
TLP:AMBER

# ASM-VP REPORT

## GOAA

July 05, 2024

# TLP AMBER
## ASM-VP REPORT

**About this report**

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

# Assets

## MSS-VME

## Overview

### Vulnerability Level

**12%**

### Discovered Hosts

**43**

### Vulnerable Hosts

**31**

### Executive Summary Vulnerability Severity Distribution

| Scanner | Critical | High | Medium | Low | Total |
|---|---|---|---|---|---|
| GOAA | 0 | 0 | 51 | 8 | 59 |
| Domain Scan: www.orlandoairports.net | 34 | 0 | 3 | 17 | 54 |

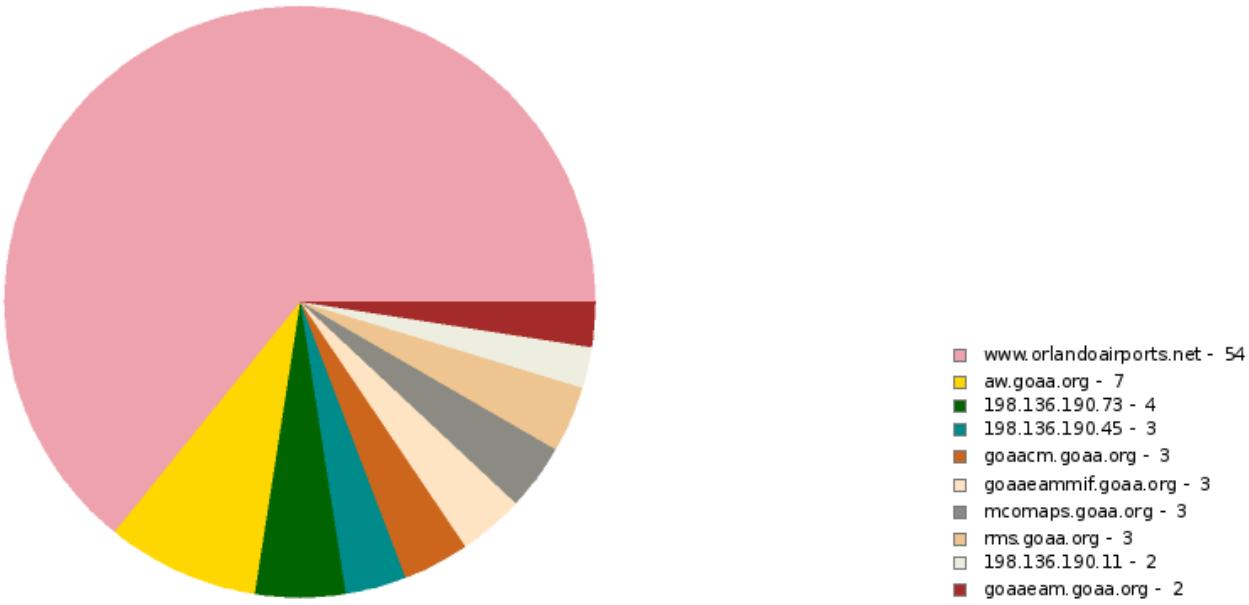


LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

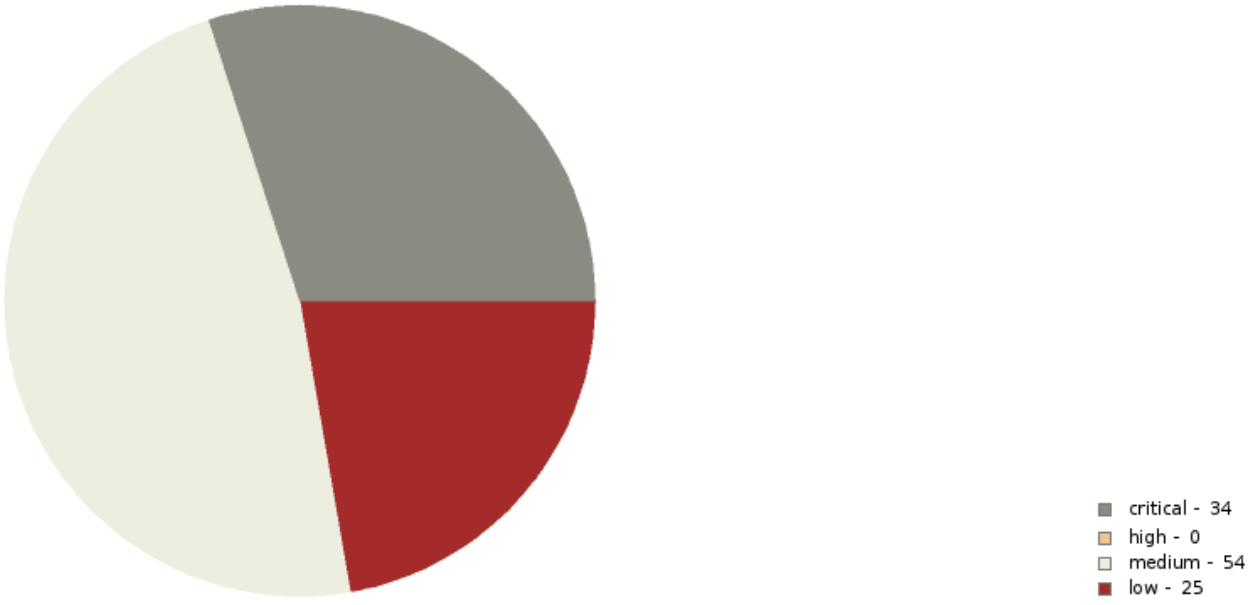
# ASM-VP REPORT

GOAA 07/05/2024

## Most Vulnerable Host *




## Vulnerability Distribution





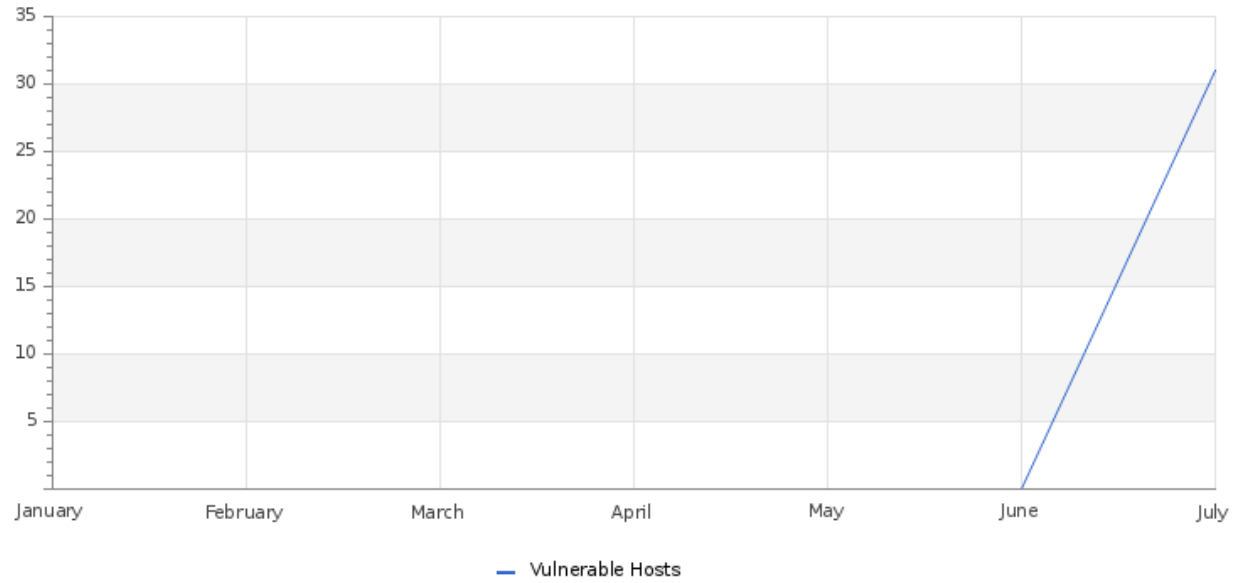

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

### Top 10 Most Common Vulnerabilities

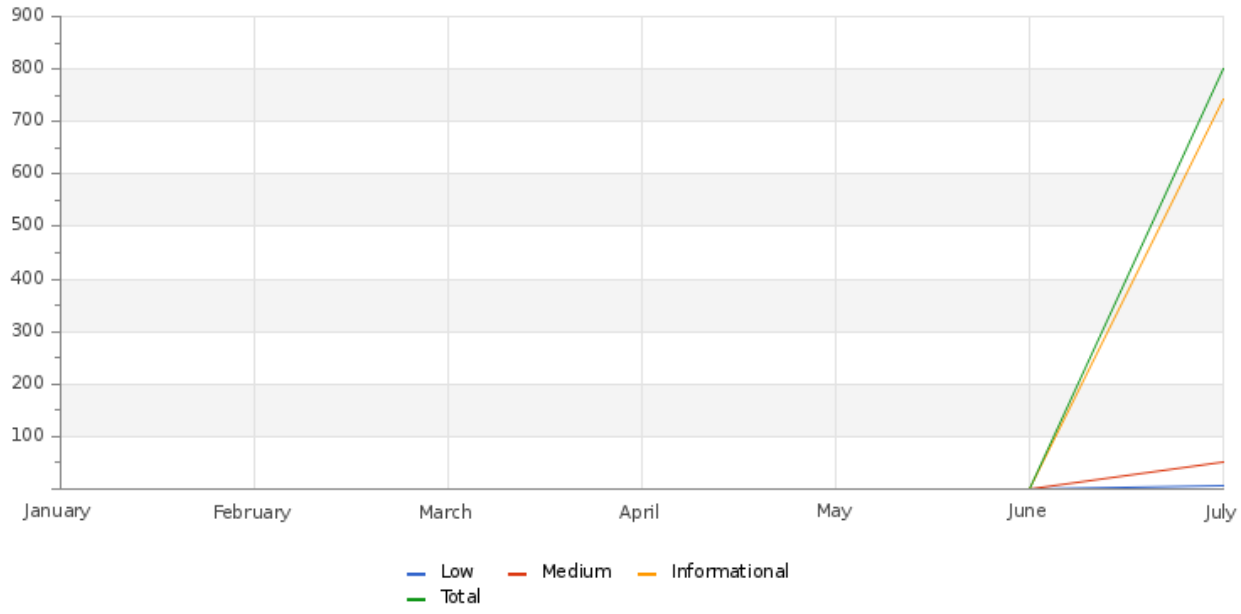
| Vulnerability |
|---|
| Web cache poisoning |
| HSTS Missing From HTTPS Server (RFC 6,797) |
| TLS Version 1.10 Deprecated Protocol |
| Open redirection (DOM-based) |
| SSL Certificate Cannot Be Trusted |
| ICMP Timestamp Request Remote Date Disclosure |
| SSL Medium Strength Cipher Suites Supported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

# History

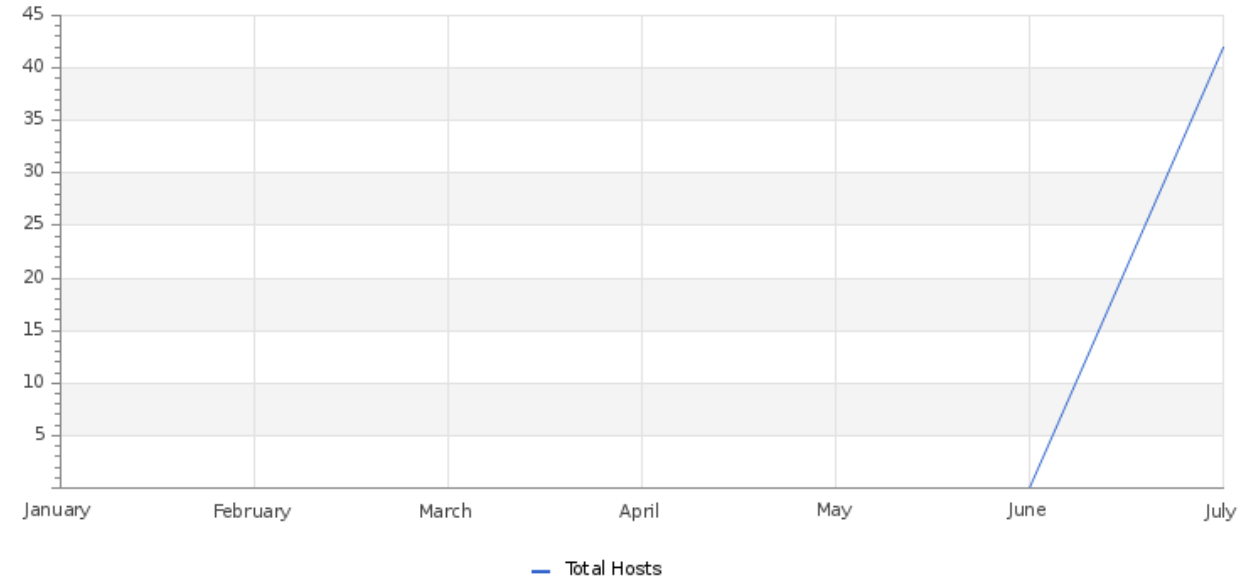
### Vulnerable Host History



## Vulnerability Severity History




## Discovered Host History



# Open Port Monitoring

# Penetration Tab


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

# Vulnerability

## MSS-BAS Email

**Cymulate Score**

**0%**

## MSS-BAS Web

**Cymulate Score**

**35%**

**Simulation Summary**

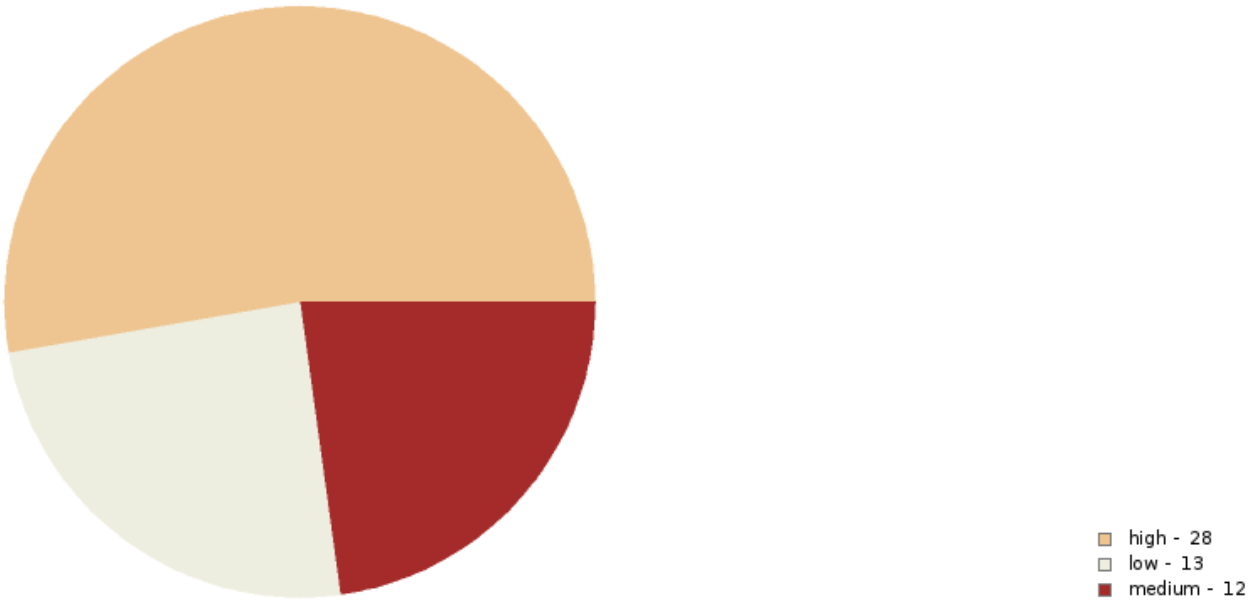
**Penetrated : 53 / Total Tests: 92**


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

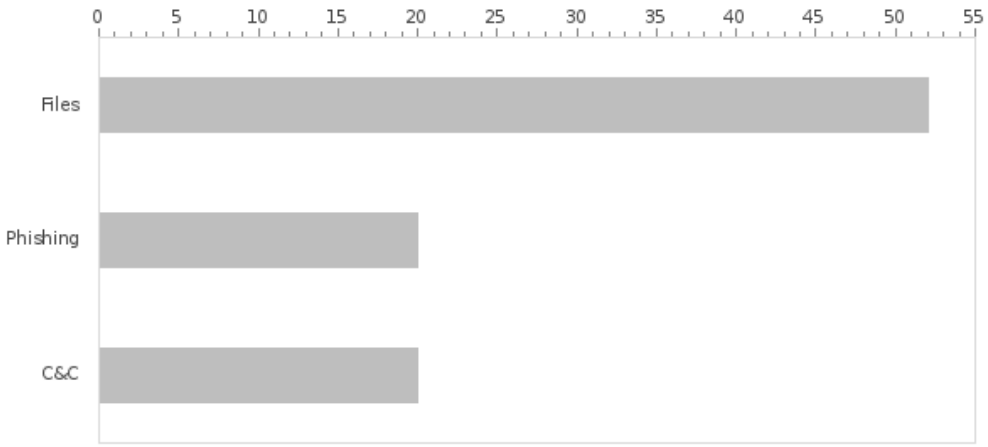
# ASM-VP REPORT

GOAA 07/05/2024

## Penetrations by Severity




## Browsing Sent






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

# ASM-VP REPORT

GOAA 07/05/2024

## Browsing Penetrated


## Percent Penetrated

**58%**

## Simulations Sent/Penetrated

| Category | Penetrated | Total |
|---|---|---|
| Files | 52 | 52 |
| Phishing | 0 | 20 |
| C&C | 1 | 20 |



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

# Security Validation

## MSS-BAS EDR

**cymulate score**

**13%**

**Simulation Summary**

**Penetrated : 3 / Sent : 27**

**Ransomware based code execution**

**Penetrated : 3 / Total Tests: 27**

**Malware based execution**

**Not detected : 0 / Total: 0**

**Trojan based code execution**

**penetrated : 0 / Total tests : 0**

**Ransomware Scenarios blocked**

**89%**

**Malware Signatures blocked**

**100%**



LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

### Trojan Scenarios blocked

**100%**

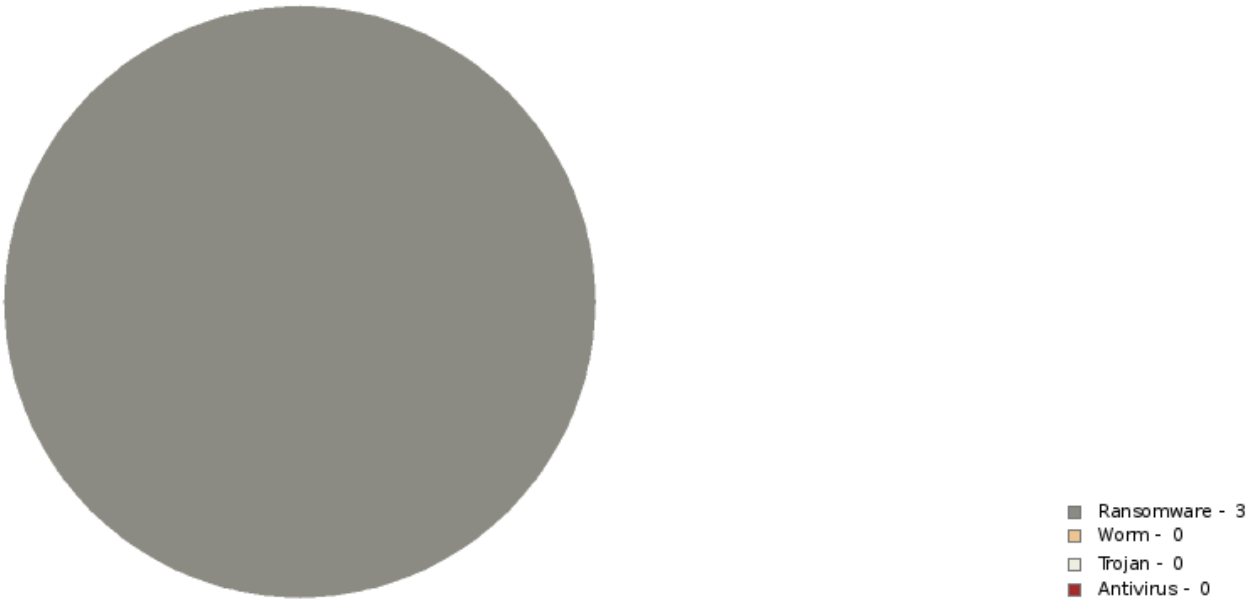
### Worm based code execution

**penetrated : 0 / Total tests : 0**

### Worm Scenarios blocked

**100%**

### Distribution Of Attack Types Penetrated




### Percent Penetrated

**11%**

TLP:AMBER

# ASM-VP REPORT

GOAA 07/05/2024

## Simulations Sent/Penetrated

| Category | Penetrated | Total |
|---|---|---|
| Ransomware | 3 | 27 |
| Worm | 0 | 0 |
| Trojan | 0 | 0 |
| Antivirus | 0 | 0 |

# MSS-BAS IMTHREAT

## Cymulate Score

**38%**

## Percent Penetrated

**34%**

## Simulation Summary

**Penetrated: 56 / Total: 165**

## Immediate Threats Campaigns

| Timestamp | Name | Attack_Payload | Attack_Vector | Target | Status |
|---|---|---|---|---|---|
| 2024-07-04 | New Ransomware Operator Volcano Demon Serving Up LukaLocker | f83abe3d9_edr717238755f1276c87b3b320d8c30421984a897099ce3741d9143906XxX37Exe.exe | Endpoint Security | IT55 | Prevented |
| 2024-07-04 | New Ransomware Operator Volcano Demon Serving Up LukaLocker | hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/new_ransomware_operator_volcano_demon_serving_up_lukalocker_46e633a0-07c9-4db4-969c-ca783331cb37/4e58629158a6c46ad420f_browsing729330030f5e0b0ef374e9bb24cd203c89ec3262669XxX35Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240704%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240704T062702Z&X-Amz-Expires=600&X-Amz-Signature=a47d9caadb947dee0c09cbbbcd57816575ac14d78af1182449faafb953ba507f&X-Amz-SignedHeaders=host&x-id=GetObject | Web Gateway | IT55 | Penetrated |



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

TLP:AMBER

# ASM-VP REPORT

GOAA 07/05/2024

| Timestamp | Name | Attack_Payload | Attack_Vector | Target | Status |
|---|---|---|---|---|---|
| 2024-07-03 | Unfurling Hemlock Threat group uses cluster bomb campaigns | 229e859dda6cc0bc99a395824f4524693bdd0292b4b9c55d06b4fa382_edr79b3ea2XxX29Exe.exe | Endpoint Security | IT55 | Prevented |
| 2024-07-03 | Unfurling Hemlock Threat group uses cluster bomb campaigns | 3_edr7b9e74da5fe5e27aaedc25e4aac7678553b6d7d89ec4d99e8b9d0627dcbdc12XxX30Exe.exe | Endpoint Security | IT55 | Prevented |
| 2024-07-03 | Unfurling Hemlock Threat group uses cluster bomb campaigns | be25926929b1aae025_edr7d7f7614dd5ad637b8fd8e139c68f4d717e3dc9913e3cfXxX49Exe.exe | Endpoint Security | IT55 | Prevented |
| 2024-07-03 | Unfurling Hemlock Threat group uses cluster bomb campaigns | 0c48529d29_edr79698341e89d6ea5f7e9211fa277e40d3f6a55a8996135944ebdadXxX37Exe.exe | Endpoint Security | IT55 | Prevented |
| 2024-07-03 | Unfurling Hemlock Threat group uses cluster bomb campaigns | 301a1c9f4e82fc8f5_edr7577ea399a2591557ff57d337472c3f8482a89c5b4105d5XxX40Exe.exe | Endpoint Security | IT55 | Prevented |
| 2024-07-03 | Unfurling Hemlock Threat group uses cluster bomb campaigns | 7f101603fbb2821504cf2c_edr71fca0450689dfcd6d1f36e57e27f0392be0f2d1ddXxX45Exe.exe | Endpoint Security | IT55 | Prevented |
| 2024-07-03 | Unfurling Hemlock Threat group uses cluster bomb campaigns | 7d18c6_edr7c13ec919f3950092319d11eda129c8498e171612e681eebf1c977493dXxX44Exe.exe | Endpoint Security | IT55 | Prevented |
| 2024-07-03 | Unfurling Hemlock Threat group uses cluster bomb campaigns | 65,923,603a6f11_edr7c7460b8cc69009105208bdfa544b90446580915db8fe127ae8XxX43Exe.exe | Endpoint Security | IT55 | Prevented |
| 2024-07-03 | Unfurling Hemlock Threat group uses cluster bomb campaigns | hxxp://77.91.68.29/fks/ | Web Gateway | IT55 | Offline/Removed |
| 2024-07-03 | Unfurling Hemlock Threat group uses cluster bomb campaigns | hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/unfurling_hemlock_threat_group_uses_cluster_bomb_campaigns_e96df6ab-765c-4746-90c1-94ebb0dfb343/fd_browsing7a9b8e52e2fbcb090d5f5046a73d6e42b421abf063083210889f3fcb47dee0XxX52Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240703%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240703T080326Z&X-Amz-Expires=600&X-Amz-Signature=7d20d49fb143be9dc0603dec2bd68e950e7f88e40bc7739251fc05096cfa0e0c&X-Amz-SignedHeaders=host&x-id=GetObject | Web Gateway | IT55 | Penetrated |



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

TLP:AMBER

# ASM-VP REPORT

GOAA 07/05/2024

| Timestamp | Name | Attack_Payload | Attack_Vector | Target | Status |
|---|---|---|---|---|---|
| 2024-07-03 | Unfurling Hemlock Threat group uses cluster bomb campaigns | hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/unfurling_hemlock_threat_group_uses_cluster_bomb_campaigns_e96df6ab-765c-4746-90c1-94ebb0dfb343/edfb43_browsing74d5c586f0690c95ff8cacb36bda6fb4743f20dda5e6f17e7e241edd47XxX51Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240703%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240703T080325Z&X-Amz-Expires=600&X-Amz-Signature=a80c4dc30fd034bb54cbbd9e4352654533f6cb3201cae425f8d9f67a073c173a&X-Amz-SignedHeaders=host&x-id=GetObject | Web Gateway | IT55 | Penetrated |
| 2024-07-03 | Unfurling Hemlock Threat group uses cluster bomb campaigns | hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/unfurling_hemlock_threat_group_uses_cluster_bomb_campaigns_e96df6ab-765c-4746-90c1-94ebb0dfb343/da4f614c983fa226d813de39093_browsing7389ae4d1e043dd86524aa7a5246fd587826bXxX50Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240703%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240703T080325Z&X-Amz-Expires=600&X-Amz-Signature=b2d5004e27ef1e35af2c176cd121b9c2a6ab939e28c5f981833c65b93072da45&X-Amz-SignedHeaders=host&x-id=GetObject | Web Gateway | IT55 | Penetrated |
| 2024-07-03 | Unfurling Hemlock Threat group uses cluster bomb campaigns | hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/unfurling_hemlock_threat_group_uses_cluster_bomb_campaigns_e96df6ab-765c-4746-90c1-94ebb0dfb343/8fe4d34a6a245c5acd3d1_browsing741213c1dd195468089b1a3fe80adfa6d8d8c94f2d8XxX47Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240703%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240703T080324Z&X-Amz-Expires=600&X-Amz-Signature=718b10ec516f45c6af33ca1970abd223ff6b6d89c4b5de72aa400cefe43aa358&X-Amz-SignedHeaders=host&x-id=GetObject | Web Gateway | IT55 | Penetrated |
| 2024-07-03 | Unfurling Hemlock Threat group uses cluster bomb campaigns | hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/unfurling_hemlock_threat_group_uses_cluster_bomb_campaigns_e96df6ab-765c-4746-90c1-94ebb0dfb343/80df101f1f93fa53b3dcbc315d3ec5d8c8330c08b5622ac320_browsing7f746d016b66dcXxX46Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240703%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240703T080324Z&X-Amz-Expires=600&X-Amz-Signature=1b5ee21aa36759ab26ec077c0586ca2303644fad1a6cbfd7532d8318ddbe6920&X-Amz-SignedHeaders=host&x-id=GetObject | Web Gateway | IT55 | Penetrated |
| 2024-07-03 | Unfurling Hemlock Threat group uses cluster bomb campaigns | hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/unfurling_hemlock_threat_group_uses_cluster_bomb_campaigns_e96df6ab-765c-4746-90c1-94ebb0dfb343/569_browsing7652d0fd5b4a05ac00f6ec028fd3dc3e34ed7b112c4b8c6048eae72a8d326XxX42Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240703%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240703T080316Z&X-Amz-Expires=600&X-Amz-Signature=ad20f79f684f5bed7147491b20c0e7fe3de262e82e33e8297bd0ea08fee040fe&X-Amz-SignedHeaders=host&x-id=GetObject | Web Gateway | IT55 | Penetrated |
| 2024-07-03 | Unfurling Hemlock Threat group uses cluster bomb campaigns | hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/unfurling_hemlock_threat_group_uses_cluster_bomb_campaigns_e96df6ab-765c-4746-90c1-94ebb0dfb343/35c55b402e_browsing770e25adf57ffbd408a428af9ce21a735474b5d94ccdd4123e68f8XxX41Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240703%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240703T080316Z&X-Amz-Expires=600&X-Amz-Signature=a1367677df2f872fc8710301d3dd37b6451f41cd600dd0e6e8bff777f87d38f4&X-Amz-SignedHeaders=ho st&x-id=GetObject | Web Gateway | IT55 | Penetrated |
| 2024-07-03 | Unfurling Hemlock Threat group uses cluster bomb campaigns | hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/unfurling_hemlock_threat_group_uses_cluster_bomb_campaigns_e96df6ab-765c-4746-90c1-94ebb0dfb343/1f224093b955_browsing7dd73caaf1c6a823028c286ddd3414bceb0860e0fe084fb8c2abXxX39Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240703%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240703T080315Z&X-Amz-Expires=600&X-Amz-Signature=7ad31bbbf45836a838102a8b72d8c6e94875c0f59ee715fa299ab2bc42e7ee50&X-Amz-SignedHeaders=host&x-id=GetObject | Web Gateway | IT55 | Penetrated |
| 2024-07-03 | Unfurling Hemlock Threat group uses cluster bomb campaigns | hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/unfurling_hemlock_threat_group_uses_cluster_bomb_campaigns_e96df6ab-765c-4746-90c1-94ebb0dfb343/0ef_browsing7459cebfe9bd9102c5eccc16eedddec5931e69bf705aa44aa3c7af584f209XxX38Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240703%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240703T080313Z&X-Amz-Expires=600&X-Amz-Signature=a944d69b50324a75af2cf082efc86383e77b0393384c31100456381ca1bd7a00&X-Amz-SignedHeaders=host&x-id=GetObject | Web Gateway | IT55 | Penetrated |
| 2024-07-03 | Unfurling Hemlock Threat group uses cluster bomb campaigns | hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/unfurling_hemlock_threat_group_uses_cluster_bomb_campaigns_e96df6ab-765c-4746-90c1-94ebb0dfb343/94115d0eae0422b6605f0f25841c29b_browsing7cc6c029472a983b21d1cedcd7fdcd647XxX35Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240703%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240703T080312Z&X-Amz-Expires=600&X-Amz-Signature=1f3138feda766329c845d8f8f5228928b3fc7372682708d399c3e0a21c952908&X-Amz-SignedHeaders=host&x-id=GetObject | Web Gateway | IT55 | Penetrated |



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

TLP:AMBER

# ASM-VP REPORT

GOAA 07/05/2024

| Timestamp | Name | Attack_Payload | Attack_Vector | Target | Status |
|---|---|---|---|---|---|
| 2024-07-03 | Supply Chain Compromise Leads to Trojanized Installers | 2eae4f06f2c3_edr76c6206c632ac93f4e8c4b3e0e63eca3118e883f8ac479b2f852XxX10Exe.exe | Endpoint Security | IT55 | Prevented |
| 2024-07-03 | Supply Chain Compromise Leads to Trojanized Installers | fdc84cb0845f8_edr7a39b29027d6433f4a1bbd8c5b808280235cf867a6b0b7a91ebXxX28Exe.exe | Endpoint Security | IT55 | Prevented |
| 2024-07-03 | Supply Chain Compromise Leads to Trojanized Installers | bfa99c41aecc814de5b9eb839_edr7a27e516c8b0a4e31edd9ed1304da6c996b4aaaXxX23Exe.exe | Endpoint Security | IT55 | Prevented |
| 2024-07-03 | Supply Chain Compromise Leads to Trojanized Installers | de4e032880_edr71cdebe5c26913888b135fb2424132856cc892baea9792d6c66249XxX26Exe.exe | Endpoint Security | IT55 | Prevented |
| 2024-07-03 | Supply Chain Compromise Leads to Trojanized Installers | hxxp://170.130.34.114 | Web Gateway | IT55 | Offline/Removed |
| 2024-07-03 | Supply Chain Compromise Leads to Trojanized Installers | hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/supply_chain_compromise_leads_to_trojanized_installers_d393005f-03bd-4d35-af94-aff4991999c4/70bce9c228aacbdadaaf18596c0eb308c102382d04632b01b826e9db96210093_browsingXxX21Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240703%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240703T080038Z&X-Amz-Expires=600&X-Amz-Signature=ed504db716db6dab88227a8aac4b322dd251fb49d3e058aa98406d83b281397e&X-Amz-SignedHeaders=host&x-id=GetObject | Web Gateway | IT55 | Penetrated |
| 2024-07-03 | Supply Chain Compromise Leads to Trojanized Installers | hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/supply_chain_compromise_leads_to_trojanized_installers_d393005f-03bd-4d35-af94-aff4991999c4/6f49_browsing756749d175058f15d5f3c80c8a7d46e80ec3e5eb9fb31f4346abdb72a0e7XxX20Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240703%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240703T080033Z&X-Amz-Expires=600&X-Amz-Signature=e3e31636fc1f3bb1088f07e81b6e5228437d97bb9610ef4e9f8acf370ec6dc49&X-Amz-SignedHeaders=host&x-id=GetObject | Web Gateway | IT55 | Penetrated |
| 2024-07-03 | Supply Chain Compromise Leads to Trojanized Installers | hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/supply_chain_compromise_leads_to_trojanized_installers_d393005f-03bd-4d35-af94-aff4991999c4/4df9b_browsing7da9590990230ed2ab9b4c3d399cf770ed7f6c36a8a10285375fd5a292fXxX18Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240703%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240703T080030Z&X-Amz-Expires=600&X-Amz-Signature=06d39cde2a032c03600ac68ffafbfd297d0b67ffab12e17225551abe4ffbae33&X-Amz-SignedHeaders=host&x-id=GetObject | Web Gateway | IT55 | Penetrated |
| 2024-07-04 | RisePro Information Stealer | 222,932_edr7fa653ffd07f11773ee22eb00e580b6824ce122a1e788f19859aa9dca2XxX1Exe.exe | Endpoint Security | IT55 | Prevented |
| 2024-07-04 | RisePro Information Stealer | 7_edr7e97faca59d8de34ddc7272791efac41da9ff5b7b175a99e09a255e2701d725XxX7Exe.exe | Endpoint Security | IT55 | Prevented |
| 2024-07-04 | RisePro Information Stealer | 30baf54d503_edr79893b23b24203611da331d436dfc35f2d0a805bac4da0d310489XxX9Exe.exe | Endpoint Security | IT55 | Prevented |
| 2024-07-04 | RisePro Information Stealer | 6b82e6f228cbb8143b68e1_edr739f3d083cf6ab0ba9c202ce1ec769bb12c9030619XxX11Exe.exe | Endpoint Security | IT55 | Prevented |
| 2024-07-04 | RisePro Information Stealer | 0_edr78b3f37483cfc697fbd67120311e6109843804f5cae9c46f04fa1b51ba7120aXxX20Exe.exe | Endpoint Security | IT55 | Prevented |
| 2024-07-04 | RisePro Information Stealer | ce930238a02a55d_edr7b6f13fdf9b3306de61c5c25513ed396c7e9a8dbd4c45dbd9XxX17Exe.exe | Endpoint Security | IT55 | Prevented |



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

TLP:AMBER

GLESEC
COMPLETELY PERCEPTI

# ASM-VP REPORT

GOAA 07/05/2024

| Timestamp | Name | Attack_Payload | Attack_Vector | Target | Status |
|---|---|---|---|---|---|
| 2024-07-04 | RisePro Information Stealer | d435d_edr7cf9077533a7c23129a8d7462e7596505e3990664dd5888fce40652bb14XxX21Exe.exe | Endpoint Security | IT55 | Prevented |
| 2024-07-04 | RisePro Information Stealer | hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/risepro_information_stealer_dbcc8998-07d5-4a55-adfd-08a15abf9712/f8_browsing7dd2b6a63e850b6c2128ec139c6334b572b1c80698fcc30de6f39ffc788f4fXxX25Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240704%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240704T075926Z&X-Amz-Expires=600&X-Amz-Signature=bd508d50aea0230e52ff464e22d4905e18843428e765915fceda2983ef565e22&X-Amz-SignedHeaders=host&x-id=GetObject | Web Gateway | IT55 | Penetrated |
| 2024-07-04 | RisePro Information Stealer | hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/risepro_information_stealer_dbcc8998-07d5-4a55-adfd-08a15abf9712/cb21be43_browsing7c800875400a94b2442bbe02ccaf31ee49e1f440aac378fc2b0b756dXxX24Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240704%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240704T075925Z&X-Amz-Expires=600&X-Amz-Signature=7e55cf41bdf091da463307e3d9ba9db27a8d77441f16ba24c41325195a24be7b&X-Amz-SignedHeaders=host&x-id=GetObject | Web Gateway | IT55 | Penetrated |
| 2024-07-04 | RisePro Information Stealer | hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/risepro_information_stealer_dbcc8998-07d5-4a55-adfd-08a15abf9712/0d5bb8b8da18abd1f3934103c501abf9b9cd3a6e1656853359a568dca3229_browsing765XxX23Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240704%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240704T075924Z&X-Amz-Expires=600&X-Amz-Signature=c3c7b9fa4ffb8d50510621b4af91344f3c87224c072ab8ca43d5f293754b86bf&X-Amz-SignedHeaders=host&x-id=GetObject | Web Gateway | IT55 | Penetrated |
| 2024-07-04 | RisePro Information Stealer | hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/risepro_information_stealer_dbcc8998-07d5-4a55-adfd-08a15abf9712/d_browsing7c3c01d62fb59e186b2256894fb089c01e1aeda5dbd86a3004f1857a13313adXxX22Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240704%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240704T075923Z&X-Amz-Expires=600&X-Amz-Signature=5c8a55070b5bd4517e13062cd7f8c24d758065df665a47c4cfad2f8f34ab4888&X-Amz-SignedHeaders=host&x-id=GetObject | Web Gateway | IT55 | Penetrated |
| 2024-07-04 | RisePro Information Stealer | hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/risepro_information_stealer_dbcc8998-07d5-4a55-adfd-08a15abf9712/d2cbb_browsing7a5ef2ecdf7c6f8c965df5886a18ea0e630009cdedb3692ed1b8c77b487XxX19Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240704%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240704T075913Z&X-Amz-Expires=600&X-Amz-Signature=0bd7637d5be3ad90cc4dc8d921b05f73743b0a5d902a2e45e6e7309de60a9a80&X-Amz-SignedHeaders=host&x-id=GetObject | Web Gateway | IT55 | Penetrated |
| 2024-07-04 | RisePro Information Stealer | hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/risepro_information_stealer_dbcc8998-07d5-4a55-adfd-08a15abf9712/19c98cba0d803_browsing7a36b00d2c11cc24d25e1f388ba5093a4b6e9017508371fb34bXxX18Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240704%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240704T075912Z&X-Amz-Expires=600&X-Amz-Signature=4465e62007d99732fb94aa74fceb3c2433bcd21a494aedf60c1ba8f8c836e600&X-Amz-SignedHeaders=host&x-id=GetObject | Web Gateway | IT55 | Penetrated |
| 2024-07-04 | RisePro Information Stealer | hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/risepro_information_stealer_dbcc8998-07d5-4a55-adfd-08a15abf9712/6113bc3f3f9_browsing72393acff5022f5ba95fb96c3d9038386ada49ccf244fa5f885faXxX16Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240704%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240704T075909Z&X-Amz-Expires=600&X-Amz-Signature=0caf3ffa4bebbca769a111aafbb8e129fe3fbf6aeb32d93bb4ebf97bec34bdce&X-Amz-SignedHeaders=host&x-id=GetObject | Web Gateway | IT55 | Penetrated |
| 2024-07-04 | RisePro Information Stealer | hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/risepro_information_stealer_dbcc8998-07d5-4a55-adfd-08a15abf9712/c_browsing7a40fb4aa017a0d17b535c1857d51f95b7ed8684a1ea860294bf5d8976678 39XxX15Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240704%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240704T075909Z&X-Amz-Expires=600&X-Amz-Signature=12471175f6b4c1e18e7550ba46f28c109b19fa108dcc61d40c0428565c02077e&X-Amz-SignedHeaders=host&x-id=GetObject | Web Gateway | IT55 | Penetrated |
| 2024-07-04 | RisePro Information Stealer | hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/risepro_information_stealer_dbcc8998-07d5-4a55-adfd-08a15abf9712/15dfbd2df433c9_browsing725239d6602bdfc56d00db62f88a1769a534d98cad50536c27XxX14Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240704%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240704T075907Z&X-Amz-Expires=600&X-Amz-Signature=91ebffe27af59d6b039e7f25e5dffe80142ba96cd21d367730b702d01681d4fc&X-Amz-SignedHeaders=host&x-id=GetObject | Web Gateway | IT55 | Penetrated |
| 2024-07-04 | RisePro Information Stealer | hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/risepro_information_stealer_dbcc8998-07d5-4a55-adfd-08a15abf9712/9d540839e_browsing75daf4f31eb36271fef6eb16a913446384d07e4d8dbb2602f18bf0fXxX13Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240704%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240704T075906Z&X-Amz-Expires=600&X-Amz-Signature=dfc69e1808ef3f47e5188d790b05ff4daa2079b97fdabe7256535afb1fdc6496&X-Amz-SignedHeaders=host&x-id=GetObject | Web Gateway | IT55 | Penetrated |



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

TLP:AMBER

GLESEC
COMPLETELY PERCEPTI

# ASM-VP REPORT

GOAA 07/05/2024

| Timestamp | Name | Attack_Payload | Attack_Vector | Target | Status |
|---|---|---|---|---|---|
| 2024-07-04 | RisePro Information Stealer | hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/risepro_information_stealer_dbcc8998-07d5-4a55-adfd-08a15abf9712/5_browsing719a862d5a32ec56328f8e066a83b6b0577a6965074ca671d0cecce681d5f79XxX12Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240704%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240704T075905Z&X-Amz-Expires=600&X-Amz-Signature=3e4888ad201a66cdfb524d2667ecbe932cbc760472217aeedbe8f2d651623353&X-Amz-SignedHeaders=host&x-id=GetObject | Web Gateway | IT55 | Penetrated |
| 2024-07-04 | RisePro Information Stealer | hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/risepro_information_stealer_dbcc8998-07d5-4a55-adfd-08a15abf9712/c48eb226b641b382fd4155f10c96aacc585c6e65814865cd_browsing762e88b8a5cffd14XxX10Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240704%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240704T075857Z&X-Amz-Expires=600&X-Amz-Signature=f3f73217258e77489178ec10878c25fc2b138c487bf1948cdb04586895ceb730&X-Amz-SignedHeaders=host&x-id=GetObject | Web Gateway | IT55 | Penetrated |
| 2024-07-04 | RisePro Information Stealer | hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/risepro_information_stealer_dbcc8998-07d5-4a55-adfd-08a15abf9712/a_browsing78513831b47f4b35ee9063aa167bf5d05c61559b2ac7f8fb93fa966a36e34d2XxX8Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240704%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240704T075855Z&X-Amz-Expires=600&X-Amz-Signature=dac3ef3b62bb77dd71d1435a2c6c4838ad5be99308461b3756f9d842ea6b84de&X-Amz-SignedHeaders=host&x-id=GetObject | Web Gateway | IT55 | Penetrated |
| 2024-07-04 | RisePro Information Stealer | hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/risepro_information_stealer_dbcc8998-07d5-4a55-adfd-08a15abf9712/b4ad80860c_browsing773c79c946c3a4df13e534153bd17ceebad6acedac3156dfe0144cXxX6Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240704%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240704T075853Z&X-Amz-Expires=600&X-Amz-Signature=35805a39893d475abbe9119a31dea306dca435dcce3233d4ad7149eab38da583&X-Amz-SignedHeaders=host&x-id=GetObject | Web Gateway | IT55 | Penetrated |
| 2024-07-04 | RisePro Information Stealer | hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/risepro_information_stealer_dbcc8998-07d5-4a55-adfd-08a15abf9712/56108c_browsing707fcaf87b2220c081db115171ff35811946b3ad2d76105715e8530fbeXxX5Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240704%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240704T075851Z&X-Amz-Expires=600&X-Amz-Signature=174ce2f580799be519c0a488b58d7a738dde9b6e3da771000878c67a7718e248&X-Amz-SignedHeaders=host&x-id=GetObject | Web Gateway | IT55 | Penetrated |
| 2024-07-04 | RisePro Information Stealer | hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/risepro_information_stealer_dbcc8998-07d5-4a55-adfd-08a15abf9712/4f0e839393df_browsing72db99a05ade0848979ff375399b104e59a7cc3847d746c17e5cXxX4Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240704%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240704T075850Z&X-Amz-Expires=600&X-Amz-Signature=b3140111129385e27cebedee91123d9356d186374da6a57d4a5e2d30a956bc97&X-Amz-SignedHeaders=host&x-id=GetObject | Web Gateway | IT55 | Penetrated |
| 2024-07-04 | RisePro Information Stealer | hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/risepro_information_stealer_dbcc8998-07d5-4a55-adfd-08a15abf9712/a36d5e_browsing790ca17fb6f70884942d868d29c6854054f2db79ed8f4e2d0d16ef1647XxX3Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240704%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240704T075850Z&X-Amz-Expires=600&X-Amz-Signature=3bc1e1d7ee34448d86037231660b0e75e9b6281f520679e2aeda55a92902bf2a&X-Amz-SignedHeaders=host&x-id=GetObject | Web Gateway | IT55 | Penetrated |
| 2024-07-04 | RisePro Information Stealer | hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/risepro_information_stealer_dbcc8998-07d5-4a55-adfd-08a15abf9712/5e1a1b2e2c20bc50b54e02393fa6f26a2b8c2f4d8_browsing7f2abdecaca73472b5c5dbaXxX2Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240704%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240704T075849Z&X-Amz-Expires=600&X-Amz-Signature=7899a8fc3ab95b0541e3d11a5111c445b4cbb37e9ae3ed3baebc7695ce1507d8&X-Amz-SignedHeaders=host&x-id=GetObject | Web Gateway | IT55 | Penetrated |
| 2024-07-04 | RisePro Information Stealer | 5e1a1b2e2c20bc50b54e02393fa6f26a2b8c2f4d8_edr7f2abdecaca73472b5c5dbaXxX2Exe.exe | Endpoint Security | IT55 | Prevented |
| 2024-07-04 | RisePro Information Stealer | 4f0e839393df_edr72db99a05ade0848979ff375399b104e59a7cc3847d746c17e5cXxX4Exe.exe | Endpoint Security | IT55 | Prevented |
| 2024-07-04 | RisePro Information Stealer | a36d5e_edr790ca17fb6f70884942d868d29c6854054f2db79ed8f4e2d0d16ef1647XxX3Exe.exe | Endpoint Security | IT55 | Prevented |
| 2024-07-04 | RisePro Information Stealer | 56,108c_edr707fcaf87b2220c081db115171ff35811946b3ad2d76105715e8530fbeXxX5Exe.exe | Endpoint Security | IT55 | Prevented |
| 2024-07-04 | RisePro Information Stealer | a_edr78513831b47f4b35ee9063aa167bf5d05c61559b2ac7f8fb93fa966a36e34d2XxX8Exe.exe | Endpoint Security | IT55 | Prevented |



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

TLP:AMBER

GLESEC
COMPLETELY PERCEPTI

# ASM-VP REPORT

GOAA 07/05/2024

| Timestamp | Name | Attack_Payload | Attack_Vector | Target | Status |
|---|---|---|---|---|---|
| 2024-07-04 | RisePro Information Stealer | b4ad80860c_edr773c79c946c3a4df13e534153bd17ceebad6acedac3156dfe0144cXxX6Exe.exe | Endpoint Security | IT55 | Prevented |
| 2024-07-04 | RisePro Information Stealer | 5_edr719a862d5a32ec56328f8e066a83b6b0577a6965074ca671d0cecce681d5f79XxX12Exe.exe | Endpoint Security | IT55 | Prevented |
| 2024-07-04 | RisePro Information Stealer | c48eb226b641b382fd4155f10c96aacc585c6e65814865cd_edr762e88b8a5cffd14XxX10Exe.exe | Endpoint Security | IT55 | Prevented |
| 2024-07-04 | RisePro Information Stealer | c_edr7a40fb4aa017a0d17b535c1857d51f95b7ed8684a1ea860294bf5d897667839XxX15Exe.exe | Endpoint Security | IT55 | Prevented |
| 2024-07-04 | RisePro Information Stealer | 9d540839e_edr75daf4f31eb36271fef6eb16a913446384d07e4d8dbb2602f18bf0fXxX13Exe.exe | Endpoint Security | IT55 | Prevented |
| 2024-07-04 | RisePro Information Stealer | 15dfbd2df433c9_edr725239d6602bdfc56d00db62f88a1769a534d98cad50536c27XxX14Exe.exe | Endpoint Security | IT55 | Prevented |
| 2024-07-04 | RisePro Information Stealer | cb21be43_edr7c800875400a94b2442bbe02ccaf31ee49e1f440aac378fc2b0b756dXxX24Exe.exe | Endpoint Security | IT55 | Prevented |
| 2024-07-04 | RisePro Information Stealer | d_edr7c3c01d62fb59e186b2256894fb089c01e1aeda5dbd86a3004f1857a13313adXxX22Exe.exe | Endpoint Security | IT55 | Prevented |
| 2024-07-04 | RisePro Information Stealer | 0d5bb8b8da18abd1f3934103c501abf9b9cd3a6e1656853359a568dca3229_edr765XxX23Exe.exe | Endpoint Security | IT55 | Prevented |
| 2024-07-04 | RisePro Information Stealer | 6,113bc3f3f9_edr72393acff5022f5ba95fb96c3d9038386ada49ccf244fa5f885faXxX16Exe.exe | Endpoint Security | IT55 | Prevented |
| 2024-07-04 | RisePro Information Stealer | 19c98cba0d803_edr7a36b00d2c11cc24d25e1f388ba5093a4b6e9017508371fb34bXxX18Exe.exe | Endpoint Security | IT55 | Prevented |
| 2024-07-04 | RisePro Information Stealer | f8_edr7dd2b6a63e850b6c2128ec139c6334b572b1c80698fcc30de6f39ffc788f4fXxX25Exe.exe | Endpoint Security | IT55 | Prevented |
| 2024-07-04 | RisePro Information Stealer | d2cbb_edr7a5ef2ecdf7c6f8c965df5886a18ea0e630009cdedb3692ed1b8c77b487XxX19Exe.exe | Endpoint Security | IT55 | Prevented |
| 2024-07-04 | RisePro Information Stealer | hxxp://94.156.8.188 | Web Gateway | IT55 | Offline/Removed |
| 2024-07-04 | RisePro Information Stealer | hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/risepro_information_stealer_dbcc8998-07d5-4a55-adfd-08a15abf9712/d435d_browsing7cf9077533a7c23129a8d7462e7596505e3990664dd5888fce40652bb14XxX21Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240704%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240704T075921Z&X-Amz-Expires=600&X-Amz-Signature=4c580ee6f1dbeccc160654b67ce410887f0dac85a66ceefca2120b12e1d07f77&X-Amz-SignedHeaders=host&x-id=GetObject | Web Gateway | IT55 | Penetrated |
| 2024-07-04 | RisePro Information Stealer | hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/risepro_information_stealer_dbcc8998-07d5-4a55-adfd-08a15abf9712/0_browsing78b3f37483cfc697fbd67120311e6109843804f5cae9c46f04fa1b51ba7120aXxX20Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240704%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240704T075914Z&X-Amz-Expires=600&X-Amz-Signature=47384eb084998c64a8e48837a28f28093c2d5deb966307f7b7cc5c62a98fa735&X-Amz-SignedHeaders=host&x-id=GetObject | Web Gateway | IT55 | Penetrated |
| 2024-07-04 | RisePro Information Stealer | hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/risepro_information_stealer_dbcc8998-07d5-4a55-adfd-08a15abf9712/ce930238a02a55d_browsing7b6f13fdf9b3306de61c5c25513ed396c7e9a8dbd4c45dbd9XxX17Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240704%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240704T075910Z&X-Amz-Expires=600&X-Amz-Signature=f4e35be937415c396ed18b2b6448be608acb304b80cf763867fe05f90ba2e530&X-Amz-SignedHeaders=host&x-id=GetObject | Web Gateway | IT55 | Penetrated |
| 2024-07-04 | RisePro Information Stealer | hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/risepro_information_stealer_dbcc8998-07d5-4a55-adfd-08a15abf9712/6b82e6f228cbb8143b68e1_browsing739f3d083cf6ab0ba9c202ce1ec769bb12c9030619XxX11Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240704%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240704T075903Z&X-Amz-Expires=600&X-Amz-Signature=cb9183d7b8e22cb85087f01067d170a62c74760822feefa8fd23db0a72b86108&X-Amz-SignedHeaders=host&x-id=GetObject | Web Gateway | IT55 | Penetrated |



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

TLP:AMBER

# ASM-VP REPORT

GOAA 07/05/2024

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

TLP:AMBER

GLESEC
COMPLETELY PERCEPTI

# ASM-VP REPORT

GOAA 07/05/2024

| Timestamp | Name | Attack_Payload | Attack_Vector | Target | Status |
|---|---|---|---|---|---|
| 2024-07-03 | Unfurling Hemlock Threat group uses cluster bomb campaigns | da4f614c983fa226d813de39093_edr7389ae4d1e043dd86524aa7a5246fd587826bXxX50Exe.exe | Endpoint Security | IT55 | Prevented |
| 2024-07-03 | Unfurling Hemlock Threat group uses cluster bomb campaigns | 569_edr7652d0fd5b4a05ac00f6ec028fd3dc3e34ed7b112c4b8c6048eae72a8d326XxX42Exe.exe | Endpoint Security | IT55 | Prevented |
| 2024-07-03 | Unfurling Hemlock Threat group uses cluster bomb campaigns | edfb43_edr74d5c586f0690c95ff8cacb36bda6fb4743f20dda5e6f17e7e241edd47XxX51Exe.exe | Endpoint Security | IT55 | Prevented |
| 2024-07-03 | Unfurling Hemlock Threat group uses cluster bomb campaigns | 80df101f1f93fa53b3dcbc315d3ec5d8c8330c08b5622ac320_edr7f746d016b66dcXxX46Exe.exe | Endpoint Security | IT55 | Prevented |
| 2024-07-03 | Unfurling Hemlock Threat group uses cluster bomb campaigns | fd_edr7a9b8e52e2fbcb090d5f5046a73d6e42b421abf063083210889f3fcb47dee0XxX52Exe.exe | Endpoint Security | IT55 | Prevented |
| 2024-07-03 | Unfurling Hemlock Threat group uses cluster bomb campaigns | hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/unfurling_hemlock_threat_group_uses_cluster_bomb_campaigns_e96df6ab-765c-4746-90c1-94ebb0dfb343/be25926929b1aae025_browsing7d7f7614dd5ad637b8fd8e139c68f4d717e3dc9913e3cfXxX49Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240703%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240703T080324Z&X-Amz-Expires=600&X-Amz-Signature=857d02be08d6ab1942d9ced80a5d5bde6334fc47054c570a3cb306d5760d7e30&X-Amz-SignedHeaders=host&x-id=GetObject | Web Gateway | IT55 | Penetrated |
| 2024-07-03 | Unfurling Hemlock Threat group uses cluster bomb campaigns | hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/unfurling_hemlock_threat_group_uses_cluster_bomb_campaigns_e96df6ab-765c-4746-90c1-94ebb0dfb343/7f101603fbb2821504cf2c_browsing71fca0450689dfcd6d1f36e57e27f0392be0f2d1ddXxX45Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240703%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240703T080323Z&X-Amz-Expires=600&X-Amz-Signature=fd2da5638045c4e87a6299cd3dd8dd50e9b35cc7784a594fb05bfcec535049d5&X-Amz-SignedHeaders=host&x-id=GetObject | Web Gateway | IT55 | Penetrated |
| 2024-07-03 | Unfurling Hemlock Threat group uses cluster bomb campaigns | hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/unfurling_hemlock_threat_group_uses_cluster_bomb_campaigns_e96df6ab-765c-4746-90c1-94ebb0dfb343/7d18c6_browsing7c13ec919f3950092319d11eda129c8498e171612e681eebf1c977493dXxX44Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240703%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240703T080323Z&X-Amz-Expires=600&X-Amz-Signature=ed91a80bc2fa44666f16a042ac81dbb5c5648580a2a7762dc0bf3fec2f3ea713&X-Amz-SignedHeaders=host&x-id=GetObject | Web Gateway | IT55 | Penetrated |
| 2024-07-03 | Unfurling Hemlock Threat group uses cluster bomb campaigns | hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/unfurling_hemlock_threat_group_uses_cluster_bomb_campaigns_e96df6ab-765c-4746-90c1-94ebb0dfb343/65923603a6f11_browsing7c7460b8cc69009105208bdfa544b90446580915db8fe127ae8XxX43Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240703%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240703T080317Z&X-Amz-Expires=600&X-Amz-Signature=5c09b307213be76a0f00e4bc07868310957a4f0018e206b16b5aebf11ece7d24&X-Amz-SignedHeaders=host&x-id=GetObject | Web Gateway | IT55 | Penetrated |
| 2024-07-03 | Unfurling Hemlock Threat group uses cluster bomb campaigns | hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/unfurling_hemlock_threat_group_uses_cluster_bomb_campaigns_e96df6ab-765c-4746-90c1-94ebb0dfb343/301a1c9f4e82fc8f5_browsing7577ea399a2591557ff57d337472c3f8482a89c5b4105d5XxX40Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240703%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240703T080315Z&X-Amz-Expires=600&X-Amz-Signature=5bcb76fe6143a118060fe0fbc69cf6da7f1f861a78d444767a5d0090de9608ba&X-Amz-SignedHeaders=host&x-id=GetObject | Web Gateway | IT55 | Penetrated |

# ASM-VP REPORT

GOAA 07/05/2024

| Timestamp | Name | Attack_Payload | Attack_Vector | Target | Status |
|---|---|---|---|---|---|
| 2024-07-03 | Unfurling Hemlock Threat group uses cluster bomb campaigns | hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/unfurling_hemlock_threat_group_uses_cluster_bomb_campaigns_e96df6ab-765c-4746-90c1-94ebb0dfb343/0c48529d29_browsing79698341e89d6ea5f7e9211fa277e40d3f6a55a8996135944ebdadXxX37Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240703%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240703T080313Z&X-Amz-Expires=600&X-Amz-Signature=2f4d41832318ea79ce33ad3bfc294eb60c9e5c7dd0cdea0fb46b7ec1b092df7b&X-Amz-SignedHeaders=host&x-id=GetObject | Web Gateway | IT55 | Penetrated |
| 2024-07-03 | Unfurling Hemlock Threat group uses cluster bomb campaigns | hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/unfurling_hemlock_threat_group_uses_cluster_bomb_campaigns_e96df6ab-765c-4746-90c1-94ebb0dfb343/3_browsing7b9e74da5fe5e27aaedc25e4aac7678553b6d7d89ec4d99e8b9d0627dcbdc12XxX30Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240703%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240703T080311Z&X-Amz-Expires=600&X-Amz-Signature=6ab9ff6d160413d78e762c5e64dc7fa071f8e089334fc3ef38bbbb54b2ea392d&X-Amz-SignedHeaders=host&x-id=GetObject | Web Gateway | IT55 | Penetrated |
| 2024-07-03 | Unfurling Hemlock Threat group uses cluster bomb campaigns | hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/unfurling_hemlock_threat_group_uses_cluster_bomb_campaigns_e96df6ab-765c-4746-90c1-94ebb0dfb343/229e859dda6cc0bc99a395824f4524693bdd0292b4b9c55d06b4fa382_browsing79b3ea2XxX29Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240703%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240703T080309Z&X-Amz-Expires=600&X-Amz-Signature=fa1a1e05f9641784812c666951e5e188366b77fb5d9b5cc5198a5c96866f0c08&X-Amz-SignedHeaders=host&x-id=GetObject | Web Gateway | IT55 | Penetrated |
| 2024-07-03 | Supply Chain Compromise Leads to Trojanized Installers | 4df9b_edr7da9590990230ed2ab9b4c3d399cf770ed7f6c36a8a10285375fd5a292fXxX18Exe.exe | Endpoint Security | IT55 | Prevented |
| 2024-07-03 | Supply Chain Compromise Leads to Trojanized Installers | 6f49_edr756749d175058f15d5f3c80c8a7d46e80ec3e5eb9fb31f4346abdb72a0e7XxX20Exe.exe | Endpoint Security | IT55 | Prevented |
| 2024-07-03 | Supply Chain Compromise Leads to Trojanized Installers | 70bce9c228aacbdadaaf18596c0eb308c102382d04632b01b826e9db96210093_edrXxX21Exe.exe | Endpoint Security | IT55 | Prevented |
| 2024-07-03 | Supply Chain Compromise Leads to Trojanized Installers | hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/supply_chain_compromise_leads_to_trojanized_installers_d393005f-03bd-4d35-af94-aff4991999c4/fdc84cb0845f8_browsing7a39b29027d6433f4a1bbd8c5b808280235cf867a6b0b7a91ebXxX28Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240703%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240703T080043Z&X-Amz-Expires=600&X-Amz-Signature=c8c87a80e65f43c4513c1f406269a6ee0c8069c9a045e6159e3379bfa555f0ae&X-Amz-SignedHeaders=host&x-id=GetObject | Web Gateway | IT55 | Penetrated |
| 2024-07-03 | Supply Chain Compromise Leads to Trojanized Installers | hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/supply_chain_compromise_leads_to_trojanized_installers_d393005f-03bd-4d35-af94-aff4991999c4/de4e032880_browsing71cdebe5c26913888b135fb2424132856cc892baea9792d6c66249XxX26Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240703%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240703T080042Z&X-Amz-Expires=600&X-Amz-Signature=f578869f64bbf06fa282edc89864c442cd3f0d9f07b3a64d8d6a412eab53d56c&X-Amz-SignedHeaders=host&x-id=GetObject | Web Gateway | IT55 | Penetrated |
| 2024-07-03 | Supply Chain Compromise Leads to Trojanized Installers | hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/supply_chain_compromise_leads_to_trojanized_installers_d393005f-03bd-4d35-af94-aff4991999c4/bfa99c41aecc814de5b9eb839_browsing7a27e516c8b0a4e31edd9ed1304da6c996b4aaaXxX23Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240703%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240703T080038Z&X-Amz-Expires=600&X-Amz-Signature=5cb70b37a29b38fbbf0d9a9fc9793ae18469c3e2dd887de29e8b900c22e6165e&X-Amz-SignedHeaders=host&x-id=GetObject | Web Gateway | IT55 | Penetrated |
| 2024-07-03 | Supply Chain Compromise Leads to Trojanized Installers | hxxps://cym-files-download.s3.eu-west-1.amazonaws.com/hotfiles/manual_upload/supply_chain_compromise_leads_to_trojanized_installers_d393005f-03bd-4d35-af94-aff4991999c4/2eae4f06f2c3_browsing76c6206c632ac93f4e8c4b3e0e63eca3118e883f8ac479b2f852XxX10Exe.exe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIAJPJC2Q3D5GWFTK3Q%2F20240703%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20240703T080019Z&X-Amz-Expires=600&X-Amz-Signature=50c32ffb1731d7377cc6cd292bcd2dc2ba2cfb2e363325678b61b5299f1f130c&X-Amz-SignedHeaders=host&x-id=GetObject | Web Gateway | IT55 | Penetrated |



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

# Threats


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

# Trusted Access

## MSS-TAS

## MSS-USB

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



LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500


TLP:AMBER

# ASM-VP REPORT

## HOW CAN WE HELP?

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



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