

Date of Publication
September 29, 2025



HiveForce Labs
WEEKLY
THREAT DIGEST

Attacks, Vulnerabilities, and Actors
22 to 28 SEPTEMBER 2025

Table Of Contents

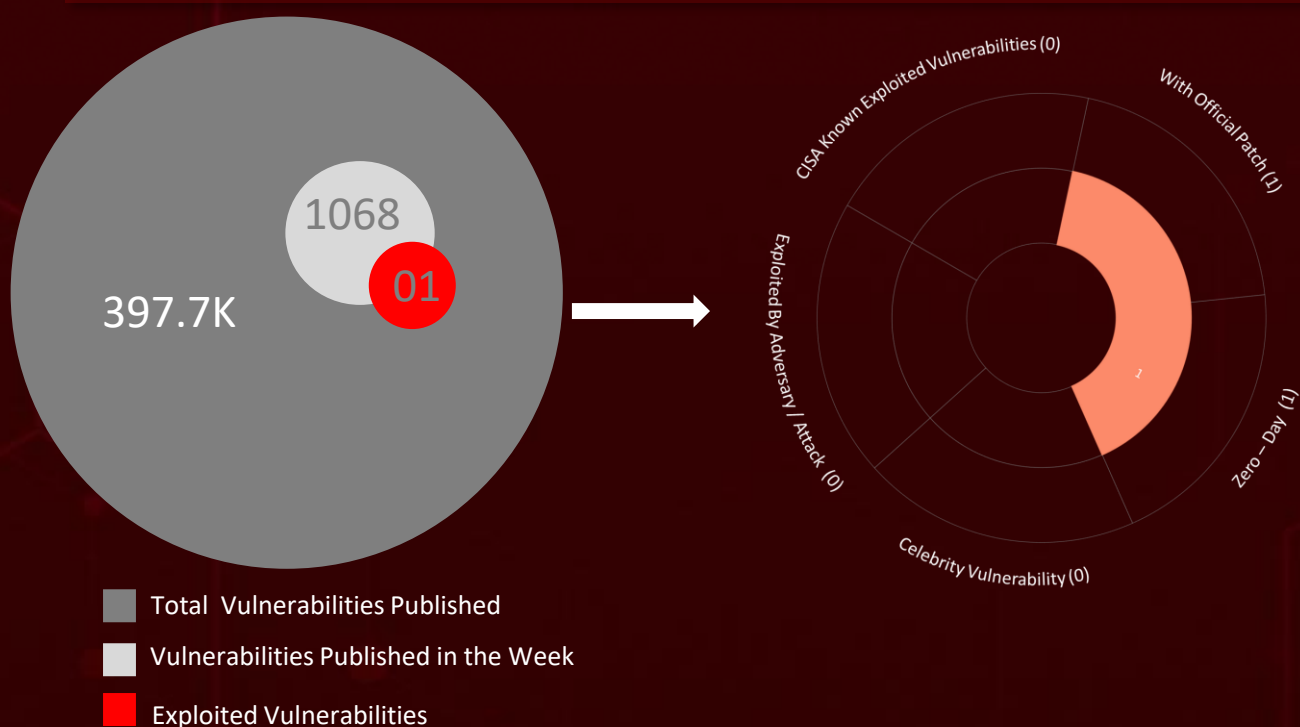
<u>Summary</u>	03
<u>High Level Statistics</u>	04
<u>Insights</u>	05
<u>Targeted Countries</u>	06
<u>Targeted Industries</u>	07
<u>Top MITRE ATT&CK TTPs</u>	07
<u>Attacks Executed</u>	08
<u>Vulnerabilities Exploited</u>	13
<u>Adversaries in Action</u>	14
<u>Recommendations</u>	19
<u>Threat Advisories</u>	20
<u>Appendix</u>	21
<u>What Next?</u>	23

Summary

HiveForce Labs has reported a sharp rise in cyber threats, highlighting the increasing complexity and frequency of attacks. Over the past week alone, **nine** major attacks were detected, **one** vulnerability was actively exploited, and **five** threat actor groups were closely tracked, signaling an alarming escalation in malicious activity across digital environments.

Among the most pressing developments is a zero-day in Cisco's IOS and IOS XE SNMP subsystem (**CVE-2025-20352**), now under active exploitation. The flaw allows attackers to crash devices or seize root-level control, posing a severe risk to organizations relying on Cisco infrastructure. At the same time, Russia-linked espionage groups **Turla** and **Gamaredon** have amplified their joint campaigns against Ukraine. By combining Turla's stealthy Kazuar backdoor with Gamaredon's aggressive Ptero toolkit, they've created a potent blend of wide access and long-term espionage.

Meanwhile, Chinese-speaking hackers have launched "**Operation Rewrite**," a stealthy campaign that weaponizes search engines through **BadIIS**, a malicious IIS module that secretly rewrites web traffic. On another front, **DeerStealer**, an advanced infostealer marketed by the dark-web user LuciferXfiles, is making rounds on Telegram and underground forums. Disguised as everyday tools like document readers, it tricks victims into execution while quietly siphoning off credentials, financial details, cryptocurrency wallets, and browser data. Together, these developments illustrate the urgency of proactive defenses, timely patching, and a resilient cybersecurity posture in today's increasingly hostile digital landscape.



High Level Statistics

9

Attacks
Executed

1

Vulnerabilities
Exploited

5

Adversaries in
Action

- Kazuar
 - PteroOdd
 - MINIBIKE
 - Atomic Stealer
 - BadIIS
 - DeerStealer
 - BAITSWITCH
 - SIMPLEFIX
 - BRICKSTORM
- CVE-2025-20352
- Gamaredon
 - Turla
 - Subtle Snail
 - COLDRIVER
 - UNC5221



Insights

DeerStealer, peddled by 'LuciferXfiles,' is sold on dark-web forums and Telegram through a tiered subscription model starting at \$200 and climbing to \$3,000 per month.

COLDRIVER's new ClickFix campaign exploits trust and urgency to infiltrate Russia's civil society.

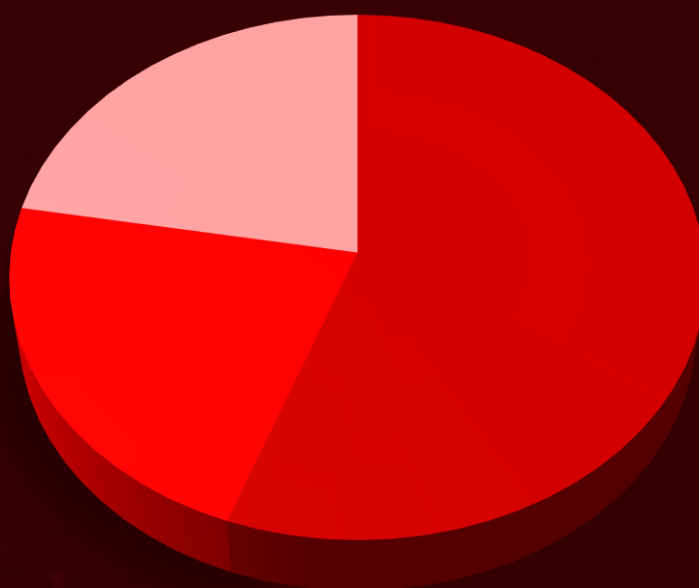
FSB-linked **Turla** and **Gamaredon** have stepped up joint cyber-espionage on Ukraine, fusing Turla's stealthy Kazuar backdoor with Gamaredon's aggressive Ptero arsenal.

Cisco zero-day flaw (**CVE-2025-20352**) under active attack lets hackers crash devices or seize root access via the SNMP subsystem.

China-linked **UNC5221** is deploying **BRICKSTORM**, a Go-based backdoor, in active campaigns against U.S. organizations.

Operation Rewrite sees Chinese-speaking hackers weaponize search engines with BadIIS, a malicious IIS module that covertly rewrites web traffic.

Threat Distribution



■ Backdoor

■ Downloader

■ Stealer

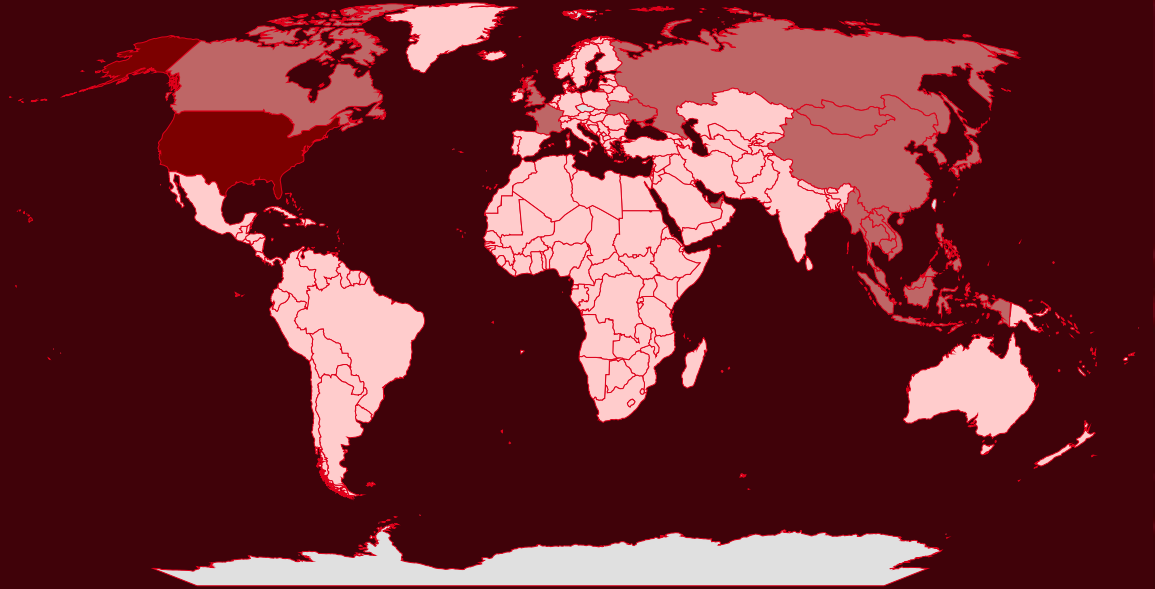


Targeted Countries

Most



Least

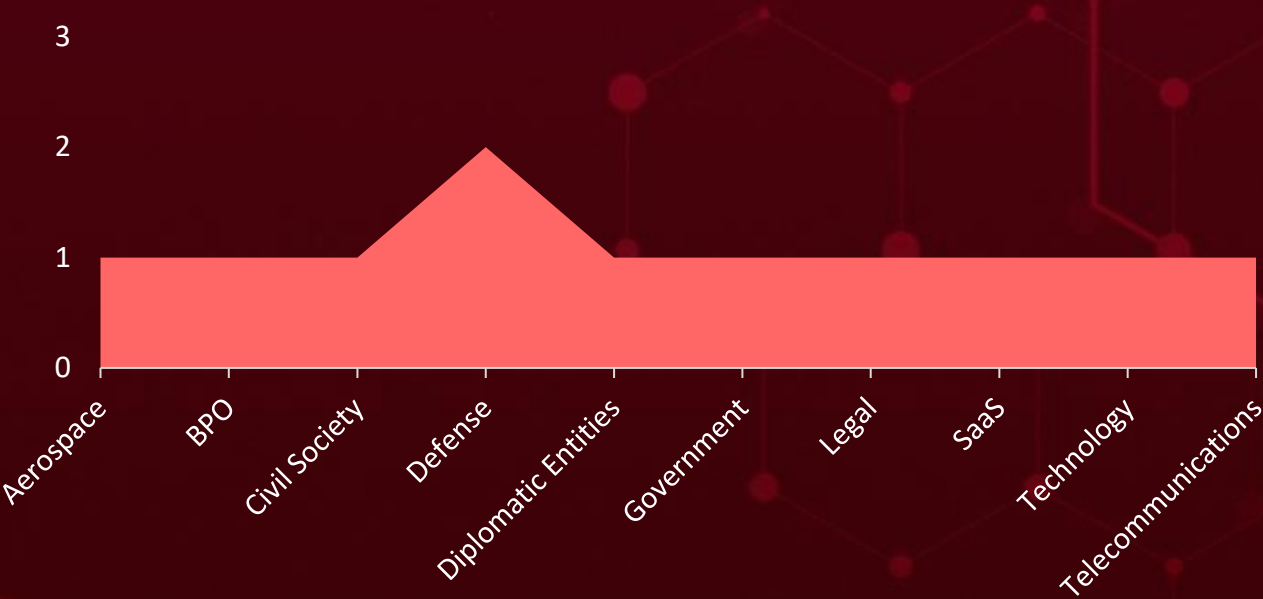


Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, Overture Maps Foundation, TomTom, Zenrin

Countries	Countries	Countries	Countries
United States	Turkmenistan	Colombia	Oman
South Korea	Albania	Saint Kitts & Nevis	DR Congo
North Korea	Palau	Comoros	Papua New Guinea
United Arab Emirates	Bulgaria	Seychelles	Ecuador
Cambodia	St. Vincent & Grenadines	Congo	Poland
Russia	Burkina Faso	Belgium	Egypt
Canada	Mauritania	Costa Rica	Barbados
Timor-Leste	Burundi	Sweden	El Salvador
China	Nicaragua	Côte d'Ivoire	Samoa
Myanmar	Cabo Verde	Tonga	Equatorial Guinea
France	Qatar	Croatia	Senegal
Philippines	Algeria	Bolivia	Eritrea
Indonesia	Slovenia	Cuba	Belarus
Singapore	Cameroon	Malta	Estonia
Japan	Tanzania	Cyprus	Somalia
Thailand	Andorra	Mexico	Eswatini
Vietnam	Brazil	Czech Republic	Spain
Ukraine	Central African Republic	Azerbaijan	Ethiopia
Malaysia	Moldova	Denmark	Sudan
Brunei	Chad	Bahamas	Fiji
United Kingdom	Nauru	Djibouti	Syria
Mongolia	Chile	Netherlands	Finland
Laos	North Macedonia	Dominica	Benin
Sao Tome & Principe		Nigeria	Antigua and Barbuda
Morocco		Dominican Republic	Tunisia



Targeted Industries



TOP MITRE ATT&CK TTPs

T1059

Command and Scripting Interpreter

T1036

Masquerading

T1071

Application Layer Protocol

T1027

Obfuscated Files or Information

T1041

Exfiltration Over C2 Channel

T1204

User Execution

T1082

System Information Discovery

T1566

Phishing

T1608

Stage Capabilities

T1005

Data from Local System

T1071.001

Web Protocols

T1087

Account Discovery

T1574.001

DLL

T1555

Credentials from Password Stores

T1083

File and Directory Discovery

T1583.001

Domains

T1057

Process Discovery

T1140

Deobfuscate/Decode Files or Information

T1583

Acquire Infrastructure

T1078

Valid Accounts



Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Kazuar	Kazuar backdoor is an advanced espionage implant used by Turla in its attack chain. Kazuar Versions 2 and 3 share the same codebase. This modular malware provides persistent remote control over infected systems, making it a powerful tool.	-	-
		IMPACT	AFFECTED PRODUCT
TYPE		Data Theft, System Compromise	-
Backdoor			
ASSOCIATED ACTOR			PATCH LINK
Turla, Gamaredon			-
IOC TYPE	VALUE		
SHA256	3ecb09e659bcb500f9f40d022579a09acb11aec3a92c03e7d3fd2e56982d9eea		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
PteroOdd	PteroOdd is a PowerShell downloader used by Gamaredon to retrieve payloads that executed the Kazuar backdoor.	-	-
		IMPACT	AFFECTED PRODUCT
TYPE		Downloads other malware	-
Downloader			
ASSOCIATED ACTOR			PATCH LINK
Turla, Gamaredon			-
IOC TYPE	VALUE		
SHA1	7db790f75829d3e6207d8ec1cbcd3c133f596d67, 2610a899fe73b8f018d19b50be55d66a6c78b2af		

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>MINIBIKE</u>	MINIBIKE is a backdoor that maintains a foothold by loading additional DLLs and keeping a persistent link to its operators; it hides key data with runtime XOR decryption, using a separate routine for each string length to frustrate static analysis and routes command-and-control traffic through Microsoft Azure to blend in with legitimate cloud activity. From an infected host, the attackers can run arbitrary commands and browse the file system remotely.	Social Engineering	-
		IMPACT	AFFECTED PLATFORM
TYPE		Data Theft	Windows
Backdoor			
ASSOCIATED ACTOR			PATCH LINK
Subtle Snail			-
IOC TYPE	VALUE		
SHA256	0e4ff052250ade1edaab87de194e87a9afeff903695799bcb3571918b131100		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>Atomic Stealer</u>	Atomic Stealer, or AMOS, is a prevalent macOS-targeting malware designed to harvest and exfiltrate sensitive data, including account credentials, browser information, and cryptocurrency wallet details.	By abusing GitHub Pages and SEO	-
		IMPACT	AFFECTED PLATFORM
TYPE		Data Theft	macOS
Stealer			
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	e52dd70113d1c6eb9a09eafa0a7e7bcf1da816849f47ebcdc66ec9671eb9b350		

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>BadIIS</u>	BadIIS is a family of malicious native IIS modules that embed directly into a web server’s request pipeline and inherit the server’s full privileges, allowing a single implant to manipulate traffic and site behavior with powerful stealth. BadIIS can inject JavaScript or invisible iframes into pages, tunnel traffic through a built-in reverse proxy, issue 302 redirects that mislead search engine crawlers, and exfiltrate sensitive data from visitors. Attackers leverage these capabilities to perform SEO poisoning.	Social Engineering	-
		IMPACT	AFFECTED PRODUCT
TYPE		System Compromise	-
Backdoor			PATCH LINK
ASSOCIATED ACTOR			
-			-
IOC TYPE	VALUE		
SHA256	01a616e25f1ac661a7a9c244fd31736188ceb5fce8c1a5738e807fdbef70fd60		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>DeerStealer</u>	DeerStealer is a commercially marketed information-stealer that poses as legitimate software to trick victims into running it and then quietly harvests passwords, browser data, cryptocurrency wallets, and other sensitive information from infected machines. The malware is openly sold on dark-web forums and Telegram channels by an actor using the handle “LuciferXfiles,” offered through tiered subscriptions, from a \$200/month “Premium” tier up to a \$3,000/month “Professional” package, making it a turnkey tool for criminal operators who want scalable, low-effort access to harvested credentials and financial data.	Phishing	-
		IMPACT	AFFECTED PRODUCT
TYPE		Data Theft	-
Information stealer			PATCH LINK
ASSOCIATED ACTOR			
-			-
IOC TYPE	VALUE		
SHA256	b57c56e5f0d15eea013c39b5c169f3308ca3e8ffd0cf5b1ef001dba894beeeef0		

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>BAITSWITCH</u>	BAITSWITCH is a downloader that establishes persistence on a victim machine and reaches out to attacker-controlled servers to fetch and run a PowerShell stager that installs the SIMPLEFIX backdoor. It uses a hard-coded user-agent string as a gatekeeper, the C2 only returns commands when that exact user-agent is presented and otherwise serves a “404 Not Found” page, and performs five HTTP requests to the actor-controlled domain to retrieve different commands and payloads.	Phishing	-
		IMPACT	AFFECTED PRODUCT
TYPE		Downloads other payloads	-
Downloader			PATCH LINK
ASSOCIATED ACTOR			
COLDRIVER			-
IOC TYPE	VALUE		
SHA256	87138f63974a8ccbbf5840c31165f1a4bf92a954baccfbf1e7e5525d750aa48		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>SIMPLEFIX</u>	SIMPLEFIX is a PowerShell-based backdoor delivered by the BAITSWITCH that uses the same layered obfuscation techniques found in the installer to hide its true logic; when those layers are stripped away the deobfuscated script reveals the backdoor’s core runtime logic invoked by the stager, making SIMPLEFIX a stealthy, script-native implant that is designed to be hard to detect and straightforward for operators to control once executed.	Phishing	-
		IMPACT	AFFECTED PRODUCT
TYPE		System Compromise	-
Backdoor			PATCH LINK
ASSOCIATED ACTOR			
COLDRIVER			-
IOC TYPE	VALUE		
SHA256	16a79e36d9b371d1557310cb28d412207827db2759d795f4d8e27d5f5afaf63f		

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>BRICKSTORM</u>	BRICKSTORM is a Go-based backdoor attributed to a China-nexus group tracked as UNC5221 and first observed in early 2024 amid attacks exploiting Ivanti Connect Secure flaws. The implant works alongside a companion tool, BRICKSTEAL, to harvest vCenter credentials and escalate privileges, and it uses advanced evasion techniques that let intrusions persist for long periods, on average about 393 days, before detection. Operators using BRICKSTORM have also been observed cloning sensitive VMware vCenter virtual machines, notably domain controllers and password vaults, to siphon secrets and broaden their foothold, making the toolkit both opportunistic and highly targeted against high-value virtualization infrastructure.	Exploiting Vulnerabilities	-
		IMPACT	AFFECTED PRODUCT
TYPE		Data Theft	-
Backdoor			PATCH LINK
ASSOCIATED ACTOR			
UNC5221			-
IOC TYPE	VALUE		
SHA256	90b760ed1d0dcb3ef0f2b6d6195c9d852bcb65eca293578982a8c4b64f51b035, 2388ed7aee0b6b392778e8f9e98871c06499f476c9e7eae6ca0916f827fe65df		

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



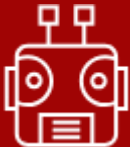
Vulnerabilities Exploited

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-20352</u>		Cisco IOS & IOS XE Software, Meraki MS390 Switches – Meraki CS 17 and earlier, Cisco Catalyst 9300 Series Switches - Meraki CS 17 and earlier	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:cisco:ios:*:*:*:*:*:*:* cpe:2.3:o:cisco:ios_xe:*:*:*:*:*:*:*	-
Cisco IOS and IOS XE Software SNMP Denial of Service and Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-121	T1059:Command and Scripting Interpreter; T1499: Endpoint Denial of Service	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snmp-x4LPhte



Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 <u>Gamaredon (aka Primitive Bear, Winterflounder, BlueAlpha, Blue Otso, Iron Tilden, Armageddon, SectorC08, Callisto, Shuckworm, Actinium, Trident Ursa, DEV-0157, UAC-0010, Aqua Blizzard)</u>	Russia	Government, Defense, Diplomatic Entities	Ukraine
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	-	Kazuar backdoor, PteroOdd	-
TTPs			
TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0011: Command and Control; T1583: Acquire Infrastructure; T1583.001: Domains; T1583.004: Server; T1583.007: Serverless; T1584: Compromise Infrastructure; T1584.003: Virtual Private Server; T1608: Stage Capabilities; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1574: Hijack Execution Flow; T1574.001: DLL; T1140: Deobfuscate/Decode Files or Information; T1480: Execution Guardrails; T1480.001: Environmental Keying; T1036: Masquerading; T1036.005: Match Legitimate Resource Name or Location; T1057: Process Discovery; T1012: Query Registry; T1082: System Information Discovery; T1083: File and Directory Discovery; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1573: Encrypted Channel; T1573.001: Symmetric Cryptography; T1102: Web Service			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 <u>Turla (aka Waterbug, Venomous Bear, Group 88, SIG2, SIG15, SIG23, Iron Hunter, CTG-8875, Pacifier APT, ATK 13, ITG12, Makersmark, Krypton, Belugasturgeon)</u>	Russia	Government, Defense, Diplomatic Entities	Ukraine
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	-	Kazuar backdoor, PteroOdd	-
TTPs			
TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0011: Command and Control; T1583: Acquire Infrastructure; T1583.001: Domains; T1583.004: Server; T1583.007: Serverless; T1584: Compromise Infrastructure; T1584.003: Virtual Private Server; T1608: Stage Capabilities; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1574: Hijack Execution Flow; T1574.001: DLL; T1140: Deobfuscate/Decode Files or Information; T1480: Execution Guardrails; T1480.001: Environmental Keying; T1036: Masquerading; T1036.005: Match Legitimate Resource Name or Location; T1057: Process Discovery; T1012: Query Registry; T1082: System Information Discovery; T1083: File and Directory Discovery; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1573: Encrypted Channel; T1573.001: Symmetric Cryptography; T1102: Web Service			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 <u>Subtle Snail (aka</u> <u>UNC1549, TA455,</u> <u>Smoke Sandstorm,</u> <u>Bohrium, DEV-0056,</u> <u>Yellow Dev 13)</u>	Iran	Telecommunications, Aerospace, Defense	Canada, USA, UK, France, UAE
	MOTIVE		
	Information theft and espionage	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	TARGETED CVE		
	-	MINIBIKE	-
TTPs			
TA0043: Reconnaissance; TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0009: Collection; TA0010: Exfiltration; TA0011: Command and Control; T1589: Gather Victim Identity Information; T1591: Gather Victim Org Information; T1598: Phishing for Information; T1598.003: Spearphishing Link; T1583: Acquire Infrastructure; T1583.001: Domains; T1583.003: Virtual Private Server; T1587: Develop Capabilities; T1587.001: Malware; T1585: Establish Accounts; T1585.001: Social Media Accounts; T1585.002: Email Accounts; T1585.003: Cloud Accounts; T1588: Obtain Capabilities; T1588.003: Code Signing Certificates; T1566: Phishing; T1566.002: Spearphishing Link; T1566.001: Spearphishing Attachment; T1204: User Execution; T1204.001: Malicious Link; T1204.002: Malicious File; T1059: Command and Scripting Interpreter; T1059.003: Windows Command Shell; T1016: System Network Configuration Discovery; T1070: Indicator Removal; T1574: Hijack Execution Flow; T1574.001: DLL; T1055: Process Injection; T1055.012: Process Hollowing; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys / Startup Folder; T1497: Virtualization/Sandbox Evasion; T1622: Debugger Evasion; T1140: Deobfuscate/Decode Files or Information; T1027: Obfuscated Files or Information; T1027.007: Dynamic API Resolution; T1036: Masquerading; T1036.003: Rename Legitimate Utilities; T1070.004: File Deletion; T1056: Input Capture; T1056.001: Keylogging; T1555: Credentials from Password Stores; T1555.003: Credentials from Web Browsers; T1539: Steal Web Session Cookie; T1552: Unsecured Credentials; T1552.001: Credentials In Files; T1552.004: Private Keys; T1552.003: Bash History; T1555.005: Password Managers; T1087: Account Discovery; T1016: System Network Configuration Discovery; T1033: System Owner/User Discovery; T1082: System Information Discovery; T1069: Permission Groups Discovery; T1069.002: Domain Groups; T1083: File and Directory Discovery; T1057: Process Discovery; T1217: Browser Information Discovery; T1005: Data from Local System; T1119: Automated Collection; T1560: Archive Collected Data; T1560.001: Archive via Utility; T1114: Email Collection; T1114.001: Local Email Collection; T1025: Data from Removable Media; T1039: Data from Network Shared Drive; T1115: Clipboard Data; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1020: Automated Exfiltration; T1041: Exfiltration Over C2 Channel; T1029: Scheduled Transfer			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
	Russia	Civil Society	Russia
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
<u>COLDRIVER (aka Nahr el bared, Nahr Elbard, Cobalt Edgewater, TA446, Seaborgium, TAG-53, BlueCharlie, Blue Callisto, Calisto, Star Blizzard, UNC4057, IRON FRONTIER, Grey Pro, Mythic Ursa, Gossamer Bear)</u>	-	BAITSWITCH, SIMPLEFIX	-

TTPs

TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0009: Collection; TA0010: Exfiltration; TA0011: Command and Control; T1583: Acquire Infrastructure; T1583.001: Domains; T1583.006: Web Services; T1585: Establish Accounts; T1585.002: Email Accounts; T1585.003: Cloud Accounts; T1587: Develop Capabilities; T1587.001: Malware; T1608: Stage Capabilities; T1608.001: Upload Malware; T1608.003: Install Digital Certificate; T1608.005: Link Target; T1204: User Execution; T1204.004: Malicious Copy and Paste; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1059.003: Windows Command Shell; T1037: Boot or Logon Initialization Scripts; T1037.001: Logon Script (Windows); T1112: Modify Registry; T1140: Deobfuscate/Decode Files or Information; T1564: Hide Artifacts; T1564.003: Hidden Window; T1218: System Binary Proxy Execution; T1218.011: Rundll32; T1205: Traffic Signaling; T1070: Indicator Removal; T1070.003: Clear Command History; T1027: Obfuscated Files or Information; T1027.011: Fileless Storage; T1027.013: Encrypted/Encoded File; T1033: System Owner/User Discovery; T1082: System Information Discovery; T1135: Network Share Discovery; T1016: System Network Configuration Discovery; T1016.001: Internet Connection Discovery; T1087: Account Discovery; T1087.001: Local Account; T1083: File and Directory Discovery; T1049: System Network Connections Discovery; T1057: Process Discovery; T1018: Remote System Discovery; T1046: Network Service Discovery; T1124: System Time Discovery; T1005: Data from Local System; T1530: Data from Cloud Storage; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1104: Multi-Stage Channels; T1001: Data Obfuscation; T1001.003: Protocol or Service Impersonation; T1105: Ingress Tool Transfer; T1132: Data Encoding; T1132.001: Standard Encoding; T1573: Encrypted Channel; T1573.002: Asymmetric Cryptography; T1566: Phishing; T1036: Masquerading; T1059.007: JavaScript; T1041: Exfiltration Over C2 Channel
--

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 <u>UNC5221 (alias UTA0178, Red Dev 61)</u>	China	Legal, Software-as-a-Service (SaaS) Providers, Business Process Outsourcers (BPOs), Technology	United States
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	-	BRICKSTORM	-
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; T1190: Exploit Public-Facing Application; T1078: Valid Accounts; T1136: Create Account; T1543: Create or Modify System Process; T1027: Obfuscated Files or Information; T1021: Remote Services; T1021.001: Remote Desktop Protocol; T1555: Credentials from Password Stores; T1673: Virtual Machine Discovery; T1564: Hide Artifacts; T1564.006: Run Virtual Instance; T1114: Email Collection; T1114.002: Remote Email Collection; T1671: Cloud Application Integration; T1003: OS Credential Dumping; T1087: Account Discovery; T1059: Command and Scripting Interpreter; T1505.003: Web Shell; T1547: Boot or Logon Autostart Execution; T1021.004: SSH; T1071.001: Web Protocols; T1041: Exfiltration Over C2 Channel; T1071.004: DNS; T1567: Exfiltration Over Web Service; T1071: Application Layer Protocol			

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 actors **Gamaredon, Turla, Subtle Snail, COLDRIVER, UNC5221**, and malware **Kazuar, PteroOdd, MINIBIKE, Atomic Stealer, BadIIS, DeerStealer, BAITSWITCH, SIMPLEFIX, BRICKSTORM**.

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 **one exploited vulnerability**.
- Testing the efficacy of their security controls by simulating the attacks related to the threat actors **Gamaredon, Turla, Subtle Snail, COLDRIVER, UNC5221**, and malware **MINIBIKE, Atomic Stealer, BadIIS, DeerStealer, BAITSWITCH**, in Breach and Attack Simulation(BAS).

Threat Advisories

[Gamaredon Tools Revive Turla's Kazuar Backdoor to Target Ukraine](#)

[Subtle Snail's Silent Espionage Across Europe](#)

[Atomic Stealer Targeting Mac Users via Malicious GitHub Pages](#)

[Operation Rewrite: How BadIIS Rewired the Web for SEO Poisoning](#)

[DeerStealer the \\$200 Doorway to Your Digital Secrets](#)

[Critical Cisco SNMP Flaw Exploited: Root Access at Risk](#)

[COLDRIVER's ClickFix Campaign Targets Civil Voices](#)

[September 2025 Linux Patch Roundup](#)

[BRICKSTORM Malware Quietly Builds the Perfect Hideout in US Networks](#)

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)

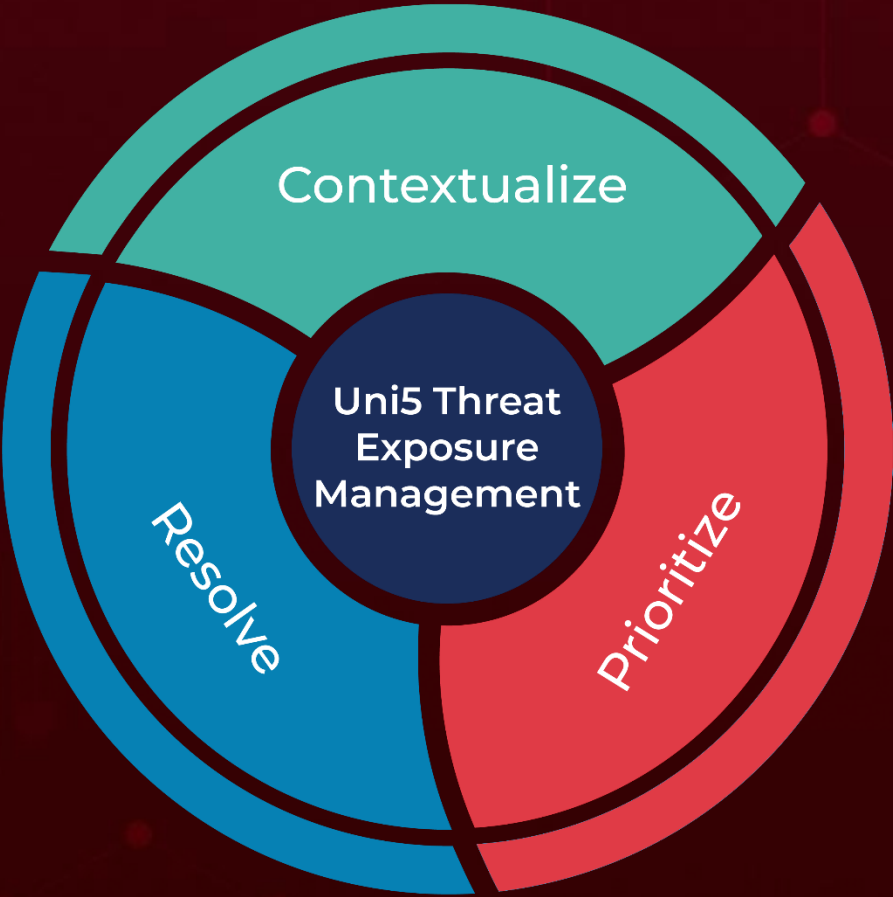
Attack Name	TYPE	VALUE
<u>Kazuar</u>	SHA256	3ecb09e659bcb500f9f40d022579a09acb11aec3a92c03e7d3fd2e56982d9eea
	SHA1	da7d5b9ab578ef6487473180b975a4b2701fda9e,d7df1325f66e029f4b77e211a238aa060d7217ed,a7acee41d66b537d900403f0e6a26ab6a1290a32,54f2245e0d3adec566e4d822274623bf835e170c,371ab9eb2a3da44099b2b7716de0916600450cfd,4a58365eb8f928ec3cd62ff59e59645c2d8c0ba5,214dc22fa25314f9c0dda54f669ede72000c85a4
<u>PteroOdd</u>	SHA1	7db790f75829d3e6207d8ec1cbcd3c133f596d67,2610a899fe73b8f018d19b50be55d66a6c78b2af,3a24520566bbe2e262a2911e38fd8130469ba830
<u>MINIBIKE</u>	MD5	b40533e67e70b7ff7bb53d34a4b9170e,67e09818d1aa650896a432b1de54d376
	SHA256	0e4ff052250ade1edaab87de194e87a9afeff903695799bcbcb3571918b131100
<u>Atomic Stealer</u>	SHA256	e52dd70113d1c6eb9a09eafa0a7e7bcf1da816849f47ebcdc66ec9671eb9b350

Attack Name	TYPE	VALUE
<u>BadIIIS</u>	SHA256	01a616e25f1ac661a7a9c244fd31736188ceb5fce8c1a5738e807fdbef70fd60
<u>DeerStealer</u>	SHA256	b57c56e5f0d15eea013c39b5c169f3308ca3e8ffd0cf5b1ef001dba894beeeef0, 24475ae7781189075f64a2de1a7d1fd69b341b7adee67f0bd2286cfbf1f0b7f9, eb17f8296482b0c096a2249844a62988b6abdd8ffe8cbbe3398f422968d46875, e34d753f2b992cf74c1b9db61bad4d6c6089ab8ef9fb942c865290b2dd64b4ad, 9163f9237ad869a74715f9b126f7c577bd1f12afb8eae37ba07c11f00a39fa3e, 4640d425d8d43a95e903d759183993a87bafcb9816850efe57cfcfa4ace889ec, 569ac32f692253b8ab7f411fec83f31ed1f7be40ac5c4027f41a58073fef8d7d, 66282239297c60bad7eeae274e8a2916ce95afeb932d3be64bb615ea2be1e07a, a6f6175998e96fcecad5f9b3746db5ced144ae97c017ad98b2caa9d0be8a3cb5, b5ab21ddb7cb5bfbedee68296a3d98f687e9acd8ebcc4539f7fd234197de2227, d9db8cdef549e4ad0e33754d589a4c299e7082c3a0b5efdee1a0218a0a1bf1ee, e24c311a64f57fd16ffc98f339d5d537c16851dc54d7bb3db8778c26ccb5f2d1
<u>BAITSWITCH</u>	SHA256	87138f63974a8ccbbf5840c31165f1a4bf92a954bacccfbf1e7e5525d750aa48
<u>SIMPLEFIX</u>	SHA256	16a79e36d9b371d1557310cb28d412207827db2759d795f4d8e27d5f5afaf63f
<u>BRICKSTORM</u>	SHA256	90b760ed1d0dcb3ef0f2b6d6195c9d852bcb65eca293578982a8c4b64f51b035, 2388ed7aee0b6b392778e8f9e98871c06499f476c9e7eae6ca0916f827fe65df, aa688682d44f0c6b0ed7f30b981a609100107f2d414a3a6e5808671b112d1878

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

September 29, 2025 • 10:30 AM

© 2025 All Rights are Reserved by Hive Pro



More at www.hivepro.com