe.exe	Endpoint Security	ACME	Blocked
2023-07-11	Threat Trend Report On Kimsuky	Threatbgijafbfgb38_acme-119.com	Endpoint Security	ACME	Penetrated
2023-07-10	Operation Brainleeches Targets Microsoft 365 Users	Operationbgiihibied11_edrJs.js	Endpoint Security	ACME	Penetrated
2023-07-10	Operation Brainleeches Targets Microsoft 365 Users	hxxp://73.108.178.106	Web Gateway	ACME	Offline/Removed

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

Threats

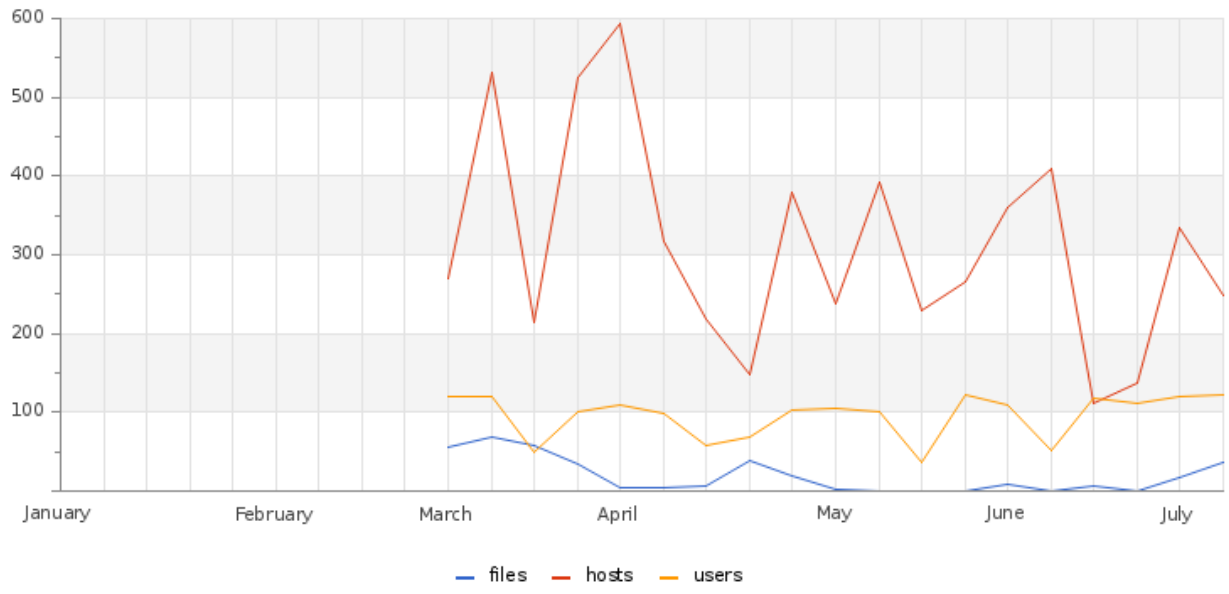
MSS-UTM

MSS-EDR

Average Threat - User Defined

98

Threat Score



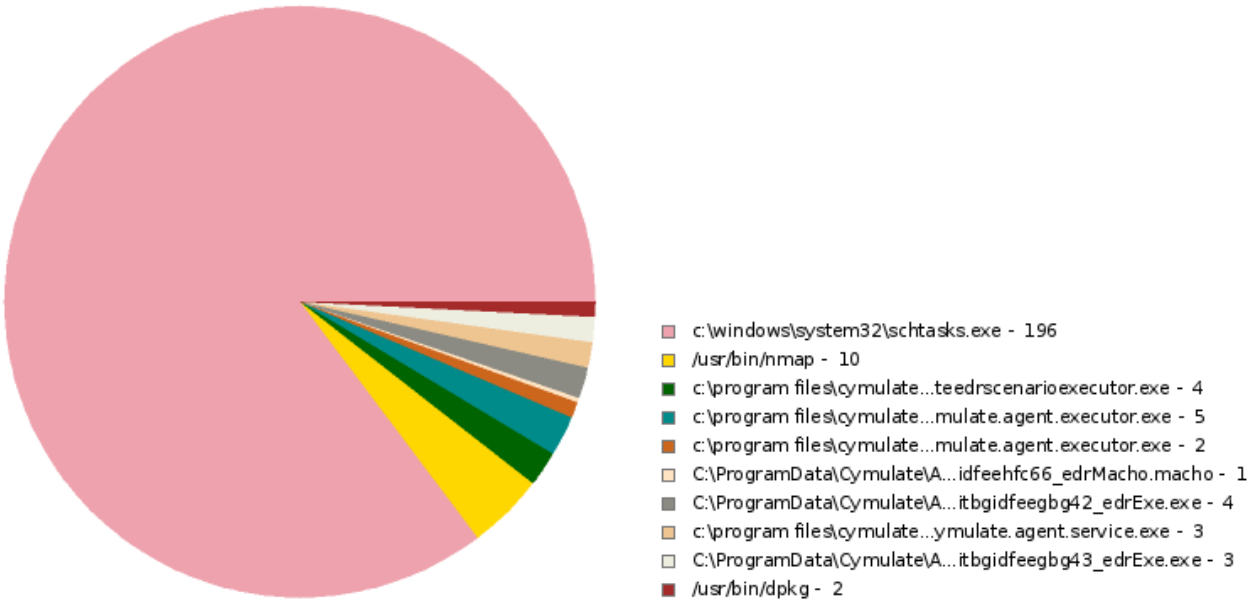
LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

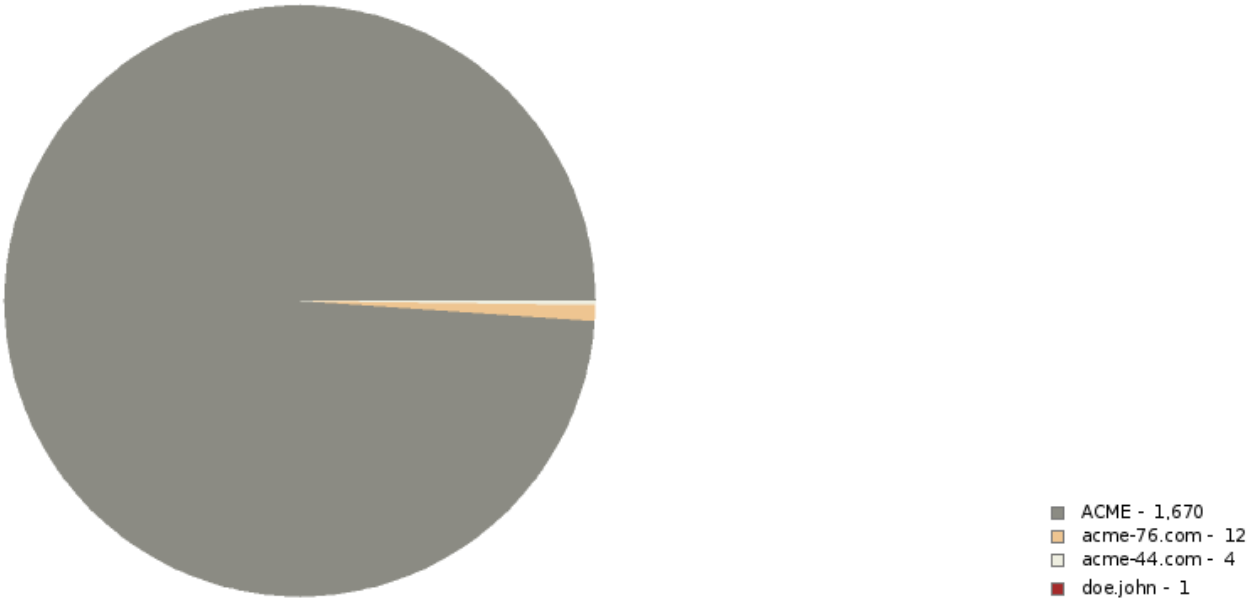
ASM-VP REPORT

ACME FINANCIAL SERVICES 08/11/2023

Events by File Path - User Defined



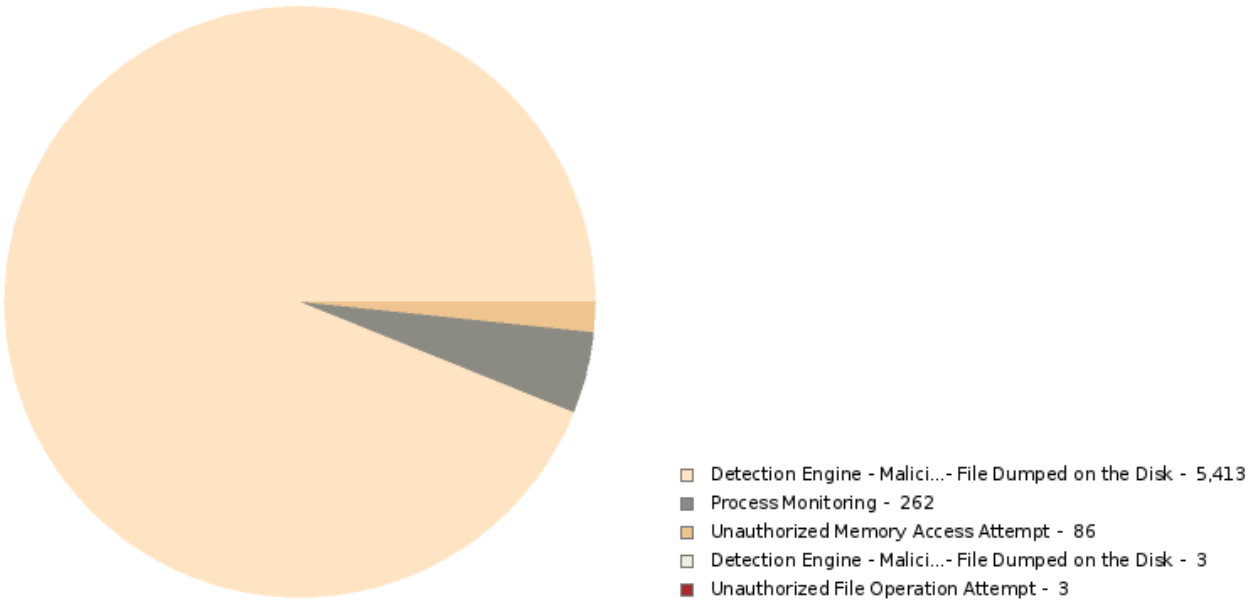
Events by Host Name - User Defined



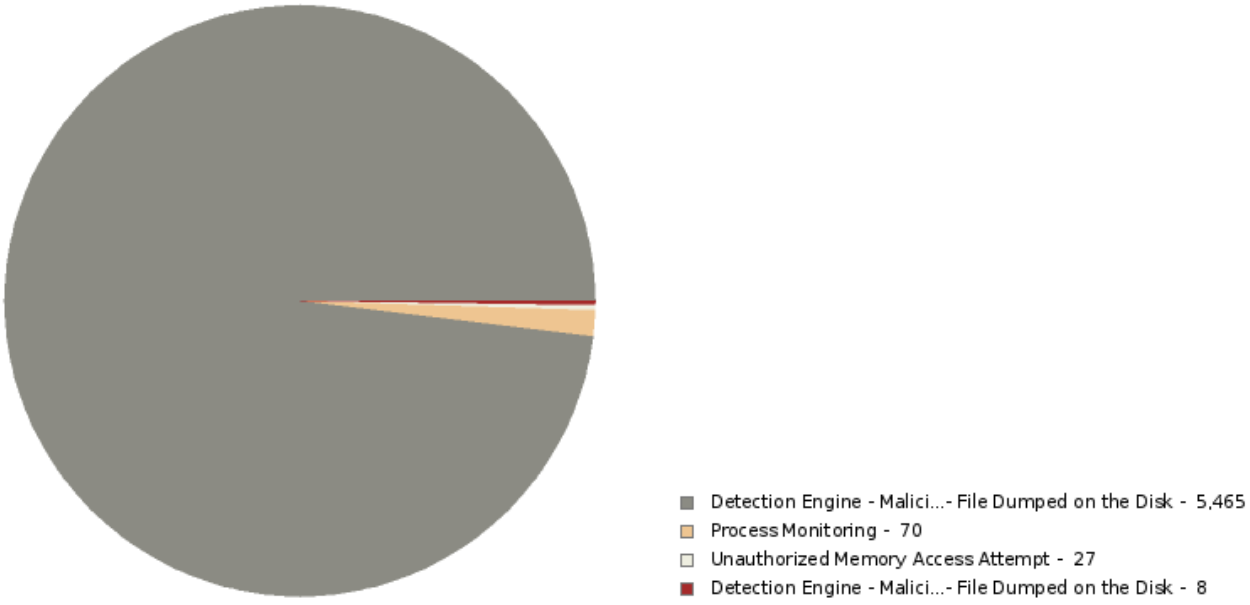
LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

Events by Event Name - User Defined



High Severity Events by Event Name - User Defined



Brute Force Detection by Ratio - User Defined

Host \ User Name	Ratio (Bad : Good)	Probability
pdoe	2 : 1	2
jane21	153 : 97	1.58
john.doe	3 : 86	0.02
jdoe	1 : 87	0.01
jane57	1 : 137	0.01
john.doe	1 : 301	3

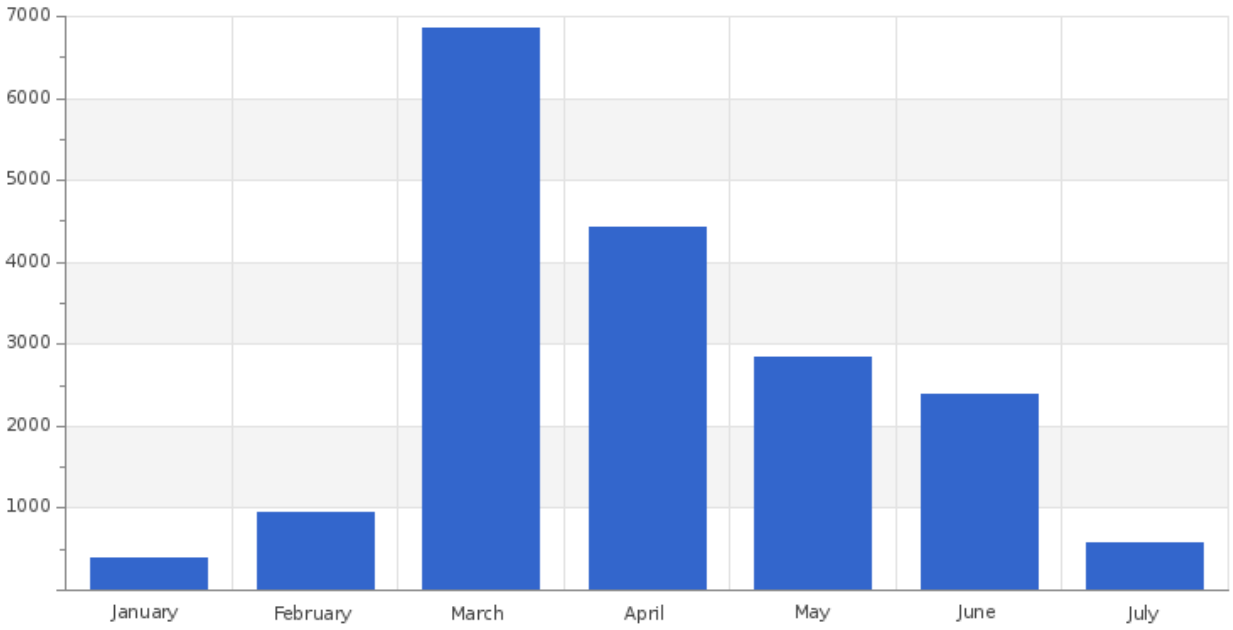
High Severity Events

Host	File Path	Severity	count
ACME	c:\windows\system32\control.exe	7	1
ACME	c:\windows\system32\mshta.exe	7	1
ACME	c:\windows\system32\regsvr32.exe	6	1
ACME	c:\windows\system32\schtasks.exe	7	61
ACME	c:\windows\system32\windowspowershell\v1.0\powershell.exe	2	2
doe.john	pdoe	2	2
jane36	udoe	5	2
acme-44.com	/bin/cat	6	2
acme-44.com	/bin/systemctl	2	2

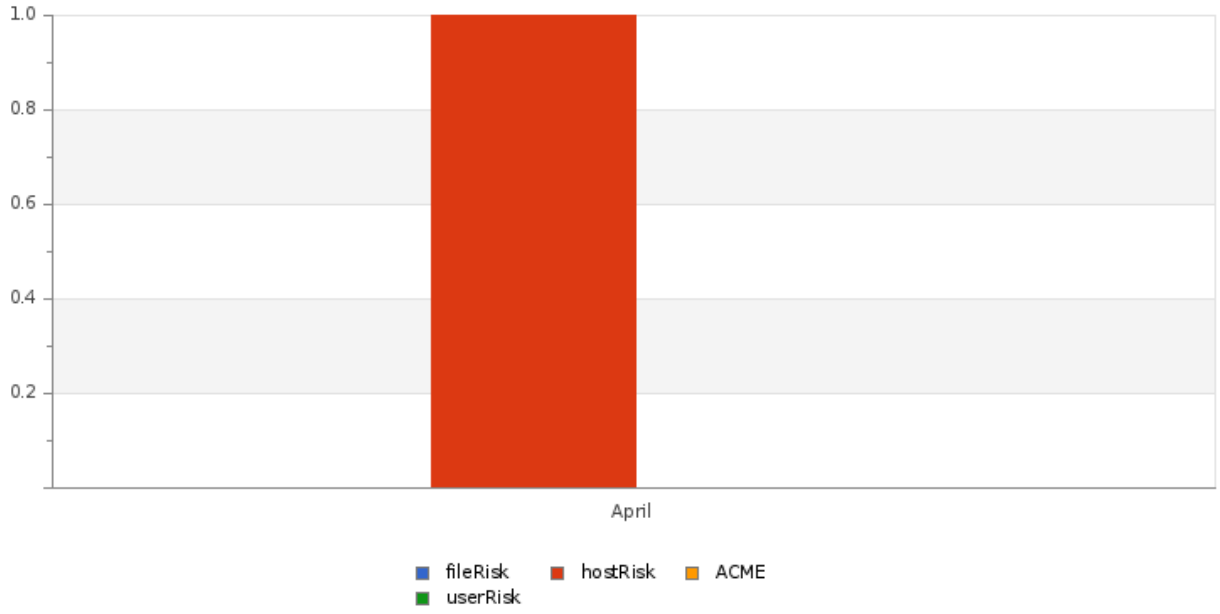
ASM-VP REPORT

ACME FINANCIAL SERVICES 08/11/2023

Events



Close Alerts *



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

Total Hosts - User Defined

30

High Severity Events by File Path - User Defined

File Path	Severity	Event Count
C:\ProgramData\Cymulate\AV\64889a45063343e6a9618093\acme-106.com	7	2
C:\ProgramData\Cymulate\AV\64889a45063343e6a9618093\acme-106.com	5	2
C:\ProgramData\Cymulate\AV\64889a45063343e6a9618093\Sample11Xlsx.xlsx	3	2
C:\ProgramData\Cymulate\AV\64889a45063343e6a9618093\acme-106.com	9	1
C:\ProgramData\Cymulate\AV\64889a45063343e6a9618093\Sample13Exe_upx.exe_upx	7	1
C:\ProgramData\Cymulate\AV\64889a45063343e6a9618093\acme-106.com	5	2
C:\ProgramData\Cymulate\AV\64889a45063343e6a9618093\acme-106.com	10	2
C:\ProgramData\Cymulate\AV\64889a45063343e6a9618093\Sample13Xlsx.xlsx	5	2
C:\ProgramData\Cymulate\AV\64889a45063343e6a9618093\acme-106.com	6	1
C:\ProgramData\Cymulate\AV\64889a45063343e6a9618093\acme-106.com	3	1

High Severity Events by Host Name - User Defined

Host	Severity	Event Count
ACME	8	1,496
ACME	7	3,812
acme-44.com	6	11
doe.john	3	3

MSS-DDOS

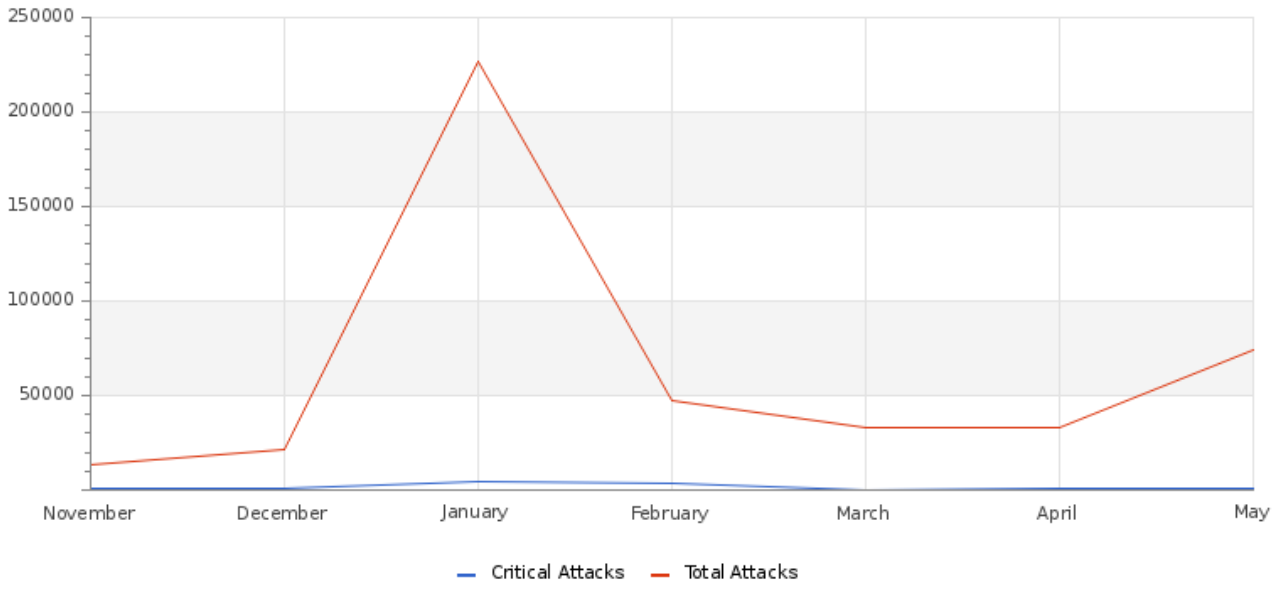
Total Attacks over 24 hours

5

Critical Attacks over 24 hours

2

Total & Critical Attacks Per Month In Last 6 Months



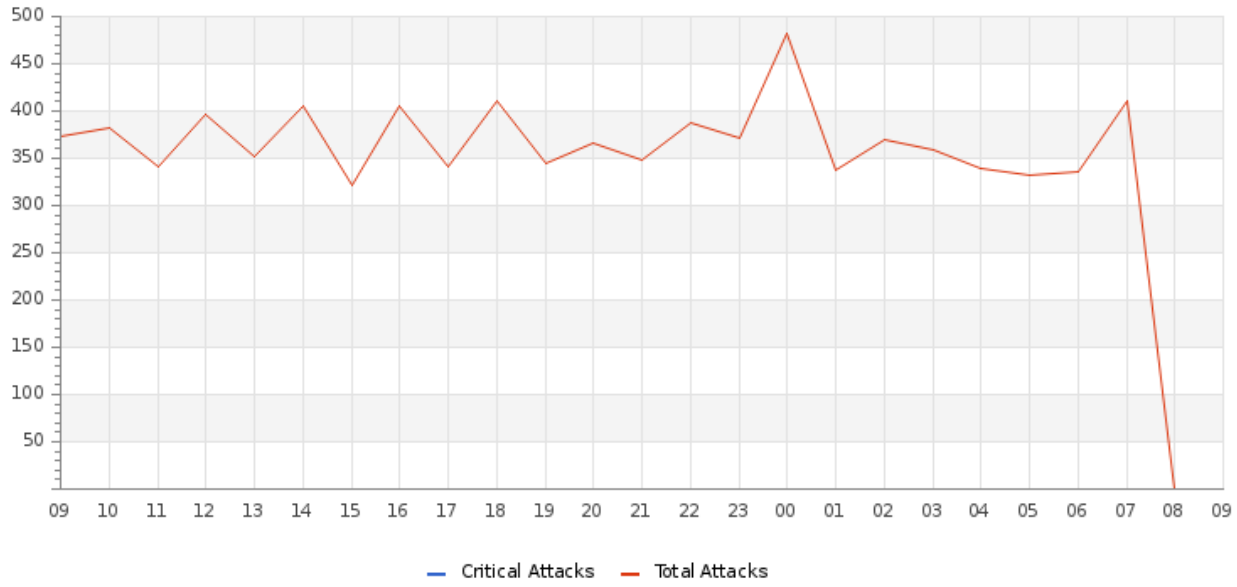
LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

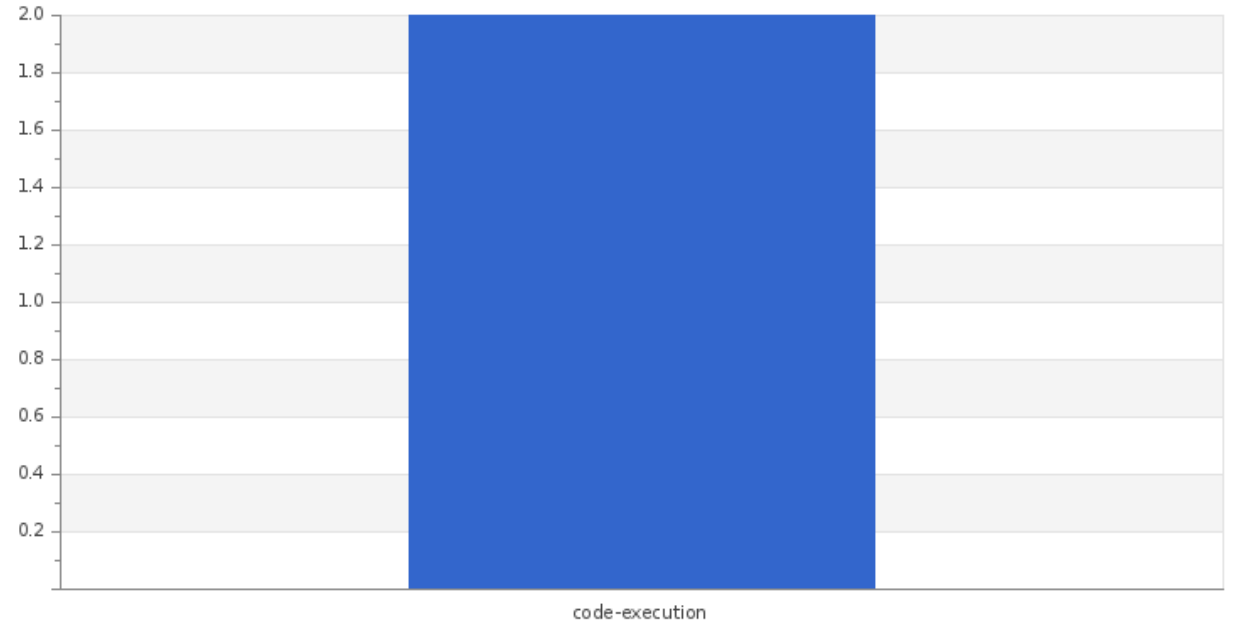
ASM-VP REPORT

ACME FINANCIAL SERVICES 08/11/2023

Executive Summary - Critical and Total Attacks In Past 24 Hours



Critical Attacks Blocked



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

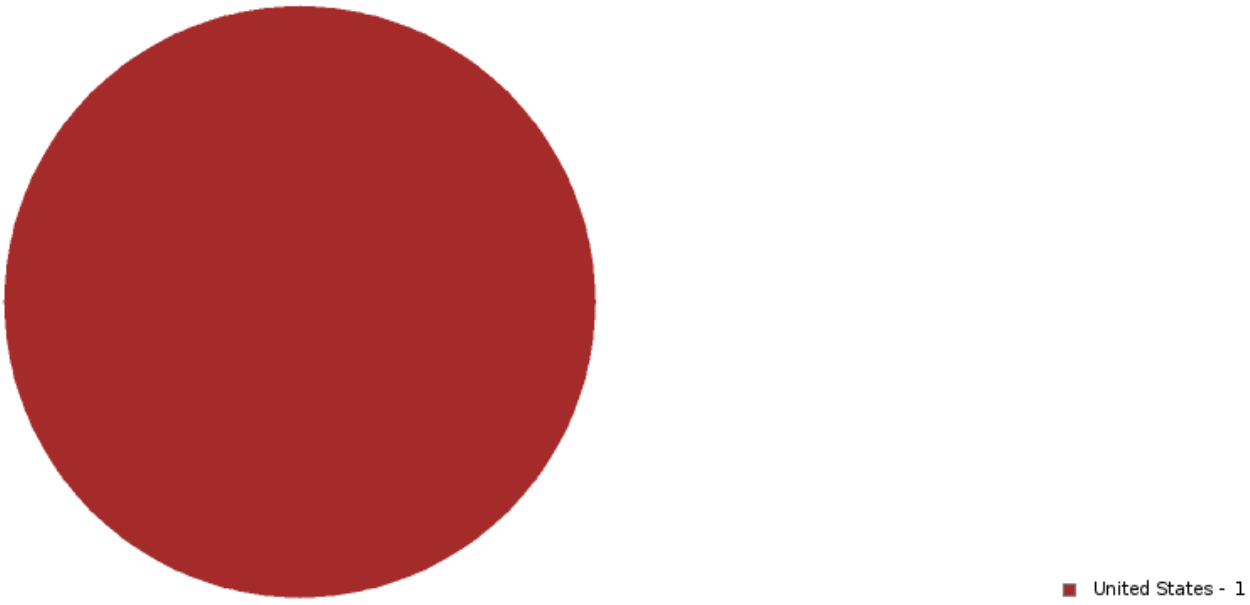
ASM-VP REPORT

ACME FINANCIAL SERVICES 08/11/2023

Executive Summary - Most Common Attack Durations

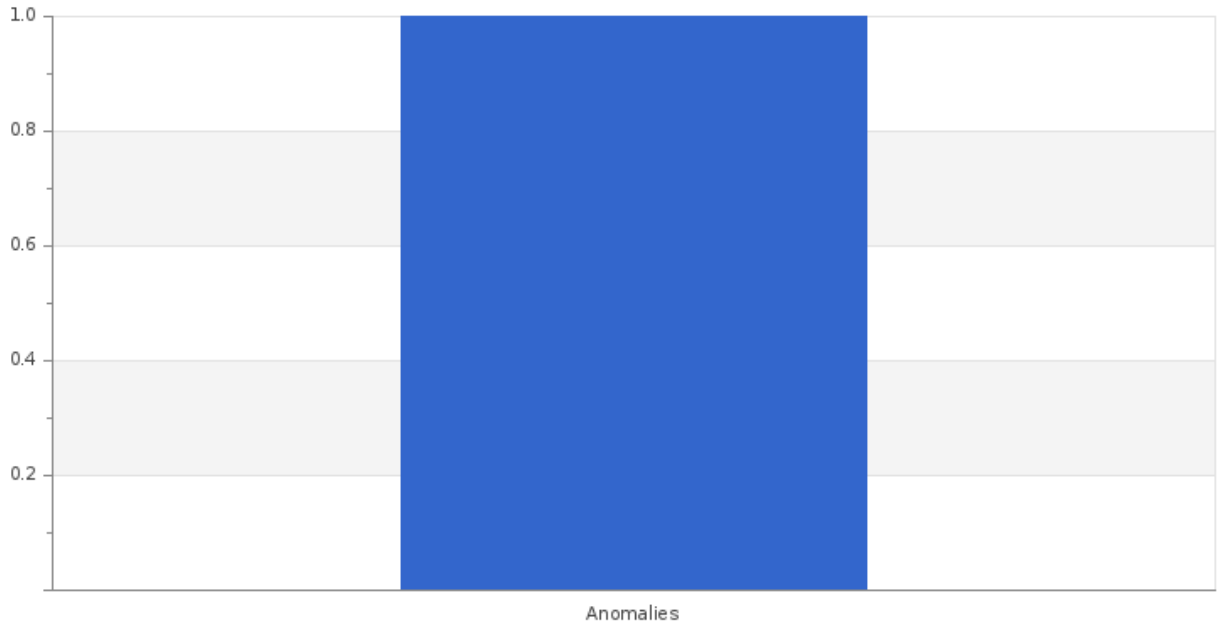
range	Anomalies
Less Than A Minute	1

Executive Summary - Top Attacking Countries

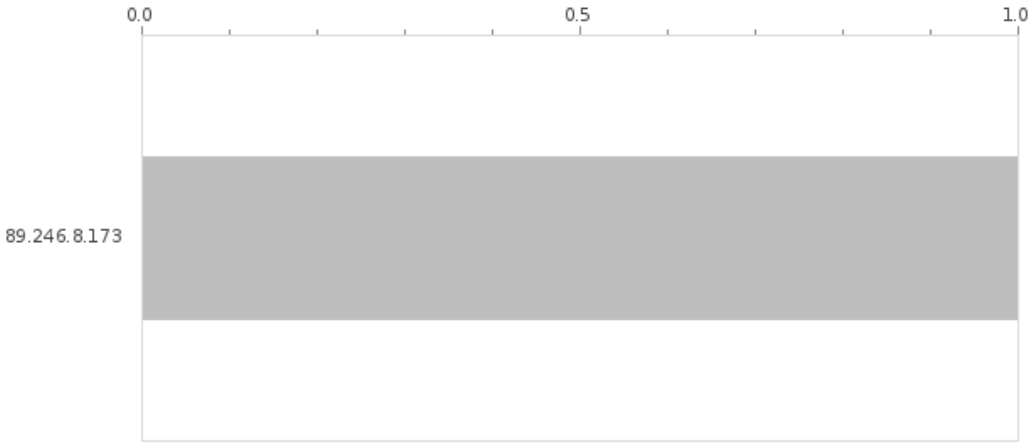


LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

Types of Blocked Attacks



Top Attack Sources



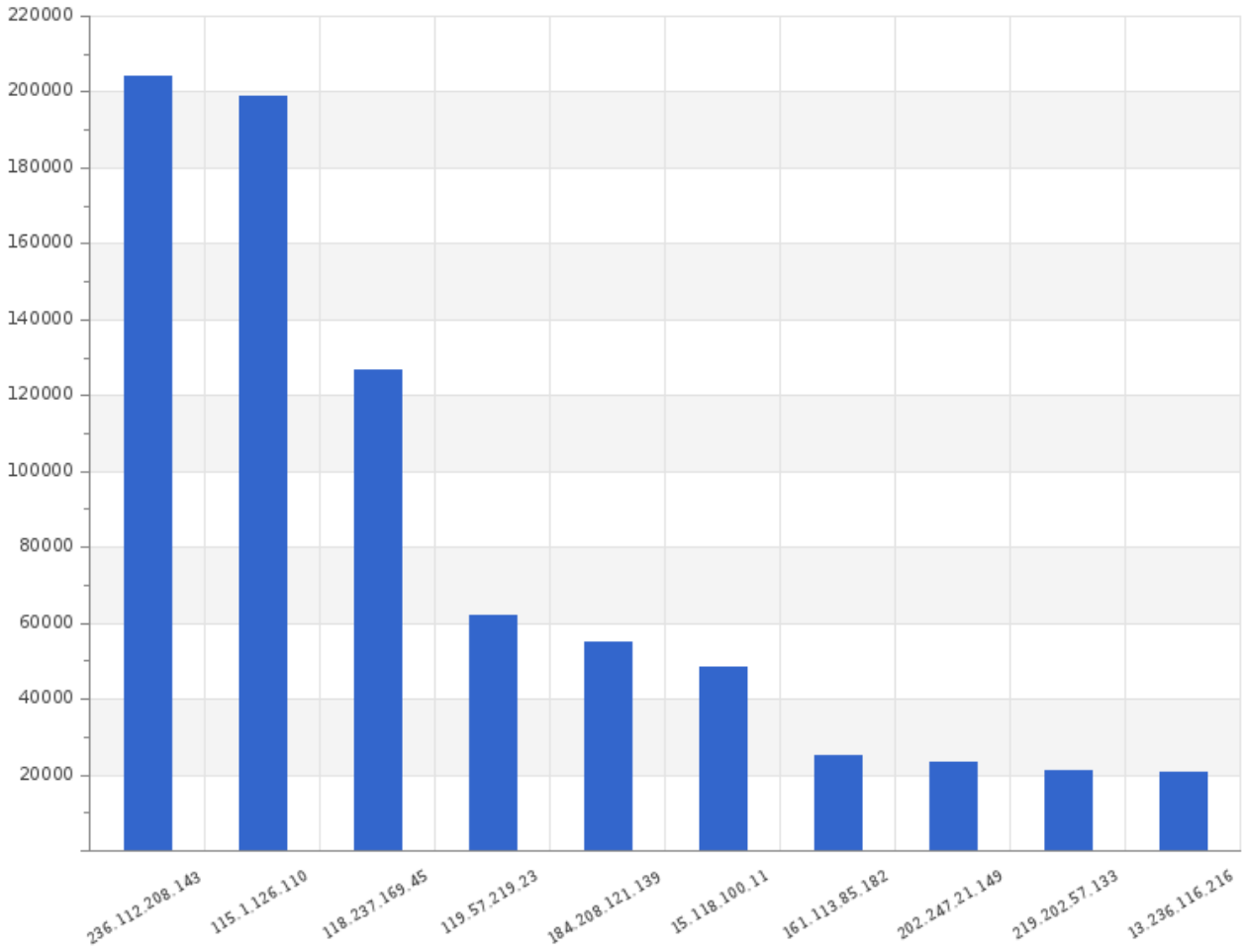
LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

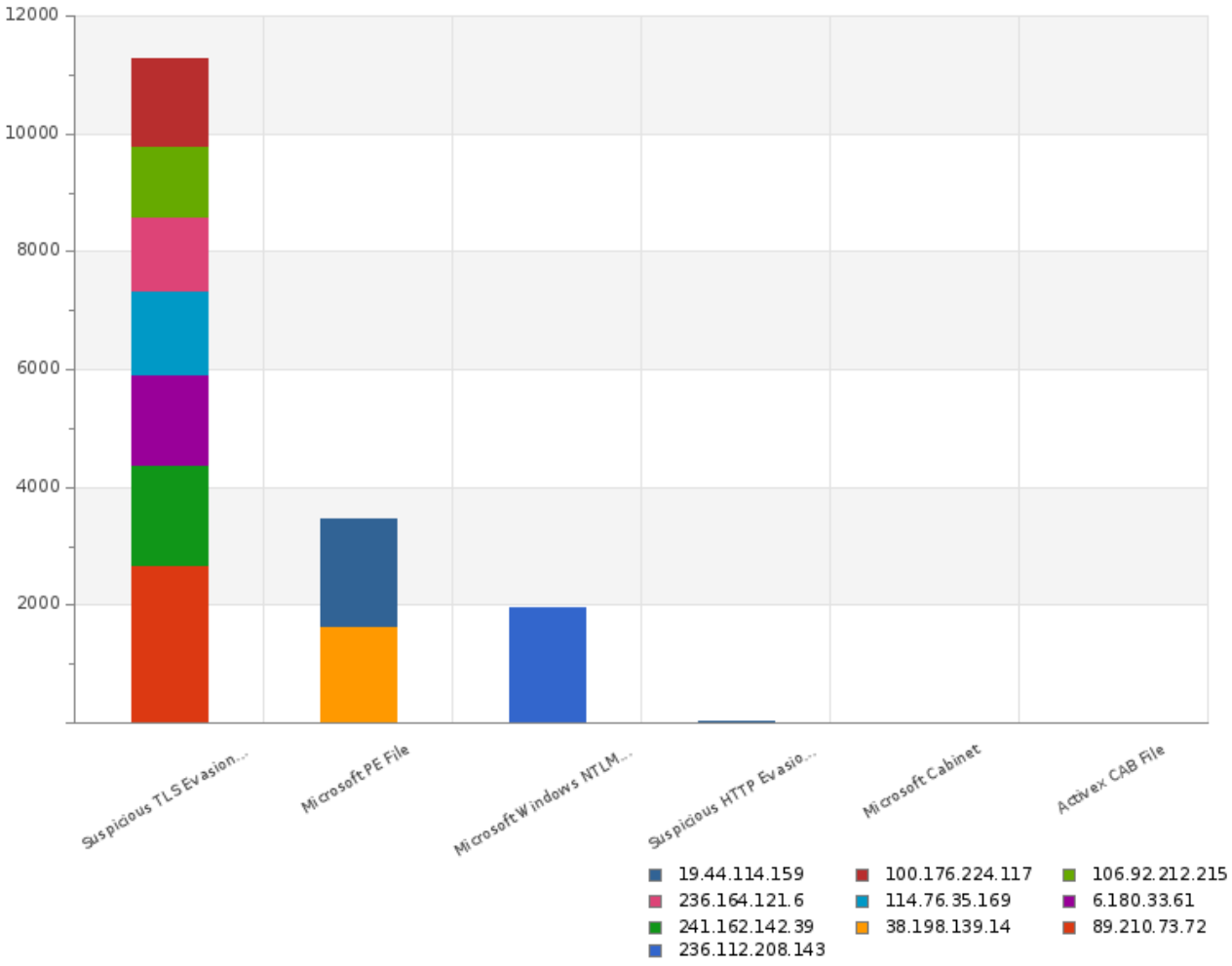
ASM-VP REPORT

ACME FINANCIAL SERVICES 08/11/2023

Top Assets Protected



Top Attack Type Per Protected Asset



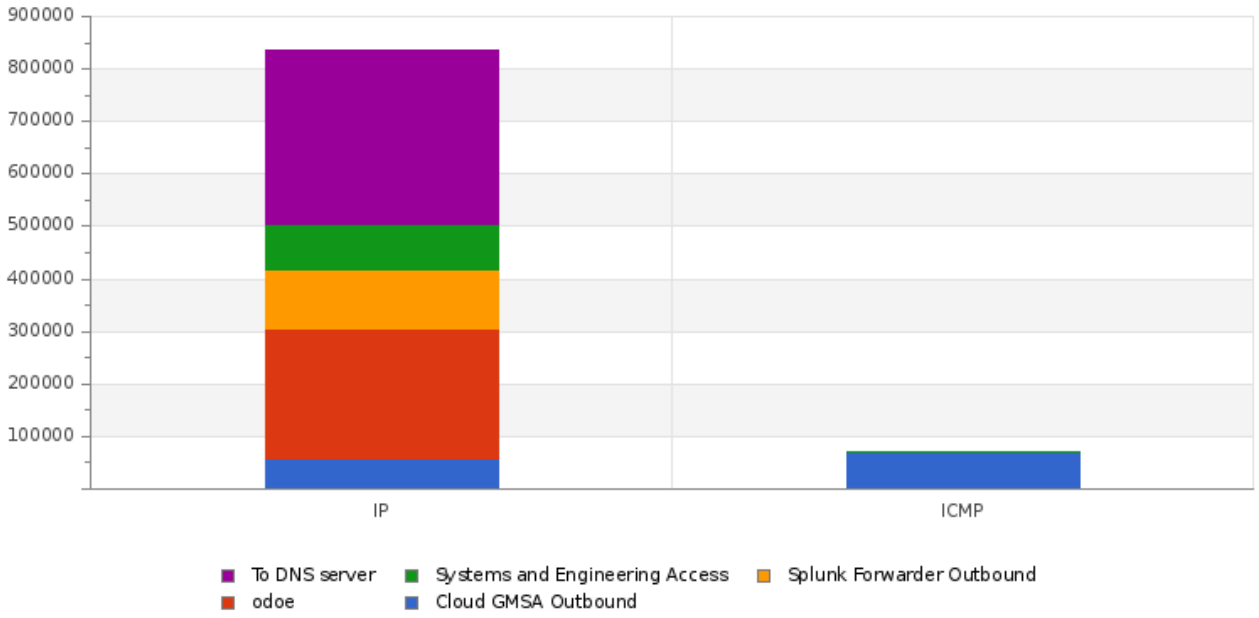
LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

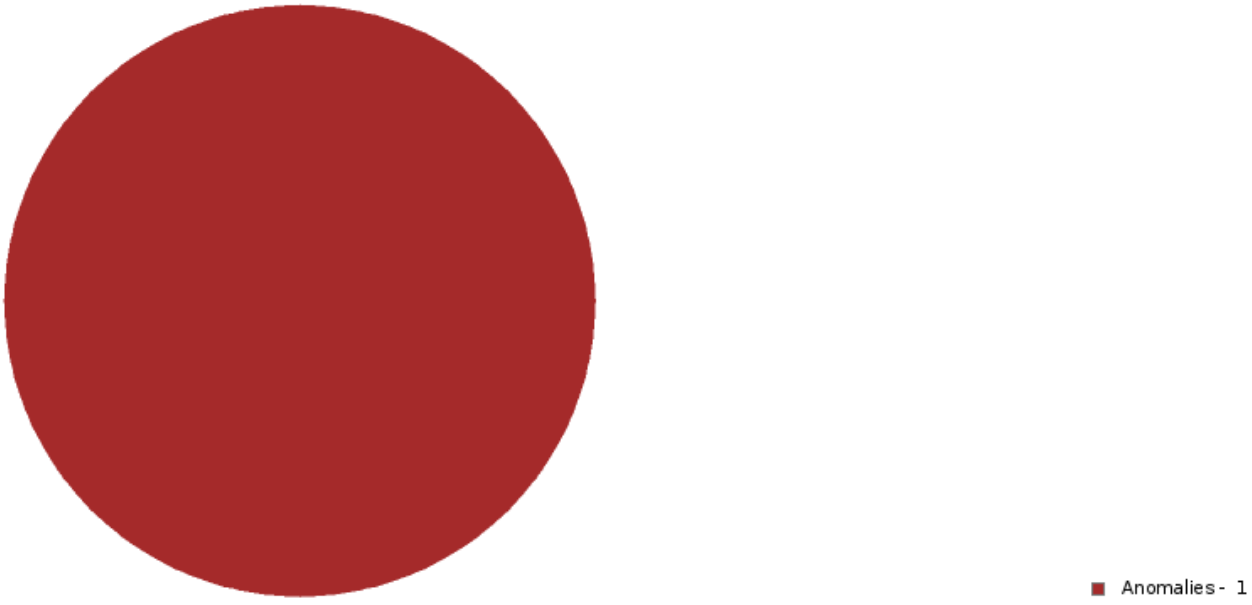
ASM-VP REPORT

ACME FINANCIAL SERVICES 08/11/2023

Top Blocked DDOS Types



Executive Summary - Types of Blocked Attacks



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

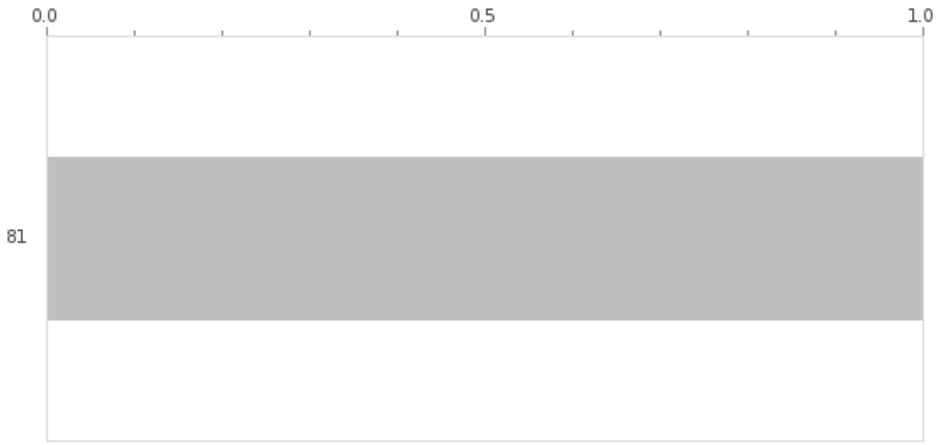
ASM-VP REPORT

ACME FINANCIAL SERVICES 08/11/2023

Executive Summary - Total Bandwidth/Packet Count by Attack Type

Category	MB/s	KB/s
Anomalies	0.01	5.63
--Total Bandwidth--	0.01	5.63

Executive Summary - Attacks Blocked by Destination Port



MSS-WAF

Block Events

0

Applications

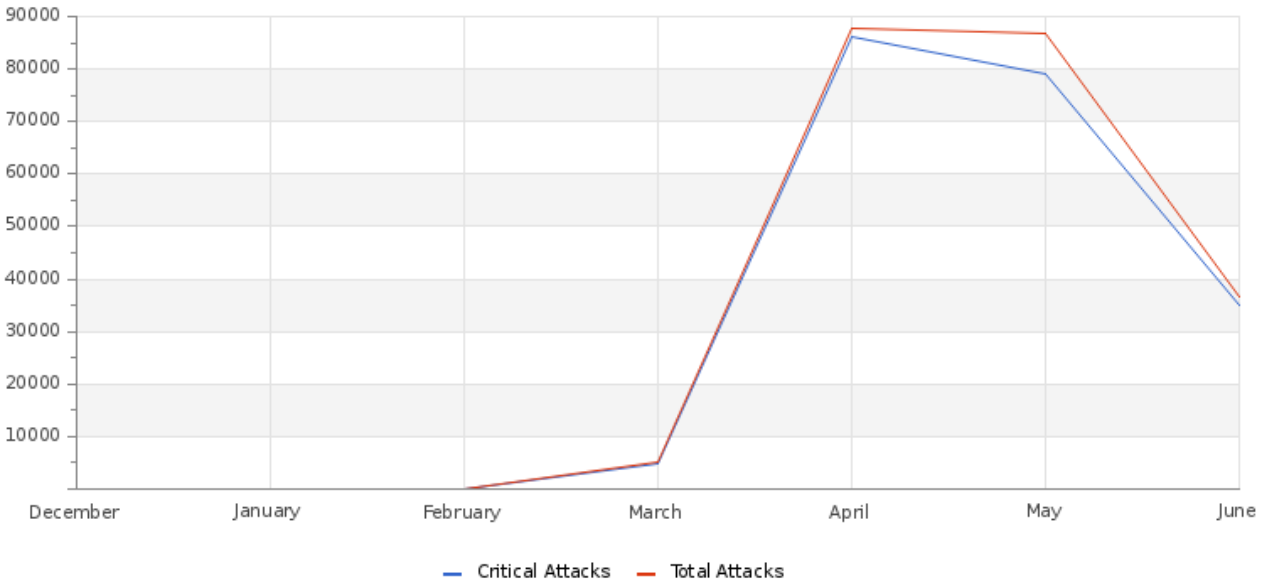
0

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

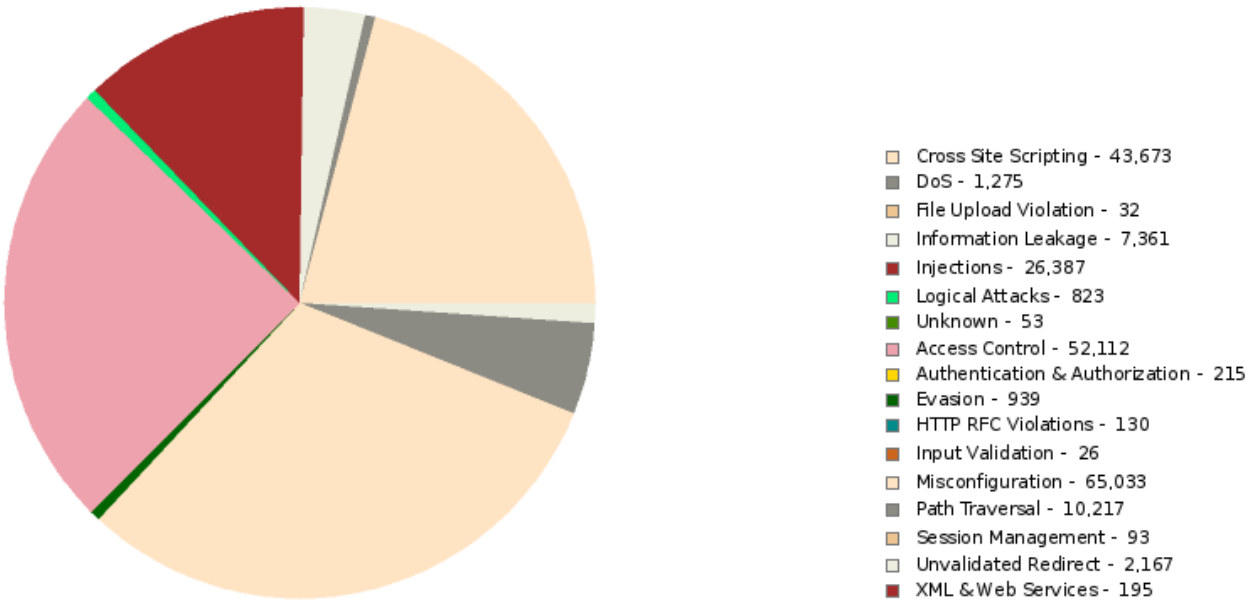
ASM-VP REPORT

ACME FINANCIAL SERVICES 08/11/2023

Total & Critical Attacks Per Month In Last 6 Months

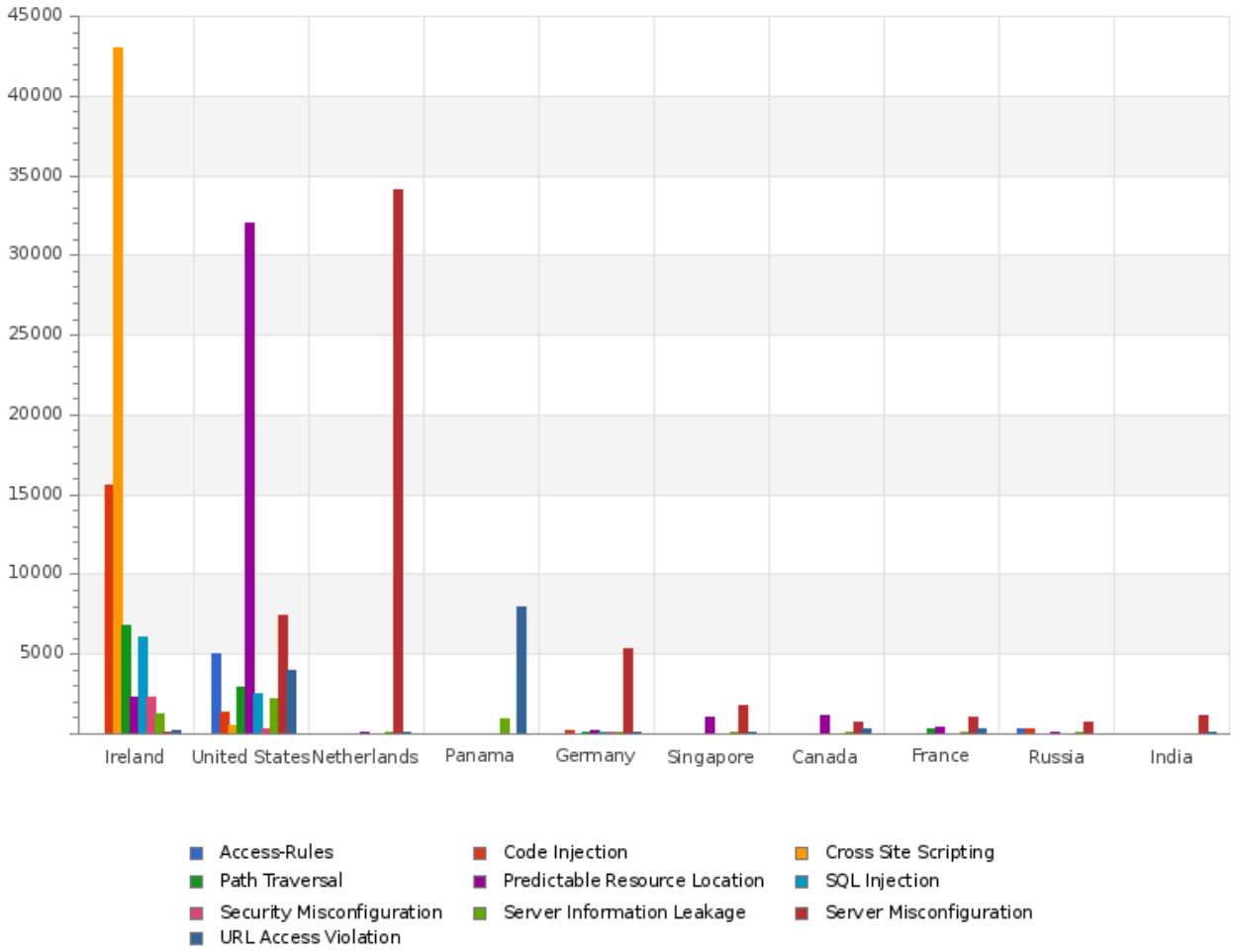


Attack Types Blocked



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

Top 10 Attacking Countries Blocked



MSS-DLP

Users Causing Alerts

Username: acme@acme.com Counter: 266

ASM-VP REPORT

ACME FINANCIAL SERVICES 08/11/2023

Activity Alerts

Total
26
26
266

Recent Opened Cases

Action	Total
Downloaded	2,758
WriteFile	98

ASM-VP REPORT

ACME FINANCIAL SERVICES 08/11/2023

Alerts per User

User	Action	Count
acme@acme.com		392
acme@acme.com	Downloaded	391
acme@acme.com		288
acme@acme.com	Downloaded	266
acme@acme.com		254
acme@acme.com		252
acme@acme.com	Downloaded	243
acme@acme.com		241
acme@acme.com	Downloaded	240
acme@acme.com	Downloaded	239
acme@acme.com		26
acme@acme.com	WriteFile	14
acme@acme.com	WriteFile	13
acme@acme.com	WriteFile	12
acme@acme.com	WriteFile	10

Total Users - Last 30 days

369

DLP Data

Type	IP	Username	Description
CASE_CREATE_CASE_CREATE	4.135.138.110	doe.jane	xdoe

MSS-BOT

Bot Hits

183,391

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

TLP:AMBER

ASM-VP REPORT

ACME FINANCIAL SERVICES 08/11/2023

Signatures

1,260

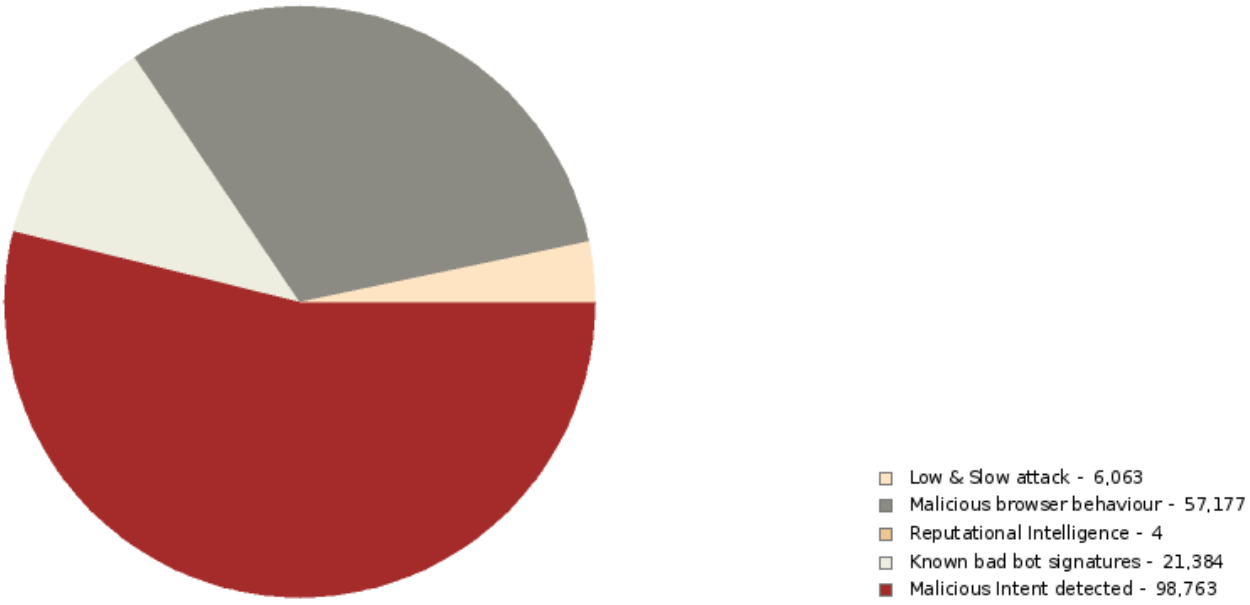
Transactions

177,251

Impacted Paths

51,305

Bot Classification

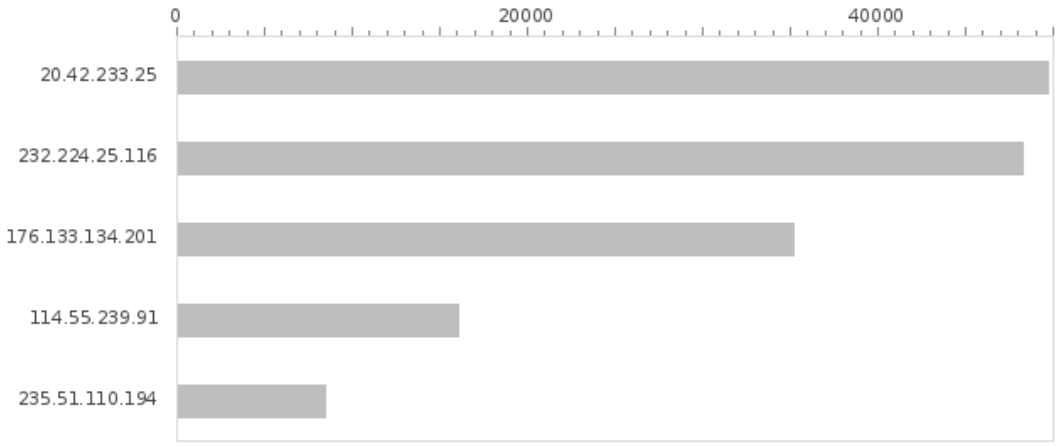


LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

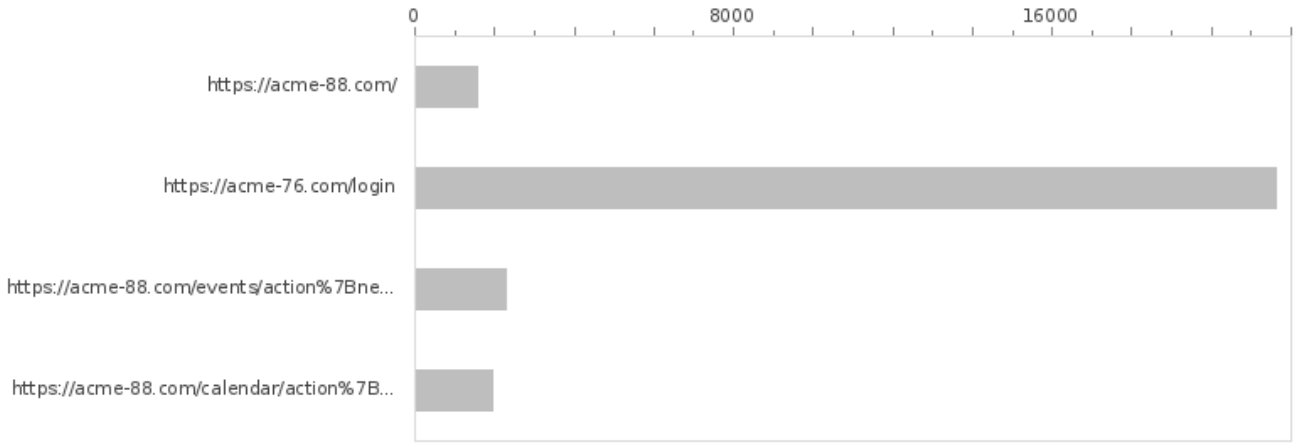
ASM-VP REPORT

ACME FINANCIAL SERVICES 08/11/2023

Top Bad Bot IPs



Top Impacted Paths



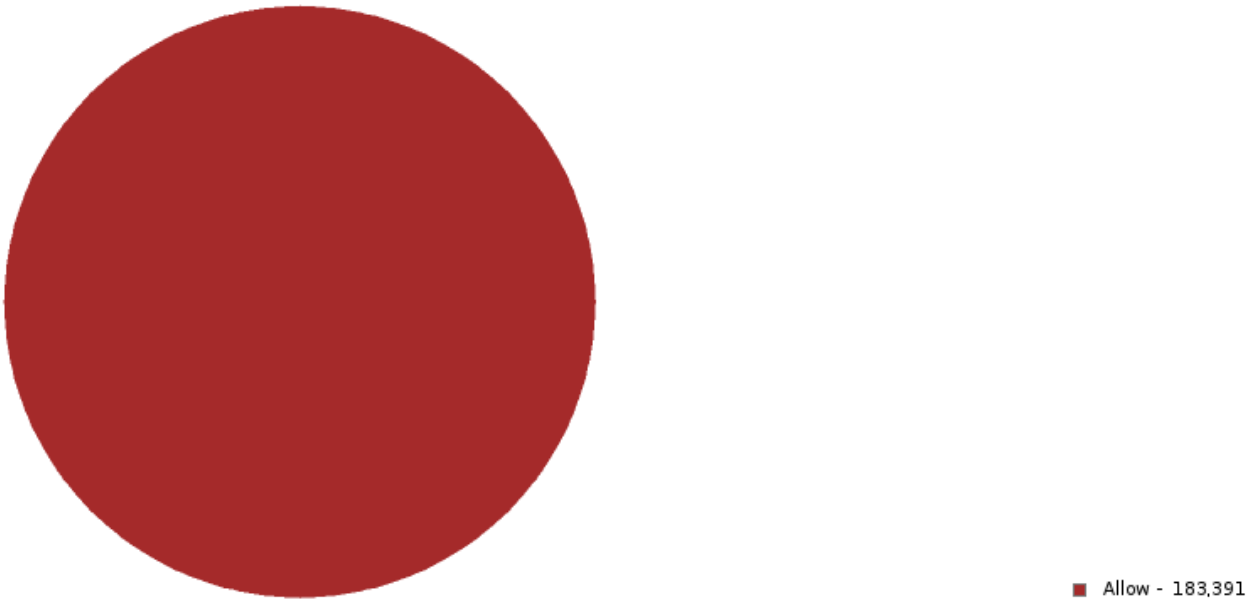
LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

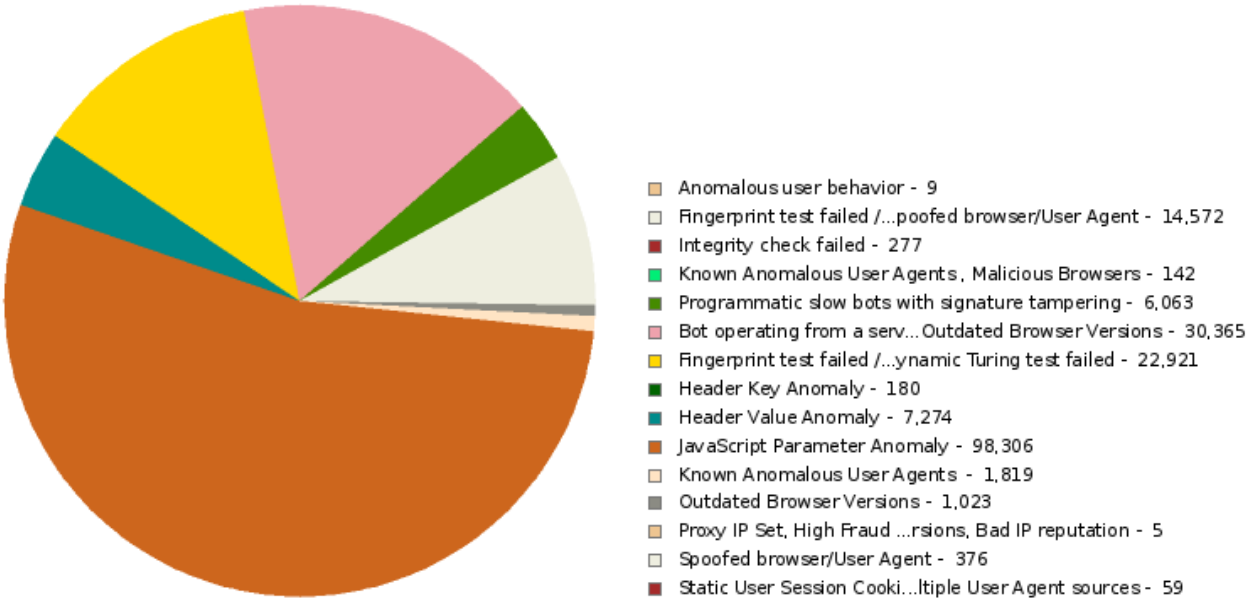
ASM-VP REPORT

ACME FINANCIAL SERVICES 08/11/2023

Bot Action



Bot Violation

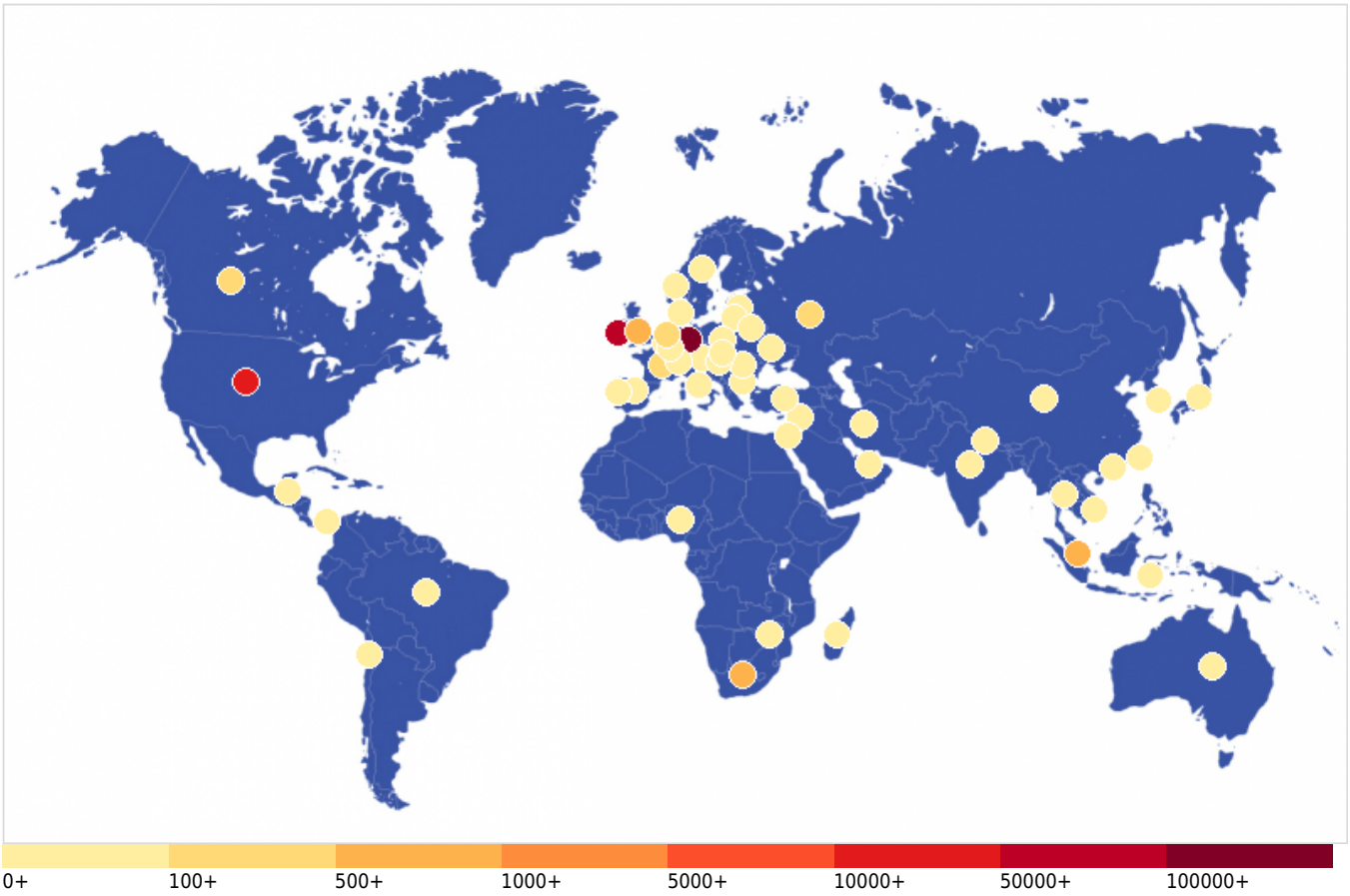


LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

ASM-VP REPORT

ACME FINANCIAL SERVICES 08/11/2023

Bot Activity Map



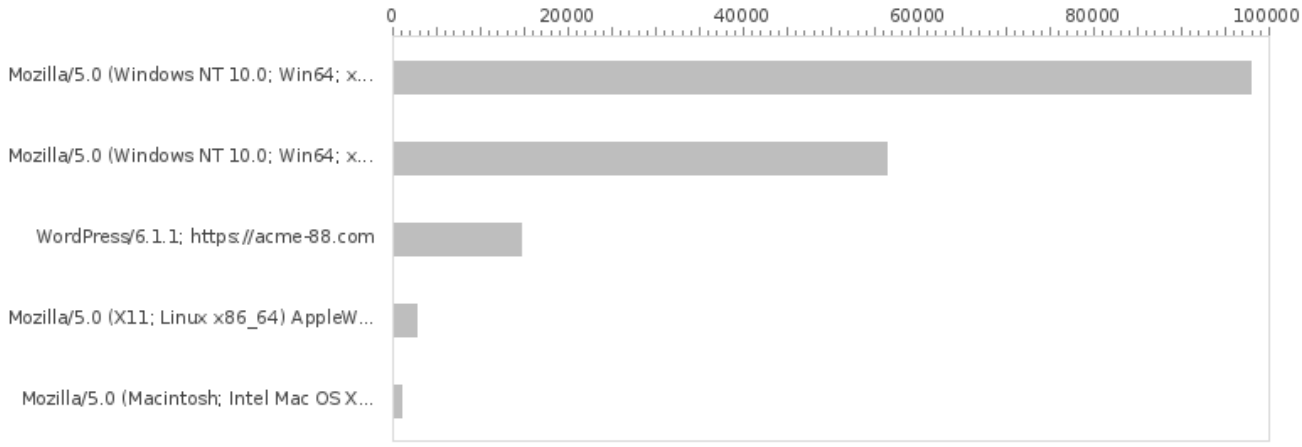
ACME - 3
Austria - 9
Belgium - 40
Belize - 1
Bulgaria - 12
Chile - 5
China - 50
France - 238
Germany - 100,070
Hong Kong - 62
India - 74
Ireland - 59,793
Italy - 13
Latvia - 4
Lithuania - 1
Nigeria - 1
Romania - 16
Russia - 237
South Africa - 662
South Korea - 18
Spain - 10
Switzerland - 49
Thailand - 14
Ukraine - 54
United Arab Emirates - 4
United States - 19,257
Zimbabwe - 2
Australia - 7
Belarus - 2
Bermuda - 377
Brazil - 6
Canada - 381
Denmark - 21
Georgia - 1
Hungary - 4
Indonesia - 8
Iran - 4
Israel - 1
Japan - 13
Luxembourg - 45
Madagascar - 35
Nepal - 1
Netherlands - 368
Norway - 26
Palestinian Territory - 1
Panama - 27
Poland - 97
Portugal - 3
Singapore - 519
Slovakia - 10
Sweden - 41
Taiwan - 3
Turkey - 4
United Kingdom - 693
Vietnam - 4

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

ASM-VP REPORT

ACME FINANCIAL SERVICES 08/11/2023

Top User Agents



Peak Times By Bot Classification

Peak Time	Category	Count
14/03/2023 4:00:00 AM	Low & Slow attack	111
20/03/2023 13:00:00 PM	Malicious browser behaviour	3,992
21/03/2023 19:00:00 PM	Reputational Intelligence	4
13/03/2023 13:00:00 PM	Known bad bot signatures	2,256
24/03/2023 15:00:00 PM	Malicious Intent detected	17,236

LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

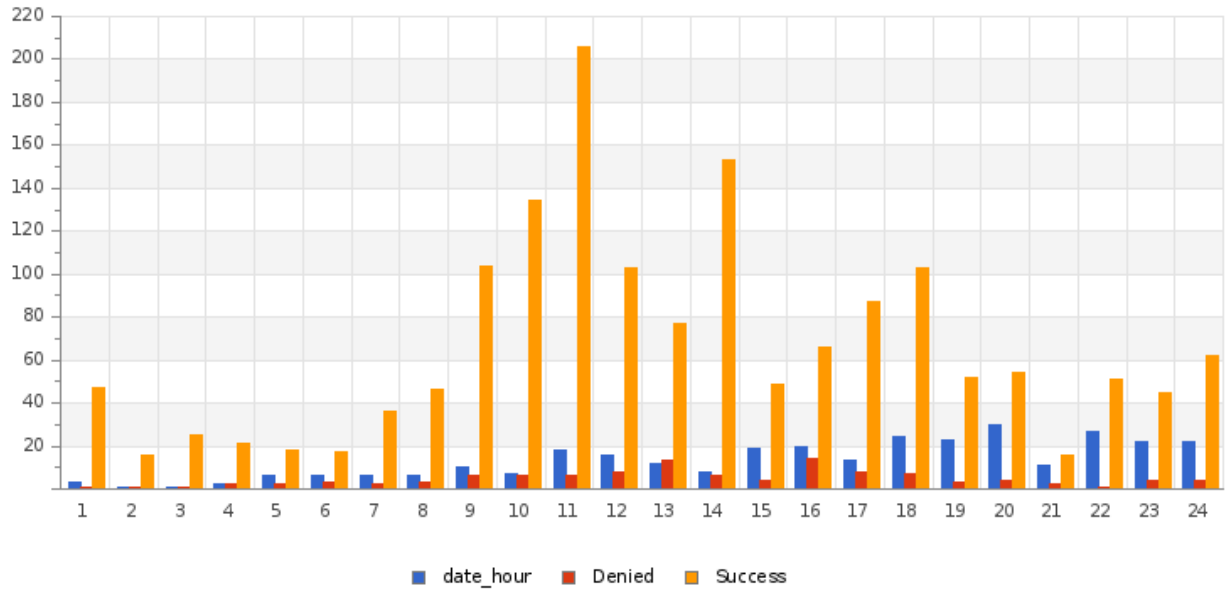
Trusted Access

MSS-TAS

Total Users *

45

Average Authentications by Hour of the Day



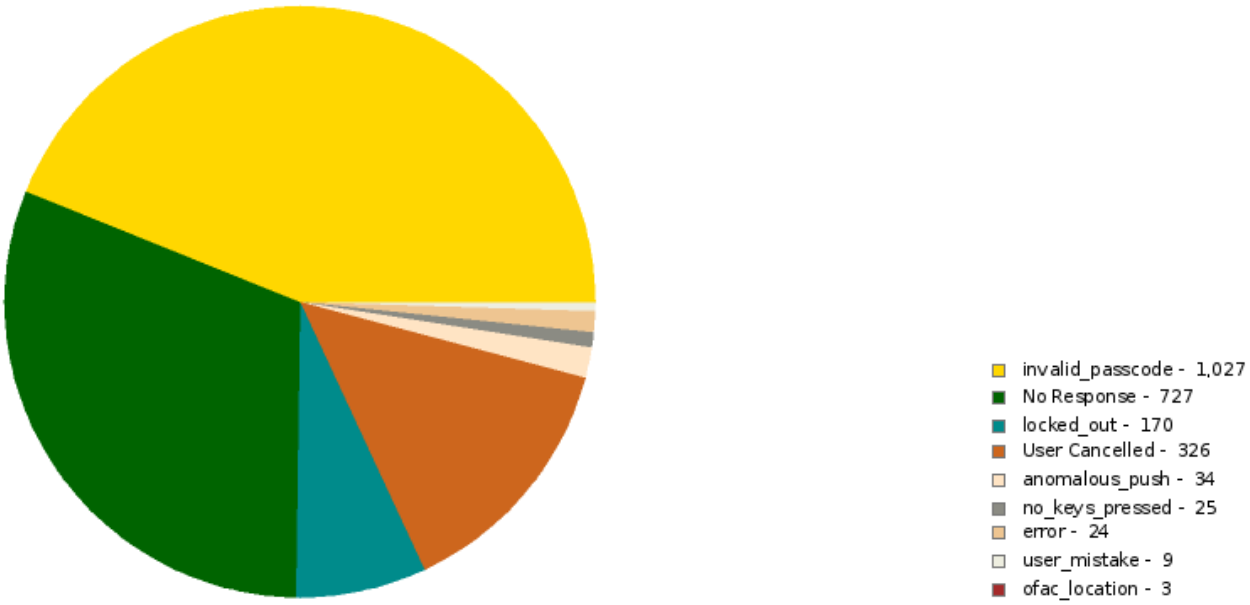
LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

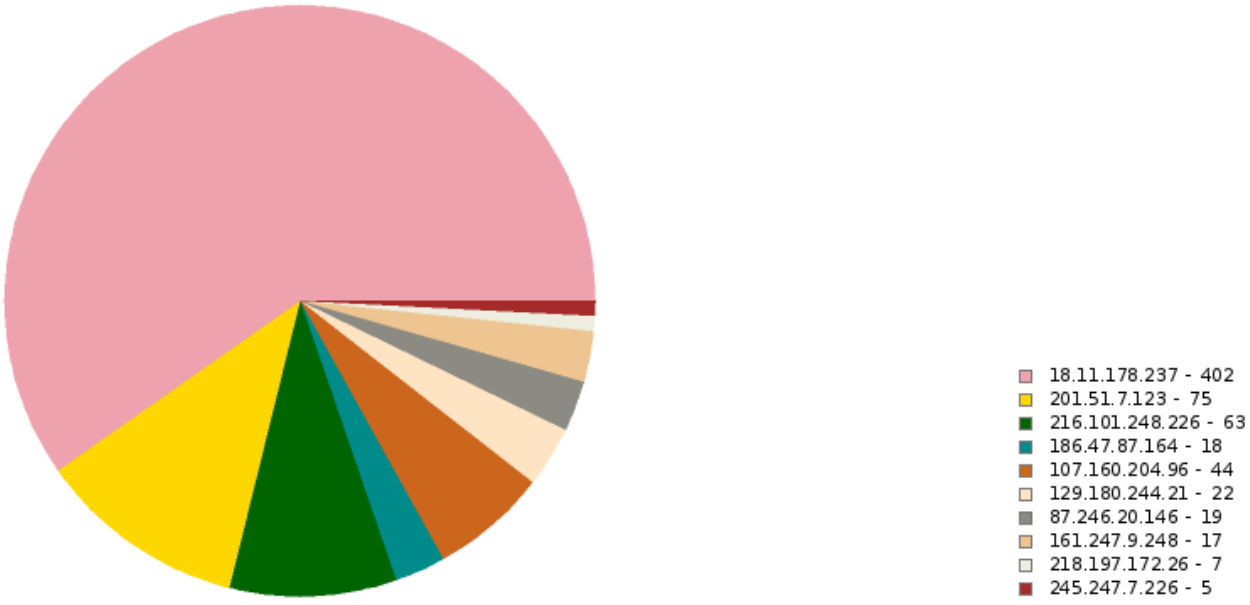
ASM-VP REPORT

ACME FINANCIAL SERVICES 08/11/2023

Top of Failed Authentications *



Top Authentications Failed by IPs *

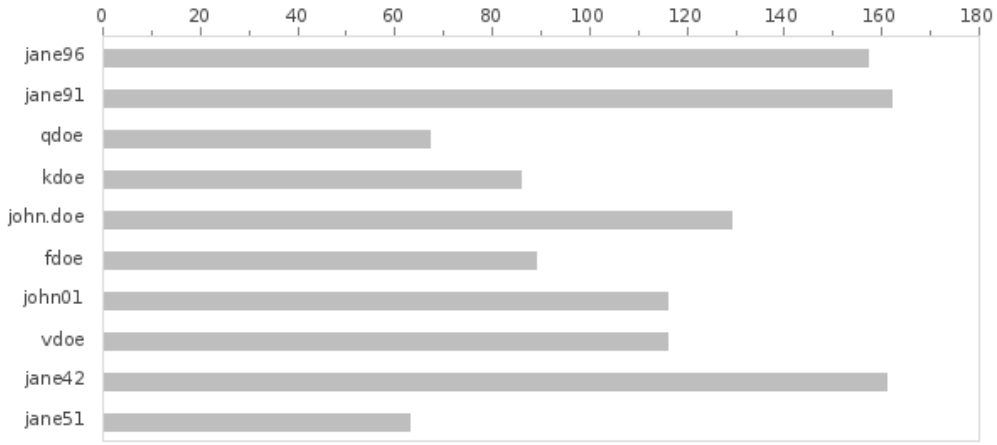


LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

ASM-VP REPORT

ACME FINANCIAL SERVICES 08/11/2023

Top Authenticated Users *



Most Active Applications *

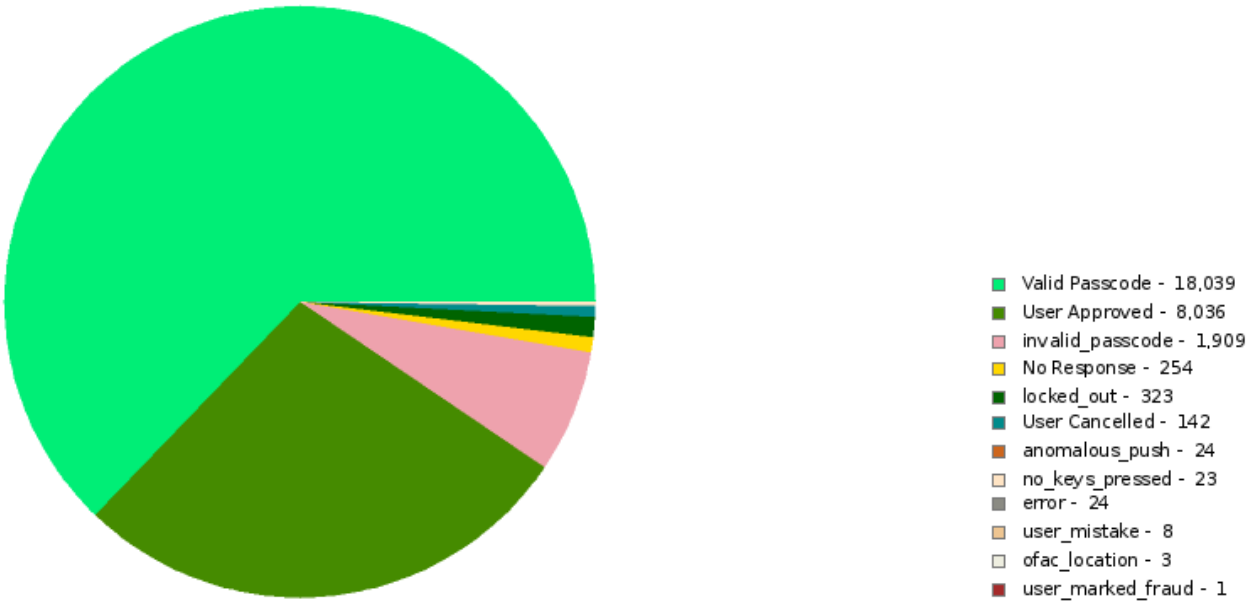
app	Denied	fraud	Success	Total
ACME	2,607	0	27,887	32,888
Microsoft ADFS	867	1	4,872	16,981
Microsoft RDP	34	10	968	736
Cisco ISE RADIUS 1	10	2	498	242
CyberArk Privileged Account Security LDAPS	3	2	87	60
Web SDK	13	2	51	133
portal	6	1	41	32
Cisco ASA - SSO - Azure	0	7	24	43

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

ASM-VP REPORT

ACME FINANCIAL SERVICES 08/11/2023

Authentication Status in the Last 24 Hours *



Users with failed authentications *

user	Time	src_ip
jdoe	Sat Jul 8 13:55:36 2,023 EDT	190.103.133.224
john42	Sat Jul 8 13:56:49 2,023 EDT	190.103.133.224
john36	Sat Jul 8 14:09:47 2,023 EDT	190.103.133.224
doe.jane	Sat Jul 8 14:11:29 2,023 EDT	190.103.133.224
doe.jane	Sat Jul 8 0:34:59 2,023 EDT	190.103.133.224
john.doe	Sat Jul 8 0:35:38 2,023 EDT	190.103.133.224
jane.doe	Sat Jul 8 0:36:10 2,023 EDT	190.103.133.224
jdoe	Sat Jul 8 0:36:34 2,023 EDT	190.103.133.224
doe.john	Sat Jul 8 0:38:01 2,023 EDT	190.103.133.224
john63	Sat Jul 8 0:44:31 2,023 EDT	190.103.133.224
doe.jane	Mon Jul 10 13:56:17 2,023 EDT	109.202.153.131
john.doe	Mon Jul 10 13:57:45 2,023 EDT	190.103.133.224
jane.doe	Mon Jul 10 14:00:55 2,023 EDT	216.101.248.226
doe.jane	Mon Jul 10 14:01:56 2,023 EDT	216.101.248.226
jane06	Mon Jul 10 14:02:58 2,023 EDT	216.101.248.226
idoe	Mon Jul 10 14:05:31 2,023 EDT	190.103.133.224

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

ASM-VP REPORT

ACME FINANCIAL SERVICES 08/11/2023

user	Time	src_ip
john.doe	Mon Jul 10 14:06:06 2,023 EDT	190.103.133.224
jane.doe	Mon Jul 10 14:06:13 2,023 EDT	190.103.133.224
john.doe	Sun Jul 9 20:04:18 2,023 EDT	116.57.74.180
jane.doe	Mon Jul 10 13:18:49 2,023 EDT	190.103.133.224
jane63	Mon Jul 10 13:21:09 2,023 EDT	190.103.133.224
jane92	Mon Jul 10 13:23:01 2,023 EDT	201.51.7.123
john69	Mon Jul 10 13:24:24 2,023 EDT	190.103.133.224
john94	Mon Jul 10 13:29:49 2,023 EDT	190.103.133.224
doe.jane	Mon Jul 10 13:39:08 2,023 EDT	190.103.133.224
ldoe	Mon Jul 10 13:40:40 2,023 EDT	18.11.178.237
john89	Mon Jul 10 13:46:04 2,023 EDT	190.103.133.224
jane.doe	Mon Jul 10 13:46:43 2,023 EDT	190.103.133.224
john.doe	Sun Jul 9 11:15:16 2,023 EDT	190.103.133.224
doe.john	Sun Jul 9 11:53:36 2,023 EDT	190.103.133.224
john57	Sun Jul 9 10:06:55 2,023 EDT	190.103.133.224
vdoe	Sun Jul 9 10:36:16 2,023 EDT	216.214.0.196
jane.doe	Sun Jul 9 10:36:28 2,023 EDT	190.103.133.224
jane.doe	Sun Jul 9 10:48:40 2,023 EDT	190.103.133.224
jane74	Sun Jul 9 10:49:34 2,023 EDT	190.103.133.224
jane.doe	Sun Jul 9 10:49:58 2,023 EDT	190.103.133.224
jane.doe	Sat Jul 8 19:08:29 2,023 EDT	107.160.204.96
ndoe	Sat Jul 8 19:11:54 2,023 EDT	193.127.236.237
jane.doe	Sat Jul 8 19:23:04 2,023 EDT	190.103.133.224
jane.doe	Sat Jul 8 19:48:47 2,023 EDT	190.103.133.224
jane40	Sat Jul 8 19:49:33 2,023 EDT	190.103.133.224
jane.doe	Sat Jul 8 16:42:10 2,023 EDT	85.116.53.228
doe.jane	Sat Jul 8 16:54:47 2,023 EDT	75.93.8.51
adoe	Sat Jul 8 17:08:07 2,023 EDT	18.11.178.237
doe.jane	Sat Jul 8 17:09:43 2,023 EDT	18.11.178.237
john05	Sat Jul 8 17:11:38 2,023 EDT	18.11.178.237
jdoe	Sat Jul 8 17:28:52 2,023 EDT	190.103.133.224
john.doe	Sat Jul 8 17:29:16 2,023 EDT	190.103.133.224
hdoe	Sat Jul 8 9:56:46 2,023 EDT	129.180.244.21
tdoe	Mon Jul 10 10:17:58 2,023 EDT	190.103.133.224
john21	Mon Jul 10 10:18:40 2,023 EDT	190.103.133.224

ASM-VP REPORT

ACME FINANCIAL SERVICES 08/11/2023

user	Time	src_ip
john.doe	Mon Jul 10 10:20:12 2,023 EDT	216.101.248.226
doe.jane	Mon Jul 10 10:21:27 2,023 EDT	216.101.248.226
jane66	Mon Jul 10 10:22:08 2,023 EDT	18.11.178.237
jane61	Mon Jul 10 10:30:05 2,023 EDT	18.11.178.237
john.doe	Mon Jul 10 10:30:37 2,023 EDT	201.51.7.123
cdoe	Mon Jul 10 10:35:31 2,023 EDT	218.128.139.191
jdoe	Mon Jul 10 10:37:12 2,023 EDT	18.11.178.237
kdoe	Mon Jul 10 10:37:34 2,023 EDT	190.103.133.224
doe.john	Mon Jul 10 10:41:47 2,023 EDT	190.103.133.224
doe.john	Mon Jul 10 10:46:23 2,023 EDT	190.103.133.224
doe.john	Mon Jul 10 10:49:38 2,023 EDT	190.103.133.224
jane.doe	Mon Jul 10 10:52:32 2,023 EDT	2.204.209.25
jane21	Mon Jul 10 10:53:51 2,023 EDT	190.103.133.224
jane42	Mon Jul 10 10:53:53 2,023 EDT	216.101.248.226
doe.john	Mon Jul 10 10:54:22 2,023 EDT	190.103.133.224
jane53	Mon Jul 10 10:54:40 2,023 EDT	190.103.133.224
doe.jane	Mon Jul 10 10:55:05 2,023 EDT	190.103.133.224
zdoe	Mon Jul 10 10:56:45 2,023 EDT	216.101.248.226
ldoe	Mon Jul 10 11:04:41 2,023 EDT	18.11.178.237
john72	Tue Jul 4 14:24:28 2,023 EDT	87.165.244.53
doe.john	Tue Jul 4 14:26:47 2,023 EDT	190.103.133.224
john.doe	Tue Jul 4 14:27:25 2,023 EDT	190.103.133.224
john.doe	Tue Jul 4 14:28:00 2,023 EDT	190.103.133.224
ndoe	Tue Jul 4 14:28:41 2,023 EDT	190.103.133.224
bdoe	Tue Jul 4 14:29:33 2,023 EDT	190.103.133.224
jane.doe	Tue Jul 4 14:35:08 2,023 EDT	18.11.178.237
doe.john	Tue Jul 4 14:39:25 2,023 EDT	18.11.178.237
doe.john	Tue Jul 4 14:50:53 2,023 EDT	190.103.133.224
doe.john	Tue Jul 4 14:51:03 2,023 EDT	190.103.133.224
doe.john	Tue Jul 4 14:51:28 2,023 EDT	190.103.133.224
jane19	Tue Jul 4 14:51:41 2,023 EDT	190.103.133.224
jane82	Tue Jul 4 14:51:46 2,023 EDT	190.103.133.224
jane.doe	Tue Jul 4 14:56:15 2,023 EDT	190.103.133.224
doe.jane	Tue Jul 4 14:58:35 2,023 EDT	190.103.133.224
doe.john	Tue Jul 4 14:58:40 2,023 EDT	18.11.178.237

user	Time	src_ip
john46	Tue Jul 4 15:01:25 2,023 EDT	190.103.133.224
jane21	Tue Jul 4 15:03:42 2,023 EDT	190.103.133.224
ddoe	Tue Jul 4 15:05:08 2,023 EDT	190.103.133.224
john48	Tue Jul 4 15:07:35 2,023 EDT	190.103.133.224
doe.jane	Tue Jul 4 15:07:58 2,023 EDT	190.103.133.224
vdoe	Tue Jul 4 15:10:32 2,023 EDT	18.11.178.237
doe.john	Mon Jul 3 20:22:28 2,023 EDT	190.103.133.224
pdoe	Mon Jul 3 20:53:17 2,023 EDT	190.103.133.224
ndoe	Thu Jul 6 12:34:18 2,023 EDT	155.202.125.28
idoe	Thu Jul 6 12:34:27 2,023 EDT	190.103.133.224
john75	Thu Jul 6 12:39:05 2,023 EDT	190.103.133.224
john65	Thu Jul 6 12:39:52 2,023 EDT	190.103.133.224
doe.john	Thu Jul 6 12:40:14 2,023 EDT	190.103.133.224
john87	Thu Jul 6 12:40:48 2,023 EDT	190.103.133.224

Authentications left as No response by Users *

Username	IP Address	Time
john12	1.174.111.208	Fri Jul 7 17:46:05 2,023 EDT
doe.john	61.193.65.20	Sat Jul 8 21:13:19 2,023 EDT
doe.jane	216.101.248.226	Sat Jul 8 22:01:28 2,023 EDT
jane.doe	86.220.110.108	Sat Jul 8 22:58:21 2,023 EDT
doe.john	86.220.110.108	Sat Jul 8 22:59:40 2,023 EDT
jane.doe	86.220.110.108	Sat Jul 8 23:02:18 2,023 EDT
tdoe	18.11.178.237	Fri Jul 7 23:13:16 2,023 EDT
ldoe	164.52.87.194	Sun Jul 9 8:50:09 2,023 EDT
jdoe	86.220.110.108	Sun Jul 9 21:16:41 2,023 EDT
doe.jane	86.220.110.108	Sun Jul 9 21:36:55 2,023 EDT
doe.jane	18.11.178.237	Sun Jul 9 22:01:38 2,023 EDT
odoe	218.54.82.73	Thu Jul 6 22:55:03 2,023 EDT
john.doe	190.103.133.224	Thu Jul 6 15:20:49 2,023 EDT
doe.john	218.197.172.26	Thu Jul 6 11:33:56 2,023 EDT
ydoe	18.11.178.237	Thu Jul 6 9:32:12 2,023 EDT
ndoe	18.11.178.237	Thu Jul 6 9:37:48 2,023 EDT
doe.john	245.247.7.226	Thu Jul 6 10:00:24 2,023 EDT

ASM-VP REPORT

ACME FINANCIAL SERVICES 08/11/2023

Username	IP Address	Time
john.doe	18.11.178.237	Thu Jul 6 10:14:00 2,023 EDT
john39	18.11.178.237	Mon Jul 3 6:15:11 2,023 EDT
doe.john	18.11.178.237	Mon Jul 3 6:17:25 2,023 EDT
jane.doe	18.11.178.237	Mon Jul 3 16:22:28 2,023 EDT
john03	107.160.204.96	Mon Jul 3 16:25:40 2,023 EDT
john91	107.160.204.96	Mon Jul 3 16:26:43 2,023 EDT
john63	22.184.74.154	Mon Jul 3 16:43:00 2,023 EDT
jane02	18.11.178.237	Mon Jul 3 17:07:26 2,023 EDT
doe.john	216.101.248.226	Mon Jul 3 14:32:27 2,023 EDT
john49	216.101.248.226	Mon Jul 3 14:33:28 2,023 EDT
john.doe	216.101.248.226	Mon Jul 3 14:34:30 2,023 EDT
jane.doe	18.11.178.237	Mon Jul 3 14:58:15 2,023 EDT
doe.john	18.11.178.237	Wed Jul 5 11:39:06 2,023 EDT
adoe	18.11.178.237	Wed Jul 5 11:41:19 2,023 EDT
gdoe	201.51.7.123	Wed Jul 5 11:54:28 2,023 EDT
jane17	201.51.7.123	Wed Jul 5 11:55:30 2,023 EDT
ldoe	161.228.182.71	Wed Jul 5 12:05:31 2,023 EDT
doe.jane	149.87.69.55	Wed Jul 5 10:01:25 2,023 EDT
john.doe	186.47.87.164	Wed Jul 5 15:22:08 2,023 EDT
doe.jane	186.47.87.164	Wed Jul 5 15:23:59 2,023 EDT
doe.john	222.181.97.52	Wed Jul 5 15:27:05 2,023 EDT
jane56	18.11.178.237	Wed Jul 5 15:40:19 2,023 EDT
jane.doe	186.47.87.164	Wed Jul 5 15:48:47 2,023 EDT
tdoe	18.11.178.237	Wed Jul 5 15:50:30 2,023 EDT
tdoe	18.11.178.237	Wed Jul 5 15:51:34 2,023 EDT
jane.doe	18.11.178.237	Wed Jul 5 15:55:12 2,023 EDT
kdoe	99.20.184.239	Wed Jul 5 16:12:45 2,023 EDT
odoe	190.103.133.224	Wed Jul 5 12:55:31 2,023 EDT
jane.doe	18.11.178.237	Fri Jul 7 9:48:28 2,023 EDT
udoe	244.136.239.246	Sun Jul 2 0:05:27 2,023 EDT
john.doe	244.136.239.246	Sun Jul 2 0:06:52 2,023 EDT
jane07	244.136.239.246	Sun Jul 2 0:07:56 2,023 EDT
jane.doe	18.11.178.237	Sun Jul 2 11:37:47 2,023 EDT
doe.john	18.11.178.237	Thu Jun 29 17:59:52 2,023 EDT
jane07	69.106.52.55	Fri Jun 30 10:05:27 2,023 EDT

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

ASM-VP REPORT

ACME FINANCIAL SERVICES 08/11/2023

Username	IP Address	Time
doe.john	216.101.248.226	Fri Jun 30 9:38:30 2,023 EDT
doe.jane	18.11.178.237	Fri Jun 30 9:12:54 2,023 EDT
xdoe	18.11.178.237	Fri Jun 30 11:36:59 2,023 EDT
jane04	1.138.51.216	Fri Jun 30 11:37:18 2,023 EDT
jane.doe	56.199.115.228	Fri Jun 30 11:40:44 2,023 EDT
john88	18.11.178.237	Fri Jun 30 11:40:50 2,023 EDT
ndoe	1.138.51.216	Fri Jun 30 11:54:16 2,023 EDT
doe.jane	252.87.54.247	Thu Jun 29 13:07:48 2,023 EDT
ndoe	190.103.133.224	Fri Jun 30 11:16:32 2,023 EDT
jane.doe	69.106.52.55	Fri Jun 30 11:29:58 2,023 EDT
wdoe	218.11.239.164	Thu Jun 29 10:35:08 2,023 EDT
john93	145.37.144.62	Thu Jun 29 10:35:48 2,023 EDT
john.doe	18.11.178.237	Thu Jun 29 10:54:14 2,023 EDT
ddoe	180.18.176.2	Thu Jun 29 10:08:11 2,023 EDT
doe.jane	180.18.176.2	Thu Jun 29 10:10:26 2,023 EDT
pdoe	18.11.178.237	Thu Jun 29 10:16:36 2,023 EDT
adoe	18.11.178.237	Thu Jun 29 10:16:59 2,023 EDT
john.doe	239.44.101.231	Tue Jun 27 17:23:30 2,023 EDT
john.doe	89.12.184.104	Tue Jun 27 17:40:44 2,023 EDT
jane41	18.11.178.237	Tue Jun 27 17:44:30 2,023 EDT
john13	129.180.244.21	Mon Jun 26 17:18:14 2,023 EDT
qdoe	129.180.244.21	Mon Jun 26 17:19:46 2,023 EDT
jane.doe	18.11.178.237	Mon Jun 26 17:22:16 2,023 EDT
doe.john	107.160.204.96	Tue Jun 27 9:37:29 2,023 EDT
xdoe	216.101.248.226	Tue Jun 27 9:53:27 2,023 EDT
doe.john	13.206.187.153	Tue Jun 27 10:01:18 2,023 EDT
john47	120.97.251.167	Tue Jun 27 10:05:47 2,023 EDT
doe.john	190.103.133.224	Tue Jun 27 12:53:26 2,023 EDT
john67	18.11.178.237	Tue Jun 27 12:56:18 2,023 EDT
ndoe	18.11.178.237	Tue Jun 27 12:57:23 2,023 EDT
pdoe	18.11.178.237	Tue Jun 27 13:05:28 2,023 EDT
john.doe	27.57.202.72	Tue Jun 27 11:48:39 2,023 EDT
doe.jane	216.101.248.226	Tue Jun 27 11:54:38 2,023 EDT
john30	151.37.86.192	Mon Jun 26 14:08:24 2,023 EDT
john.doe	236.250.120.33	Mon Jun 26 13:20:46 2,023 EDT

LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

ASM-VP REPORT

ACME FINANCIAL SERVICES 08/11/2023

Username	IP Address	Time
mdoe	10.101.64.149	Mon Jun 26 13:33:59 2,023 EDT
jane.doe	31.175.211.228	Mon Jun 26 14:06:57 2,023 EDT
ddoe	10.0.3.250	Sun Jun 25 2:24:25 2,023 EDT
john.doe	10.0.3.250	Sun Jun 25 2:25:29 2,023 EDT
wdoe	107.160.204.96	Sun Jun 25 10:01:53 2,023 EDT
doe.jane	18.11.178.237	Fri Jun 23 14:57:25 2,023 EDT
jane00	18.11.178.237	Fri Jun 23 15:13:55 2,023 EDT
jane25	18.11.178.237	Fri Jun 23 15:16:22 2,023 EDT
john54	107.160.204.96	Thu Jun 22 11:40:57 2,023 EDT
doe.jane	111.83.126.72	Thu Jun 22 12:07:19 2,023 EDT
jane.doe	18.11.178.237	Thu Jun 22 11:26:43 2,023 EDT
doe.john	23.56.137.211	Thu Jun 22 11:26:55 2,023 EDT
jane83	190.103.133.224	Thu Jun 22 14:58:31 2,023 EDT

Users with Invalid Passcode *

Username	Time	IP Address
opteze6	Sat Jul 8 0:34:59 2,023 EDT	190.103.133.224
opteze6	Sat Jul 8 0:35:38 2,023 EDT	190.103.133.224
opteze6	Sat Jul 8 0:36:10 2,023 EDT	190.103.133.224
opteze6	Sat Jul 8 0:36:34 2,023 EDT	190.103.133.224
opteze6	Sat Jul 8 0:38:01 2,023 EDT	190.103.133.224
opteze4	Sat Jul 8 0:44:31 2,023 EDT	190.103.133.224
ptycap12	Sat Jul 8 13:55:36 2,023 EDT	190.103.133.224
ptycap05	Sat Jul 8 13:56:49 2,023 EDT	190.103.133.224
mkoonjan	Sat Jul 8 14:09:47 2,023 EDT	190.103.133.224
optuio1	Sat Jul 8 14:11:29 2,023 EDT	190.103.133.224
jbonilla	Mon Jul 10 13:18:49 2,023 EDT	190.103.133.224
optfll1	Mon Jul 10 13:21:09 2,023 EDT	190.103.133.224
emmcastillo	Mon Jul 10 13:24:24 2,023 EDT	190.103.133.224
mmvega	Mon Jul 10 13:29:49 2,023 EDT	190.103.133.224
optfll1	Mon Jul 10 13:39:08 2,023 EDT	190.103.133.224
optfll1	Mon Jul 10 13:46:04 2,023 EDT	190.103.133.224
optfll2	Mon Jul 10 13:46:43 2,023 EDT	190.103.133.224
optfll1	Mon Jul 10 13:57:45 2,023 EDT	190.103.133.224

LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

ASM-VP REPORT

ACME FINANCIAL SERVICES 08/11/2023

Username	Time	IP Address
yeortiz	Mon Jul 10 14:05:31 2,023 EDT	190.103.133.224
akamc	Mon Jul 10 14:06:06 2,023 EDT	190.103.133.224
akamc	Mon Jul 10 14:06:13 2,023 EDT	190.103.133.224
gmiraglia	Sun Jul 9 10:06:55 2,023 EDT	190.103.133.224
sapcun1	Sun Jul 9 10:36:28 2,023 EDT	190.103.133.224
roportillo	Sun Jul 9 10:48:40 2,023 EDT	190.103.133.224
roportillo	Sun Jul 9 10:49:34 2,023 EDT	190.103.133.224
roportillo	Sun Jul 9 10:49:58 2,023 EDT	190.103.133.224
kaguilar	Sat Jul 8 19:08:29 2,023 EDT	107.160.204.96
joabad	Sat Jul 8 19:23:04 2,023 EDT	190.103.133.224
optlim4	Sat Jul 8 19:48:47 2,023 EDT	190.103.133.224
optlim4	Sat Jul 8 19:49:33 2,023 EDT	190.103.133.224
cceron	Sat Jul 8 17:28:52 2,023 EDT	190.103.133.224
cceron	Sat Jul 8 17:29:16 2,023 EDT	190.103.133.224
ptycap05	Mon Jul 10 10:17:58 2,023 EDT	190.103.133.224
mcasis	Mon Jul 10 10:37:34 2,023 EDT	190.103.133.224
rcostam	Mon Jul 10 10:41:47 2,023 EDT	190.103.133.224
opthav2	Mon Jul 10 10:46:23 2,023 EDT	190.103.133.224
vmunozd	Mon Jul 10 10:49:38 2,023 EDT	190.103.133.224
junavarro	Mon Jul 10 10:53:51 2,023 EDT	190.103.133.224
optmco4	Mon Jul 10 10:54:22 2,023 EDT	190.103.133.224
optmco4	Mon Jul 10 10:54:40 2,023 EDT	190.103.133.224
optmco4	Mon Jul 10 10:55:05 2,023 EDT	190.103.133.224
camina	Mon Jul 10 10:56:45 2,023 EDT	216.101.248.226
aadiaz	Sun Jul 9 11:15:16 2,023 EDT	190.103.133.224
optccs1	Sun Jul 9 11:53:36 2,023 EDT	190.103.133.224
marisalazar	Mon Jul 10 14:37:41 2,023 EDT	190.103.133.224
ptycap05	Mon Jul 10 14:38:31 2,023 EDT	190.103.133.224
optfll1	Mon Jul 10 14:38:31 2,023 EDT	190.103.133.224
dsolares	Mon Jul 10 14:47:43 2,023 EDT	242.200.204.2
ptycap08	Mon Jul 10 14:47:57 2,023 EDT	190.103.133.224
ptycap08	Mon Jul 10 14:47:59 2,023 EDT	190.103.133.224
ptycap08	Mon Jul 10 14:48:17 2,023 EDT	190.103.133.224
ptycap08	Mon Jul 10 14:48:34 2,023 EDT	190.103.133.224
ptycap08	Mon Jul 10 14:48:43 2,023 EDT	190.103.133.224

ASM-VP REPORT

ACME FINANCIAL SERVICES 08/11/2023

Username	Time	IP Address
imunoz	Mon Jul 10 14:52:27 2,023 EDT	190.103.133.224
gmiraglia	Mon Jul 10 14:55:33 2,023 EDT	190.103.133.224
almiranda	Mon Jul 10 15:05:38 2,023 EDT	190.103.133.224
optiad1	Mon Jul 10 14:16:49 2,023 EDT	190.103.133.224
optiad1	Mon Jul 10 14:17:48 2,023 EDT	190.103.133.224
optuio1	Mon Jul 10 14:27:44 2,023 EDT	190.103.133.224
optmco3	Mon Jul 10 14:29:09 2,023 EDT	190.103.133.224
optmco3	Mon Jul 10 14:29:29 2,023 EDT	190.103.133.224
optfll1	Mon Jul 10 14:32:14 2,023 EDT	190.103.133.224
optaxm1	Tue Jul 4 14:26:47 2,023 EDT	190.103.133.224
optaxm1	Tue Jul 4 14:27:25 2,023 EDT	190.103.133.224
optaxm1	Tue Jul 4 14:28:00 2,023 EDT	190.103.133.224
optaxm1	Tue Jul 4 14:28:41 2,023 EDT	190.103.133.224
disoto	Tue Jul 4 14:29:33 2,023 EDT	190.103.133.224
ptycap19	Tue Jul 4 14:50:53 2,023 EDT	190.103.133.224
ptycap12	Tue Jul 4 14:51:03 2,023 EDT	190.103.133.224
ptycap19	Tue Jul 4 14:51:28 2,023 EDT	190.103.133.224
ptycap12	Tue Jul 4 14:51:41 2,023 EDT	190.103.133.224
ptycap19	Tue Jul 4 14:51:46 2,023 EDT	190.103.133.224
optaxm1	Tue Jul 4 14:56:15 2,023 EDT	190.103.133.224
elmoran	Tue Jul 4 14:58:40 2,023 EDT	18.11.178.237
ptycap12	Tue Jul 4 15:07:58 2,023 EDT	190.103.133.224
dchockee	Mon Jul 3 20:22:28 2,023 EDT	190.103.133.224
jkpineda	Mon Jul 3 20:53:17 2,023 EDT	190.103.133.224
vortega	Thu Jul 6 12:34:27 2,023 EDT	190.103.133.224
optord1	Thu Jul 6 12:39:05 2,023 EDT	190.103.133.224
optord1	Thu Jul 6 12:39:52 2,023 EDT	190.103.133.224
optord2	Thu Jul 6 12:42:39 2,023 EDT	190.103.133.224
optord2	Thu Jul 6 12:43:23 2,023 EDT	190.103.133.224
itgomez	Thu Jul 6 12:50:34 2,023 EDT	190.103.133.224
optord1	Thu Jul 6 12:50:44 2,023 EDT	190.103.133.224
nopena	Thu Jul 6 12:50:44 2,023 EDT	190.103.133.224
itgomez	Thu Jul 6 12:50:44 2,023 EDT	190.103.133.224
optord1	Thu Jul 6 12:52:41 2,023 EDT	190.103.133.224
optord1	Thu Jul 6 12:53:13 2,023 EDT	190.103.133.224

Username	Time	IP Address
optord1	Thu Jul 6 12:54:04 2,023 EDT	190.103.133.224
optord2	Thu Jul 6 12:56:16 2,023 EDT	190.103.133.224
ghernandezh	Thu Jul 6 12:57:59 2,023 EDT	190.103.133.224
libanez	Wed Jul 5 9:26:10 2,023 EDT	190.103.133.224
jorgruiz	Wed Jul 5 9:53:48 2,023 EDT	190.103.133.224
jorgruiz	Wed Jul 5 9:54:33 2,023 EDT	190.103.133.224
jorgruiz	Wed Jul 5 9:54:54 2,023 EDT	190.103.133.224
jcen	Wed Jul 5 9:55:30 2,023 EDT	190.103.133.224
jorgruiz	Wed Jul 5 9:55:52 2,023 EDT	190.103.133.224
optmde2	Tue Jul 4 23:02:18 2,023 EDT	190.103.133.224
optmde2	Tue Jul 4 23:03:08 2,023 EDT	190.103.133.224
ccunningham	Tue Jul 4 23:04:09 2,023 EDT	190.103.133.224

Locked Out Users *

Username	Time	IP Address
optfll1	Mon Jul 10 14:34:30 2,023 EDT	190.103.133.224
optfll1	Mon Jul 10 14:34:57 2,023 EDT	190.103.133.224
optaxm1	Tue Jul 4 15:03:42 2,023 EDT	190.103.133.224
optaxm1	Tue Jul 4 15:05:08 2,023 EDT	190.103.133.224
optaxm1	Tue Jul 4 15:07:35 2,023 EDT	190.103.133.224
optaxm1	Tue Jul 4 14:58:35 2,023 EDT	190.103.133.224
optaxm1	Tue Jul 4 15:01:25 2,023 EDT	190.103.133.224
optord1	Thu Jul 6 12:40:14 2,023 EDT	190.103.133.224
optord1	Thu Jul 6 12:40:48 2,023 EDT	190.103.133.224
optord1	Thu Jul 6 12:41:13 2,023 EDT	190.103.133.224
flujano	Thu Jun 29 16:55:58 2,023 EDT	190.103.133.224
flujano	Thu Jun 29 16:56:34 2,023 EDT	190.103.133.224
optuio1	Wed Jun 28 6:15:39 2,023 EDT	190.103.133.224
optsdq1	Wed Jun 28 13:53:05 2,023 EDT	190.103.133.224
optsdq1	Wed Jun 28 13:53:25 2,023 EDT	190.103.133.224
opthav3	Mon Jun 26 22:27:09 2,023 EDT	190.103.133.224
opthav3	Mon Jun 26 22:28:00 2,023 EDT	190.103.133.224
opthav3	Mon Jun 26 22:29:31 2,023 EDT	190.103.133.224
opthav3	Mon Jun 26 22:34:34 2,023 EDT	190.103.133.224

LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

ASM-VP REPORT

ACME FINANCIAL SERVICES 08/11/2023

Username	Time	IP Address
opthav3	Mon Jun 26 22:36:16 2,023 EDT	190.103.133.224
opthav3	Mon Jun 26 22:23:43 2,023 EDT	190.103.133.224
optctg2	Sat Jun 24 23:05:48 2,023 EDT	190.103.133.224
optctg2	Sat Jun 24 23:23:20 2,023 EDT	190.103.133.224
mafaure	Thu Jun 22 17:13:37 2,023 EDT	190.103.133.224
optden1	Thu Jun 22 19:37:01 2,023 EDT	190.103.133.224
optden1	Thu Jun 22 19:38:10 2,023 EDT	190.103.133.224
optden1	Thu Jun 22 19:39:04 2,023 EDT	190.103.133.224
optden1	Thu Jun 22 19:39:46 2,023 EDT	190.103.133.224
optden1	Thu Jun 22 19:40:47 2,023 EDT	190.103.133.224
optden1	Thu Jun 22 19:46:07 2,023 EDT	190.103.133.224
ocuellar	Fri Jun 23 9:37:31 2,023 EDT	216.101.248.226
ocuellar	Fri Jun 23 9:37:56 2,023 EDT	216.101.248.226
optvln1	Sun Jun 18 15:10:02 2,023 EDT	190.103.133.224
optvln1	Sun Jun 18 15:10:30 2,023 EDT	190.103.133.224
optvln1	Sun Jun 18 15:15:21 2,023 EDT	190.103.133.224
optvln1	Sun Jun 18 15:16:20 2,023 EDT	190.103.133.224
optvln1	Sun Jun 18 15:18:25 2,023 EDT	190.103.133.224
optvln1	Sun Jun 18 15:19:53 2,023 EDT	190.103.133.224
optvln1	Sun Jun 18 15:20:38 2,023 EDT	190.103.133.224
optvln1	Sun Jun 18 15:21:26 2,023 EDT	190.103.133.224
dagrisales	Tue Jun 20 10:42:24 2,023 EDT	190.103.133.224
dagrisales	Tue Jun 20 10:46:28 2,023 EDT	201.51.7.123
dagrisales	Tue Jun 20 10:46:56 2,023 EDT	201.51.7.123
optmde1	Tue Jun 13 20:45:00 2,023 EDT	190.103.133.224
optmde1	Tue Jun 13 20:45:31 2,023 EDT	190.103.133.224
optmde1	Tue Jun 13 20:48:37 2,023 EDT	190.103.133.224
optmde1	Tue Jun 13 20:49:18 2,023 EDT	190.103.133.224
optmde1	Tue Jun 13 20:51:34 2,023 EDT	190.103.133.224
optmde1	Tue Jun 13 20:53:50 2,023 EDT	190.103.133.224
optmde1	Tue Jun 13 20:57:09 2,023 EDT	190.103.133.224
optmde1	Tue Jun 13 20:58:25 2,023 EDT	190.103.133.224
optmde1	Tue Jun 13 21:05:20 2,023 EDT	190.103.133.224
optmde1	Tue Jun 13 21:09:14 2,023 EDT	190.103.133.224
optmde1	Tue Jun 13 21:12:44 2,023 EDT	190.103.133.224

ASM-VP REPORT

ACME FINANCIAL SERVICES 08/11/2023

Username	Time	IP Address
optlim1	Sun Jun 11 20:46:33 2,023 EDT	190.103.133.224
opteze6	Sun Jul 9 0:37:49 2,023 EDT	190.103.133.224
opteze6	Sun Jul 9 0:38:14 2,023 EDT	190.103.133.224
opteze6	Sun Jul 9 0:40:13 2,023 EDT	190.103.133.224
opteze6	Sun Jul 9 0:41:33 2,023 EDT	190.103.133.224
optccs2	Sun Jul 9 13:48:39 2,023 EDT	190.103.133.224
optccs2	Sun Jul 9 13:50:43 2,023 EDT	190.103.133.224
optccs2	Sun Jul 9 14:04:31 2,023 EDT	190.103.133.224
jsalasp	Sun Jul 9 21:46:24 2,023 EDT	190.103.133.224
jsalasp	Sun Jul 9 21:49:15 2,023 EDT	190.103.133.224
optord2	Thu Jul 6 0:49:17 2,023 EDT	190.103.133.224
optord2	Thu Jul 6 0:57:02 2,023 EDT	190.103.133.224
optiad1	Wed Jul 5 10:09:11 2,023 EDT	190.103.133.224
optord2	Thu Jul 6 0:34:50 2,023 EDT	190.103.133.224
optord2	Thu Jul 6 0:35:56 2,023 EDT	190.103.133.224
optord2	Thu Jul 6 0:36:52 2,023 EDT	190.103.133.224
optord2	Thu Jul 6 0:37:53 2,023 EDT	190.103.133.224
optord2	Thu Jul 6 0:39:17 2,023 EDT	190.103.133.224
optord2	Thu Jul 6 0:47:09 2,023 EDT	190.103.133.224
opteze6	Fri Jul 7 10:12:25 2,023 EDT	190.103.133.224
opteze6	Fri Jul 7 10:13:36 2,023 EDT	190.103.133.224
opthav2	Thu Jun 29 10:52:20 2,023 EDT	190.103.133.224
opthav2	Thu Jun 29 10:52:44 2,023 EDT	190.103.133.224
opthav2	Thu Jun 29 10:53:12 2,023 EDT	190.103.133.224
opthav2	Thu Jun 29 10:53:48 2,023 EDT	190.103.133.224
opthav2	Thu Jun 29 10:56:21 2,023 EDT	190.103.133.224
opthav2	Thu Jun 29 10:57:31 2,023 EDT	190.103.133.224
opthav2	Thu Jun 29 10:59:54 2,023 EDT	190.103.133.224
optccs2	Tue Jun 27 16:12:32 2,023 EDT	190.103.133.224
optccs1	Sat Jun 24 14:46:21 2,023 EDT	190.103.133.224
optccs1	Sat Jun 24 14:53:28 2,023 EDT	190.103.133.224
optccs1	Sat Jun 24 14:53:49 2,023 EDT	190.103.133.224
optccs1	Sat Jun 24 14:54:40 2,023 EDT	190.103.133.224
optccs1	Sat Jun 24 14:55:48 2,023 EDT	190.103.133.224
optccs1	Sat Jun 24 14:56:19 2,023 EDT	190.103.133.224

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

ASM-VP REPORT

ACME FINANCIAL SERVICES 08/11/2023

Username	Time	IP Address
optccs1	Sat Jun 24 14:57:53 2,023 EDT	190.103.133.224
mluchsinger	Thu Jun 22 11:23:32 2,023 EDT	186.47.87.164
optbog1	Wed Jun 21 12:34:21 2,023 EDT	190.103.133.224
optbog1	Wed Jun 21 12:34:50 2,023 EDT	190.103.133.224
optbog1	Wed Jun 21 12:36:36 2,023 EDT	190.103.133.224
optuio3	Wed Jun 21 12:47:10 2,023 EDT	190.103.133.224
optuio3	Wed Jun 21 12:47:44 2,023 EDT	190.103.133.224
optsjo6	Thu Jun 22 9:52:21 2,023 EDT	190.103.133.224
optsjo6	Thu Jun 22 9:52:45 2,023 EDT	190.103.133.224
optsjo6	Thu Jun 22 9:55:23 2,023 EDT	190.103.133.224
optsjo6	Thu Jun 22 9:58:29 2,023 EDT	190.103.133.224

ASM-VP REPORT

ACME FINANCIAL SERVICES 08/11/2023

Anomalous push by Users *

Username	Time	IP Address
masantos	Sun Jul 9 20:04:18 2,023 EDT	116.57.74.180
dsolares	Mon Jul 10 14:47:24 2,023 EDT	242.200.204.2
dsolares	Mon Jul 10 14:47:29 2,023 EDT	242.200.204.2
mtejedor	Wed Jul 5 9:52:23 2,023 EDT	186.47.87.164
liliao	Fri Jul 7 7:41:43 2,023 EDT	18.11.178.237
liliao	Fri Jul 7 7:42:00 2,023 EDT	18.11.178.237
edelrosario	Fri Jul 7 15:36:27 2,023 EDT	66.218.109.123
eherreras	Mon Jul 3 6:14:17 2,023 EDT	18.11.178.237
jjayo	Mon Jul 3 16:48:52 2,023 EDT	18.11.178.237
jjayo	Mon Jul 3 16:48:55 2,023 EDT	18.11.178.237
irgonzalezm	Sun Jul 2 0:05:50 2,023 EDT	244.136.239.246
julrobles	Sun Jul 2 19:08:05 2,023 EDT	171.134.204.195
afreire	Sun Jul 2 19:47:45 2,023 EDT	15.75.132.76
polive	Tue Jun 27 12:29:12 2,023 EDT	219.89.38.184
jprieto	Tue Jun 20 12:19:49 2,023 EDT	252.14.227.52
jprieto	Tue Jun 20 12:19:53 2,023 EDT	252.14.227.52
jprieto	Tue Jun 20 12:19:56 2,023 EDT	252.14.227.52
jprieto	Fri Jun 16 15:23:32 2,023 EDT	116.112.82.9
monofre	Sun Jun 18 6:14:07 2,023 EDT	213.116.237.200
ryeung	Mon Jun 19 16:07:30 2,023 EDT	186.47.87.164
ryeung	Mon Jun 19 16:08:34 2,023 EDT	186.47.87.164
evasquezv	Fri Jun 30 15:31:28 2,023 EDT	24.244.248.201
ocabeza	Sun Jun 25 12:48:02 2,023 EDT	229.234.229.3
tpertab	Mon Jun 12 4:33:17 2,023 EDT	24.244.248.201
lefolch	Thu Jun 15 22:44:23 2,023 EDT	218.197.172.26

Call timed out by Users *

Username	Time	IP Address
remanuel	Fri Jul 7 17:46:05 2,023 EDT	1.174.111.208
hocampo	Sat Jul 8 21:13:19 2,023 EDT	61.193.65.20
apgarcia	Sat Jul 8 22:01:28 2,023 EDT	216.101.248.226
dlumbi	Sat Jul 8 22:58:21 2,023 EDT	86.220.110.108
dlumbi	Sat Jul 8 22:59:40 2,023 EDT	86.220.110.108

ASM-VP REPORT

ACME FINANCIAL SERVICES 08/11/2023

Username	Time	IP Address
dlumbi	Sat Jul 8 23:02:18 2,023 EDT	86.220.110.108
ygonzalez	Fri Jul 7 23:13:16 2,023 EDT	18.11.178.237
julrobles	Sat Jul 8 8:02:58 2,023 EDT	18.11.178.237
ealvarez	Sun Jul 9 8:50:09 2,023 EDT	164.52.87.194
dlumbi	Sun Jul 9 21:16:41 2,023 EDT	86.220.110.108
dlumbi	Sun Jul 9 21:36:55 2,023 EDT	86.220.110.108
gsgonzalez	Sun Jul 9 22:01:38 2,023 EDT	18.11.178.237
cbarrera	Thu Jul 6 22:55:03 2,023 EDT	218.54.82.73
reperez	Thu Jul 6 15:20:49 2,023 EDT	190.103.133.224
pogando	Thu Jul 6 11:33:56 2,023 EDT	218.197.172.26
ebruno	Thu Jul 6 9:32:12 2,023 EDT	18.11.178.237
fatenciop	Thu Jul 6 9:37:48 2,023 EDT	18.11.178.237
mprotasowicki	Thu Jul 6 10:00:24 2,023 EDT	245.247.7.226
norillac	Thu Jul 6 10:14:00 2,023 EDT	18.11.178.237
liliao	Mon Jul 3 6:15:11 2,023 EDT	18.11.178.237
liliao	Mon Jul 3 6:17:25 2,023 EDT	18.11.178.237
adehermoso	Mon Jul 3 16:22:28 2,023 EDT	18.11.178.237
rastacio	Mon Jul 3 16:25:40 2,023 EDT	107.160.204.96
rastacio	Mon Jul 3 16:26:43 2,023 EDT	107.160.204.96
cmelasecca	Mon Jul 3 16:43:00 2,023 EDT	22.184.74.154
llarac	Mon Jul 3 17:07:26 2,023 EDT	18.11.178.237
mprotasowicki	Mon Jul 3 14:32:27 2,023 EDT	216.101.248.226
mprotasowicki	Mon Jul 3 14:33:28 2,023 EDT	216.101.248.226
mprotasowicki	Mon Jul 3 14:34:30 2,023 EDT	216.101.248.226
sdeleon	Mon Jul 3 14:58:15 2,023 EDT	18.11.178.237
rturner	Wed Jul 5 11:39:06 2,023 EDT	18.11.178.237
rquiel	Wed Jul 5 11:41:19 2,023 EDT	18.11.178.237
elvargas	Wed Jul 5 11:54:28 2,023 EDT	201.51.7.123
elvargas	Wed Jul 5 11:55:30 2,023 EDT	201.51.7.123
rchavarria	Wed Jul 5 12:05:31 2,023 EDT	161.228.182.71
aferreira	Wed Jul 5 10:01:25 2,023 EDT	149.87.69.55
aburgess	Wed Jul 5 15:22:08 2,023 EDT	186.47.87.164
aburgess	Wed Jul 5 15:23:59 2,023 EDT	186.47.87.164
caarjona	Wed Jul 5 15:27:05 2,023 EDT	222.181.97.52
magomez	Wed Jul 5 15:40:19 2,023 EDT	18.11.178.237

ASM-VP REPORT

ACME FINANCIAL SERVICES 08/11/2023

Username	Time	IP Address
jdelaguardia	Wed Jul 5 15:48:47 2,023 EDT	186.47.87.164
plopez	Wed Jul 5 15:50:30 2,023 EDT	18.11.178.237
plopez	Wed Jul 5 15:51:34 2,023 EDT	18.11.178.237
rturner	Wed Jul 5 15:55:12 2,023 EDT	18.11.178.237
ekreitz	Wed Jul 5 16:12:45 2,023 EDT	99.20.184.239
eavega	Wed Jul 5 12:55:31 2,023 EDT	190.103.133.224
jperezp	Fri Jul 7 9:48:28 2,023 EDT	18.11.178.237
irgonzalezm	Sun Jul 2 0:05:27 2,023 EDT	244.136.239.246
irgonzalezm	Sun Jul 2 0:06:52 2,023 EDT	244.136.239.246
irgonzalezm	Sun Jul 2 0:07:56 2,023 EDT	244.136.239.246
gsgonzalez	Sun Jul 2 11:37:47 2,023 EDT	18.11.178.237
alfernandez	Thu Jun 29 17:59:52 2,023 EDT	18.11.178.237
hlopez	Fri Jun 30 10:05:27 2,023 EDT	69.106.52.55
rbennett	Fri Jun 30 9:38:30 2,023 EDT	216.101.248.226
aybarrios	Fri Jun 30 9:12:54 2,023 EDT	18.11.178.237
wross	Fri Jun 30 11:36:59 2,023 EDT	18.11.178.237
yortegab	Fri Jun 30 11:37:18 2,023 EDT	1.138.51.216
aadiaz	Fri Jun 30 11:40:44 2,023 EDT	56.199.115.228
wross	Fri Jun 30 11:40:50 2,023 EDT	18.11.178.237
yortegab	Fri Jun 30 11:54:16 2,023 EDT	1.138.51.216
ltejada	Thu Jun 29 13:07:48 2,023 EDT	252.87.54.247
piannicelli	Fri Jun 30 11:16:32 2,023 EDT	190.103.133.224
hlopez	Fri Jun 30 11:29:58 2,023 EDT	69.106.52.55
yortegab	Thu Jun 29 10:35:08 2,023 EDT	218.11.239.164
ekreitz	Thu Jun 29 10:35:48 2,023 EDT	145.37.144.62
rturner	Thu Jun 29 10:54:14 2,023 EDT	18.11.178.237
juespinosa	Thu Jun 29 10:08:11 2,023 EDT	180.18.176.2
juespinosa	Thu Jun 29 10:10:26 2,023 EDT	180.18.176.2
iracine	Thu Jun 29 10:16:36 2,023 EDT	18.11.178.237
iracine	Thu Jun 29 10:16:59 2,023 EDT	18.11.178.237
hlopez	Tue Jun 27 17:23:30 2,023 EDT	239.44.101.231
jose34240	Tue Jun 27 17:40:44 2,023 EDT	89.12.184.104
nrodrigueza	Tue Jun 27 17:44:30 2,023 EDT	18.11.178.237
pfigueroa	Mon Jun 26 17:18:14 2,023 EDT	129.180.244.21
pfigueroa	Mon Jun 26 17:19:46 2,023 EDT	129.180.244.21

Username	Time	IP Address
lylee	Mon Jun 26 17:22:16 2,023 EDT	18.11.178.237
mzavan	Tue Jun 27 9:37:29 2,023 EDT	107.160.204.96
rbennett	Tue Jun 27 9:53:27 2,023 EDT	216.101.248.226
yecheverry	Tue Jun 27 10:01:18 2,023 EDT	13.206.187.153
lamarino	Tue Jun 27 10:05:47 2,023 EDT	120.97.251.167
rvonchong	Tue Jun 27 12:53:26 2,023 EDT	190.103.133.224
ahgonzalez	Tue Jun 27 12:56:18 2,023 EDT	18.11.178.237
ahgonzalez	Tue Jun 27 12:57:23 2,023 EDT	18.11.178.237
ahgonzalez	Tue Jun 27 13:05:28 2,023 EDT	18.11.178.237
edelrosario	Tue Jun 27 11:48:39 2,023 EDT	27.57.202.72
smchavez	Tue Jun 27 11:54:38 2,023 EDT	216.101.248.226
cllanque	Mon Jun 26 14:08:24 2,023 EDT	151.37.86.192
mquiros	Mon Jun 26 13:20:46 2,023 EDT	236.250.120.33
carellano	Mon Jun 26 13:33:59 2,023 EDT	10.101.64.149
aygonzalez	Mon Jun 26 14:06:57 2,023 EDT	31.175.211.228
joestrada	Sun Jun 25 2:24:25 2,023 EDT	10.0.3.250
joestrada	Sun Jun 25 2:25:29 2,023 EDT	10.0.3.250
jcen	Sun Jun 25 10:01:53 2,023 EDT	107.160.204.96
gsgonzalez	Fri Jun 23 14:57:25 2,023 EDT	18.11.178.237
lmendez	Fri Jun 23 15:13:55 2,023 EDT	18.11.178.237
kabrego	Fri Jun 23 15:16:22 2,023 EDT	18.11.178.237
mzavan	Thu Jun 22 11:40:57 2,023 EDT	107.160.204.96
hlopez	Thu Jun 22 12:07:19 2,023 EDT	111.83.126.72
mpinzon	Thu Jun 22 11:26:43 2,023 EDT	18.11.178.237
wquintero	Thu Jun 22 11:26:55 2,023 EDT	23.56.137.211

Authentications Cancelled by the Users *

Username	Time	IP Address
fzambrano	Fri Jul 7 17:37:52 2,023 EDT	107.160.204.96
kbastian	Sun Jul 9 2:43:57 2,023 EDT	107.160.204.96
ogomez	Sun Jul 9 6:01:13 2,023 EDT	242.200.204.2
ramesquita	Tue Jul 4 7:33:27 2,023 EDT	18.11.178.237
eherreras	Mon Jul 3 6:14:16 2,023 EDT	18.11.178.237
erangel	Mon Jul 3 16:25:52 2,023 EDT	18.11.178.237

ASM-VP REPORT

ACME FINANCIAL SERVICES 08/11/2023

Username	Time	IP Address
erangel	Mon Jul 3 16:26:08 2,023 EDT	18.11.178.237
aoromero	Mon Jul 3 16:45:36 2,023 EDT	163.211.40.101
jjayo	Mon Jul 3 16:48:51 2,023 EDT	18.11.178.237
elvargas	Wed Jul 5 11:56:02 2,023 EDT	201.51.7.123
arussell	Fri Jul 7 7:26:46 2,023 EDT	18.11.178.237
fabiurriola	Fri Jul 7 9:27:11 2,023 EDT	44.160.82.139
irgonzalezm	Sun Jul 2 0:05:49 2,023 EDT	244.136.239.246
aestrada	Sun Jul 2 0:26:17 2,023 EDT	107.160.204.96
julrobles	Sun Jul 2 19:08:04 2,023 EDT	171.134.204.195
afreire	Sun Jul 2 19:47:44 2,023 EDT	15.75.132.76
aybarrios	Fri Jun 30 9:13:11 2,023 EDT	18.11.178.237
aybarrios	Fri Jun 30 9:13:26 2,023 EDT	18.11.178.237
apereira	Tue Jun 27 15:57:31 2,023 EDT	18.11.178.237
jcastanon	Tue Jun 27 9:47:37 2,023 EDT	138.16.137.139
apereira	Tue Jun 27 9:51:28 2,023 EDT	18.11.178.237
apereira	Tue Jun 27 9:51:40 2,023 EDT	18.11.178.237
pkerguelen	Tue Jun 27 11:42:19 2,023 EDT	201.51.7.123
fzambrano	Tue Jun 27 12:19:51 2,023 EDT	13.206.187.153
polive	Tue Jun 27 12:29:11 2,023 EDT	219.89.38.184
slgonzalez	Mon Jun 26 13:33:26 2,023 EDT	18.11.178.237
apgarcia	Sat Jun 24 21:24:53 2,023 EDT	216.101.248.226
ylobelo	Sun Jun 25 2:40:49 2,023 EDT	61.193.65.20
ylobelo	Sun Jun 25 2:41:09 2,023 EDT	61.193.65.20
aygonzalez	Fri Jun 23 14:58:30 2,023 EDT	18.11.178.237
jvelasquezc	Fri Jun 23 15:00:21 2,023 EDT	31.175.211.228
echang	Fri Jun 23 14:28:42 2,023 EDT	18.11.178.237
ebarnola	Thu Jun 22 11:46:06 2,023 EDT	18.11.178.237
rcgonzalez	Thu Jun 22 11:28:24 2,023 EDT	18.11.178.237
mcasis	Thu Jun 22 14:53:40 2,023 EDT	161.247.9.248
mcasis	Wed Jun 21 13:09:02 2,023 EDT	161.247.9.248
dfruiz	Thu Jun 22 9:24:36 2,023 EDT	206.32.64.87
jprieto	Tue Jun 20 12:19:48 2,023 EDT	252.14.227.52
joestrada	Wed Jun 14 2:05:43 2,023 EDT	52.122.234.42
joestrada	Wed Jun 14 2:08:55 2,023 EDT	52.122.234.42
dcamargo	Thu Jun 15 11:44:35 2,023 EDT	216.101.248.226

LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

ASM-VP REPORT

ACME FINANCIAL SERVICES 08/11/2023

Username	Time	IP Address
joestrada	Wed Jun 14 4:33:25 2,023 EDT	42.205.3.29
khurtado	Fri Jun 16 11:33:26 2,023 EDT	61.193.65.20
khurtado	Fri Jun 16 11:33:39 2,023 EDT	61.193.65.20
ewalters	Fri Jun 16 11:48:57 2,023 EDT	109.202.153.131
ewalters	Thu Jun 15 18:13:53 2,023 EDT	109.202.153.131
monofre	Sun Jun 18 6:13:54 2,023 EDT	213.116.237.200
monofre	Sun Jun 18 6:14:04 2,023 EDT	213.116.237.200
jprieto	Fri Jun 16 15:23:31 2,023 EDT	116.112.82.9
wquintero	Mon Jun 12 17:18:16 2,023 EDT	129.180.244.21
wquintero	Mon Jun 12 17:18:29 2,023 EDT	129.180.244.21
wquintero	Mon Jun 12 17:19:21 2,023 EDT	129.180.244.21
wquintero	Mon Jun 12 17:21:04 2,023 EDT	129.180.244.21
dgalvarado	Sun Jun 11 17:17:04 2,023 EDT	174.156.192.120
ovidales	Thu Jun 15 9:36:40 2,023 EDT	18.11.178.237
jdewindt	Wed Jun 14 8:13:29 2,023 EDT	216.101.248.226
ryeung	Mon Jun 19 16:08:18 2,023 EDT	186.47.87.164
ryeung	Mon Jun 19 16:08:30 2,023 EDT	186.47.87.164
mjaescke	Thu Jun 15 9:23:30 2,023 EDT	18.11.178.237
jjayo	Mon Jul 10 13:40:40 2,023 EDT	18.11.178.237
dlumbi	Sun Jul 9 10:36:16 2,023 EDT	216.214.0.196
dsolares	Mon Jul 10 14:47:22 2,023 EDT	242.200.204.2
gsgonzalez	Tue Jul 4 15:10:32 2,023 EDT	18.11.178.237
ducaceres	Fri Jul 7 8:04:44 2,023 EDT	216.101.248.226
cemaduro	Fri Jul 7 15:39:52 2,023 EDT	216.101.248.226
cemaduro	Fri Jul 7 15:40:25 2,023 EDT	216.101.248.226
cemaduro	Fri Jul 7 15:42:15 2,023 EDT	216.101.248.226
eaguirree	Wed Jul 5 18:12:40 2,023 EDT	191.201.61.70
sbravoc	Tue Jul 4 19:13:03 2,023 EDT	9.230.58.3
abdesedas	Mon Jul 3 6:06:29 2,023 EDT	18.11.178.237
suwilliams	Mon Jul 3 8:15:33 2,023 EDT	18.11.178.237
rjhaman	Sat Jul 1 16:00:15 2,023 EDT	46.99.193.148
dcordoba	Sun Jul 2 8:23:23 2,023 EDT	107.7.158.153
dcordoba	Sun Jul 2 8:23:33 2,023 EDT	107.7.158.153
khurtado	Thu Jun 29 21:17:54 2,023 EDT	169.79.21.153
smonsalve	Thu Jun 29 16:45:06 2,023 EDT	83.62.155.68

ASM-VP REPORT

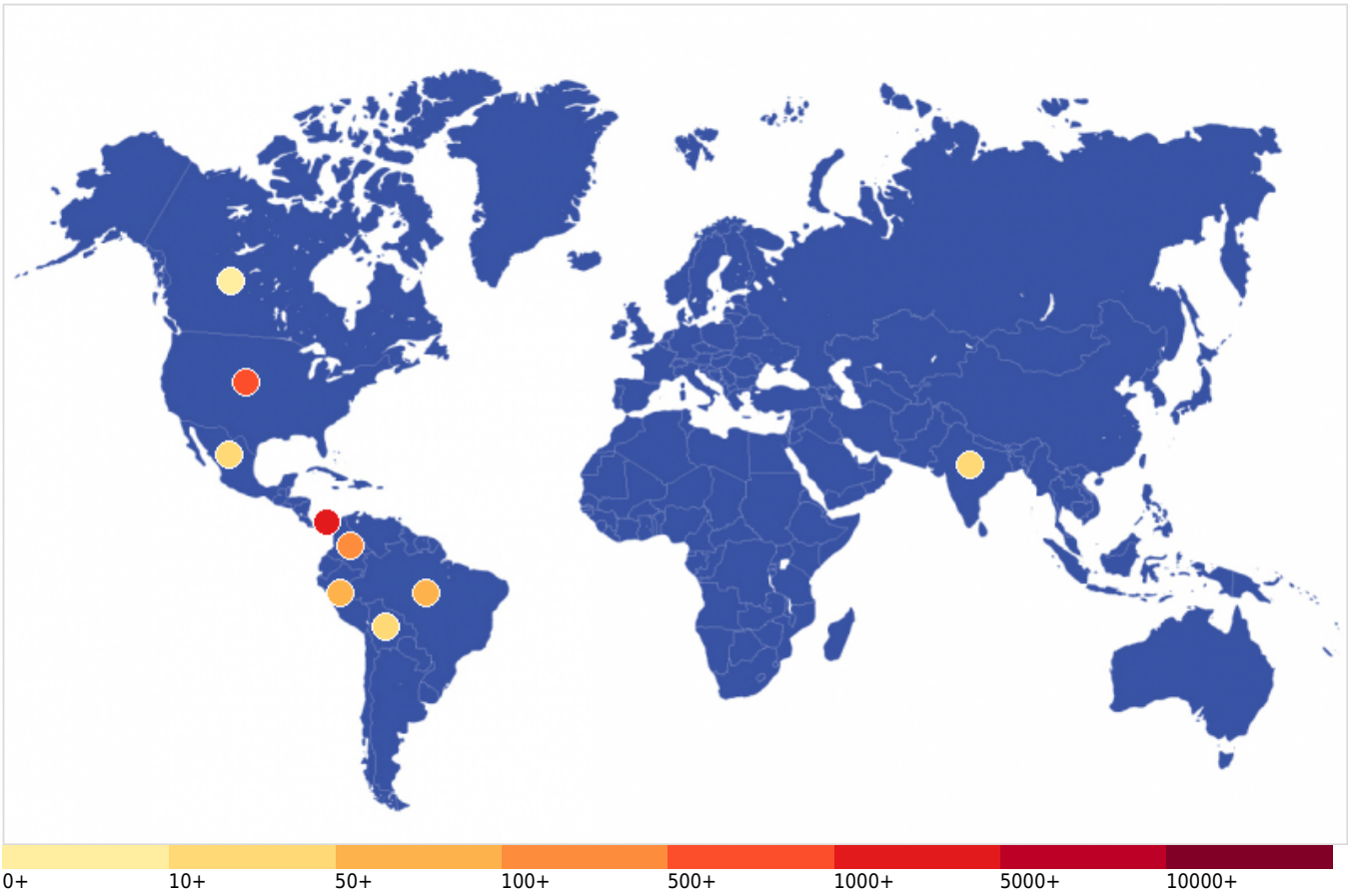
ACME FINANCIAL SERVICES 08/11/2023

Username	Time	IP Address
ocabeza	Wed Jun 28 17:13:12 2,023 EDT	18.11.178.237
ocabeza	Wed Jun 28 18:17:47 2,023 EDT	18.11.178.237
jdsolis	Wed Jun 28 7:42:05 2,023 EDT	18.11.178.237
cpatino	Wed Jun 28 13:44:30 2,023 EDT	212.5.242.61
elvargas	Wed Jun 28 13:29:09 2,023 EDT	201.51.7.123
echiari	Sun Jun 25 15:14:06 2,023 EDT	18.11.178.237
apereira	Thu Jun 22 20:04:44 2,023 EDT	18.11.178.237
spaez	Thu Jun 22 1:08:50 2,023 EDT	218.197.172.26
jdsolis	Fri Jun 16 5:26:29 2,023 EDT	18.11.178.237
msagel	Sat Jun 17 11:11:38 2,023 EDT	174.196.157.98
apereira	Tue Jun 20 10:25:51 2,023 EDT	18.11.178.237
mcasis	Mon Jun 12 8:31:13 2,023 EDT	161.247.9.248
mcasis	Mon Jun 12 8:31:29 2,023 EDT	161.247.9.248
mcasis	Mon Jun 12 8:31:59 2,023 EDT	161.247.9.248
mcasis	Mon Jun 12 8:32:50 2,023 EDT	161.247.9.248
mlizarazo	Sat Jun 10 21:21:54 2,023 EDT	162.202.207.188
janglero	Mon Jun 12 17:03:22 2,023 EDT	129.180.244.21
mjaescke	Mon Jun 12 14:43:25 2,023 EDT	18.11.178.237
agamarra	Tue Jun 13 9:46:14 2,023 EDT	201.51.7.123
jchang	Tue Jun 13 9:46:36 2,023 EDT	18.11.178.237
agamarra	Tue Jun 13 9:46:36 2,023 EDT	201.51.7.123
ocabeza	Tue Jun 13 11:38:38 2,023 EDT	18.11.178.237
eaguirree	Sun Jul 9 14:39:53 2,023 EDT	83.165.51.88
jsalasp	Sun Jul 9 23:15:33 2,023 EDT	18.11.178.237

Most Successful Authenticated Countries *

ASM-VP REPORT

ACME FINANCIAL SERVICES 08/11/2023

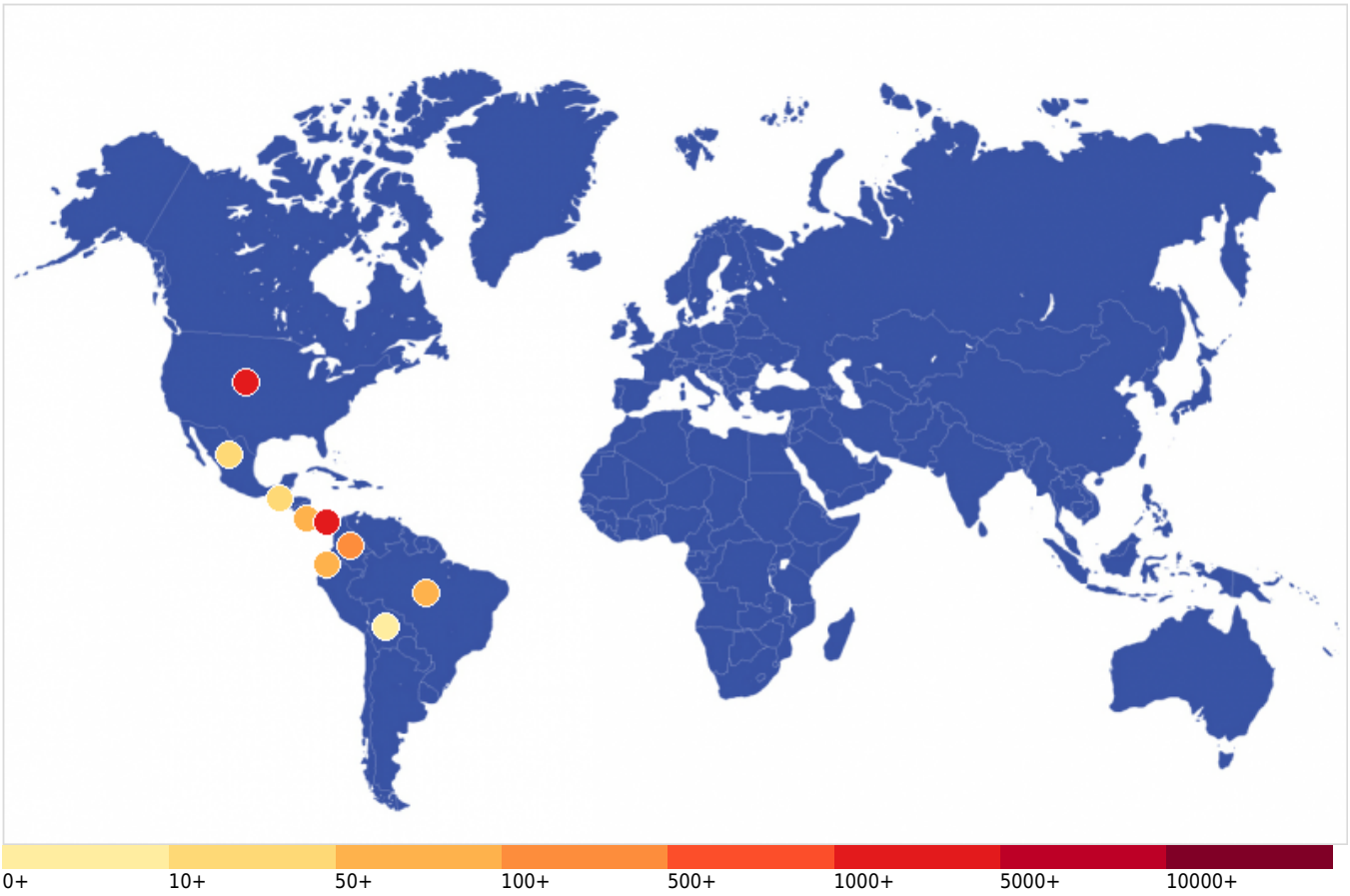


Countries with Most Failed Authentications *

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

ASM-VP REPORT

ACME FINANCIAL SERVICES 08/11/2023

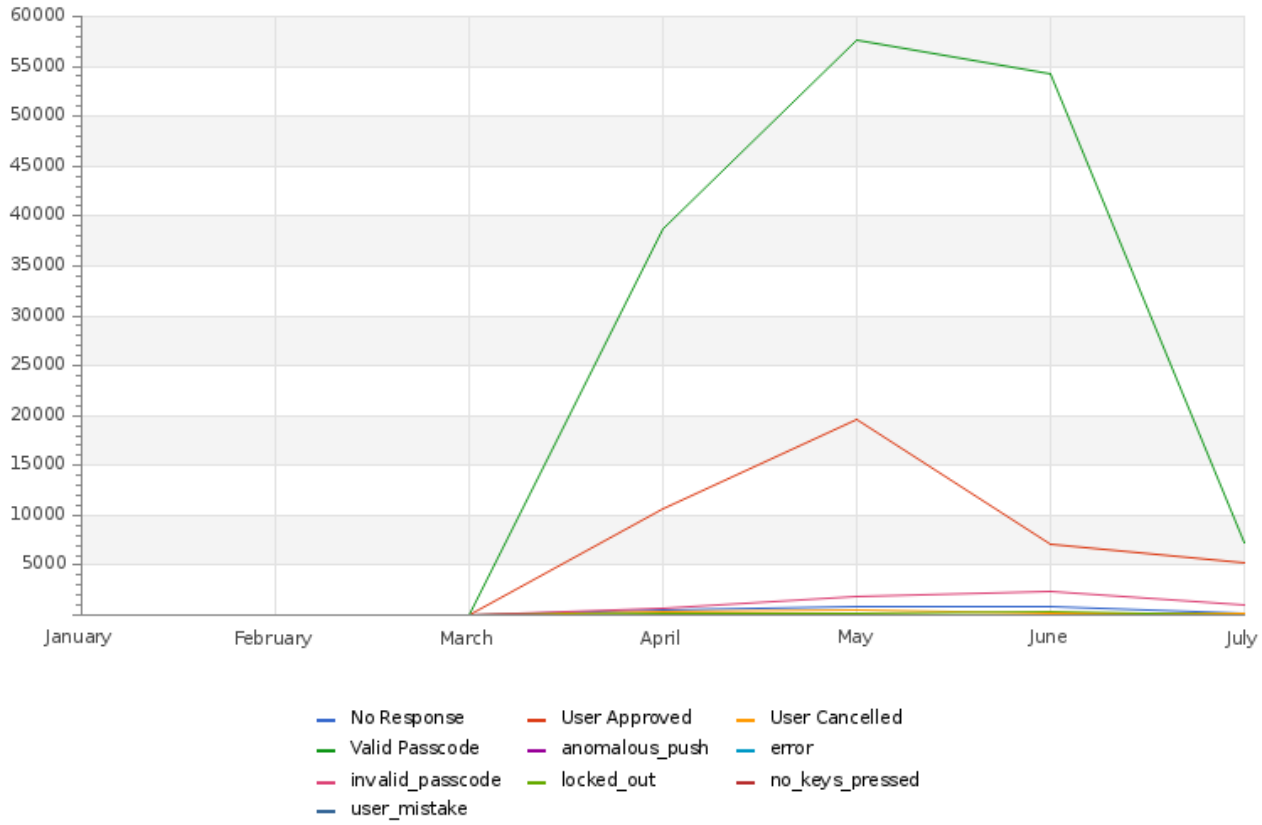


LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

ASM-VP REPORT

ACME FINANCIAL SERVICES 08/11/2023

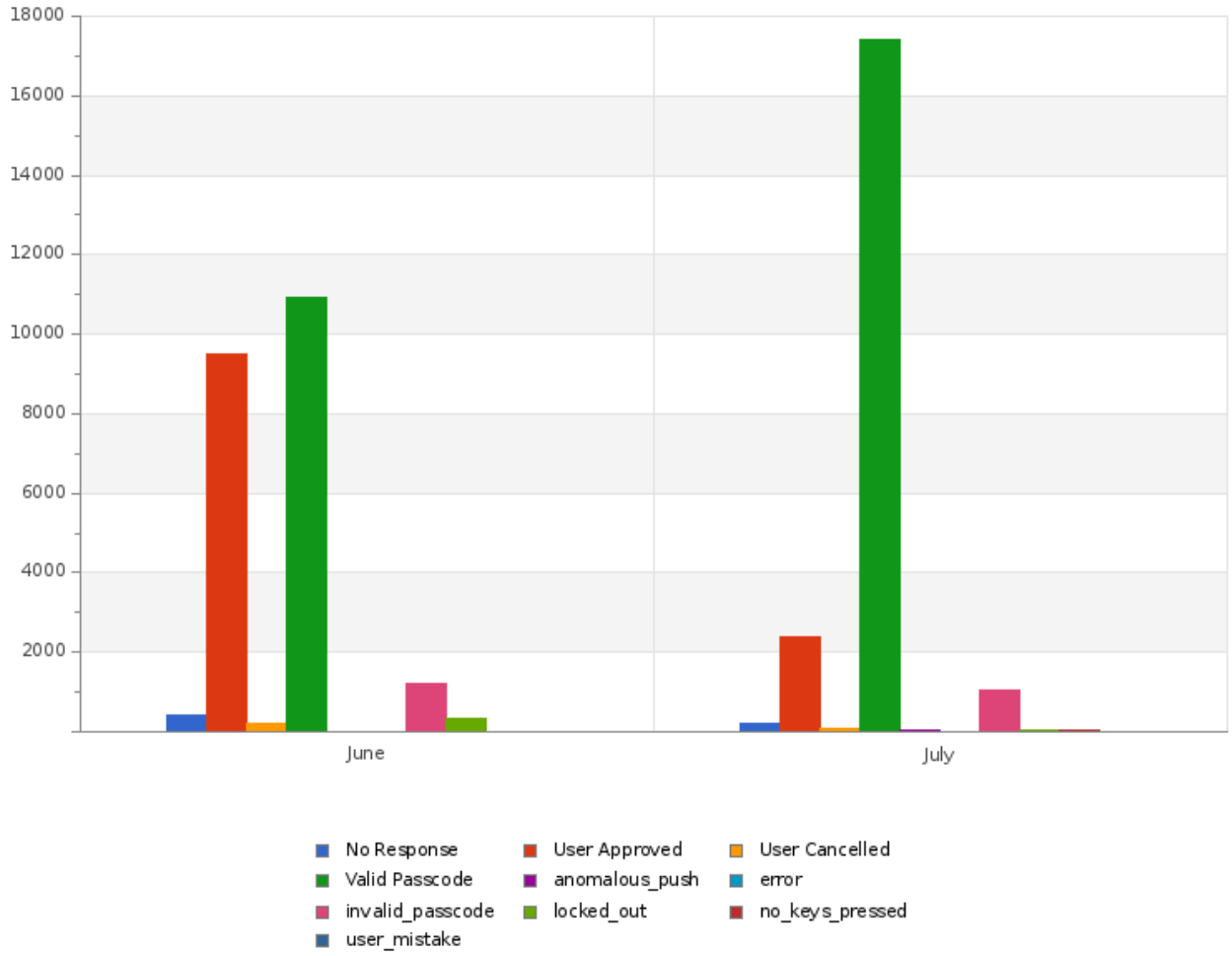
Trusted Access In Last 6 Months



Successful and Failed Authentications *

ASM-VP REPORT

ACME FINANCIAL SERVICES 08/11/2023

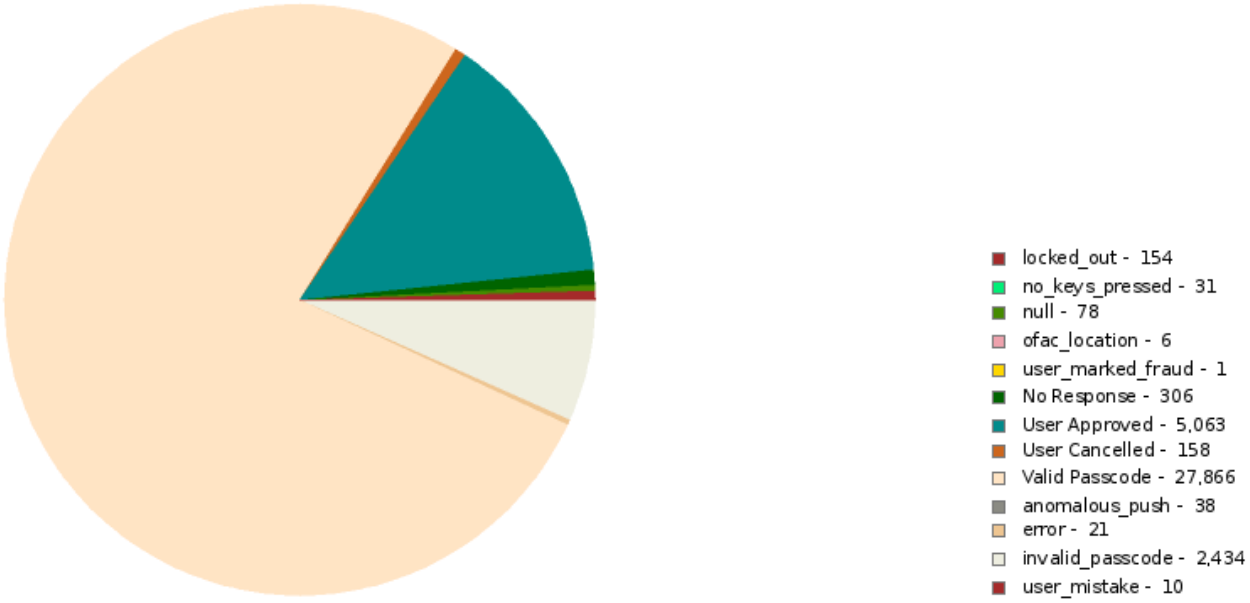


LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

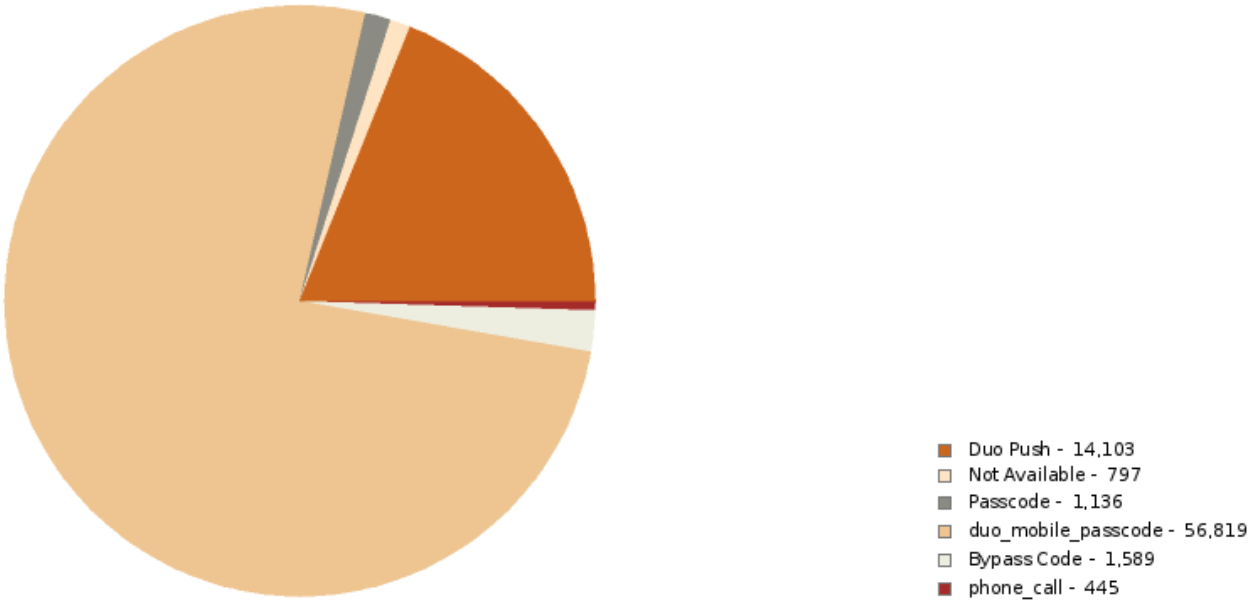
ASM-VP REPORT

ACME FINANCIAL SERVICES 08/11/2023

Successful Authentications *



Successful Authentications by Factor *

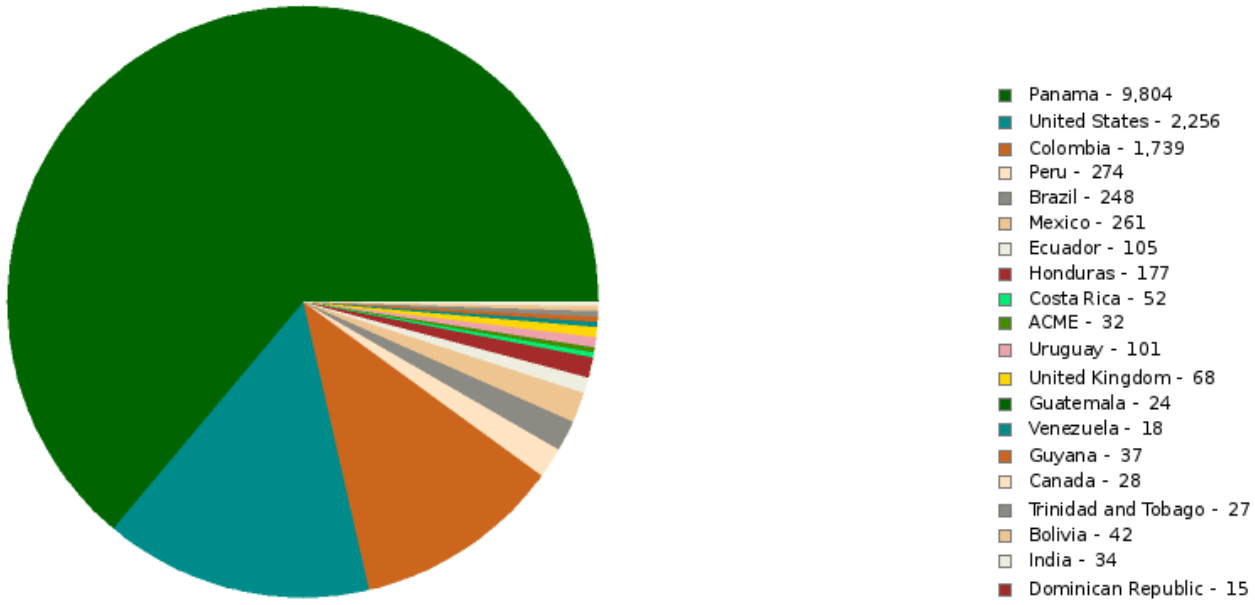


LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

ASM-VP REPORT

ACME FINANCIAL SERVICES 08/11/2023

Authentication Per Country *



MSS-USB

Top Actions

action	count
file_create	4
file_delete	3
file_modified	2
logout	1

Top Locations - Cities

City	Country	Count
Orlando	US	5

ASM-VP REPORT

ACME FINANCIAL SERVICES 08/11/2023

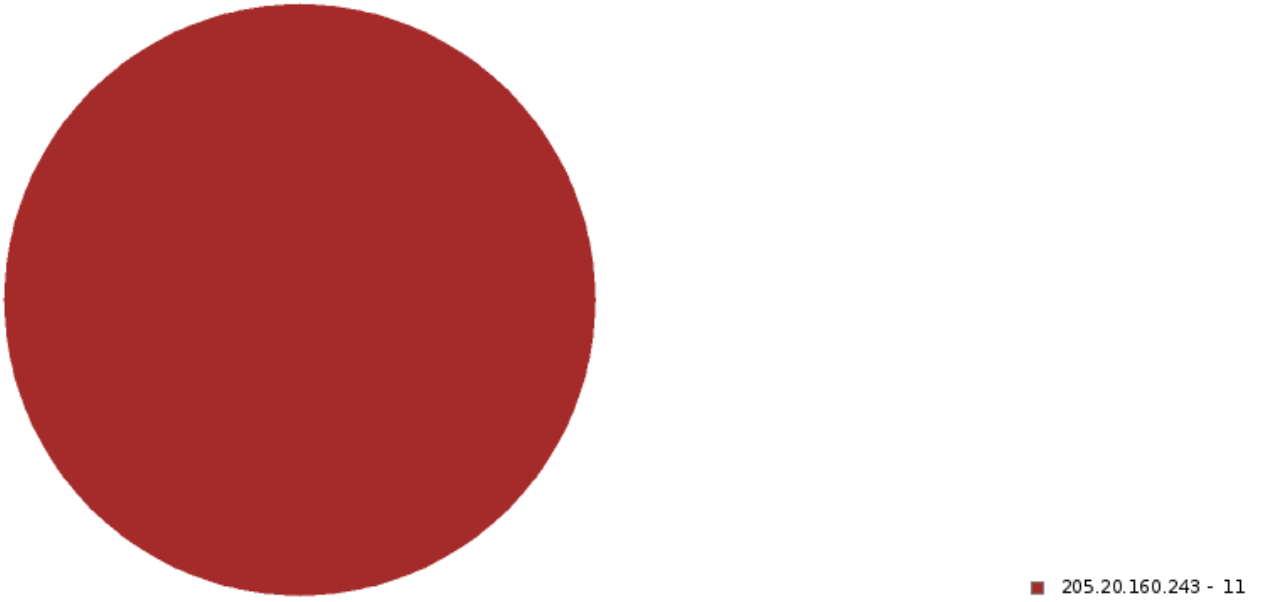
IP Addresses - List

IP Address	Count
205.20.160.243	16

Drives used in Last 30 days

Serial	Drive Model	User	Computer	City	Country	IP
K350000474	K350	acme-44.com/GLESEC/Users/Orlando/Chad Vega	USASYSTEMSWS02	Orlando	US	205.20.160.243

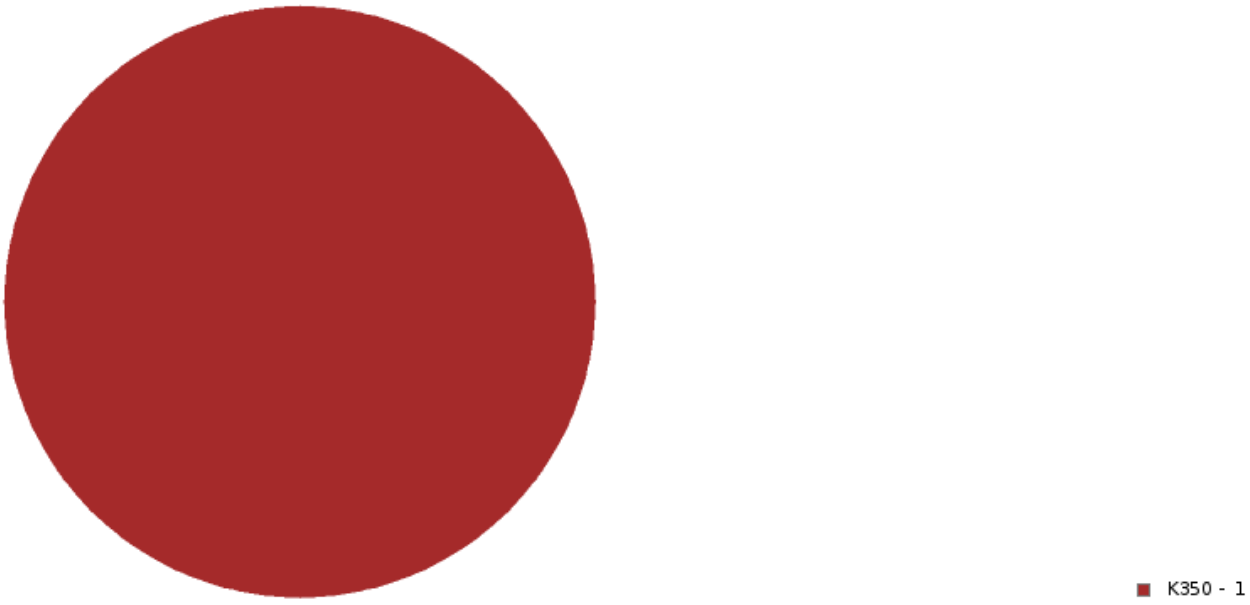
IP Addresses - Top 10



ASM-VP REPORT

ACME FINANCIAL SERVICES 08/11/2023

Drive Inventory - Model Count



Drive Inventory

Drive Model	Serial	User	Location
K350	K350000474	acme-44.com/GLESEC/Users/Orlando/Chad Vega	Orlando, US

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

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

TLP:AMBER

ASM-VP REPORT

HOW CAN WE HELP?

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

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