Date of Publication
April 8, 2024

Hive Pro

HiveForce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities and Actors

1 to 7 APRIL 2024

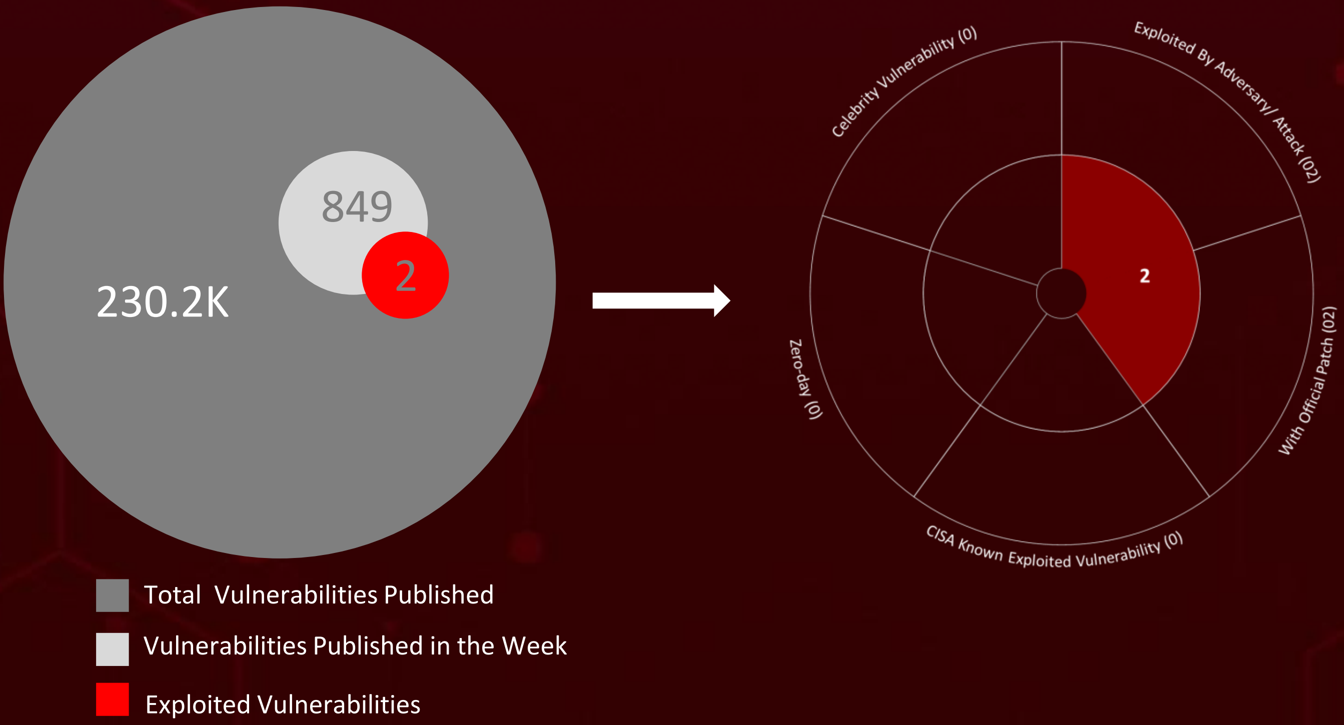
Table Of Contents

Summary

HiveForce Labs recently made several significant discoveries in the realm of cybersecurity threats. In the past week alone, a total of **seven** attacks were executed, **two** vulnerabilities were uncovered, and **two** active adversaries were identified. These findings underscore the persistent danger of cyberattacks.

Furthermore, HiveForce Labs discovered that Multiple Linux distributions face a potential supply chain threat due to the introduction of malicious code into a widely-used XZ Utils library across most distributions. This flaw (**CVE-2024-3094**) allows attackers to manipulate and intercept data exchanged by software routines that rely on XZ Utils as a dependency.

Earth Freybug, a cyberthreat group, employs diverse tools for espionage and financial gain since 2012. Their recent attack involves **UNAPIMON** malware, evading detection by hijacking legitimate processes and unhooking critical APIs. These attacks are on the rise, posing a significant threat to users worldwide.



High Level Statistics

7

Attacks Executed

- Atomic Stealer
- Realst stealer
- UNAPIMON
- SYNC-SCHEDULER
- Agent Tesla
- RotBot
- XClient stealer

2

Vulnerabilities Exploited

- CVE-2024-3094
- CVE-2024-2879

2

Adversaries in Action

- Earth Freybug
- CoralRaider

Insights

Earth Freybug

Threat group utilizes the UNAPIMON malware to evade detection while targeting worldwide

Atomic Stealer & Realst stealer

Are being distributed to Apple macOS users through deceptive advertisements and counterfeit websites.

Agent Tesla

Targeting Australia and USA through phishing campaigns, since November 2023

XZ-Utils backdoored

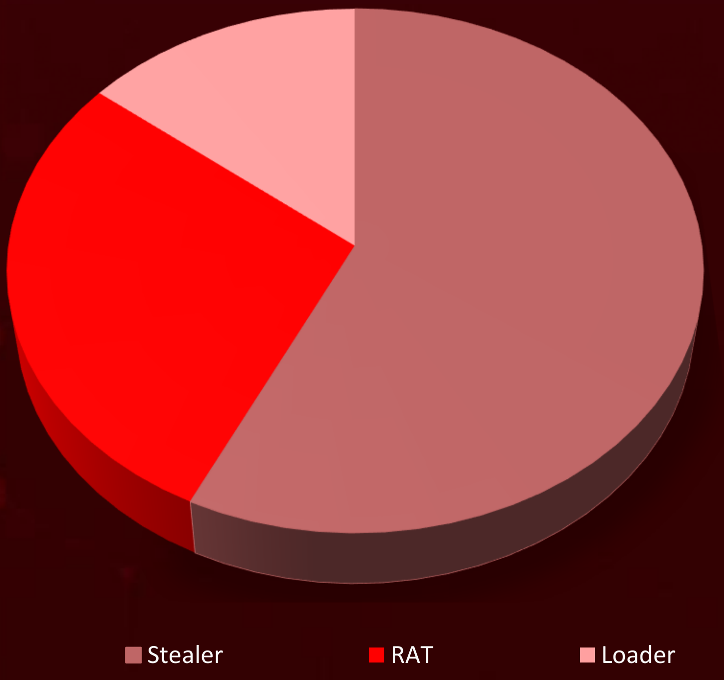
A backdoor (CVE-2024-3094) in XZ Utils library poses supply chain threat to multiple Linux distributions, allowing attackers to manipulate data

CoralRaider A new Vietnamese threat actor group, CoralRaider, has been targeting victims in several Asian countries since at least 2023, focusing on stealing credentials, financial data and social media accounts

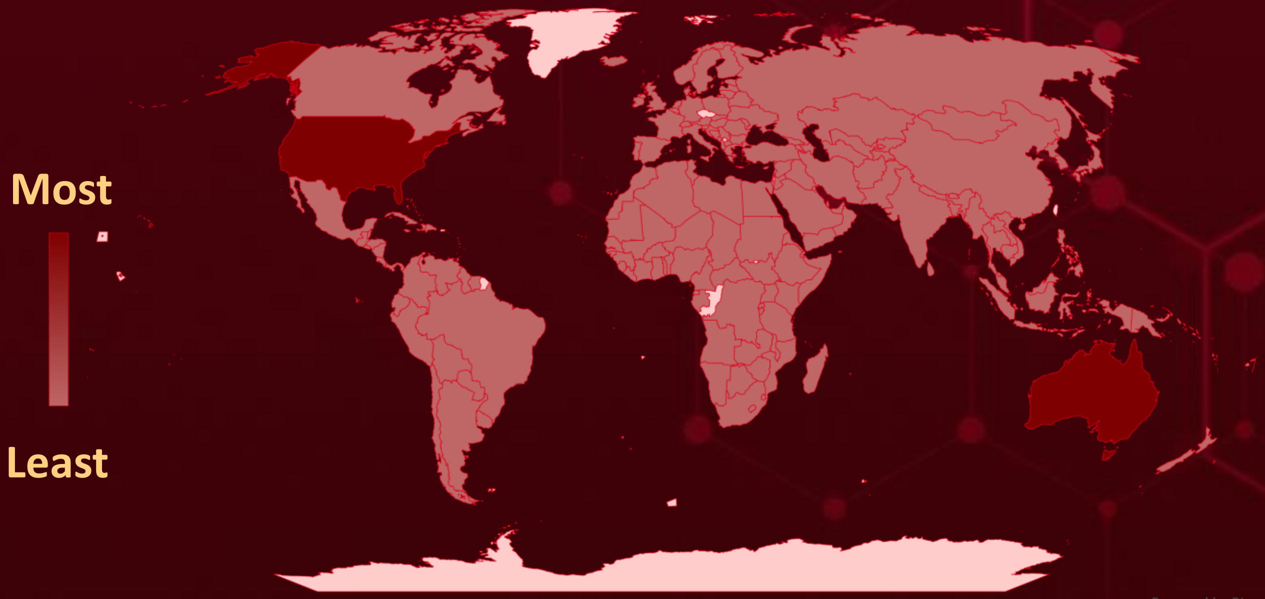
Sync-Scheduler

Infostealer, developed in C++, has emerged as a significant threat, hidden within Office document files

Threat Distribution



Targeted Countries

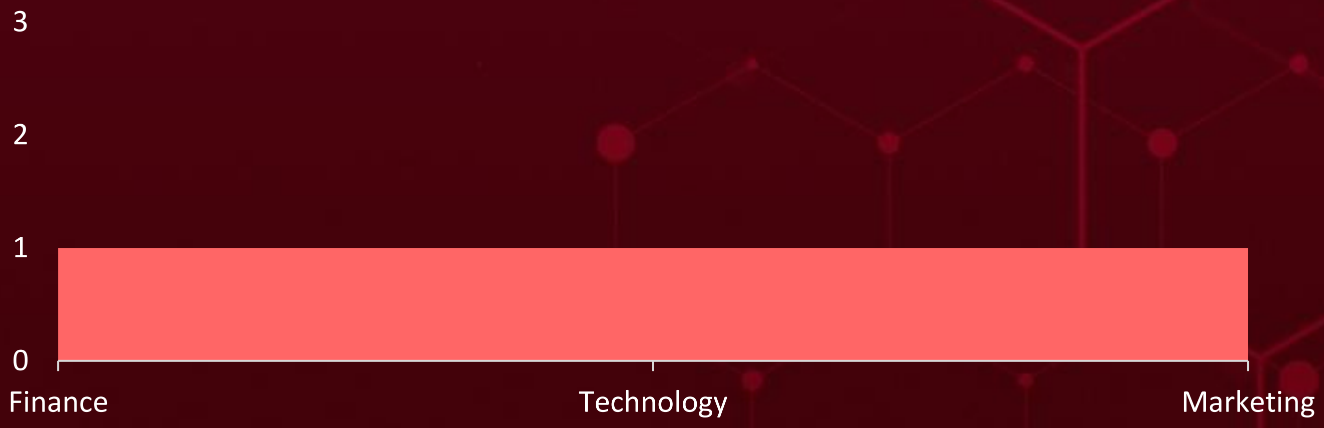


Powered by Bing

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

	Countries
■	Australia
■	United States
□	Norway
□	Afghanistan
□	South Sudan
□	Andorra
□	Monaco
□	Angola
□	Saint Lucia
□	Antigua and Barbuda
□	Trinidad and Tobago
□	Argentina
□	Mali
□	Armenia
□	Nepal
□	Albania
□	Philippines
□	Austria
□	Sierra Leone
□	Azerbaijan
□	Switzerland
□	Bahamas
□	Algeria
□	Bahrain
□	Madagascar
□	Bangladesh
□	Mauritius
□	Barbados
□	Mozambique
□	Belarus
□	Niger
□	Belgium
□	Panama
□	Belize
□	Romania
□	Benin
□	Saudi Arabia
□	Bhutan
□	Solomon Islands
□	Bolivia
□	State of Palestine
□	Bosnia and Herzegovina
□	Thailand
□	Botswana
□	Tuvalu
□	Brazil
□	Vietnam
□	Brunei
□	Lithuania
□	Bulgaria
□	Malaysia
□	Burkina Faso
□	Marshall Islands
□	Burundi
□	Micronesia
□	Cabo Verde
□	Montenegro
□	Cambodia
□	Namibia
□	Cameroon
□	New Zealand
□	Canada
□	North Korea
□	Central African Republic
□	Pakistan
□	Chad
□	Paraguay
□	Chile
□	Portugal
□	China
□	Rwanda
□	Colombia
□	San Marino
□	Comoros
□	Serbia
□	Congo
□	Slovakia
□	Costa Rica
□	South Africa
□	Côte d'Ivoire
□	Sri Lanka
□	Croatia
□	Suriname
□	Cuba
□	Tajikistan
□	Cyprus
□	Togo
□	Czech Republic (Czechia)
□	Turkey
□	Denmark
□	Ukraine
□	Djibouti
□	Vanuatu
□	Dominica

Targeted Industries



TOP MITRE ATT&CK TTPs

T1566 Phishing	**T1059** Command and Scripting Interpreter	**T1036** Masquerading	**T1055** Process Injection	**T1204** User Execution
T1218 System Binary Proxy Execution	**T1588.006** Vulnerabilities	**T1083** File and Directory Discovery	**T1574.002** DLL Side-Loading	**T1071.001** Web Protocols
T1041 Exfiltration Over C2 Channel	**T1204.002** Malicious File	**T1588** Obtain Capabilities	**T1588.005** Exploits	**T1195** Supply Chain Compromise
T1082 System Information Discovery	**T1027** Obfuscated Files or Information	**T1555** Credentials from Password Stores	**T1068** Exploitation for Privilege Escalation	**T1203** Exploitation for Client Execution

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Atomic Stealer	Atomic Stealer, also known as AMOS (Atomic macOS Stealer), is a malicious program that targets macOS devices. It's classified as a stealer, a type of malware designed to extract and steal sensitive information from infected computers.	Malicious ads, fake software updates	-
TYPE		IMPACT	AFFECTED PRODUCTS
Stealer		Data Theft	macOS
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	ffaaf40512080e2edbee3c284fe9c01826edb82d27a5a0982ffe912f73a6e3c6, ff53c5f0e03f272a4df3feda0f870e33172d05b023930d59dbbe6175ed4ac11f, fec965095a51547e3629ee78753df064b00ce51dab8c491a177d016ff455e76a, fec92daa9859a9a84569934c652e01fc132bb25685b2d9e06fc17f6d11ede3ea, fce6b9ad6179b829bdc3ff75b17ac02734a2d9ddcaf93438139df2719a8d48f4		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Realst stealer	Realst stealer malware is a type of information-stealer malware that targets macOS devices. It is designed to steal a variety of sensitive information from infected computers.	Disguised as fake blockchain games	-
TYPE		IMPACT	AFFECTED PRODUCTS
Stealer		Data Theft	-
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	6574315524dde9a8c47d7f1ba411fb5fa6421721c24a629c72ce8cd32c0d1b34, 6344fb8cd00b8e94671144c2877dbb337e8e98648f43e7954fa3fa01b4ae3357		

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

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVEs</th></tr>
<tr><td>UNAPIMON</td><td rowspan="6">UNAPIMON is a straightforward DLL malware written in C++, designed to prevent monitoring of child processes. It achieves this by hooking into the CreateProcessW function and unhooking critical API functions in child processes, thereby allowing malicious activities to go undetected.</td><td>Phishing</td><td>-</td></tr>
<tr><td>TYPE</td><td>IMPACT</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>Loader</td><td rowspan="3">Evasion of Security Measures and Financial loss</td><td>Windows and VMware</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td>PATCH LINK</td></tr>
<tr><td>Earth Freybug</td><td>-</td></tr>
<tr><td>IOC TYPE</td><td colspan="3">VALUE</td></tr>
<tr><td>SHA256</td><td colspan="3">62ad0407a9cce34afb428dee972292d2aa23c78cbc1a44627cb2e8b945195bc2</td></tr>
</table>

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVEs</th></tr>
<tr><td>SYNC-SCHEDULER</td><td rowspan="5">The Sync-Scheduler Infostealer, developed in C++, has emerged as a significant threat, hidden within Office document files. This malicious software boasts sophisticated anti-analysis features, allowing it to swiftly terminate operations upon detecting any analytical environment.</td><td>-</td><td>-</td></tr>
<tr><td>TYPE</td><td>IMPACT</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>Stealer</td><td rowspan="3">Data Theft</td><td>-</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td>PATCH LINK</td></tr>
<tr><td>-</td><td>-</td></tr>
<tr><td>IOC TYPE</td><td colspan="3">VALUE</td></tr>
<tr><td>URL</td><td colspan="3">http[:]//syncscheduler[.]com/r3diRecT/redirector/proxy[.]php</td></tr>
<tr><td>IPv4</td><td colspan="3">146[.]70[.]157[.]120</td></tr>
<tr><td>SHA256</td><td colspan="3">2027a5acbfea586f2d814fb57a97dcfce6c9d85c2a18a0df40811006d74aa7e3,
203d60fe1ebbfafc835e082774ee56088273d9455fb12ac1de2c1be410cceeec,
6e4a4d25c2e8f5bacc7e0f1c8b538b8ad61571266f271cfdfc14725b3be02613,
316e01b962bf844c3483fce26ff3b2d188338034b1dbd41f15767b06c6e56041</td></tr>
</table>

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

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVEs</th></tr>
<tr><td>Agent Tesla</td><td rowspan="5">The Agent Tesla malware, classified as a remote access trojan (RAT), demonstrates remarkable proficiency in infiltrating systems to extract sensitive information like keystrokes and login credentials from web browsers and email clients.</td><td>Phishing</td><td>-</td></tr>
<tr><td><b>TYPE</b></td><td><b>IMPACT</b></td><td><b>AFFECTED PRODUCTS</b></td></tr>
<tr><td>RAT</td><td rowspan="3">Data Theft</td><td>-</td></tr>
<tr><td><b>ASSOCIATED ACTOR</b></td><td><b>PATCH LINK</b></td></tr>
<tr><td>-</td><td>-</td></tr>
<tr><td><b>IOC TYPE</b></td><td colspan="3"><b>VALUE</b></td></tr>
<tr><td>SHA256</td><td colspan="3">8ba55cc754638714764780542eefd629c55703ecf63ae20d5eb65b8c14d3e645,
87709f72683c5ffc166f348212b37aadb7943b5653419f2f0edf694fb50f1878,
691761d401a6650872d724c30b7ef5972e3792e9a2ba88fdca98b4312fb318d8</td></tr>
</table>

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVEs</th></tr>
<tr><td>RotBot</td><td rowspan="5">RotBot malware is a variant of the QuasarRAT client, a malicious remote access tool (RAT) designed for stealing information and granting remote access to attackers.</td><td>Phishing</td><td>-</td></tr>
<tr><td><b>TYPE</b></td><td><b>IMPACT</b></td><td><b>AFFECTED PRODUCTS</b></td></tr>
<tr><td>RAT</td><td rowspan="3">Data Theft and Remote Access</td><td>Windows</td></tr>
<tr><td><b>ASSOCIATED ACTOR</b></td><td><b>PATCH LINK</b></td></tr>
<tr><td>CoralRaider</td><td>-</td></tr>
<tr><td><b>IOC TYPE</b></td><td colspan="3"><b>VALUE</b></td></tr>
<tr><td>SHA256</td><td colspan="3">e9e9d5ab6307a9ce98b1b3450def66df7a00d9dc5af613434af8d9b9cb3f2a0f,
0790bb235f27fa3843f086dbdaac314c2c1b857e3b2b94c2777578765a7894a0,
28f827afd3bafa1e39526f84f8e1271c15d073c9d049a9bc8d03048c455dd33f,
d60bb69da27799d822608902c59373611c18920c77887de7489d289ebf2bd53e,
de8a5d881cfc913a24c846bec8c13f3ad98e60fde881352845d928015bc6a5a4</td></tr>
</table>

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
XClient stealer	XClient is a dangerous stealer malware targeting Windows users. It can steal a wide range of information including login credentials, browser data, social media information, financial data, and even cryptocurrency holdings. XClient spreads through phishing campaigns and can have severe consequences for victims, leading to identity theft, privacy breaches, and financial losses.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Stealer		Data Theft and Financial loss	Windows
ASSOCIATED ACTOR			**PATCH LINK**
CoralRaider			-

IOC TYPE	VALUE
SHA256	4dc9fe269cd668894c7ea4dd797cba1d2a8df565e9bdd814e969247c94b39643

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
CVE-2024-3094	❌	XZ Utils or liblzma Versions 5.6.0,5.6.1 Fedora : Versions 40, 41(Rawhide)	-
	ZERO-DAY		
	❌	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:tukaani:xz-utils:*:*:*:*:*:*:*	-
XZ Utils Embedded Malicious code	❌		
	CWE ID	ASSOCIATED TTPs	WORKAROUND
	CWE-506	T1195.001 Supply Chain Compromise: Compromise Software Dependencies and Development Tools	Downgrade XZ Utils to a stable version before 5.6.0, such as XZ Utils 5.4.6

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-2879	⊗	LayerSlider Version 7.9.11 – 7.10.0	-
	ZERO-DAY		
	⊗	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:a:layerslider_plugin:layerslider_plugin:7.9.11:*:*:*:*:*:*:* cpe:2.3:a:layerslider_plugin:layerslider_plugin:7.10.0:*:*:*:*:*:*:*	-
WordPress LayerSlider SQL Injection Vulnerability	⊗		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-89	T1190 : Exploit Public-Facing Application, 1505 : Server Software Component	https://www.wordfence.com/threatintel/vulnerabilities/wordpressplugins/layerslider/layerslider-7911-7100-unauthenticated-sql-injection

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
Earth Freybug	China	-	Worldwide
	MOTIVE		
	Espionage and Financial gain		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	UNAPIMON	Windows and VMware
TTPs			
TA0004: Privilege Escalation, TA0043: Reconnaissance, T1574: Hijack Execution Flow, T1106: Native API, T1053.005: Scheduled Task, T1053: Scheduled Task/Job, T1592: Gather Victim Host Information, T1574.002: DLL Side-Loading, T1190: Exploit Public-Facing Application, T1059.001: PowerShell, T1059: Command and Scripting Interpreter, T1082: System Information Discovery, T1574.006: Dynamic Linker Hijacking, T1036: Masquerading, T1547.001: Registry Run Keys /Startup Folder, T1547: Boot or Logon Autostart Execution, T1489: Service Stop			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
CoralRaider	Vietnam	Social media accounts (personal and business), financial information, credentials	Asia
	MOTIVE		
	Financial gain		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	RotBot, XClient stealer	Windows
TTPs			
TA0001: Initial Access, TA0002: Execution, TA0040: Impact, TA0003: Persistence, TA0005: Defense Evasion, TA0006: Credential Access, TA0009: Collection, TA0011: Command and Control, TA0010: Exfiltration, T1566: Phishing, T1204: User Execution, T1027: Obfuscated Files or Information, T1140: Deobfuscate/Decode Files or Information, T1059.001: PowerShell, T1059: Command and Scripting Interpreter, T1547.001: Registry Run Keys / Startup Folder, T1547: Boot or Logon Autostart Execution, T1036: Masquerading, T1564: Hide Artifacts, T1555: Credentials from Password Stores, T1539: Steal Web Session Cookie, T1083: File and Directory Discovery, T1518: Software Discovery, T1113: Screen Capture, T1005: Data from Local System, T1071: Application Layer Protocol, T1090: Proxy, T1041: Exfiltration Over C2 Channel, T1137: Office Application Startup			

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **two exploited vulnerabilities** and block the indicators related to the threat actors **Earth Freybug, CoralRaider** and malware **Atomic Stealer, Realst stealer, UNAPIMON, SYNC-SCHEDULER, Agent Tesla, RotBot, XClient stealer.**

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

- Running a Scan to discover the assets impacted by the **two exploited vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **Earth Freybug, CoralRaider** and malware **Atomic Stealer, SYNC-SCHEDULER, Agent Tesla** in Breach and Attack Simulation(BAS).

Threat Advisories

XZ Utils Backdoored, A Supply Chain Nightmare

Stealer Malwares Delivered Through Malicious Ads and Bogus Websites

Unveiling Earth Freybug's New TTPs Adoption with UNAPIMON

Sync-Scheduler: The Premier Document Stealer

LayerSlider WordPress Plugin Flaw Impacts Over 1 Million Sites

Tracing the Footprints of Agent Tesla's Conspirators

Over 170K Users Hit by Fake Python Infrastructure

CoralRaider Targeting Social Media Accounts Across Asia for Financial Gain

Ivanti Addresses Flaws Leading to DoS Attacks and Code Execution

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
Atomic Stealer	SHA256	4cb531bd83a1ebf4061c98f799cdc2922059aff1a49939d427054a556e89f464, be634e786d5d01b91f46efd63e8d71f79b423bfb2d23459e5060a9532b4dcc7b, 5b5ffb0d2fb1f2de5147ec270d60a3ac3f02c36153c943fbfe2a3427ce39d13d,
	IPv4	194.169.175[.]117
XClient Stealer	SHA256	4dc9fe269cd668894c7ea4dd797cba1d2a8df565e9bdd814e969247c94b39643
Rotbot	SHA256	e9e9d5ab6307a9ce98b1b3450def66df7a00d9dc5af613434af8d9b9cb3f2a0f, 0790bb235f27fa3843f086dbdaac314c2c1b857e3b2b94c2777578765a7894a0, 28f827afd3bafa1e39526f84f8e1271c15d073c9d049a9bc8d03048c455dd33f, d60bb69da27799d822608902c59373611c18920c77887de7489d289ebf2bd53e, de8a5d881cfc913a24c846bec8c13f3ad98e60fde881352845d928015bc6a5a4, 020d3d03ede3a80f1287ab58053f30ae7bfaf916ab0b1fc927f07b4b9d1f5c34, 1db18d89a636f9d9307e51798c0545664fae38711a2a72139d62c7dbd6f17fe3, 93c747fff1ec919d981aa4ad2e42cda3d76c9d0634707a62066dbadda1653d1c,

Attack Name	TYPE	VALUE
Realst stealer	SHA256	6574315524dde9a8c47d7f1ba411fb5fa6421721c24a629c72ce8cd32c0d1b34, 6344fb8cd00b8e94671144c2877dbb337e8e98648f43e7954fa3fa01b4ae3357
SYNC-SCHEDULER stealer	URL	http[:]//syncscheduler[.]com/r3diRecT/redirector/proxy[.]php
	SHA256	2027a5acbfea586f2d814fb57a97dcfce6c9d85c2a18a0df40811006d74aa7e3, 203d60fe1ebbfafc835e082774ee56088273d9455fb12ac1de2c1be410cceeec, 6e4a4d25c2e8f5bacc7e0f1c8b538b8ad61571266f271cfdfc14725b3be02613, 316e01b962bf844c3483fce26ff3b2d188338034b1dbd41f15767b06c6e56041
	IPv4	146[.]70[.]157[.]120
UNAPIMON	SHA256	62ad0407a9cce34afb428dee972292d2aa23c78cbc1a44627cb2e8b945195bc2
Agent Tesla	SHA256	8ba55cc754638714764780542eefd629c55703ecf63ae20d5eb65b8c14d3e645, 87709f72683c5ffc166f348212b37aadb7943b5653419f2f0edf694fb50f1878, 691761d401a6650872d724c30b7ef5972e3792e9a2ba88fdca98b4312fb318d8

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

April 8, 2024 • 6:30 AM

More at www.hivepro.com