

Date of Publication  
October 28, 2024



HiveForce Labs

WEEKLY

# THREAT DIGEST

**Attacks, Vulnerabilities and Actors**

21 to 27 OCTOBER 2024

# Table Of Contents

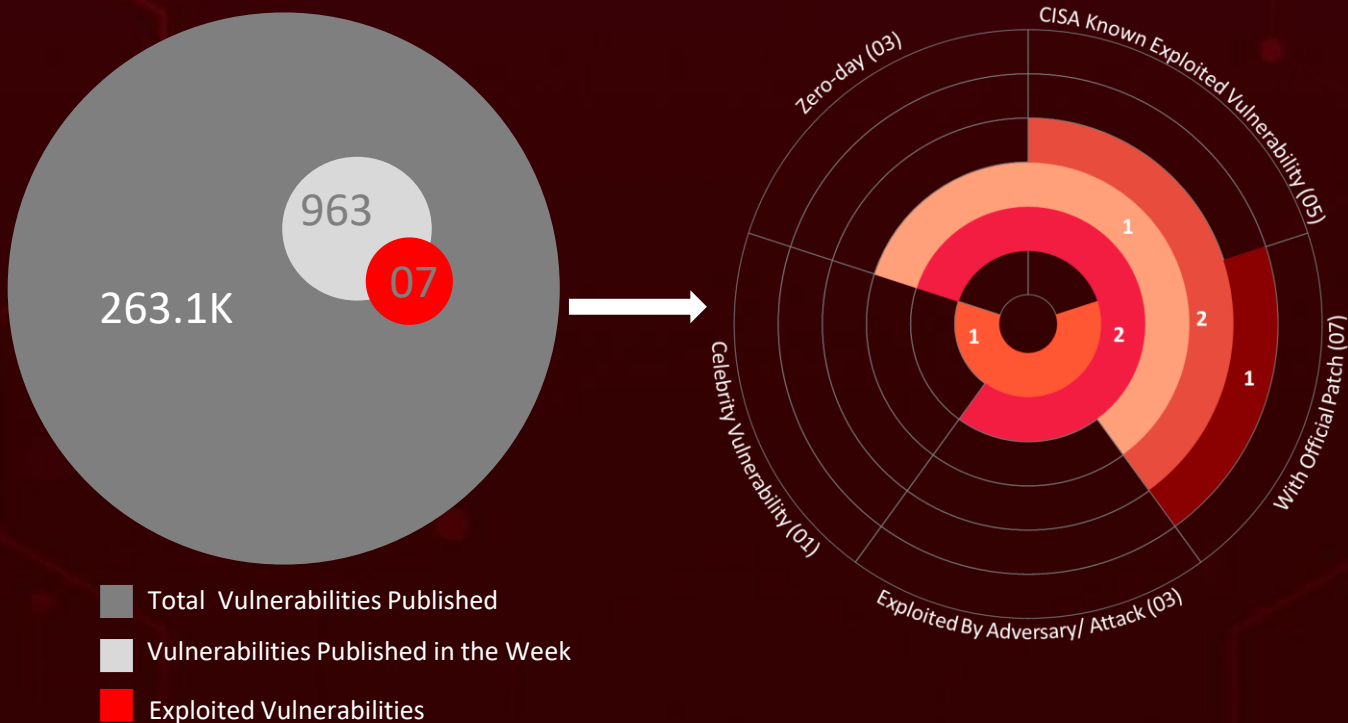
|                                  |    |
|----------------------------------|----|
| <u>Summary</u>                   | 03 |
| <u>High Level Statistics</u>     | 04 |
| <u>Insights</u>                  | 05 |
| <u>Targeted Countries</u>        | 06 |
| <u>Targeted Industries</u>       | 07 |
| <u>Top MITRE ATT&amp;CK TTPs</u> | 07 |
| <u>Attacks Executed</u>          | 08 |
| <u>Vulnerabilities Exploited</u> | 13 |
| <u>Adversaries in Action</u>     | 18 |
| <u>Recommendations</u>           | 21 |
| <u>Threat Advisories</u>         | 22 |
| <u>Appendix</u>                  | 23 |
| <u>What Next?</u>                | 27 |

# Summary

HiveForce Labs has uncovered several critical cybersecurity threats, highlighting the alarming frequency and sophistication of cyber incidents. Over the past week, **nine** attacks were executed, **seven** exploited vulnerabilities, and **three** active threat groups were identified, underscoring the relentless rise in cyber intrusions.

One significant vulnerability, **CVE-2024-44133**, known as "**HM Surf**," enables attackers to bypass macOS's TCC framework, granting unauthorized access to sensitive data, including camera and microphone controls. Meanwhile, **Crypt Ghouls**, an emerging cybercrime group, has initiated ransomware campaigns that aggressively target Russian businesses and government entities.

Additionally, a Cross-Site Scripting (XSS) vulnerability in the **Roundcube Webmail client (CVE-2024-37383)** has been exploited in targeted phishing attacks against a government organization within a Commonwealth of Independent States (CIS) country. Fortinet has also detected active exploits of a **zero-day** vulnerability in the **FortiManager API**, tracked as **CVE-2024-47575**. These escalating threats underscore the urgent need for enhanced cybersecurity defenses worldwide.



# High Level Statistics

9

Attacks  
Executed

7

Vulnerabilities  
Exploited

3

Adversaries in  
Action

- [Adload](#)
  - [LockBit 3.0](#)
  - [Babuk](#)
  - [SRBMiner](#)
  - [Bumblebee](#)
  - [Stealc](#)
  - [Rhadamanthys](#)
  - [AMOS Stealer](#)
  - [Manuscript](#)
- [CVE-2024-44133](#)
  - [CVE-2024-9537](#)
  - [CVE-2024-37383](#)
  - [CVE-2024-47575](#)
  - [CVE-2024-4947](#)
  - [CVE-2024-20481](#)
  - [CVE-2024-20412](#)
- [Crypt Ghouls](#)
  - [UNC5820](#)
  - [Lazarus](#)



# Insights

## CIS Government Agency Under

**Attack:** Roundcube XSS Flaw Used for Credential Theft

**HM Surf Unveiled:** macOS Vulnerability Grants Hackers Access to Your Camera and Mic

## High-Stakes

**Hostage:** LockBit 3.0 and Babuk Wreak Havoc in Russia, Crypt Ghouls Demand Huge Ransoms

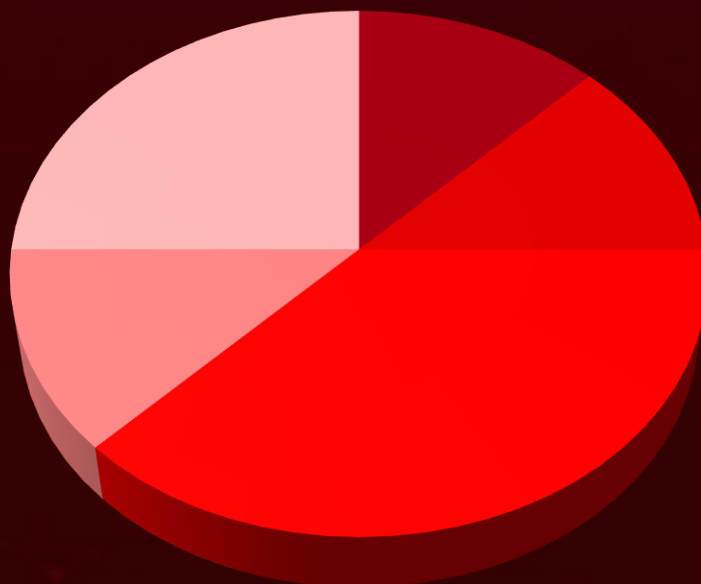
**Over 50 FortiManager Devices Compromised by Zero-Day Flaw CVE-2024-47575**

**DeFi Deception:** Lazarus Group Capitalizes on CVE-2024-4947 to Target Cryptocurrency Users

## Bumblebee Stings Back:

Sophisticated Malware Adapts After Europol's Operation Endgame

## Threat Distribution



■ Backdoor ■ Cryptominer ■ Information stealer ■ Loader ■ Ransomware

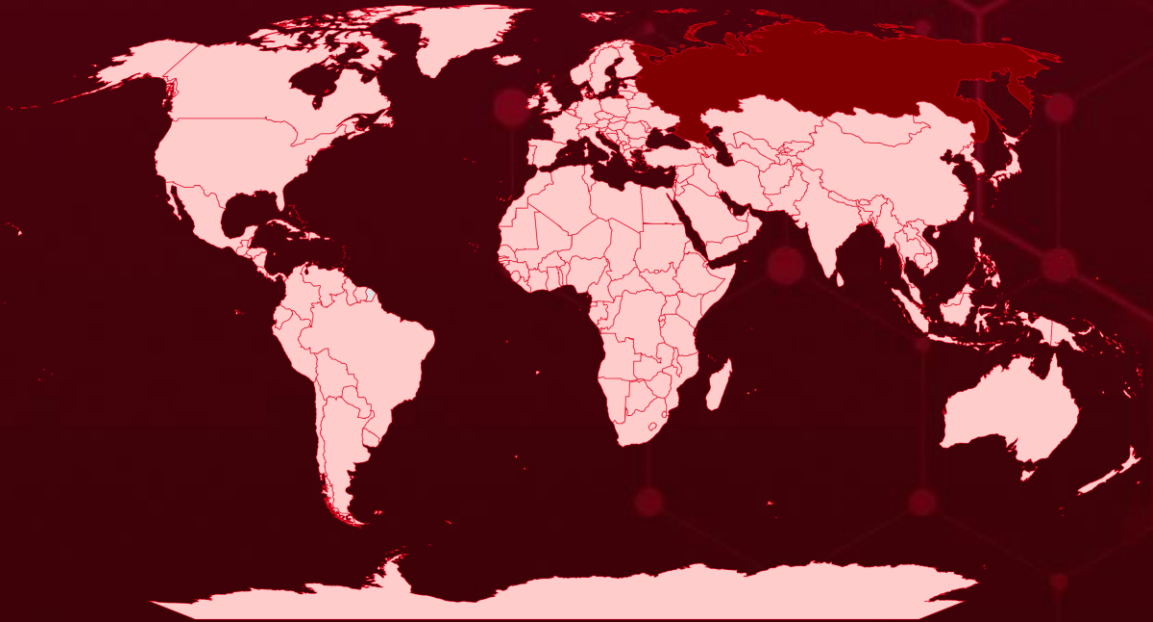


# Targeted Countries

Most



Least

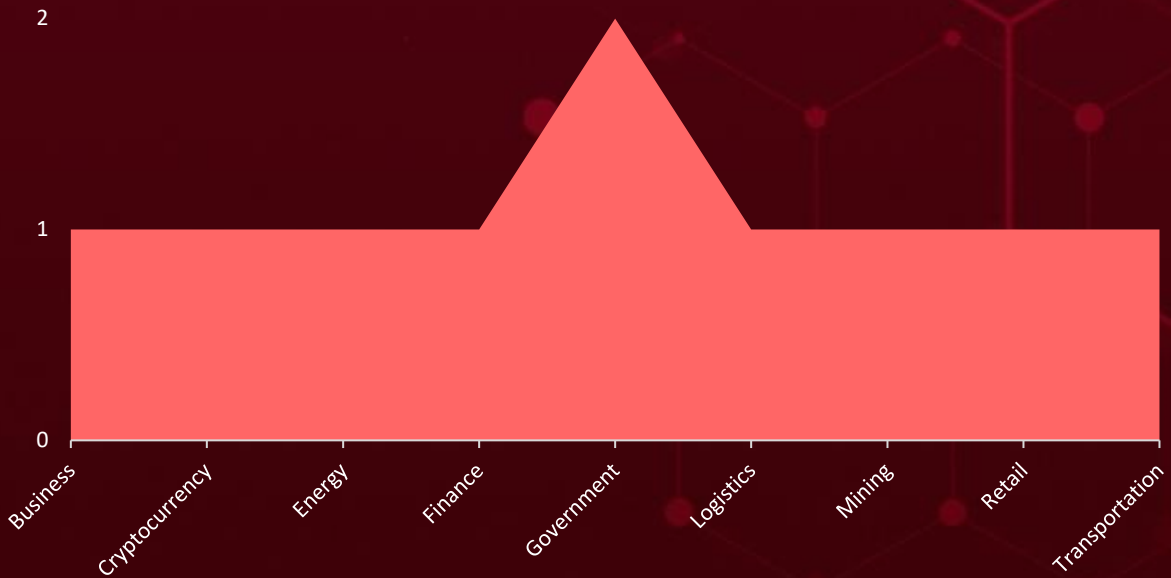


Powered by Bing

© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

| Countries                   | Countries                   | Countries                      | Countries           |
|-----------------------------|-----------------------------|--------------------------------|---------------------|
| Russia                      | Tonga                       | Bhutan                         | Palau               |
| Zambia                      | Aruba                       | Turkey                         | Cameroon            |
| Saint Lucia                 | Uzbekistan                  | Bir Tawil                      | Paraguay            |
| New Caledonia               | Ashmore and Cartier Islands | United Arab Emirates           | Canada              |
| Akrotiri and Dhekelia       | Libya                       | Bolivia                        | Poland              |
| Switzerland                 | Australia                   | Vietnam                        | Cape Verde          |
| Åland                       | Maldives                    | Bonaire                        | Afghanistan         |
| Mauritania                  | Austria                     | Lesotho                        | Cayman Islands      |
| Albania                     | Moldova                     | Bosnia and Herzegovina         | Chad                |
| Panama                      | Azerbaijan                  | Lithuania                      | Chile               |
| Algeria                     | Namibia                     | Botswana                       | Seychelles          |
| Slovenia                    | Bahamas                     | Malawi                         | China               |
| American Samoa              | Nigeria                     | Bouvet Island                  | South Korea         |
| U.S. Minor Outlying Islands | Bahrain                     | Malta                          | Cocos               |
| Andorra                     | Oman                        | Brazil                         | Colombia            |
| Macau                       | Bangladesh                  | Mexico                         | Svalbard            |
| Angola                      | Philippines                 | British Indian Ocean Territory | Comoros             |
| Montserrat                  | Barbados                    | Mongolia                       | Taiwan              |
| Anguilla                    | Saba                        | British Virgin Islands         | Cook Islands        |
| North Macedonia             | Belarus                     | Mozambique                     | Togo                |
| Puerto Rico                 | Samoa                       | Brunei                         | Trinidad and Tobago |
| Antigua and Barbuda         | Belgium                     | Nepal                          | Costa Rica          |
| Senegal                     | Singapore                   | Bulgaria                       | Croatia             |
| Argentina                   | Belize                      | Nicaragua                      | Uganda              |
| South Sudan                 | South Africa                | Burkina Faso                   | Cuba                |
| Armenia                     | Benin                       | Cambodia                       | United States       |
|                             | Sudan                       |                                | Vatican City        |
|                             | Tanzania                    |                                | Cyprus              |
|                             |                             |                                | Czech Republic      |

# Targeted Industries



## TOP MITRE ATT&CK TTPs

### T1588

Obtain Capabilities

### T1059

Command and Scripting Interpreter

### T1588.006

Vulnerabilities

### T1036

Masquerading

### T1566

Phishing

### T1588.005

Exploits

### T1204

User Execution

### T1068

Exploitation for Privilege Escalation

### T1190

Exploit Public-Facing Application

### T1204.002

Malicious File

### T1071.001

Web Protocols

### T1071

Application Layer Protocol

### T1105

Ingress Tool Transfer

### T1070

Indicator Removal

### T1016

System Network Configuration Discovery

### T1566.001

Spearphishing Attachment

### T1059.007

JavaScript

### T1203

Exploitation for Client Execution

### T1566.002

Spearphishing Link

### T1222

File and Directory Permissions Modification



# Attacks Executed

| NAME                    | OVERVIEW  | DELIVERY METHOD                                     | TARGETED CVE  |  |
|-------------------------|---|---|---|--|
| <u>Adload</u>           | AdLoad malware continues to infect Mac systems years after its initial emergence in 2017. As a package bundler, AdLoad has been documented distributing various subsequent payloads, including adware, bundleware, PiTM, backdoors, and proxy applications. It further entrenches itself by installing as a Launch Agent. | Potentially exploiting CVE-2024-44133 vulnerability | CVE-2024-44133  |  |
| <b>TYPE</b>             |   | <b>IMPACT</b>                                       | <b>AFFECTED PRODUCT</b>   |  |
| Loader                  |   |   | macOS Sequoia 15  |  |
| <b>ASSOCIATED ACTOR</b> |   | -   | Privacy Breaches, Performance Issues, Annoyance from Ads, Financial Risks | <b>PATCH LINKS</b>   |
|                         |   |   |   | <a href="https://support.apple.com/en-us/121238">https://support.apple.com/en-us/121238</a> ,<br><a href="https://support.apple.com/en-us/108382">https://support.apple.com/en-us/108382</a> |
| <b>IOC TYPE</b>         | <b>VALUE</b>  |   |   |  |
| SHA256                  | d94f62ec4b6ffcec35d5e639d02a52ce226629a5eb3e2a7190174ea8d3b40b5b, 956aae546af632ea20123bfe659d57e0d5134e39cdb5489bd6f1ba5d8bbd0472, 6587e61a8a7edb312da5798ffccf4a5ef227d3834389993b4df3ef0b173443dc  |   |   |  |

| NAME                    | OVERVIEW   | DELIVERY METHOD   | TARGETED CVE            |
|-------------------------|--|---|-------------------------|
| <u>LockBit 3.0</u>      | LockBit 3.0 ransomware, encrypts data and may exfiltrate it, threatening to leak sensitive information if a ransom is not paid. Renowned for its stealthy tactics, it primarily targets enterprises and functions as a ransomware-as-a-service (RaaS). | Exploiting login credentials  | -                       |
| <b>TYPE</b>             |  | <b>IMPACT</b>   | <b>AFFECTED PRODUCT</b> |
| Ransomware              |  |   | -                       |
| <b>ASSOCIATED ACTOR</b> |  | Data Theft, Financial Loss, Operational Downtime, Reputation Damage | <b>PATCH LINK</b>       |
| Crypt Ghouls            |  |   | -                       |
| <b>IOC TYPE</b>         | <b>VALUE</b>   |   |                         |
| SHA256                  | a54519b7530039b9fba9a4143bf549b67048f441bbebf9f8d5cff1e539752189, dec147d7628d4e3479bc0ff31413621fb4b1b64a618469a9402a42816650f92b   |   |                         |

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.



| NAME                    | OVERVIEW   | DELIVERY METHOD   | TARGETED CVE             |
|-------------------------|--|---|--------------------------|
| <b><u>Babuk</u></b>     | Babuk ransomware is a newly emerged threat identified in 2021. It is a sophisticated ransomware designed for multiple platforms, with the most commonly utilized versions being for Windows and ARM for Linux. Additionally, ESX and a 32-bit legacy PE executable have been noted. Babuk employs an Elliptic Curve Algorithm to generate its encryption keys. | Exploiting login credentials  | -                        |
| <b>TYPE</b>             |  | <b>IMPACT</b>   | <b>AFFECTED PRODUCTS</b> |
| Ransomware              |  | Data Theft, Financial Loss, Operational Downtime, Reputation Damage | -                        |
| <b>ASSOCIATED ACTOR</b> |  |   | <b>PATCH LINK</b>        |
| Crypt Ghouls            |  |   | -                        |
| <b>IOC TYPE</b>         |  | <b>VALUE</b>  |                          |
| SHA256                  | 56682344aa1dc0a0a5b0d26bd3a8dfe8ceb8772d6cd9e3f8cbd78ca78fe3c2ab   |   |                          |

| NAME                    | OVERVIEW  | DELIVERY METHOD                                    | TARGETED CVE             |
|-------------------------|---|--|--------------------------|
| <b><u>SRBMiner</u></b>  | SRBMiner is a cryptominer targeting Docker hosts, specifically for mining XRP, a cryptocurrency developed by Ripple Labs. The attacker downloads SRBMiner from GitHub, installs it in the /usr/sbin directory, and initiates mining operations. This process compromises the integrity and security of Docker-based environments. | Docker remote API servers                          | -                        |
| <b>TYPE</b>             |   | <b>IMPACT</b>                                      | <b>AFFECTED PRODUCTS</b> |
| Cryptominer             |   | Resource Drain, Financial Risk, System Instability | -                        |
| <b>ASSOCIATED ACTOR</b> |   |  | <b>PATCH LINK</b>        |
| -                       |   |  | -                        |
| <b>IOC TYPE</b>         |   | <b>VALUE</b>                                       |                          |
| SHA256                  | 0d4eb69b551cb538a9a4c46f7b57906a47bcabb8ef8a5d245584fbba09fc5084  |  |                          |

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

| NAME                    | OVERVIEW  | DELIVERY METHOD   | TARGETED CVE            |
|-------------------------|---|---|-------------------------|
| <u>Bumblebee</u>        | Bumblebee is an advanced malware loader identified in March 2022, primarily utilized by ransomware groups to deploy malicious payloads. Developed in C++, it utilizes sophisticated evasion methods, including Windows shortcut (.LNK) files and PowerShell commands, to achieve stealth and persistence. | Phishing  | -                       |
|                         |   | <b>IMPACT</b>   | <b>AFFECTED PRODUCT</b> |
| <b>TYPE</b>             |   | Malicious Payload Delivery, System Compromise, Data Theft | Windows                 |
| Loader                  |   |   | <b>PATCH LINK</b>       |
| <b>ASSOCIATED ACTOR</b> |   |   | -                       |
| -                       |   |   |                         |
| <b>IOC TYPE</b>         | <b>VALUE</b>  |   |                         |
| SHA256                  | 2bca5abfac168454ce4e97a10ccf8ffc068e1428fa655286210006b298de42fb, 106c81f547cfe8332110520c968062004ca58bcfd2dbb0accd51616dd694721f, c26344bfd07b871dd9f6bd7c71275216e18be265e91e5d0800348e8aa06543f9  |   |                         |

| NAME                    | OVERVIEW   | DELIVERY METHOD                                    | TARGETED CVE             |
|-------------------------|--|--|--------------------------|
| <u>Stealc</u>           | Stealc is an information stealer offered as Malware-as-a-Service. It operates as a non-resident stealer with customizable data collection options and is developed using features from other well-known stealers. Written in C, it utilizes WinAPI functions and primarily targets data from web browsers, extensions, and desktop applications of cryptocurrency wallets. | Phishing   | -                        |
|                         |  | <b>IMPACT</b>                                      | <b>AFFECTED PRODUCTS</b> |
| <b>TYPE</b>             |  | Operational Disruption, Data Theft, Financial Loss | Windows and macOS        |
| Information stealer     |  |  | <b>PATCH LINK</b>        |
| <b>ASSOCIATED ACTOR</b> |  |  | -                        |
| -                       |  |  |                          |
| <b>IOC TYPE</b>         | <b>VALUE</b>   |  |                          |
| SHA256                  | a834be6d2bec10f39019606451b507742b7e87ac8d19dc0643ae58df183f773c   |  |                          |

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

| NAME                       | OVERVIEW   | DELIVERY METHOD                                    | TARGETED CVE             |
|----------------------------|--|--|--------------------------|
| <b><u>Rhadamanthys</u></b> | Rhadamanthys is an information stealer featuring a versatile array of modules and a multi-layered architecture. Available on the black market and regularly updated, it poses a continual threat. Its sophisticated design enables it to evade detection while carrying out various malicious activities, including the theft and exfiltration of sensitive information. | Phishing   | -                        |
|                            |  | <b>IMPACT</b>                                      | <b>AFFECTED PRODUCTS</b> |
| <b>TYPE</b>                |  | Operational Disruption, Data Theft, Financial Loss | Windows and macOS        |
| Information stealer        |  |  | <b>PATCH LINK</b>        |
| <b>ASSOCIATED ACTOR</b>    |  |  | -                        |
| -                          |  |  |                          |
| <b>IOC TYPE</b>            | <b>VALUE</b>   |  |                          |
| SHA256                     | 2853a61188b4446be57543858adcc704e8534326d4d84ac44a60743b1a44cbfe   |  |                          |




| NAME                       | OVERVIEW  | DELIVERY METHOD                                    | TARGETED CVE             |
|----------------------------|---|--|--------------------------|
| <b><u>AMOS Stealer</u></b> | Atomic, also known as AMOS, is macOS information-stealing malware currently delivered to targets via a fraudulent web browser update scheme called ClearFake. | Phishing   | -                        |
|                            |   | <b>IMPACT</b>                                      | <b>AFFECTED PRODUCTS</b> |
| <b>TYPE</b>                |   | Operational Disruption, Data Theft, Financial Loss | Windows and macOS        |
| Information stealer        |   |  | <b>PATCH LINK</b>        |
| <b>ASSOCIATED ACTOR</b>    |   |  | -                        |
| -                          |   |  |                          |
| <b>IOC TYPE</b>            | <b>VALUE</b>  |  |                          |
| SHA256                     | 94379fa0a97cc2ecd8d5514d0b46c65b0d46ff9bb8d5a4a29cf55a473da550d5  |  |                          |




The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

| NAME              | OVERVIEW   | DELIVERY METHOD   | TARGETED CVEs   |
|-------------------|--|---|---|
| <u>Manuscript</u> | <p>Manuscript malware, also known as NukeSped, is an advanced tool for espionage and data theft. Its key features include keylogging to capture passwords, screen capture for recording user activities, and audio recording via the microphone. It also monitors clipboard data, gathers system information, and provides remote access for executing commands and manipulating files. These capabilities allow attackers extensive control over infected devices for surveillance and data exfiltration.</p> | Exploiting vulnerabilities  | CVE-2024-4947   |
| TYPE              |  | IMPACT  | AFFECTED PRODUCT  |
| Backdoor          |  | <p>Data Theft, Unauthorized Surveillance, Loss of Privacy, System Compromise, Persistent Access, Operational Disruption</p> | Google Chromium V8  |
| ASSOCIATED ACTOR  |  |   | PATCH LINK  |
| Lazarus Group     |  |   | <a href="https://www.google.com/intl/en/chrome/?standalone=1">https://www.google.com/intl/en/chrome/?standalone=1</a> |
| IOC TYPE          | VALUE  |   |   |
| SHA256            | <p>2fe78941d74d35f721556697491a438bf3573094d7ac091b42e4f59ecbd25753, 2fe78941d74d35f721556697491a438bf3573094d7ac091b42e4f59ecbd25753, 0036ef9eca61e045fd34726758631c2cb26770471f91ec39daefd81bae1a3d2c</p>  |   |   |



The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.




# Vulnerabilities Exploited

| CVE ID                                | CELEBRITY VULNERABILITY   | AFFECTED PRODUCTS  | ASSOCIATED ACTOR   |
|---------------------------------------|---|--|--|
| <u><a href="#">CVE-2024-44133</a></u> |  | macOS Sequoia versions before 15.0   | -  |
|                                       | ZERO-DAY  |  |  |
|                                       |  | AFFECTED CPE   | ASSOCIATED ATTACKS/RANSOMWARE  |
| NAME                                  | CISA KEY  | cpe:2.3:o:apple:macos:*:*:*:*:*:*:*<br>*   | Adload   |
| HM Surf                               |  |  |  |
|                                       | CWE ID  | ASSOCIATED TTPs  | PATCH LINKS  |
|                                       | CWE-284   | T1059: Command and Scripting Interpreter, T1068: Exploitation for Privilege Escalation, T1203: Exploitation for Client Execution | <a href="https://support.apple.com/en-us/121238">https://support.apple.com/en-us/121238</a> ,<br><a href="https://support.apple.com/en-us/108382">https://support.apple.com/en-us/108382</a> |




| CVE ID                                     | CELEBRITY VULNERABILITY   | AFFECTED PRODUCTS  | ASSOCIATED ACTOR  |
|--|---|--|---|
| <u><a href="#">CVE-2024-9537</a></u>       |    | ScienceLogic SL1 versions prior to 12.1.3<br>ScienceLogic SL1 versions prior to 12.2.3<br>ScienceLogic SL1 versions prior to 12.3<br>ScienceLogic SL1 versions prior to 10.1.x<br>ScienceLogic SL1 versions prior to 10.2.x<br>ScienceLogic SL1 versions prior to 11.1.x<br>ScienceLogic SL1 versions prior to 11.2.x<br>ScienceLogic SL1 versions prior to 11.3.x | -   |
|  | ZERO-DAY  |  |   |
|  |    | AFFECTED CPE   | ASSOCIATED ATTACKS/RANSOMWARE   |
| NAME                                       | CISA KEY  | cpe:2.3:a:sciencelogic:sl1:*:*:*:*:*:*:*   | -   |
| ScienceLogic SL1 Unspecified Vulnerability |  |  |   |
|  | CWE ID  | ASSOCIATED TTPs  | PATCH LINK  |
|  | CWE-829   | T1059: Command and Scripting Interpreter, T1190: Exploit Public-Facing Application, T1068: Exploitation for Privilege Escalation   | <a href="https://docs.sciencelogic.com/latest/Content/Web_Admin_and_Accounts/System_Administration/sys_admin_system_upgrade.htm">https://docs.sciencelogic.com/latest/Content/Web_Admin_and_Accounts/System_Administration/sys_admin_system_upgrade.htm</a> |




| CVE ID  | CELEBRITY VULNERABILITY   | AFFECTED PRODUCTS  | ASSOCIATED ACTOR  |
|---|---|--|---|
| <u>CVE-2024-4947</u>                            |  | Google Chrome prior to 125.0.6422.60   | Lazarus Group   |
|   | ZERO-DAY  |  |   |
|   |  | AFFECTED CPE   | ASSOCIATED ATTACKS/RAN SOMWARE  |
| NAME  | CISA KEV  | cpe:2.3:a:google:chrome:*:*:*:*:*:*:<br>*  | Manuscript  |
| Google Chromium V8 Type Confusion Vulnerability |  |  |   |
|   | CWE ID  | ASSOCIATED TTPs  | PATCH LINK  |
|   | CWE-843   | T1204: User Execution, T1059: Command and Scripting Interpreter, T1059.007: JavaScript, T1068: Exploitation for Privilege Escalation | <a href="https://www.google.com/intl/en/chrome/?standalone=1">https://www.google.com/intl/en/chrome/?standalone=1</a> |


| CVE ID  | CELEBRITY VULNERABILITY   | AFFECTED PRODUCTS  | ASSOCIATED ACTOR  |
|---|---|--|---|
| <u>CVE-2024-20481</u>                             |  | Cisco Adaptive Security Appliance Cisco Firepower Threat Defense Software  | -   |
|   | ZERO-DAY  |  |   |
|   |  | AFFECTED CPE   | ASSOCIATED ATTACKS/RANSOMWARE   |
| NAME  | CISA KEV  | cpe:2.3:a:cisco:adaptive_security_appliance:*:*:*:*:*:*:<br>:*:*:*:*<br>cpe:2.3:a:cisco:firepower_threat_defense_software:*:*:*:*:*:*:<br>:*:*:*:*:*:*:* | -   |
| Cisco ASA and FTD Denial-of-Service Vulnerability |  |  |   |
|   | CWE ID  | ASSOCIATED TTPs  | PATCH LINK  |
|   | CWE-772   | T1574: Hijack Execution Flow, T1499: Endpoint Denial of Service, T1499.004: Application or System Exploitation   | <a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asafthd-bf-dos-vDZhLqrW">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asafthd-bf-dos-vDZhLqrW</a> |




| CVE ID                                    | CELEBRITY VULNERABILITY   | AFFECTED PRODUCTS   | ASSOCIATED ACTOR  |
|---|---|---|---|
| <a href="#">CVE-2024-20412</a>            |  | Cisco Firepower Threat Defense Software for Firepower 1000, 2100, 3100, and 4200 Series | -   |
|   | ZERO-DAY  |   |   |
|   |  | AFFECTED CPE  | ASSOCIATED ATTACKS/RANSOMWARE   |
| NAME                                      | CISA KEY  | cpe:2.3:a:cisco:firepower_threat_defense:*:*:*:*:*:*                                    | -   |
|   |  |   |   |
| Cisco FTC Static Credential Vulnerability | CWE ID  | ASSOCIATED TTPs   | PATCH LINK  |
|   | CWE-259   | T1110.003: Password Spraying, T1078: Valid Accounts                                     | <a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-statcred-dFC8tXT5">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-statcred-dFC8tXT5</a> |

# Adversaries in Action

| NAME  | ORIGIN   | TARGETED INDUSTRY                                     | TARGETED REGION          |
|---|--|---|--------------------------|
| <br><b>Crypt Ghouls</b>  | -  | Business, Government, Mining, Energy, Finance, Retail | Russia                   |
|   | <b>MOTIVE</b><br>Financial Gain, Information Theft, Espionage, Sabotage, Destruction |   |                          |
|   | <b>TARGETED CVEs</b>   | <b>ASSOCIATED ATTACKS/RANSOM WARE</b>                 | <b>AFFECTED PRODUCTS</b> |
|   | -  | LockBit 3.0, Babuk                                    | -                        |
|   | <b>TTPs</b>  |   |                          |
| TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0011: Command and Control; TA0010: Exfiltration; TA0040: Impact; T1199: Trusted Relationship; T1543: Create or Modify System Process; T1070: Indicator Removal; T1070.004: File Deletion; T1055: Process Injection; T1083: File and Directory Discovery; T1040: Network Sniffing; T1057: Process Discovery; T1105: Ingress Tool Transfer; T1041: Exfiltration Over C2 Channel; T1486: Data Encrypted for Impact; T1490: Inhibit System Recovery; T1053: Scheduled Task/Job; T1047: Windows Management Instrumentation; T1059: Command and Scripting Interpreter |  |   |                          |

| NAME  | ORIGIN               | TARGETED INDUSTRIES                  | TARGETED REGION          |
|---|----------------------|--------------------------------------|--------------------------|
| <br><b>UNC5820</b>   | -                    | All                                  | All                      |
|   | <b>MOTIVE</b>        |                                      |                          |
|   | Information Theft    |                                      |                          |
|   | <b>TARGETED CVEs</b> | <b>ASSOCIATED ATTACKS/RANSOMWARE</b> | <b>AFFECTED PRODUCTS</b> |
|   | CVE-2024-47575       | -                                    | Fortinet FortiManager    |
| <b>TTPs</b>   |                      |                                      |                          |
| TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0005: Defense Evasion; TA0007: Discovery; TA0009: Collection; TA0010: Exfiltration; T1588: Obtain Capabilities; T1588.006: Vulnerabilities; T1190: Exploit Public-Facing Application; T1036: Masquerading; T1016: System Network Configuration Discovery; T1587: Develop Capabilities; T1587.003: Digital Certificates; T1074: Data Staged; T1585: Establish Accounts; T1585.002: Email Accounts; T1059: Command and Scripting Interpreter; T1222: File and Directory Permissions Modification |                      |                                      |                          |

| NAME  | ORIGIN               | TARGETED INDUSTRIES                  | TARGETED COUNTRIES       |
|---|----------------------|--------------------------------------|--------------------------|
| <br><b>Lazarus (aka UNC2970, Labyrinth Chollima, Group 77, Hastati Group, Whois Hacking Team, NewRomanic Cyber Army Team, Zinc, Hidden Cobra, Appleworm, APT-C-26, ATK 3, SectorA01, ITG03, TA404, DEV-0139, Guardians of Peace, Gods Apostles, Gods Disciples, UNC577, UNC4034, UNC4736, UNC4899, Diamond Sleet, Jade Sleet, TraderTraitor, Citrine Sleet, Gleaming Pisces)</b>   | North Korea          | Cryptocurrency                       | Russia                   |
|   | <b>MOTIVE</b>        |                                      |                          |
|   | <b>TARGETED CVEs</b> | <b>ASSOCIATED ATTACKS/RANSOMWARE</b> | <b>AFFECTED PRODUCTS</b> |
|   | CVE-2024-4947        | Manuscript                           | Google Chrome            |
| <b>TTPs</b>   |                      |                                      |                          |
| TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0011: Command and Control; T1588: Obtain Capabilities; T1588.006: Vulnerabilities; T1588.005: Exploits; T1608: Stage Capabilities; T1608.001: Upload Malware; T1190: Exploit Public-Facing Application; T1583: Acquire Infrastructure; T1583.001: Domains; T1059: Command and Scripting Interpreter; T1059.007: JavaScript; T1566: Phishing; T1566.002: Spearphishing Link; T1204: User Execution; T1204.001: Malicious Link; T1132: Data Encoding; T1132.001: Standard Encoding; T1068: Exploitation for Privilege Escalation; T1036: Masquerading |                      |                                      |                          |

# Recommendations

## Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **seven exploited vulnerabilities** and block the indicators related to the threat actors **Crypt Ghouls, UNC5820, Lazarus** and malware **Adload, LockBit 3.0, Babuk, SRBMiner, Bumblebee, Stealc, Rhadamanthys, AMOS Stealer, Manuscript**.

## Uni5 Users

This is an actionable threat digest for HivePro Uni5 customers and they can get comprehensive insights into their threat exposure and can action it effortlessly over the HivePro Uni5 dashboard by

- Run a Scan to discover the assets impacted by the **seven exploited vulnerabilities**.
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **Crypt Ghouls, UNC5820, Lazarus**, and malware **LockBit 3.0, Babuk, Adload, Bumblebee, SRBMiner, Stealc, Rhadamanthys, AMOS Stealer, Manuscript** in Breach and Attack Simulation(BAS).

# Threat Advisories

[New 'HM-Surf' Vulnerability Could Expose MacOS Data](#)

[Crypt Ghouls Deployed LockBit and Babuk to Paralyze Russian Firms](#)

[Critical Zero-Day Flaw in ScienceLogic SL1 Under Active Exploitation](#)

[Roundcube Under Siege: Critical XSS Vulnerability Exploited in Phishing Attack](#)

[Exposed Docker APIs Fuel Illicit Cryptomining Surge](#)

[Bumblebee Bites Back with New Infection Chain](#)

[UNC5820 Exploits Critical FortiManager Zero-Day to Hijack Enterprise Networks](#)

[ClickFix Con: Phishing Scam Turns Video Calls into Malware Havens](#)

[Lazarus Exploits Chrome Zero-Day in Fake DeFi Game Heist](#)

[Cisco Patches Critical VPN DoS Vulnerability in ASA and FTD](#)

# Appendix

**Known Exploited Vulnerabilities (KEV):** Software vulnerabilities for which there are public exploits or proof-of-concept (PoC) code available, and for which there is a high risk of potential harm to an organization's systems or data if left unaddressed.

**Celebrity Vulnerabilities:** Software vulnerabilities that have gained significant attention and have been branded with catchy names and logos due to their profound and multifaceted impact. These vulnerabilities provide threat actors with opportunities to breach sensitive systems, potentially resulting in unauthorized access and the compromise of critical information.

## 🔪 Indicators of Compromise (IOCs)

| Attack Name   | TYPE   | VALUE  |
|---------------|--------|--|
| <u>Adload</u> | SHA256 | d94f62ec4b6ffcec35d5e639d02a52ce226629a5eb3e2a7190174ea8d3b40b5b,<br>956aae546af632ea20123bfe659d57e0d5134e39cdb5489bd6f1ba5d8bbd0472,<br>6587e61a8a7edb312da5798ffccf4a5ef227d3834389993b4df3ef0b173443dc,<br>3d063efde737b7b2e393926358cbb32469b76395e1a05e8c127a12e47550f264,<br>2d595880cfb1691dd43de02d1a90273919f62311a7668ef078709ef2fd6bd87,<br>7cb10a70fd25645a708c81f44bb1de2b6de39d583ae3a71df0913917ad1dff3,<br>4a7c9829590e1230a448dd7a4272b9fbfbafccf7043441967c2f68f6082dde32,<br>68b6beb70bd547b75f2d36d70ca49f8b18542874480d39e33b09ee69eb1048b3,<br>1904b705105db4550371d678f8161826b98b1a9fca139fa41628214ed816d2f5,<br>2fb1d8e6454f43522f42675dcf415569e5df5d731e1d1390f793c282cce4a7aa,<br>ee9ebdb1d9a7424cd64905d39820b343c5f76e29c9cd60c0cdd3bfe069fb7d51,<br>c7721ab85bad163576c166a0a71c0dbe4cc491dda68c5a5907fd1d8cac50780d,<br>17e1b83089814128bc243315894f412026503c10b710c9c59d4aaf67bc209cb8,<br>0adab4bfe1c8d85cbaaa983ca588218086f86dc5d2c69eab5ea0563de40beecb, |

| Attack Name        | TYPE   | VALUE  |
|--------------------|--------|--|
| <b>Adload</b>      | SHA256 | 4b90225402be51bbfc307e85c99f6411295da8acb16ca2afb8eed918c69ebf,<br>b1a7e41eb188da431bd829592a5ee740e912cd47d059942c14c3d492e45c9afd  |
|                    | URLs   | hxxp://m[.]skilledobject[.]com/a/rep,<br>hxxp://m[.]browseractivity[.]com/a/rep,<br>hxxp://m[.]enchantedreign[.]com/a/rep,<br>hxxp://m[.]activitycache[.]com/a/rep,<br>hxxp://m[.]activityinput[.]com/a/rep,<br>hxxp://m[.]opticalupdater[.]com/a/rep,<br>hxxp://m[.]connectioncache[.]com/a/rep,<br>hxxp://m[.]analyzerstate[.]com/a/rep,<br>hxxp://m[.]essencecuration[.]com/a/rep,<br>hxxp://m[.]microrotator[.]com/a/rep,<br>hxxp://m[.]articlesagile[.]com/a/rep,<br>hxxp://m[.]progresshandler[.]com/a/rep,<br>hxxp://m[.]originalrotator[.]com/a/rep,<br>hxxp://m[.]productiveunit[.]com/a/rep,<br>hxxp://api[.]toolenviroment[.]com/l,<br>hxxp://api[.]inetfield[.]com/l,<br>hxxp://api[.]operativeeng[.]com/l,<br>hxxp://api[.]launchertasks[.]com/l,<br>hxxp://api[.]launchelemnt[.]com/l,<br>hxxp://api[.]validexplorer[.]com/l,<br>hxxp://api[.]majorsprint[.]com/l,<br>hxxp://api[.]essentialenumerator[.]com/l,<br>hxxp://api[.]transactioneng[.]com/l,<br>hxxp://api[.]macreationsapp[.]com/l,<br>hxxp://api[.]commondevice[.]com/l,<br>hxxp://api[.]compellingagent[.]com/l,<br>hxxp://api[.]lookupindex[.]com/l,<br>hxxp://api[.]practicalsync[.]com/l,<br>hxxp://api[.]accessiblelist[.]com/l,<br>hxxp://api[.]functionconfig[.]com/l,<br>hxxps://vpnservices[.]live,<br>hxxps://upgrader[.]live,<br>hxxp://bapp[.]pictureworld[.]co |
| <b>LockBit 3.0</b> | MD5    | 8770189ed3ee558819fd6ddf677b0c28,<br>6e3e5d703ed9bed4b7327a73bc585c04  |
|                    | SHA1   | 4dec26dfcd3fd938886c9586a8eb62d7a2495be4,<br>583f34dd59d30be4a10dc7021984df0225cef147  |
|                    | SHA256 | a54519b7530039b9fba9a4143bf549b67048f441bbebf9f8d5cff1e539752189,<br>dec147d7628d4e3479bc0ff31413621fb4b1b64a618469a9402a42816650f92b,<br>80e8defa5377018b093b5b90de0f2957f7062144c83a09a56bba1fe4eda932ce,  |



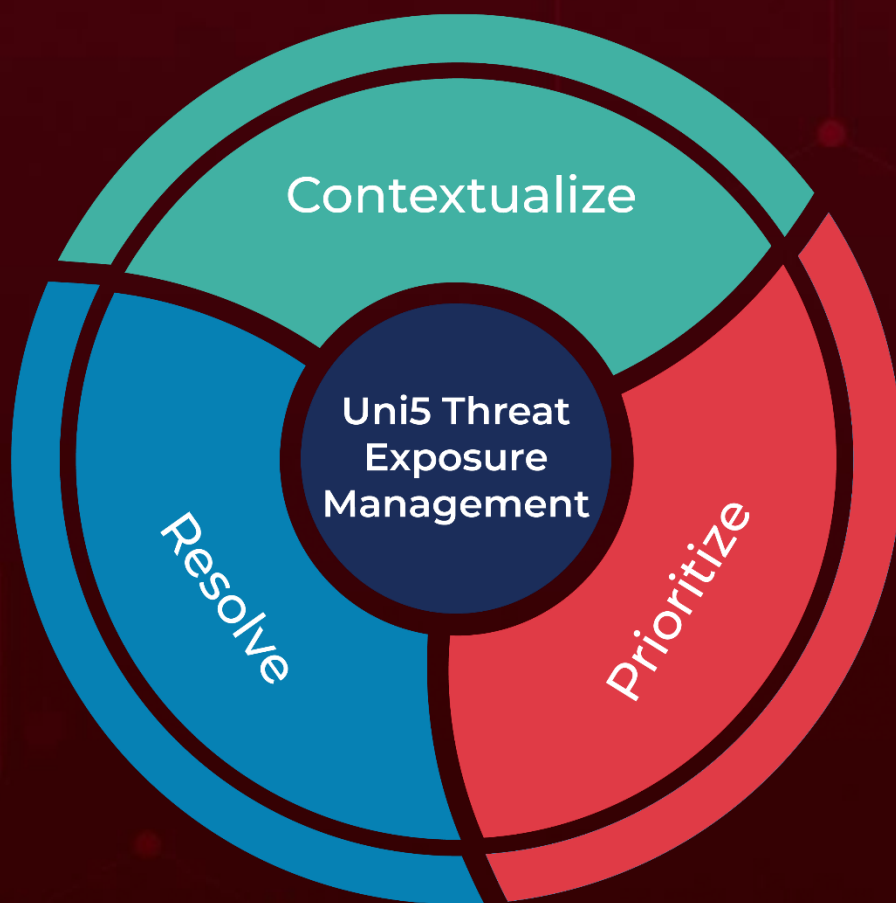
| Attack Name                | TYPE   | VALUE  |
|----------------------------|--------|--|
| <b><u>LockBit 3.0</u></b>  | SHA256 | a56b41a6023f828cccaaef470874571d169fdb8f683a75edd430fbd31a2c3f6e,<br>d61af007f6c792b8fb6c677143b7d0e2533394e28c50737588e40da475c040ee,<br>5e006f895382525e762a33e5dd5e8416bef56ae859f5e96f820cfba5c4c11226,<br>C9dd51d4295c33e1df0d275669a1de9e1de374a51eb88d7f7b1a1e65f49f7794  |
| <b><u>Babuk</u></b>        | MD5    | 87667327439292f5d2b2c68d4b88c0ad   |
|                            | SHA1   | 8a1673d5821d306209b1f540741598bbc90ed1d3   |
|                            | SHA256 | 56682344aa1dc0a0a5b0d26bd3a8dfe8ceb8772d6cd9e3f8cbd78ca78fe3c2ab   |
| <b><u>SRBMiner</u></b>     | SHA256 | 0d4eb69b551cb538a9a4c46f7b57906a47bcabb8ef8a5d245584fbbba09fc5084  |
| <b><u>Bumblebee</u></b>    | URLs   | hxxp[:]//193[.]242[.]145[.]138/mid/w1/Midjourney[.]msi,<br>hxxp[:]//193[.]176[.]190[.]41/down1/nvinstall[.]msi   |
|                            | IPv4   | 193[.]242[.]145[.]138,<br>193[.]176[.]190[.]41   |
|                            | SHA256 | 2bca5abfac168454ce4e97a10ccf8ffc068e1428fa655286210006b298de42fb,<br>106c81f547cfe8332110520c968062004ca58bcfd2dbb0accd51616dd694721f,<br>c26344bfd07b871dd9f6bd7c71275216e18be265e91e5d0800348e8aa06543f9,<br>0ab5b3e9790aa8ada1bbadd5d22908b5ba7b9f078e8f5b4e8fcc27cc0011cce7,<br>d3f551d1fb2c307edfceb65793e527d94d76eba1cd8ab0a5d1f86db11c9474c3,<br>d1cabe0d6a2f3cef5da04e35220e2431ef627470dd2801b4ed22a8ed9a918768,<br>7df703625ee06db2786650b48ffefb13fa1f0dae41e521b861a16772e800c115 |
| <b><u>Stealc</u></b>       | SHA256 | a834be6d2bec10f39019606451b507742b7e87ac8d19dc0643ae58df183f773c   |
|                            | URL    | hxxp[:]//95[.]182[.]97[.]58/84b7b6f977dd1c65[.]php   |
|                            | IPv4   | 95[.]182[.]97[.]58   |
| <b><u>Rhadamanthys</u></b> | SHA256 | 2853a61188b4446be57543858adcc704e8534326d4d84ac44a60743b1a44cbfe   |
|                            | IPv4   | 91[.]103[.]140[.]200   |
|                            | URL    | hxxp[:]//91[.]103[.]140[.]200[:]9078/3936a074a2f65761a5eb8/6fmfpmi7[.]fwf4p  |
| <b><u>AMOS Stealer</u></b> | SHA256 | 94379fa0a97cc2ecd8d5514d0b46c65b0d46ff9bb8d5a4a29cf55a473da550d5   |

| Attack Name         | TYPE   | VALUE  |
|---------------------|--------|--|
| <u>AMOS Stealer</u> | URL    | hxxp[:]//85[.]209[.]11[.]155/joinsystem  |
|                     | IPv4   | 85[.]209[.]11[.]155  |
| <u>Manuscript</u>   | SHA256 | 2fe78941d74d35f721556697491a438bf3573094d7ac091b42e4f59ecbd25753,<br>2fe78941d74d35f721556697491a438bf3573094d7ac091b42e4f59ecbd25753,<br>0036ef9eca61e045fd34726758631c2cb26770471f91ec39daefd81bae1a3d2c,<br>73534b9670133468081305bd442f7691cf2f2c1136f09d9508400546c417833a,<br>59a37d7d2bf4cffe31407edd286a811d9600b68fe757829e30da4394ab65a4cc |

# What Next?

At Hive Pro, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with HivePro Uni5:Threat Exposure Management Platform.



REPORT GENERATED ON

**October 28, 2024 • 11:30 PM**

© 2024 All Rights are Reserved by Hive Pro



More at [www.hivepro.com](http://www.hivepro.com)