

Date of Publication
December 9, 2024



HiveForce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities and Actors

2 to 8 December 2024

Table Of Contents

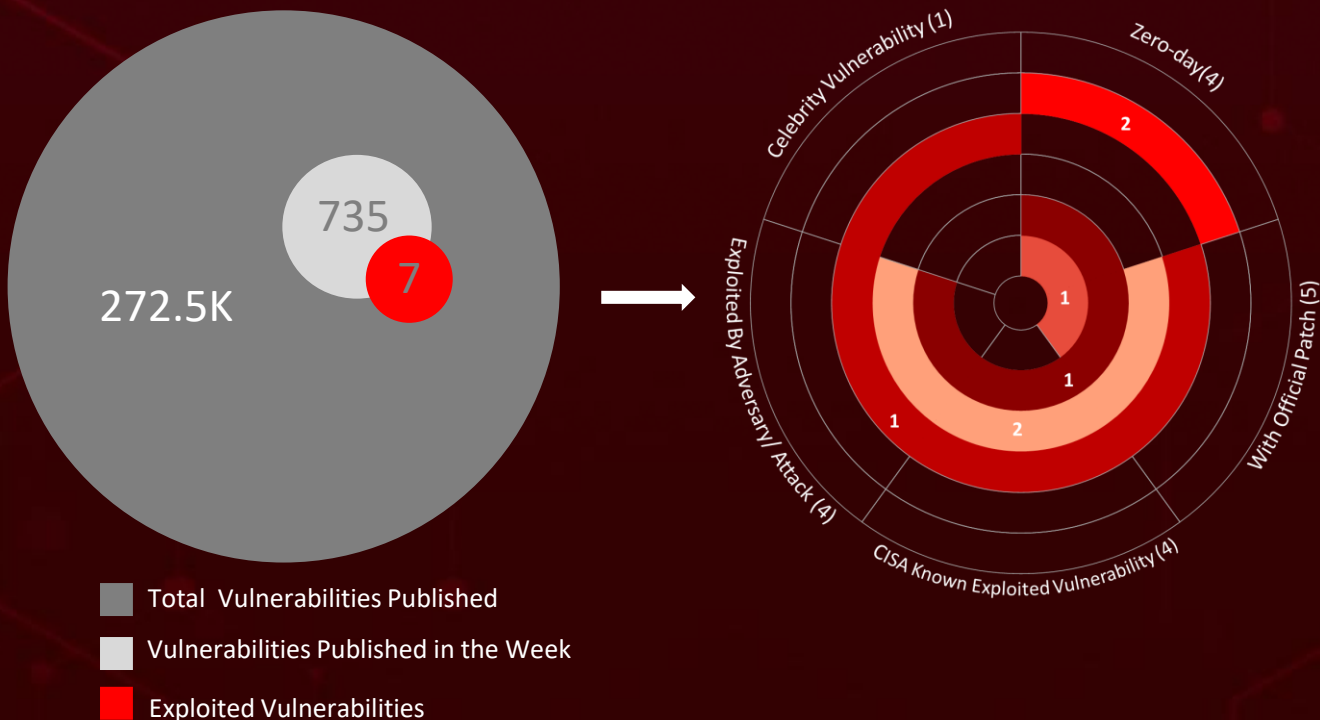
<u>Summary</u>	03
<u>High Level Statistics</u>	04
<u>Insights</u>	05
<u>Targeted Countries</u>	06
<u>Targeted Industries</u>	07
<u>Top MITRE ATT&CK TTPs</u>	07
<u>Attacks Executed</u>	08
<u>Vulnerabilities Exploited</u>	12
<u>Adversaries in Action</u>	16
<u>Recommendations</u>	19
<u>Threat Advisories</u>	20
<u>Appendix</u>	21
<u>What Next?</u>	23

Summary

HiveForce Labs has recently made significant advancements in identifying cybersecurity threats. Over the past week, detected **seven** attacks, reported **seven** vulnerabilities, and identified **three** active adversaries. These findings underscore the relentless and escalating danger of cyber intrusions.

Additionally, **SmokeLoader** malware targets Taiwanese organizations, acting as both an initial access vector and an operational threat by fetching plugins from its C2 server.

Furthermore, this week, **Venom Spider** offers Malware-as-a-Service (MaaS) tools, with campaigns between August and October 2024 deploying RevC2 and Venom Loader to steal sensitive data and enable remote code execution. Zyxel firewalls face a critical **CVE-2024-11667** vulnerability, exploited to deploy **Helldown** ransomware via directory traversal in the web interface. These rising threats pose significant and immediate dangers to users worldwide.



High Level Statistics

7

Attacks
Executed

7

Vulnerabilities
Exploited

3

Adversaries in
Action

- [SmokeLoader](#)
- [Helldown](#)
- [NetSupport RAT](#)
- [BurnsRAT](#)
- [RevC2](#)
- [Venom](#)
- [Elpaco](#)

- [CVE-2017-0199](#)
- [CVE-2017-11882](#)
- [CVE-2024-11667](#)
- [CVE-2024-45841](#)
- [CVE-2024-47133](#)
- [CVE-2024-52564](#)
- [CVE-2020-1472](#)

- [TA569](#)
- [Kimsuky](#)
- [Venom Spider](#)



Insights

Horns&Hooves campaign linked with **TA569**, targets Russian users with JScript files deploying NetSupport RAT.

Zyxel firewalls' critical **CVE-2024-11667** vulnerability is being exploited to deploy Helldown ransomware, compromising systems.

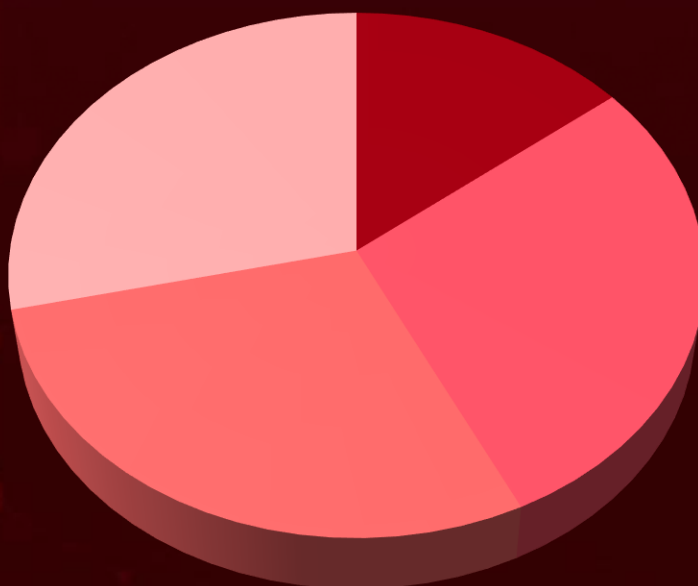
Hackers are exploiting **I-O Data router zero-day flaws** (CVE-2024-45841, CVE-2024-47133, CVE-2024-52564) to hijack devices, change settings, and disable firewalls.

Elpaco ransomware, a Mimic variant, targets organizations worldwide using RDP brute-force attacks and the Zerologon vulnerability (CVE-2020-1472) for privilege escalation.

Venom Spider, offers Malware-as-a-Service (MaaS) tools, with recent campaigns deploying RevC2 and Venom Loader to steal sensitive data and enable remote code execution.

A campaign targeting Taiwan uses **SmokeLoader** malware to fetch plugins from its C2 server, acting as both an access vector and threat.

Threat Distribution



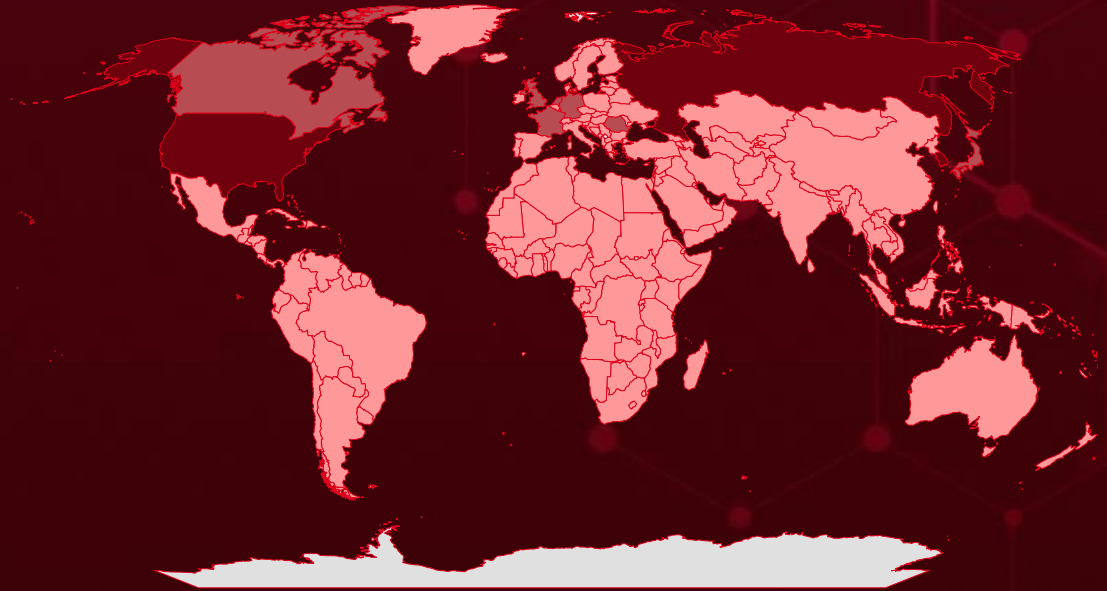
■ Backdoor ■ RAT ■ Ransomware ■ Loader



Targeted Countries

Most

Least



Powered by Bing

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

Countries	Countries	Countries	Countries
South Korea	Belize	Cameroon	Cuba
United States	South Sudan	Lithuania	San Marino
Russia	Benin	Albania	Cyprus
Netherlands	Tonga	Malaysia	Serbia
France	Bhutan	Central African Republic	Czech Republic
Romania	Madagascar	Marshall Islands	Slovakia
Canada	Bolivia	Chad	Denmark
Germany	Mauritius	Micronesia	South Africa
Japan	Bosnia and Herzegovina	Chile	Djibouti
United Kingdom	Mozambique	Montenegro	Sri Lanka
Philippines	Botswana	China	Dominica
Mali	Niger	Namibia	Suriname
Switzerland	Brazil	Colombia	Dominican Republic
Bahamas	Panama	New Zealand	Taiwan
Nepal	Brunei	Comoros	DR Congo
Bahrain	Armenia	North Korea	Timor-Leste
Sierra Leone	Bulgaria	Congo	Ecuador
Bangladesh	Saudi Arabia	Pakistan	Tunisia
Azerbaijan	Burkina Faso	Costa Rica	Egypt
Barbados	Solomon Islands	Paraguay	Uganda
Monaco	Burundi	Côte d'Ivoire	El Salvador
Belarus	State of Palestine	Portugal	Liechtenstein
Norway	Cabo Verde	Croatia	Equatorial Guinea
Belgium	Cambodia	Rwanda	Luxembourg
Saint Lucia	Maldives	Eswatini	Eritrea
Mexico	Fiji	Malta	Malawi
Finland		Ethiopia	Estonia
		Mauritania	

Targeted Industries



TOP MITRE ATT&CK TTPs

T1566

Phishing

T1566.001

Spearphishing
Attachment

T1059

Command and
Scripting
Interpreter

T1588

Obtain
Capabilities

T1574

Hijack
Execution
Flow

T1041

Exfiltration
Over C2
Channel

T1027

Obfuscated
Files or
Information

T1083

File and
Directory
Discovery

T1140

Deobfuscate/
Decode Files
or Information

T1059.001

PowerShell

T1059.005

Visual Basic

T1204

User Execution

T1204.001

Malicious Link

T1036

Masquerading

T1190

Exploit Public-
Facing
Application

T1547

Boot or Logon
Autostart
Execution

T1588.006

Vulnerabilities

T1204.002

Malicious File

T1071.001

Web Protocols

T1068

Exploitation for
Privilege
Escalation

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>SmokeLoader</u> (aka <u>Dofail</u> , <u>Sharik</u> , <u>Smoke</u>)	SmokeLoader can be used to drop other malware on infected systems, but operators can choose additional modules that allow for information-stealing capabilities.	Phishing	CVE-2017-0199 CVE-2017-11882
		IMPACT	AFFECTED PRODUCTS
TYPE		Data Theft, System compromised and Espionage	Microsoft Office
Loader			PATCH LINK
ASSOCIATED ACTOR			https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2017-0199 ;
-			https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2017-11882
IOC TYPE	VALUE		
SHA256	f7544f07b4468e38e36607b5ac5b3835eac1487e7d16dd52ca882b3d021c19b6		

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>Helldown</u>	Helldown ransomware utilizes a double extortion approach, encrypting data while simultaneously threatening to expose sensitive information unless the ransom is paid. Although Helldown shares code similarities with LockBit 3.0, it remains a distinct variant and is actively being developed.	Exploitation of vulnerabilities in Zyxel	CVE-2024-11667
TYPE		IMPACT	AFFECTED PRODUCT
Ransomware			
ASSOCIATED ACTOR			
-	Financial Loss, Data Breaches and Reputation Damage	Zyxel Multiple Firewalls	PATCH LINK
			https://www.zyxel.com/us/en-us/support/download
IOC TYPE	VALUE		
SHA256	0bfe25de8c46834e9a7c216f99057d855e272eafafdfef98a6012cecbdbcfab, 7cd7c04c62d2a8b4697ceebbe7dd95c910d687e4a6989c1d839117e55c1cafd7, 7731d73e048a351205615821b90ed4f2507abc65acf4d6fe30ecdb211f0b0872, 3e3fad9888856ce195c9c239ad014074f687ba288c78ef26660be93ddd97289e, 2621c5c7e1c12560c6062fdf2eeeb815de4ce3856376022a1a9f8421b4bae8e1		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>NetSupport RAT</u>	NetSupport RAT (Remote Access Trojan) is a legitimate remote administration tool often exploited for malicious purposes. Cybercriminals use it to gain control over compromised systems, enabling them to execute commands, transfer files, and monitor activity.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
RAT			
ASSOCIATED ACTOR			
TA569	Remote control and System compromise	Windows	PATCH LINK
			-
IOC TYPE	VALUE		
SHA256	F4e2f28169e0c88b2551b6f1d63f8ba513feb15beacc43a82f626b93d673f56d		
Domains	xoomep1[.]com, xoomep2[.]com, labudanka1[.]com, labudanka2[.]com		

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>BurnsRAT</u>	BurnsRAT is a malicious Remote Access Trojan (RAT) that allows attackers to control compromised systems remotely. It supports executing commands, transferring files, and interacting with desktops via Remote Desktop Protocol (RDP).	Phishing	-
		IMPACT	AFFECTED PRODUCTS
		Remote control and System compromise	Windows
			PATCH LINK
			-
ASSOCIATED ACTOR	TA569		
IOC TYPE	VALUE		
URLs	hxxp://193[.]42[.]32[.]138/api/, hxxp://87[.]251[.]67[.]51/api/		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>RevC2</u>	RevC2 is a recently discovered information-stealing backdoor malware that leverages WebSockets to communicate with its command-and-control (C2) server. It is capable of stealing cookies and passwords, proxying network traffic, and enabling remote code execution (RCE).	Phishing	-
		IMPACT	AFFECTED PRODUCTS
		Data theft and Data exfiltration	-
			PATCH LINK
			-
ASSOCIATED ACTOR	Venom Spider		
IOC TYPE	VALUE		
SHA256	cf45f68219c4a105fffc212895312ca9dc7f4abe37306d2f3b0f098fb6975ec7, 153cd5a005b553927a94cc7759a8909bd1b351407d8d036a1bf5fcf9ee83192e		
URLs	ws[:]//208[.]85[.]17[.]52[:]8082, ws[:]//nopsec[.]org[:]8082/		




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>Venom</u>	Venom Loader is a sophisticated malware loader designed to deliver and execute additional malicious payloads on compromised systems. It's part of the Venom Spider malware-as-a-service (MaaS) toolkit, a collection of cybercriminal tools offered by threat actors to other cybercriminals.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Loader			
ASSOCIATED ACTOR			
Venom Spider		Data theft and Loads other malware	-
		PATCH LINK	-
IOC TYPE	VALUE		
URL	hxxp[:]//170[.]75[.]168[.]151/%computername%/aaa		
SHA256	f93134f9b4ee2beb1998d8ea94e3da824e7d71f19dfb3ce566e8e9da65b1d7a2		




NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>Elpaco (aka ELPACO-team)</u>	Elpaco is a new variant of the Mimic ransomware family. Employs advanced tactics like abusing legitimate tools and exploiting vulnerabilities. It's a powerful and evolving threat that uses various techniques to compromise systems and encrypt files.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware			
ASSOCIATED ACTOR			
Venom Spider		Financial Loss, Data Breaches and Reputation Damage	-
		PATCH LINK	-
IOC TYPE	VALUE		
SHA256	9f6a696876fee8b811db8889bf4933262f4472ad41daea215d2e39bd537cf32f, e160d7d21c917344f010e58dcfc1e19bec6297c294647a06ce60efc7420d3b13		




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-2017-0199		Microsoft Office and WordPad	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:microsoft:office:*:*:*:*:*:*	SmokeLoader
Microsoft Office and WordPad Remote Code Execution Vulnerability		cpe:2.3:o:microsoft:windows:*:*:*:*:*	
	CWE ID	ASSOCIATED TTPs	
	CWE-20	T1059: Command and Scripting Interpreter, T1204 : User Execution	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2017-0199


CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR		
CVE-2017-11882		Microsoft Office: 2007 SP3 2010 SP2 2013 SP1 2016	-		
	ZERO-DAY				
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE		
NAME	CISA KEY	cpe:2.3:a:microsoft:office:2007:sp3:*:*:*:*:*	SmokeLoader		
Microsoft Office Memory Corruption Vulnerability		CWE ID		ASSOCIATED TTPs	PATCH LINK
	CWE-119	T1203 : Exploitation for Client Execution, T1059 : Command and Scripting Interpreter, T1204 : User Execution		https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11882	


CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-45841</u>		UD-LT1 firmware Ver.2.1.8 and earlier UD-LT1/EX firmware Ver.2.1.8 and earlier	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:h:i-o_data:ud-lt1:*:*:*:*:*:* cpe:2.3:h:i-o_data:ud-lt1_ex:*:*:*:*:*:*	
I-O DATA DEVICE UD-LT1/EX Incorrect Permission Assignment for Critical Resource Vulnerability			-
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-732	T1059: Command and Scripting Interpreter, T1068 : Exploitation for Privilege Escalation	-


CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-47133</u>		UD-LT1 firmware Ver.2.1.8 and earlier UD-LT1/EX firmware Ver.2.1.8 and earlier	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:h:i-o_data:ud-lt1:*:*:*:*:*:* cpe:2.3:h:i-o_data:ud-lt1_ex:*:*:*:*:*:*	
I-O DATA DEVICE UD-LT1/EX OS Command Injection Vulnerability			-
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter, T1068 : Exploitation for Privilege Escalation	-

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-52564</u>		UD-LT1 firmware Ver.2.1.8 and earlier UD-LT1/EX firmware Ver.2.1.8 and earlier	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:h:i-o_data:ud-lt1:*:*:*:*:*:* cpe:2.3:h:i-o_data:ud-lt1_ex:*:*:*:*:*:*	-
I-O DATA DEVICE UD-LT1/EX Inclusion of Undocumented Features Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-1242	T1059: Command and Scripting Interpreter	https://www.iodata.jp/support/information/2024/11_ud-lt1/

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 TA569	-	Retailers, Service Businesses, Private Users	Russia
	MOTIVE Information theft and espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	-	NetSupport RAT, BurnsRAT	Windows
TTPs			
TA0011: Command and Control; TA0003: Persistence; TA0004: TTPs: Privilege Escalation; TA0001: Initial Access; T1059: Command and Scripting Interpreter; T1574.002: DLL Side-Loading; TA0042: Resource Development; T1566.001: Spearphishing Attachment; TA0002: Execution; TA0005: Defense Evasion; TA0009: Collection; T1566: Phishing; T1574: Hijack Execution Flow; T1041: Exfiltration Over C2 Channel; T1218.005: Mshta; T1584: Compromise Infrastructure T1059.007: JavaScript; T1140: Deobfuscate/Decode Files or Information; T1059.001: PowerShell; T1027: Obfuscated Files or Information; T1059.005: Visual Basic; T1036: Masquerading; T1204: User Execution; T1123: Audio Capture; T1218: System Binary Proxy Execution; T1059.003: Windows Command Shell; T1204.002: Malicious File			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <p><u>Kimsuky (aka Sparkling Pisces, Velvet Chollima, Thallium, Black Banshee, SharpTongue, ITG16, TA406, TA427, APT 43, ARCHIPELAGO, Emerald Sleet, KTA082, UAT-5394)</u></p>	North Korea	-	Japan, South Korea, US
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
-	-	-	
TTPs			
<p>TA0042: Resource Development; TA0043: Reconnaissance; TA0001: Initial Access; TA0002: Execution; TA0005: Defense Evasion; TA0011: Command and Control; T1566: Phishing; T1566.001: Spearphishing Attachment; T1566.002: Spearphishing Link; T1568: Dynamic Resolution; T1588: Obtain Capabilities; T1588.002: Tool; T1589: Gather Victim Identity Information; T1589.001: Credentials; T1071: Application Layer Protocol; T1204: User Execution; T1036: Masquerading</p>			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <p><u>Venom Spider (aka GOLDEN CHICKENS)</u></p>	Russia	-	Worldwide
	MOTIVE		
	Financial gain		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	-	RevC2, Venom Loader	-

TTPs

TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys /Startup Folder; T1140: Deobfuscate/Decode Files or Information; T1574: Hijack Execution Flow; T1574.002: DLL Side-Loading; T1539: Steal Web Session Cookie; T1555: Credentials from Password Stores; T1113: Screen Capture; T1090: Proxy; T1059: Command and Scripting Interpreter; T1571: Non-Standard Port; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1041: Exfiltration Over C2 Channel

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 **TA569, Kimsuky, Venom Spider** and malware **SmokeLoader, Helldown, NetSupport, BurnsRAT, RevC2, Venom, Elpaco**.

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 **seven exploited vulnerabilities**.

Testing the efficacy of their security controls by simulating the attacks related to the threat actor **TA569, Kimsuky, Venom Spider** and malware **SmokeLoader, NetSupport, RevC2, Venom, Helldown, Elpaco** in Breach and Attack Simulation(BAS).

Threat Advisories

[SmokeLoader Strikes Taiwan: Unveiling a Modular Malware's Sophisticated Attack Chain](#)

[Zyxel Firewall Flaw Exploited to Unleash Helldown Ransomware Havoc](#)

[NetSupport RAT Exploited in Horns&Hooves Cyberattack](#)

[Kimsuky's Evolving Phishing Playbook: URL Tactics and Global Deception](#)

[Venom Spider's Victim-Specific Malware Tactics Decoded](#)

[Mimic's Successor Elpaco Ransomware Enhances Customization Features](#)

[Zero-Day Vulnerabilities in I-O Data Routers Expose Critical Security Risks](#)

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)

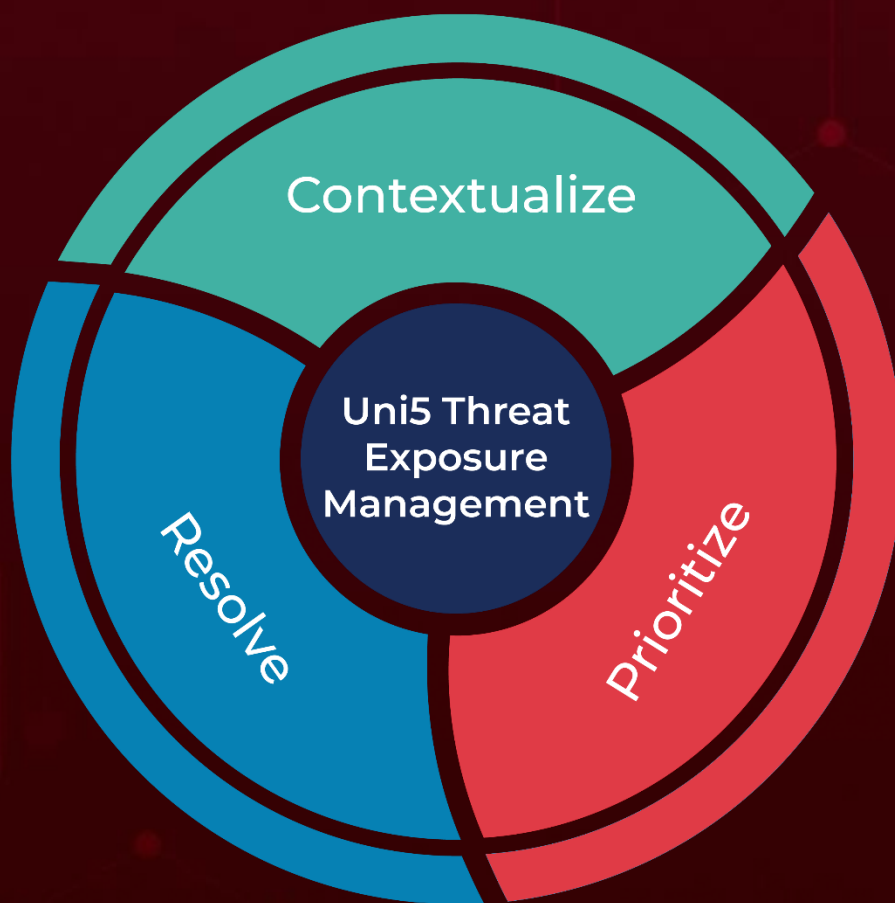
Attack Name	TYPE	VALUE
<u>SmokeLoader</u>	SHA256	f7544f07b4468e38e36607b5ac5b3835eac1487e7d16dd52ca882b3d021c19b6
<u>Helldown Ransomware</u>	SHA256	0bfe25de8c46834e9a7c216f99057d855e272eafafdfef98a6012cecbbdcfab, 7cd7c04c62d2a8b4697ceebbe7dd95c910d687e4a6989c1d839117e55c1cafd7, 7731d73e048a351205615821b90ed4f2507abc65acf4d6fe30ecdb211f0b0872, 3e3fad9888856ce195c9c239ad014074f687ba288c78ef26660be93dd97289e, 2621c5c7e1c12560c6062fdf2eeeb815de4ce3856376022a1a9f8421b4bae8e1, 47635e2cf9d41cab4b73f2a37e6a59a7de29428b75a7b4481205aee4330d4d19, cb48e4298b216ae532cfd3c89c8f2cbd1e32bb402866d2c81682c6671aa4f8ea, 67aea3de7ab23b72e02347cbf6514f28fb726d313e62934b5de6d154215ee733, 2b15e09b98bc2835a4430c4560d3f5b25011141c9efa4331f66e9a707e2a23c0, 6ef9a0b6301d737763f6c59ae6d5b3be4cf38941a69517be0f069d0a35f394dd, 9ab19741ac36e198fb2fd912620bf320aa7fdeeeb8d4a9e956f3eb3d2092c92c, ccd78d3eba6c53959835c6407d81262d3094e8d06bf2712fefa4b04baadd4bfe
<u>NetSupport RAT</u>	Domains	xoomep1[.]com, xoomep2[.]com,

Attack Name	TYPE	VALUE
<u>NetSupport RAT</u>	Domains	labudanka1[.]com, labudanka2[.]com, gribidi1[.]com, gribidi2[.]com
	SHA256	f4e2f28169e0c88b2551b6f1d63f8ba513feb15beacc43a82f626b93d673f56d
<u>BurnsRAT</u>	URLs	hxxp://193[.]42[.]32[.]138/api/ hxxp://87[.]251[.]67[.]51/api/
<u>RevC2</u>	SHA256	cf45f68219c4a105fffc212895312ca9dc7f4abe37306d2f3b0f098fb6975ec7, 153cd5a005b553927a94cc7759a8909bd1b351407d8d036a1bf5fcf9ee83192e
	URLs	ws[://208[.]85[.]17[.]52[:]:]8082, ws[://nopsec[.]org[:]:]8082/
<u>Venom</u>	SHA256	f93134f9b4ee2beb1998d8ea94e3da824e7d71f19dfb3ce566e8e9da65b1d7a2
	URL	hxxp[:]//170[.]75[.]168[.]151/%computername%/aaa
<u>Elpaco Ransomware</u>	SHA256	9f6a696876fee8b811db8889bf4933262f4472ad41daea215d2e39bd537cf32f, e160d7d21c917344f010e58dcfc1e19bec6297c294647a06ce60efc7420d3b13

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

December 9, 2024 . 05:30 AM

© 2024 All Rights are Reserved by Hive Pro



More at www.hivepro.com