Date of Publication
February 10, 2025

Hive Pro

HiveForce Labs

WEEKLY
THREAT DIGEST

Attacks, Vulnerabilities and Actors

03 to 09 FEBRUARY 2025

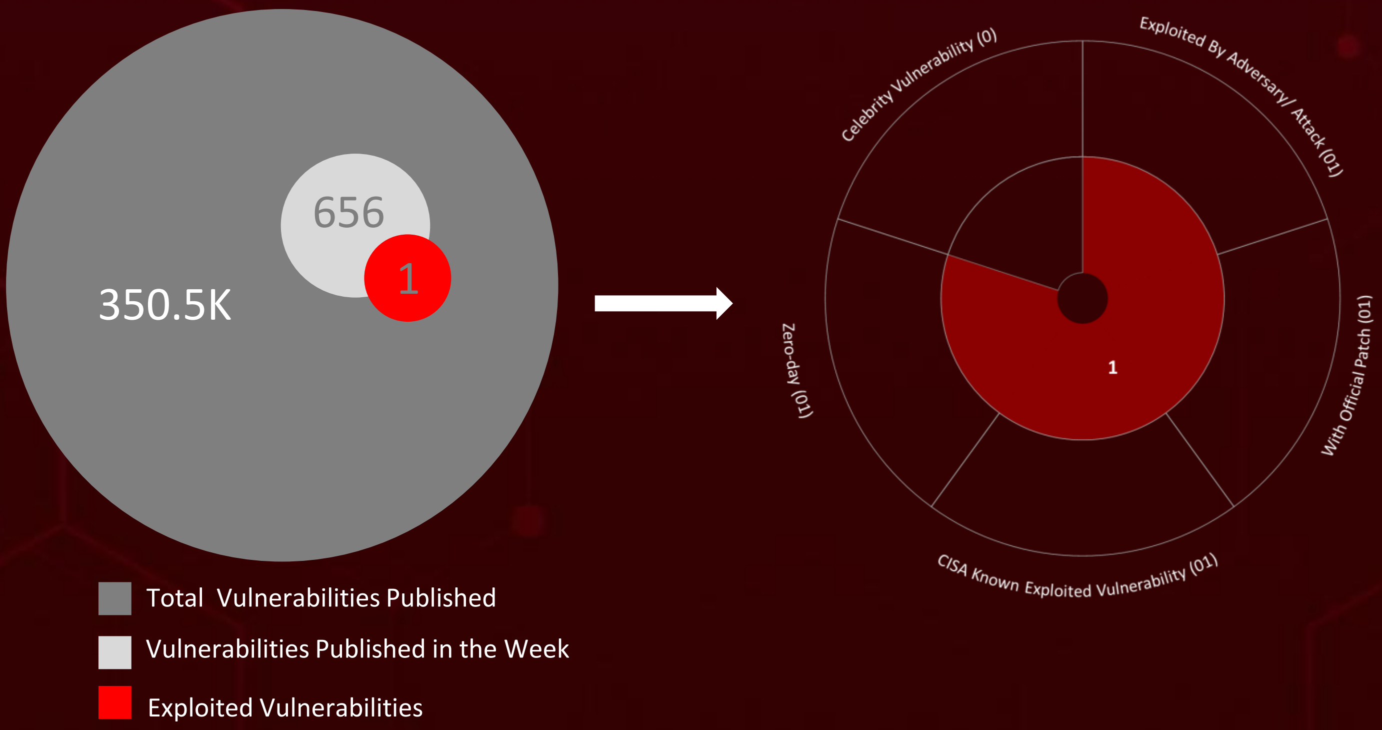
Table Of Contents

Summary

HiveForce Labs has identified a surge in cyber threats, with **ten** attacks executed, **one** vulnerability uncovered, and an active adversary exposed in the past week alone highlighting the relentless nature of cyberattacks.

HiveForce Labs has uncovered major cybersecurity threats, including an actively exploited zero-day vulnerability in 7-Zip (**CVE-2025-0411**). This flaw, exploited since September 2024, allows attackers to bypass Windows' Mark of the Web (MotW) and execute malicious files. Russian cybercriminals have weaponized it in spear-phishing campaigns, using homoglyph attacks to disguise file extensions and deliver **SmokeLoader** malware.

Meanwhile, North Korean threat actors are targeting macOS users through the "**Contagious Interview**" campaign, tricking job seekers and developers into installing malware. Additionally, the **Lynx** Ransomware-as-a-Service (RaaS) operation is growing, using double extortion tactics to encrypt data while threatening leaks. The **Kimsuky** group continues spear-phishing to spread PebbleDash malware and a custom RDP Wrapper for remote access. These evolving threats underscore the need for heightened vigilance and proactive security defenses.



High Level Statistics

10
Attacks Executed

- Coyote
- SmokeLoader
- FlexibleFerret
- FRIENDLYFERRET
- FROSTYFERRET_UI
- MULTI_FROSTYFERRET_CMDCODES
- AsyncRAT
- Lynx
- ValleyRAT
- PebbleDash

1
Vulnerabilities Exploited

- CVE-2025-0411

1
Adversaries in Action

- Kimsuky

Insights

ValleyRAT a RAT first discovered in 2023, has evolved with multi-stage infections and advanced evasion tactics for persistent access

CVE-2025-0411 7-Zip Zero-Day Exploited to Deliver SmokeLoader, has been actively exploited since September 2024, allowing attackers to bypass Windows' Mark of the Web (MotW) security feature

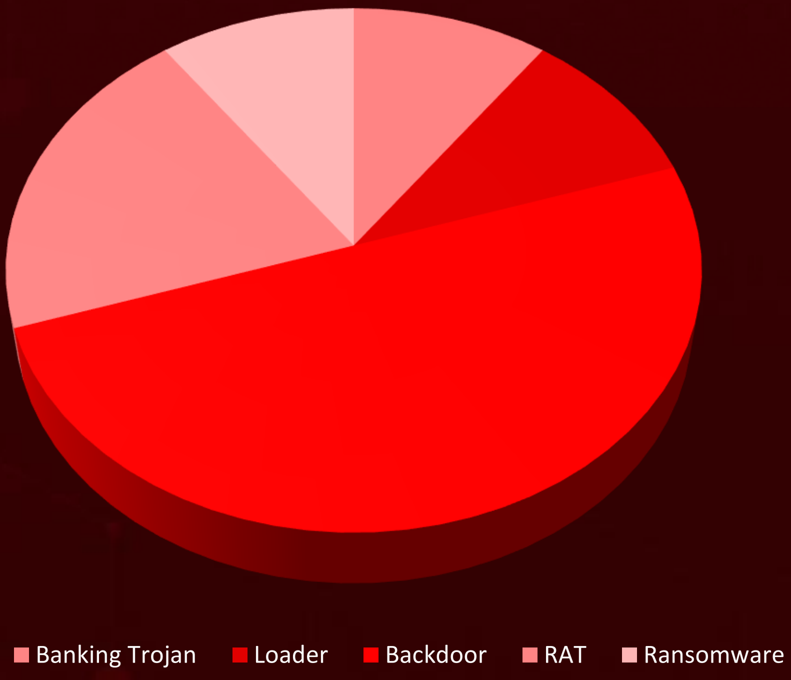
AsyncRAT Adopts Python Payloads & TryCloudflare Tunnels for Stealth

Contagious Interview campaign targets macOS job seekers and developers, infecting them with a new variant of Ferret malware through fake software installations

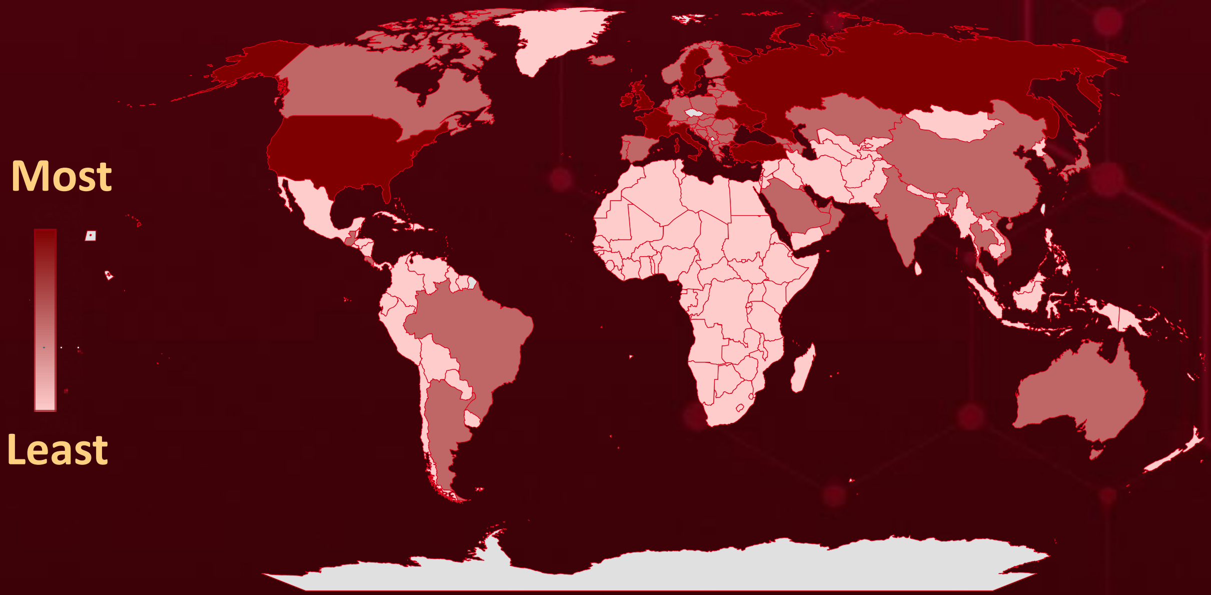
Lynx RaaS operation is rapidly evolving, using double extortion to encrypt data while leveraging stolen information for ransom. Targeting Windows, Linux, and ESXi, it employs advanced encryption and virtual machine shutdowns for maximum disruption

Kimsuky's LNK-based phishing attacks install PebbleDash malware and a custom RDP Wrapper for stealthy remote control

Threat Distribution



Targeted Countries



Powered by Bing

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

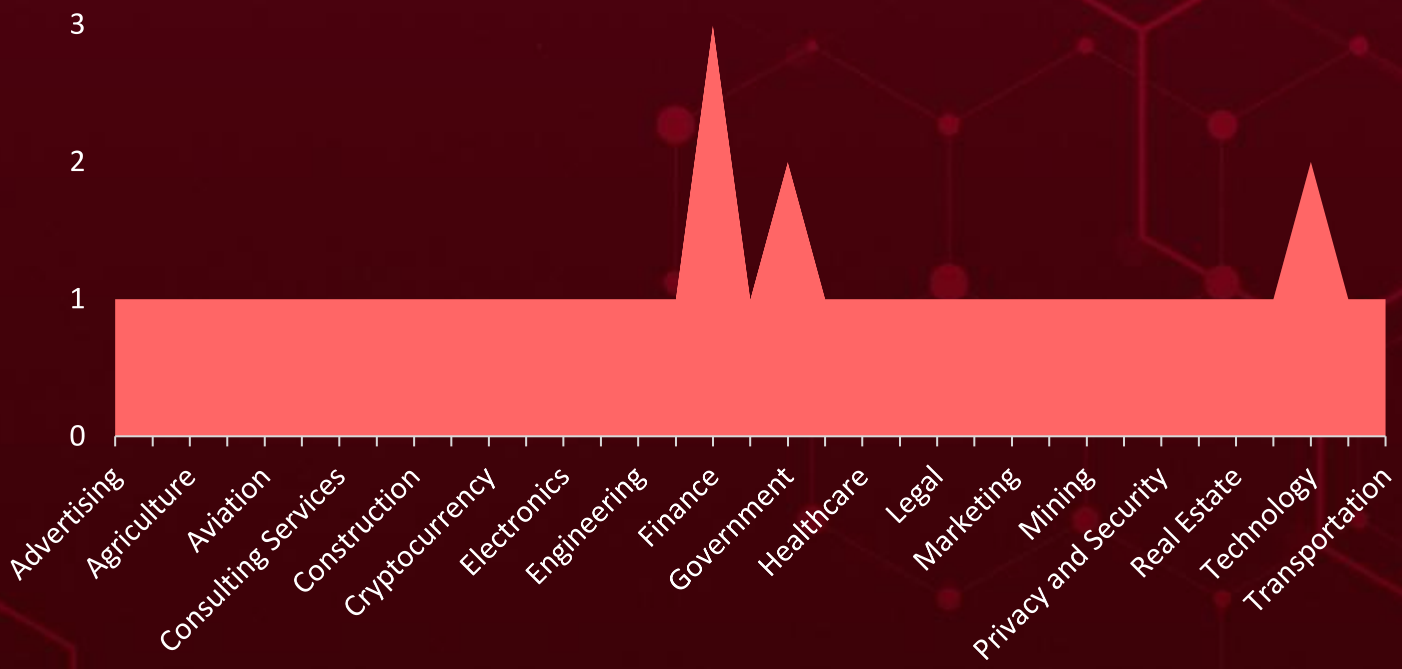
	Countries
■	Russia
■	United Kingdom
■	Turkey
■	Belgium
■	Luxembourg
■	France
■	Sweden
■	Ireland
■	Ukraine
■	Italy
■	United States
▨	Monaco
▨	Slovenia
▨	Qatar
▨	Brazil
▨	United Arab Emirates
▨	Bulgaria
▨	Norway
▨	Canada
▨	Saudi Arabia
▨	China
▨	Switzerland

	Countries
▨	Costa Rica
▨	Malta
▨	Croatia
▨	Netherlands
▨	Cyprus
▨	Poland
▨	Denmark
▨	Azerbaijan
▨	Dominica
▨	Singapore
▨	Estonia
▨	Spain
▨	Finland
▨	Belarus
▨	Andorra
▨	Austria
▨	Georgia
▨	Moldova
▨	Germany
▨	Montenegro
▨	Greece
▨	North Macedonia

	Countries
▨	Guatemala
▨	Oman
▨	Hungary
▨	Portugal
▨	Iceland
▨	Romania
▨	India
▨	San Marino
▨	Argentina
▨	Serbia
▨	Armenia
▨	Slovakia
▨	Australia
▨	South Korea
▨	Kazakhstan
▨	Bahrain
▨	Kuwait
▨	Thailand
▨	Latvia
▨	Albania
▨	Liechtenstein
▨	Bosnia and Herzegovina

	Countries
▨	Lithuania
▨	Japan
▨	Vietnam
□	Pakistan
□	South Sudan
□	Saint Lucia
□	Guinea
□	Trinidad and Tobago
□	Guinea-Bissau
□	DR Congo
□	Guyana
□	Sierra Leone
□	Haiti
□	Gambia
□	Holy See
□	Greenland
□	Honduras
□	Paraguay
□	Cabo Verde
□	Egypt
□	Cambodia
□	Eritrea

Targeted Industries



TOP MITRE ATT&CK TTPs

T1566 Phishing

T1059 Command and Scripting Interpreter

T1204 User Execution

T1055 Process Injection

T1036 Masquerading

T1566.002 Spearphishing Link

T1140 Deobfuscate/Decode Files or Information

T1204.002 Malicious File

T1497 Virtualization/ Sandbox Evasion

T1027 Obfuscated Files or Information

T1547.001 Registry Run Keys / Startup Folder

T1056.001 Keylogging

T1056 Input Capture

T1059.001 PowerShell

T1547 Boot or Logon Autostart Execution

T1057 Process Discovery

T1583 Acquire Infrastructure

T1059.004 Unix Shell

T1548 Abuse Elevation Control Mechanism

T1071 Application Layer Protocol

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Coyote	The Coyote Banking Trojan is a stealthy and highly capable malware designed to steal sensitive financial data. It can log keystrokes, take screenshots, and deploy phishing overlays to harvest login credentials. Targeting over 70 financial applications and more than 1,000 websites, Coyote operates through a multi-stage attack chain. It typically begins with malicious LNK files, which execute hidden PowerShell commands to initiate infection, ensuring a covert and persistent presence on compromised systems.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Banking Trojan		Data Theft	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
SHA256	362af8118f437f9139556c59437544ae1489376dc4118027c24c8d5ce4d84e48, 552d53f473096c55a3937c8512a06863133a97c3478ad6b1535e1976d1e0d45f, 64209e2348e6d503ee518459d0487d636639fa5e5298d28093a5ad41390ef6b0, 67f371a683b2be4c8002f89492cd29d96dceabdbfd36641a27be761ee64605b1		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
SmokeLoader	SmokeLoader is a versatile malware loader designed to deploy additional threats on infected systems while offering optional modules for information stealing. It frequently obscures its C2 traffic by generating requests to legitimate websites, making detection more challenging. Once installed, SmokeLoader can deliver various payloads, including cryptominers, ransomware, and password stealers. Beyond deploying malware, it may also exfiltrate sensitive data, corrupt files, and disrupt system operations, posing a significant risk to compromised devices.	Exploiting Vulnerability	CVE-2025-0411
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Loader		Data Theft, System compromise and Espionage	7-Zip
ASSOCIATED ACTOR			**PATCH LINK**
-			https://www.7-zip.org/
IOC TYPE	**VALUE**		
SHA256	554d9ddd6fd1ccb15d7686c8badb8653323c71884c7f20efb19b56324ff34fc1, 62eb856a5f646c2883a3982f15c3eb877641f9e69783383ce8a73c688eccd543		

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
FlexibleFerret	FlexibleFerret, part of the macOS Ferret malware family, is a stealthy backdoor designed to evade Apple's XProtect and maintain persistence on infected devices. It disguises itself as a legitimate system process, embedding itself in the User’s Library LaunchAgents folder to ensure it runs at startup. The malware communicates with a fraudulent Zoom domain, potentially delivering additional payloads for data theft and remote access.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor		System Compromise	-
ASSOCIATED ACTOR			PATCH LINK
-			-

IOC TYPE	VALUE
SHA1	388ac48764927fa353328104d5a32ad825af51ce, 1a28013e4343fddf13e5c721f91970e942073b88, 3e16c6489bac4ac2d76c555eb1c263cd7e92c9a5, 76e3cb7be778f22d207623ce1907c1659f2c8215, b0caf49884d68f72d2a62aa32d5edf0e79fd9de1

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
FRIENDLYFERRET	FRIENDLYFERRET, part of the macOS Ferret malware family, is a stealthy backdoor that disguises itself as a legitimate system file under the name com.apple.secd, alongside a fake ChromeUpdate process. By blending in with macOS system components, it evades detection while maintaining persistent access to compromised devices.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor		System Compromise	-
ASSOCIATED ACTOR			PATCH LINK
-			-

IOC TYPE	VALUE
SHA1	17e3906f6c4c97b6f5d10e0e0e7f2a2e2c97ca54, 2e51218985afcaa18eadc5775e6b374c78e2d85f, 7e07765bf8ee2d0b2233039623016d6dfb610a6d, de3f83af6897a124d1e85a65818a80570b33c47c

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
FROSTYFERRET_UI	FROSTYFERRET_UI, part of the macOS Ferret malware family, is a persistence module designed to maintain long-term access to infected systems. Masquerading as a CameraAccess component, it ensures stealthy operation while potentially enabling surveillance capabilities.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor		System Compromise	-
ASSOCIATED ACTOR			PATCH LINK
-			-

IOC TYPE	VALUE
SHA1	7da429f6d2cdd8a63b3930074797b990c02dc108, 7e07765bf8ee2d0b2233039623016d6dfb610a6d, 828a323b92b24caa5f5e3eff438db4556d15f215, 831cdcde47b4edbe27524085a6706fbfb9526cef

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
MULTI_FROSTYFERRET_CMDCODES	MULTI_FROSTYFERRET_CMDCODE is a stealthy backdoor which is a part of the macOS Ferret malware family.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor		System Compromise	-
ASSOCIATED ACTOR			PATCH LINK
-			-

IOC TYPE	VALUE
SHA1	203f7cfbf22b30408591e6148f5978350676268b, a25dff88aeeaaf9f956446151a9d786495e2c546, aa172bdccb8c14f53c059c8433c539049b6c2cdd

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>AsyncRAT</td><td rowspan="6">AsyncRAT is a malware known malicious activities since 2019. It can log keystrokes, transfer files, and gain remote desktop control, providing attackers with extensive access to the infected system.</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="4">Information Theft, Espionage</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></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">0054a0b839de6c8261a2f7ec0bd0efdcf2eb28161db6e6354ef94709c99b40c3,
398bf921701c72139dfa6d11b2eb41810170eaf847cc73f16ff00c8f86d6d30a,
7afcf780cb130e2d294e7eca704cb2914d50c738748da431ee275dacc3e5344e,
da816e315d1130151e152d0e390be7ffec1272503ed5368c3957eeeb9c9fdea9</td></tr>
</table>

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVEs</th></tr>
<tr><td>Lynx</td><td rowspan="5">Lynx is a fast-evolving Ransomware-as-a-Service (RaaS) operation that uses a ruthless double-extortion tactic encrypting victims’ data while leveraging stolen information for added pressure. Built for multi-platform attacks, it targets Windows, Linux, and ESXi systems, employing advanced encryption and disruptive techniques like shutting down virtual machines. To maximize damage, Lynx not only locks files but also disables critical recovery options, such as shadow copies and volume snapshots, making system restoration nearly impossible.</td><td>-</td><td>-</td></tr>
<tr><td><b>TYPE</b></td><td><b>IMPACT</b></td><td><b>AFFECTED PRODUCTS</b></td></tr>
<tr><td>Ransomware</td><td rowspan="3">Encrypt Data</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">571f5de9dd0d509ed7e5242b9b7473c2b2cbb36ba64d38b32122a0a337d6cf8b,
eaa0e773eb593b0046452f420b6db8a47178c09e6db0fa68f6a2d42c3f48e3bc,
80908a51e403efd47b1d3689c3fb9447d3fb962d691d856b8b97581eefc0c441</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
ValleyRAT	ValleyRAT, a remote access trojan (RAT) first identified in 2023, has evolved with a sophisticated multi-stage infection process and advanced evasion techniques to maintain long-term access to compromised systems. The malware is spread through fake websites that mimic legitimate sources, including deceptive Google Chrome download pages. ValleyRAT includes features like screenshot capture, process filtering, forced reboots or shutdowns, and Windows event log deletion. In its latest campaign, attackers have escalated their tactics by creating a fraudulent website impersonating a Chinese telecom company.	Social Engineering	-
TYPE		IMPACT	AFFECTED PRODUCTS
RAT		System Compromise	-
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	968b976167b453c15097667b8f4fa9e311b6c7fc5a648293b4abd75d 80b15562		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
PebbleDash	PebbleDash is a stealthy backdoor delivered via spear-phishing email attachments, granting attackers remote control over compromised systems. Once installed, it connects to a command-and-control (C&C) server, awaiting instructions to execute various malicious tasks. These include managing processes and files, as well as downloading and uploading data, enabling threat actors to manipulate the system at will. Through PebbleDash, attackers can establish persistent access, posing a significant risk to affected organizations.	spear phishing emails	-
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor		System Compromise	-
ASSOCIATED ACTOR			PATCH LINK
Kimsuky			-

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-2025-0411	✗	7-Zip Version Prior to 24.09	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:7-zip:7-zip:*:*:*:*:*:*:*:*	SmokeLoader
7-Zip Mark-of-the-Web Bypass Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-693	T1059: Command and Scripting Interpreter; T1553.005: Mark-of-the-Web Bypass	https://www.7-zip.org/

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
Kimsuky (aka Velvet Chollima, Thallium, Black Banshee, SharpTongue, ITG16, TA406, TA427, APT 43, ARCHIPELAGO, Emerald Sleet, KTA082, UAT-5394, Sparkling Pisces, Springtail)	North Korea	Defense, Education, Energy, Government, Healthcare, Manufacturing, Think Tanks and Ministry of Unification, Sejong Institute and Korea Institute for Defense Analyses	South Korea, United States, Japan, Russia, Vietnam and European nations
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	-	PebbleDash	-
TTPs			
TA0043: Reconnaissance; TA0004: Privilege Escalation; TA0001: Initial Access; TA0002: Exécution; TA0005: Defense Evasion; TA0011: Command and Control; T1566: Phishing; T1566.002: Spearphishing Link; T1218.005: Mshta; T1059.001: PowerShell; T1021: Remote Services; T1090: Proxy; T1056.001: Keylogging; T1056: Input Capture; T1217: Browser Information Discovery; T1548.002: Bypass User Account Control; T1548: Abuse Elevation Control Mechanism; T1055: Process Injection			

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **one exploited vulnerability** and block the indicators related to the threat actor **Kimsuky** and malware **Coyote, SmokeLoader, FlexibleFerret, FRIENDLYFERRET, FROSTYFERRET_UI, MULTI_FROSTYFERRET_CMDCODES, AsyncRAT, Lynx, ValleyRAT, PebbleDash.**

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 **one exploited vulnerability.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **Kimsuky** and malware **Coyote, SmokeLoader, FlexibleFerret, AsyncRAT, Lynx** and **ValleyRAT** in Breach and Attack Simulation(BAS).

Threat Advisories

Coyote Trojan: A Digital Predator Infiltrating 70+ Financial Apps

Zero-Day Exploit in 7-Zip Fuels SmokeLoader Attacks on Ukraine

“Contagious Interview” Targets macOS with FlexibleFerret Malware

Stealthy AsyncRAT Campaign Leverages TryCloudflare Tunnels for Evasion

Lynx Ransomware in Action: Pay Up or Face the Consequences

ValleyRAT Strikes Organizations with Stealthy DLL Hijacking Attack

Kimsuky Expands RDP Wrapper & Proxy Malware in Spear-Phishing Attacks

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
Coyote	SHA256	362af8118f437f9139556c59437544ae1489376dc4118027c24c8d5ce4d84e48, 552d53f473096c55a3937c8512a06863133a97c3478ad6b1535e1976d1e0d45f, 64209e2348e6d503ee518459d0487d636639fa5e5298d28093a5ad41390ef6b0, 67f371a683b2be4c8002f89492cd29d96dceabdbfd36641a27be761ee64605b1, 73ad6be67691b65cee251d098f2541eef3cab2853ad509dac72d8eff5bd85bc0, 839de445f714a32f36670b590eba7fc68b1115b885ac8d689d7b344189521012, bea4f753707eba4088e8a51818d9de8e9ad0138495338402f05c5c7a800695a6, f3c37b1de5983b30b9ae70c525f97727a56d3874533db1a6e3dc1355bfbf37ec, fd0ef425d34b56d0bc08bd93e6ecb11541bd834b9d4d417187373b17055c862e, 330dffe834ebbe4042747bbe00b4575629ba8f2507bccf746763cacf63d655bb, 33cba89eeeaf139a798b7fa07ff6919dd0c4c6cf4106b659e4e56f15b5809287
SmokeLoader	SHA256	554d9ddd6fd1ccb15d7686c8badb8653323c71884c7f20efb19b56324ff34fc1, 62eb856a5f646c2883a3982f15c3eb877641f9e69783383ce8a73c688eccd543, 5c7d582ba61ac95fb0d330ecc05feeb4853ac1de1f5a6fd12df6491dd0b7ea34

Attack Name	TYPE	VALUE
SmokeLoader	SHA256	2e33c2010f95cbda8bf0817f1b5c69b51c860c536064182b67261f695f54e1d5, 888f68917f9250a0936fd66ea46b6c510d0f6a0ca351ee62774dd14268fe5420
FlexibleFerret	SHA1	388ac48764927fa353328104d5a32ad825af51ce, 1a28013e4343fddf13e5c721f91970e942073b88, 3e16c6489bac4ac2d76c555eb1c263cd7e92c9a5, 76e3cb7be778f22d207623ce1907c1659f2c8215, b0caf49884d68f72d2a62aa32d5edf0e79fd9de1, bd73a1c03c24a8cdd744d8a513ae8d2ddfa2de5f, ccac0f0ba463c414b26ba67b5a3ddaabdef6d371, d8245cdf6f51216f29a71f25e70de827186bdf71, b071fbd9c42ff660e3f240e1921533e40f0067eb, ee7a557347a10f74696dc19512ccc5fcfca77bc5
	SHA256	3c4becde20e618efb209f97581e9ab6bf00cbd63f51f4ebd5677e352c57e992a, bd2aa5805b76f272b43a595b3d73e29d0fc4647e15e87950b8f904ea26dcf053
FRIENDLYFERRET	SHA1	17e3906f6c4c97b6f5d10e0e0e7f2a2e2c97ca54, 2e51218985afcaa18eadc5775e6b374c78e2d85f, 7e07765bf8ee2d0b2233039623016d6dfb610a6d, de3f83af6897a124d1e85a65818a80570b33c47c
FrostyFerret_UI	SHA1	7da429f6d2cdd8a63b3930074797b990c02dc108, 7e07765bf8ee2d0b2233039623016d6dfb610a6d, 828a323b92b24caa5f5e3eff438db4556d15f215, 831cdcde47b4edbe27524085a6706fbfb9526cef, 8667078a88dae5471f50473a332f6c80b583d3de, dba1454fbea1dd917712fbece9d6725244119f83, e876ba6e23e09206f358dbd3a3642a7fd311bb22
MULTI_FROSTYFERRET_CMDCODES	SHA1	203f7cfbf22b30408591e6148f5978350676268b, a25dff88aeeaaf9f956446151a9d786495e2c546, aa172bdccb8c14f53c059c8433c539049b6c2cdd
AsyncRAT	SHA256	0054a0b839de6c8261a2f7ec0bd0efdcf2eb28161db6e6354ef94709c99b40c3, 398bf921701c72139dfa6d11b2eb41810170eaf847cc73f16ff00c8f86d6d30a, 7afcf780cb130e2d294e7eca704cb2914d50c738748da431ee275dacc3e5344e, da816e315d1130151e152d0e390be7ffec1272503ed5368c3957eeeb9c9fdea9, 5145dcd625c43d5ccbb49e6020b62991dd8140b85685a555ef4c30f28963bef8, 6f92b2cdb8b5f68d20dbc7ca23c3a3ec78c4ef1859001940dfa22e38ce459d30,

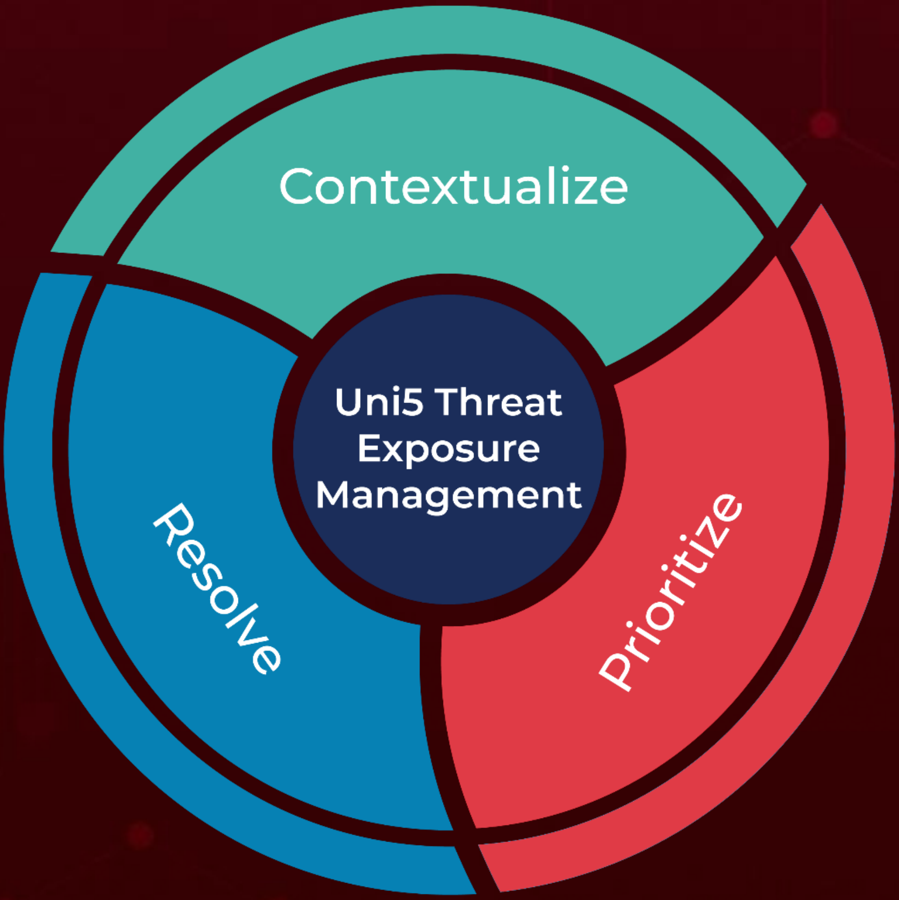
Attack Name	TYPE	VALUE
AsyncRAT	SHA256	6d240a48b5e2d1cf761a8b48b146d20729d0a7a3a557e31e75ed4c120ce71aea, c7d4e119149a7150b7101a4bd9fffbf659fba76d058f7bf6cc73c99fb36e8221, 2657fe9b88321d255fc56a81b2df4b0109ab7c525442f31765c94d75c37347aa, 124c02ed924e11b06b74e1b8c1290adbb1e50dfa2a7bcf95104c6425a1f82ef5, 3c4df2d02e4b6f4acf7b19238211892db501ee6faa04065dd11b25b56483f9c4, 9a7bc24bd814ab755a8ad67e1aeebc05ff139771928f0eae883daff6f4ae161d, 65d6130ed7d3d822e1b08e7bed8e3adca4188d787d6805935213369c05eb2a99, 90245116af6f781c72ad78b8d160fa0c0b9d95bd033c83137c75fc60236dd2d5
Lynx	Domain	hxxp[:]//lynxblog[.]net
	Email	martina[.]lestariid1898[@]proton[.]me
	SHA256	571f5de9dd0d509ed7e5242b9b7473c2b2cbb36ba64d38b32122a0a337d6cf8b, eaa0e773eb593b0046452f420b6db8a47178c09e6db0fa68f6a2d42c3f48e3bc, 80908a51e403efd47b1d3689c3fb9447d3fb962d691d856b8b97581eefc0c441, 3e68e5742f998c5ba34c2130b2d89ca2a6c048feb6474bc81ff000e1eaed044e, 97c8f54d70e300c7d7e973c4b211da3c64c0f1c95770f663e04e35421dfb2ba0, 468e3c2cb5b0bbc3004bbf5272f4ece5c979625f7623e6d71af5dc0929b89d6a
ValleyRAT	SHA256	968b976167b453c15097667b8f4fa9e311b6c7fc5a648293b4abd75d80b15562, 6ed466a2a6eeb83d1ff32ba44180352cf0a9ccc72b47e5bd55c1750157c8dc4c

A comprehensive list of IOCs (Indicators of Compromise) associated with the executed attacks is available on the Uni5Xposure platform.

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

February 10, 2025 • 6:20 AM

More at www.hivepro.com