

Date of Publication
August 17, 2026



HiveForce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities, and Actors

10 to 16 AUGUST 2026

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>	20
<u>Adversaries in Action</u>	29
<u>Recommendations</u>	33
<u>Threat Advisories</u>	34
<u>Appendix</u>	35
<u>What Next?</u>	38

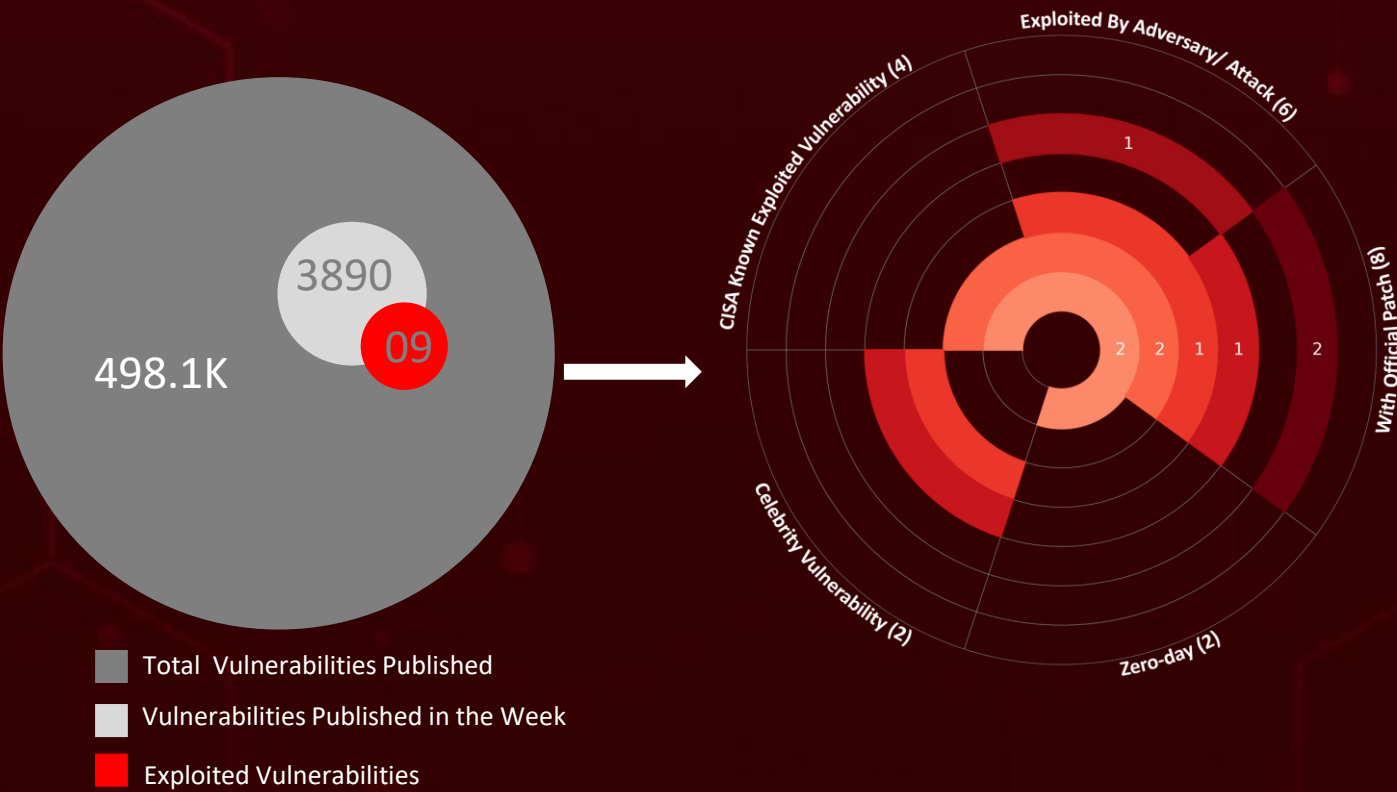
Summary

HiveForce Labs has reported a sharp rise in cybersecurity threats, highlighting the growing complexity and frequency of global cyber incidents. Over the past week, **12** major **attacks** were detected, **9** **vulnerabilities** were actively exploited, and **4** **threat actor** groups were closely monitored, signaling a concerning escalation in malicious activity worldwide.

Head Mare is punching through unpatched TrueConf servers, chaining two flaws for SYSTEM-level code execution. From there, it plants a web shell, swaps the real TrueConf installer for a trojanized one carrying the **PhantomCore** backdoor, and adds a second implant, **PhantomGraph**, that hides its command-and-control traffic inside Microsoft OneDrive.

Payroll Pirates is a money-driven phishing crew hijacking Microsoft 365 accounts to quietly mine finance and payroll mailboxes. Fake voicemail alerts route victims through trusted Google and Amazon services to an adversary-in-the-middle page that proxies the real Microsoft login and steals the session MFA and all.

Lazarus has revived **Operation Dream Job**, dangling fake recruiter offers at defense and aerospace staff to deliver weaponized PDFs or a trojanized PDF viewer. Together, these incidents underscore a growing trend of hybrid cyber operations that combine technical exploitation with social engineering, reinforcing the need for timely patching, continuous monitoring, and layered security defenses.



High Level Statistics

12

Attacks
Executed

9

Vulnerabilities
Exploited

4

Adversaries in
Action

- [PhantomCore](#)
- [PhantomGraph](#)
- [Troy](#)
- [FudModule](#)
- [RelayShell](#)
- [MISTPEN](#)
- [ForestTiger](#)
- [DeadLock](#)
- [Gunra](#)
- [PATCHCORD](#)
- [SHEETCORD](#)
- [HACKERAI C2 Agent](#)

- [CVE-2026-64638](#)
- [CVE-2026-68820](#)
- [CVE-2026-62832](#)
- [CVE-2026-72971](#)
- [CVE-2025-49113](#)
- [CVE-2024-51324](#)
- [CVE-2024-55591](#)
- [CVE-2025-24472](#)
- [CVE-2024-6387](#)

- [Head Mare](#)
- [Payroll Pirates](#)
- [Lazarus](#)
- [APT36](#)



Insights

CVE-2026-64638 (XSS2Shell): Pre-Auth XSS Hits WordPress Core

DeadLock Ransomware Exploits Vulnerable (**CVE-2024-51324**) Baidu Driver to Disable EDR

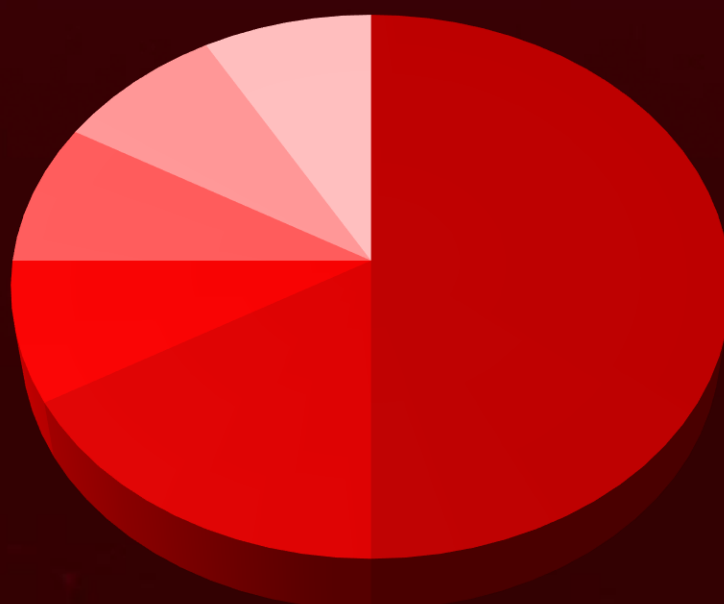
421 Fixes, 39 Ticking Clocks: August 2026 Patch Tuesday

Gunra Ransomware Escalates Double Extortion, Weaponizing **CVE-2024-55591** and **CVE-2025-24472** for Entry

Lazarus Revives Operation Dream Job, Exploiting Windows Zero-Day CVE-2026-68820

Cloned Telecom and NIC Portals Push **PATCHCORD** While Staging Servers Hold **regreSSHion** Exploit

Threat Distribution



■ Backdoor

■ Ransomware

■ Rootkit

■ Downloader

■ Webshell

■ Framework

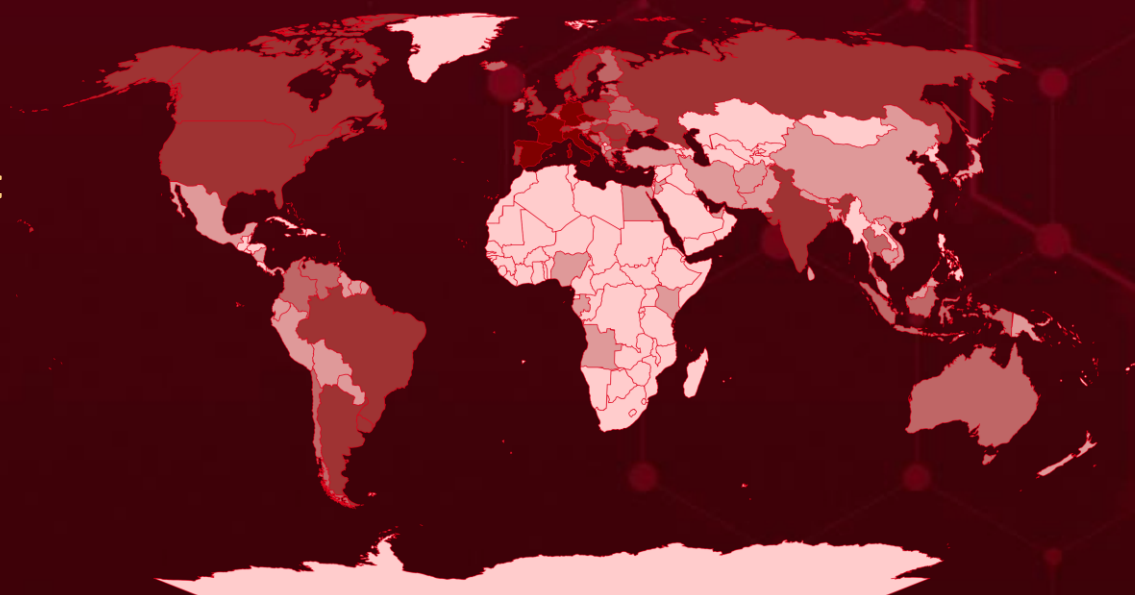


Targeted Countries

Most



Least

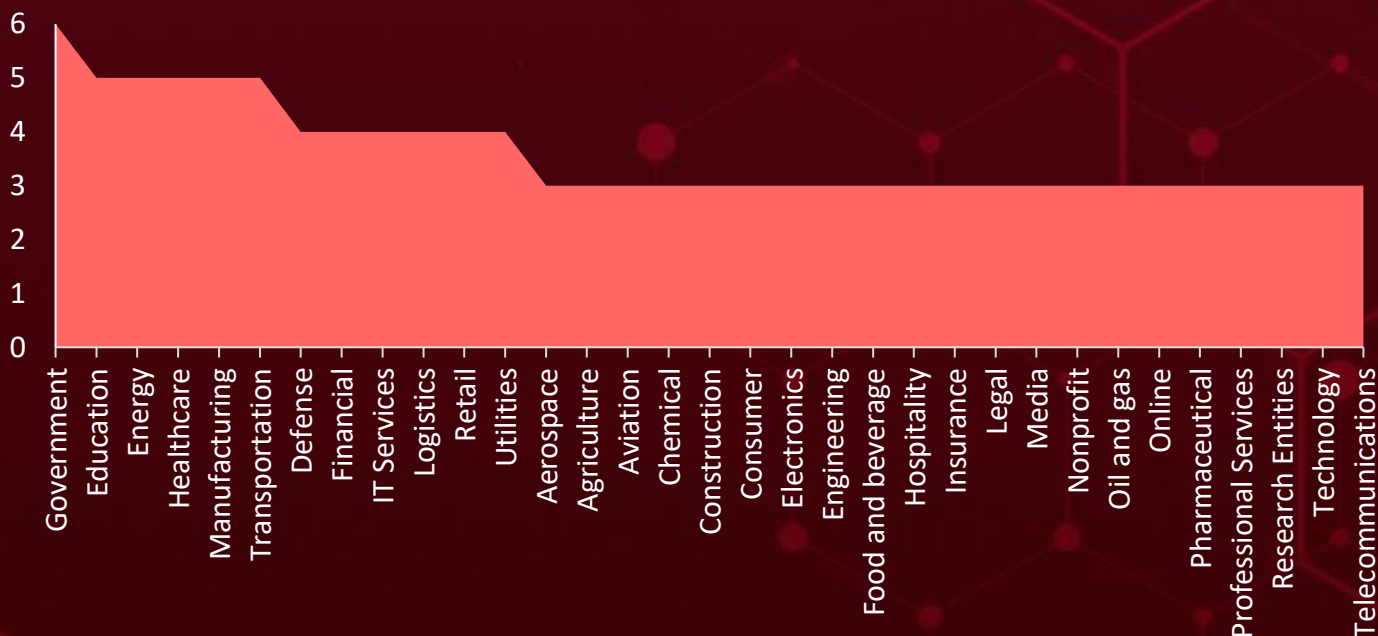


Powered by Bing

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

Countries	Countries	Countries	Countries
France	Holy See	Republic of Ireland	Nigeria
Spain	Iceland	Belgium	Iran
Germany	Slovakia	Luxembourg	Cambodia
Croatia	Venezuela	Latvia	Japan
Czech Republic	Indonesia	Peru	Panama
Italy	Liechtenstein	Nicaragua	Jordan
Russia	Serbia	Albania	Paraguay
Norway	Bosnia and Herzegovina	Ecuador	Kenya
Uruguay	Belarus	Pakistan	China
Brazil	Chile	Egypt	Afghanistan
Portugal	Ukraine	Suriname	Sri Lanka
Bulgaria	Malta	Bangladesh	Malaysia
Switzerland	Greece	Nepal	Taiwan
Canada	Moldova	French Guiana	Maldives
Netherlands	San Marino	North Macedonia	United Arab Emirates
Argentina	Monaco	Gabon	Mexico
Poland	Singapore	Papua New Guinea	Vietnam
Denmark	Montenegro	Angola	Tunisia
Romania	Slovenia	South Korea	Israel
Hungary	Estonia	Guyana	Tanzania
Sweden	Colombia	Turkey	Jamaica
India	Finland	Hong Kong	Cyprus
United Kingdom	Thailand	Bahamas	Armenia
United States	Australia	Bhutan	Jersey
Lithuania	Andorra	New Zealand	
	Austria	Bolivia	

Targeted Industries



TOP MITRE ATT&CK TTPs

T1059

Command and Scripting Interpreter

T1190

Exploit Public-Facing Application

T1566

Phishing

T1059.003

Windows Command Shell

T1036

Masquerading

T1102

Web Service

T1071

Application Layer Protocol

T1068

Exploitation for Privilege Escalation

T1548

Abuse Elevation Control Mechanism

T1505

Server Software Component

T1211

Exploitation for Defense Evasion

T1041

Exfiltration Over C2 Channel

T1003

OS Credential Dumping

T1082

System Information Discovery

T1583

Acquire Infrastructure

T1070

Indicator Removal

T1057

Process Discovery

T1204

User Execution

T1505.003

Web Shell

T1078

Valid Accounts

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
PhantomCore	PhantomCore is a backdoor used by the hacktivist group Head Mare, active since 2023 and known for consistently targeting Russia. It gathers information about the victim, including their public IP address, to build a detailed picture of the target before deploying its final-stage payload or running additional commands on the compromised system.	Unpatched TrueConf video conferencing servers	-
TYPE		IMPACT	AFFECTED PLATFORM
Backdoor		System Compromise	TrueConf Server, TrueConf Client
ASSOCIATED ACTOR			PATCH LINK
Head Mare			-
IOC TYPE	VALUE		
MD5	c5a460e4e68a088f6e51b2c6474642ec, 129462164a7d52e9ea8560b60f0412c5		
SHA256	b9e4052b310f9451eca9784a4a33bf5282d1bd07e3359eba9648be625e2e40dd		

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
PhantomGraph	PhantomGraph is a backdoor made up of two modules. The first, SysExcSvc.dll, receives commands from the attackers and sends back the results, using a Microsoft OneDrive account as its command-and-control (C2) server. The second, SysReadSvc.dll, reads the command passed along by the first module, executes it, and saves the result.	Unpatched TrueConf video conferencing servers	-
TYPE		IMPACT	AFFECTED PLATFORM
Backdoor		System Compromise	TrueConf Server, TrueConf Client
ASSOCIATED ACTOR			PATCH LINK
Head Mare			-
IOC TYPE	VALUE		
MD5	489f43be558b2679284ceabed7adc4f3, dd1fd2b459b97b7d59375cb8383cd19a		
SHA256	0fce4b732ce10c72093587e82ca9747a885430e366934ddc27e437443ff0cc0e		

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>Troy</u>	Troy backdoor is a newly identified modular remote access trojan in Lazarus' arsenal. Delivered as a 64-bit DLL, it supports 17 operator commands, giving attackers a broad range of remote access and post-exploitation capabilities. Troy is configured with three command-and-control (C2) servers, each with its own URL and port. At startup, it works through them in order, parsing each URL into its host and path, opening an HTTP connection, and sending a connection request, then validates the response against the string CONNECTED and sticks with the first server that answers successfully.	Phishing, Exploiting Vulnerability	CVE-2026-68820 CVE-2025-49113
TYPE		IMPACT	AFFECTED PLATFORM
Backdoor		System Compromise	Microsoft Windows, Roundcube Webmail
ASSOCIATED ACTOR			PATCH LINKS
Lazarus			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-68820 , https://github.com/roundcube-mail/releases
IOC TYPE	VALUE		
SHA256	590fb6ae19480d694e08ee85859cad8066f2f87e7e5abba2960c6d115e1615d6, 68d4fba7b1300a59cd6212c08910a260cd71b40cd9f51cac933030a68faac0bb		

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>FudModule</u>	FudModule is an advanced rootkit developed by the North Korean threat actor group. It's built to gain admin-to-kernel access on Windows systems, letting attackers read and write arbitrary kernel memory. With that access, FudModule can disable a range of security monitoring features, modifying kernel variables and removing kernel callbacks, to blind products like EDRs, firewalls, and antimalware tools.	Phishing, Exploiting Vulnerability	CVE-2026-68820 CVE-2025-49113
TYPE		IMPACT	AFFECTED PLATFORM
Rootkit		System Compromise	Microsoft Windows, Roundcube Webmail
ASSOCIATED ACTOR			PATCH LINKS
Lazarus			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-68820 , https://github.com/roundcube/roundcube-mail/releases
IOC TYPE	VALUE		
SHA256	3b6378df8442e63a6ed7317075913e4720847a510d95022d4a8347b2637c245d		

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
RelayShell	RelayShell is a previously undocumented PHP web shell that the threat actor deployed after compromising a web server. Unlike a traditional web shell that runs commands directly, RelayShell mainly acts as a communication relay between the attacker and an infected endpoint. It operates in two distinct modes, which we call Victim mode and Operator mode, chosen based on the password supplied in the HTTP POST request.	Phishing, Exploiting Vulnerability	CVE-2026-68820 CVE-2025-49113
TYPE		IMPACT	AFFECTED PLATFORM
Webshell		System Compromise	Microsoft Windows, Roundcube Webmail
ASSOCIATED ACTOR			PATCH LINKS
Lazarus			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-68820 , https://github.com/roundcube/roundcube-mail/releases
IOC TYPE	VALUE		
SHA256	21c3ad4838c4324bc5f081021da5fb2e9073d0c9304087811c21eb47c9e22762, cc4e06aa378a190f71384c03023bb3d18a6d66e297d46701220e132963d2e222		

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>MISTPEN</u>	MISTPEN is a lightweight, in-memory downloader that uses the Microsoft Graph API to reach attacker-controlled files hosted on OneDrive and pull down additional payloads. Every file exchanged through OneDrive is encrypted with AES, using separate keys for uploads and downloads. Its core capability is reflectively loading PE DLL files straight into memory, letting attackers deploy more payloads without ever touching disk. Before delivering the final backdoor, MISTPEN often runs several in-memory modules built for specific tasks; these modules have no network communication of their own, they simply do their job and hand the results back to MISTPEN, which then uploads the data to the C2.	Phishing, Exploiting Vulnerability	CVE-2026-68820 CVE-2025-49113
TYPE		IMPACT	AFFECTED PLATFORM
Downloader		Loads additional payload	Microsoft Windows, Roundcube Webmail
ASSOCIATED ACTOR			PATCH LINKS
Lazarus			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-68820 , https://github.com/roundcube/roundcube-mail/releases
IOC TYPE	VALUE		
SHA256	2db25ac41a66aa523c79e23e00443573530dd7bd82b8371bcc87bd7232e141eb, 5278ee922838352f1480a73e971161017d643a80b7ec22bf725897dfd088696d		

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
ForestTiger	ForestTiger is a well-documented backdoor widely attributed to the Lazarus threat group. Once deployed, it gives attackers long-term remote access to the compromised host. Its command-and-control (C2) infrastructure has historically relied mainly on compromised servers running WordPress and SharePoint, though in more recent campaigns the threat actor appears to have shifted toward using compromised Roundcube webmail servers as C2.	Phishing, Exploiting Vulnerability	CVE-2026-68820 CVE-2025-49113
TYPE		IMPACT	AFFECTED PLATFORM
Backdoor		System Compromise	Microsoft Windows, Roundcube Webmail
ASSOCIATED ACTOR			PATCH LINKS
Lazarus			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-68820 , https://github.com/roundcube/roundcube-mail/releases
IOC TYPE	VALUE		
SHA256	72dcae85e062f541fecad9ec7a18a3123e7ae5ac5d53c91709b53a46dbbd289, 231b1ef8b95bf77887d5377e2a60f649035e78f543af1b82877db36a5759d858		

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>DeadLock</u>	DeadLock is a financially motivated, human-operated ransomware operation active since mid-2025 that combines double extortion with a decentralized back end. They load a legitimate Baidu antivirus driver with a known flaw (CVE-2024-51324) and use it to kill EDR from the kernel, turning a security product into the weapon that blinds the rest.	Stolen Credentials	CVE-2024-51324
TYPE		IMPACT	AFFECTED PLATFORM
Ransomware		Data stolen, Backups disabled, Operations halted	Baidu Antivirus
ASSOCIATED ACTOR			PATCH LINK
-			
IOC TYPE	VALUE		
SHA256	a1fdf65020ce4a0f0940c793c6425baf8a0b994ec48b9baaf72788661a9d29f4, 3c1b9df801b9abbb3684670822f367b5b8cda566b749f457821b6481606995b3		

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>Gunra</u>	Gunra is a Conti-derived ransomware-as-a-service, active since April 2025, now running a formal affiliate program under the alias "Golden Community." Uses double extortion with a multi-threaded ChaCha20 + RSA-4096 locker against Windows and Linux.	Exploiting vulnerabilities	CVE-2024-55591 CVE-2025-24472
TYPE		IMPACT	AFFECTED PLATFORM
Ransomware		Data encryption, extortion	Fortinet FortiOS, FortiProxy
ASSOCIATED ACTOR			PATCH LINK
-			https://fortiguard.fortinet.com/psirt/FG-IR-24-535
IOC TYPE	VALUE		
SHA256	75e5621756e9d19efeac2bcbb2ac4711fb85243c03b0a19c05b18e31a780691e, 25c8cb27947042de89d634b3e260e614e5b1425a89494fa4e4295bcabfa8ee48		

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>PATCHCORD</u>	PATCHCORD is a compiled C/C++ backdoor delivered through sector-specific lures, including fake VPN installers impersonating Afghan Telecom (AFTEL) and telecom management tools. It abuses Google Sheets for its command-and-control (C2) communication and has been actively distributed through a domain impersonating India's National Informatics Centre (NIC). Once running, PATCHCORD hides its console window, sets up persistence by hijacking browser shortcuts, fingerprints the host, registers with its C2 server, and then enters its main tasking loop.	Phishing	CVE-2024-6387
TYPE		IMPACT	AFFECTED PLATFORM
Backdoor		System Compromise	OpenSSH server
ASSOCIATED ACTOR			PATCH LINKS
APT36			https://www.openssh.org/txt/release-9.8 , https://www.openssh.org/releasesnotes.html
IOC TYPE	VALUE		
SHA256	d46ee94d6a27ff9f02cff6fb57780acac2833ce48c95e63042a6274e24a040bb, 50fc220347f9e281037e831c3755dc70a8ba7f663025aea35b301226918b016b		

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>SHEETCORD</u>	SHEETCORD is a Go-based backdoor that blends functionality from the earlier SHEETCREEP RAT with several capabilities introduced in PATCHCORD, suggesting the operator's tooling is evolving. Like PATCHCORD, it can run remote commands (via <code>main.executeShellCommand</code>) and includes a <code>main.getHostInfo</code> function that works much like PATCHCORD's registration payload builder, collecting the victim's hostname for the initial check-in. Notably, the Go variant gathers far less system information than PATCHCORD's detailed fingerprinting, which pulled hostname, username, process details, and OS version.	Phishing	CVE-2024-6387
TYPE		IMPACT	AFFECTED PLATFORM
Backdoor		System Compromise	OpenSSH server
ASSOCIATED ACTOR			PATCH LINKS
APT36			https://www.openssh.org/txt/release-9.8 , https://www.openssh.org/releasesnotes.html
IOC TYPE	VALUE		
SHA256	959bbb09cd86ce3930406bf1cf32776ca477dfefe3fd63e90bf0017fccd90587		

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>HACKERAI C2 Agent</u>	HACKERAI C2 Agent is a previously undocumented malware framework that shares several capabilities with PATCHCORD and SHEETCORD, including system fingerprinting, remote command execution, and browser shortcut hijacking for persistence.	Phishing	CVE-2024-6387
TYPE		IMPACT	AFFECTED PLATFORM
Framework		System Compromise, persistence	OpenSSH server
ASSOCIATED ACTOR			PATCH LINKS
APT36			https://www.openssh.org/txt/release-9.8 , https://www.openssh.org/releasesnotes.ht ml
IOC TYPE	VALUE		
SHA256	74d347785dc47f8cda3876826cdd3fb3935ac55dc8e9e0c0f96d5ef4e00089a2		

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 PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-64638</u>	XSS2Shell	WordPress Core 4.7.0 through 7.0.2, all branches; before 7.0.3	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:wordpress:wordpress:*.~.~.~.~.~.~.~.*	-
XSS2Shell (WordPress Core Pre-Auth Reflected Cross-Site Scripting Vulnerability)			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-79	T1190: Exploit Public-Facing Application, T1189: Drive-by Compromise, T1059: Command and Scripting Interpreter, T1059.007: JavaScript, T1211: Exploitation for Defense Evasion, T1528: Steal Application Access Token	https://wordpress.org/news/2026/08/wordpress-7-0-3-release/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-68820</u>		Windows Server 2012, 2016, 2019, 2022, 2025, Windows 10- 11 26H1	Lazarus
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*	Troy FudModule RelayShell MISTPEN ForestTiger
Microsoft Windows Ancillary Function Driver for WinSock Use-After-Free Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1190: Exploit Public-Facing Application, T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-68820

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-62832</u>		Windows Server 2022, 2025, Windows 10 - 11 26H1	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*	-
Windows User Profile Service Elevation of Privilege Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-59	T1190: Exploit Public-Facing Application, T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62832

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-72971</u>		Windows 11 26H1	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*	-
Windows Container Isolation FS Filter Driver (unionfs.sys) Tampering Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-59	T1190: Exploit Public-Facing Application	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-72971

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2025-49113</u>		Roundcube Webmail before 1.5.10 and 1.6.x before 1.6.11	Lazarus
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV		
RoundCube Webmail Deserialization of Untrusted Data Vulnerability		cpe:2.3:a:roundcube:webmail:*:*:*:*:*:*	Troy FudModule RelayShell MISTPEN ForestTiger
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://github.com/roundcube/roundcubemail/releases

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2024-51324</u>		BdApiUtil driver of Baidu Antivirus v5.2.3.116083	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:baidu:baidu_antivirus:*.*.*.*.*.*.*	DeadLock Ransomware
Baidu Antivirus Improper Privilege Management Arbitrary Process Termination Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-269	T1588: Obtain Capabilities, T1105: Ingress Tool Transfer, T1036: Masquerading, T1068: Exploitation for Privilege Escalation	

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2024-55591</u>		FortiOS 7.0.0 - 7.0.16; FortiProxy 7.0.0 - 7.0.19, 7.2.0 - 7.2.12	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:fortinet:fortiproxy:*:*:*:*:*:* cpe:2.3:o:fortinet:fortios:*:*:*:*:*:*	Gunra Ransomware
Fortinet FortiOS and FortiProxy Authentication Bypass Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-288	T1190: Exploit Public-Facing Application, T1078: Valid Accounts , T1068 : Exploitation for Privilege Escalation	https://fortiguard.fortinet.com/psirt/FG-IR-24-535

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2025-24472</u>		FortiOS 7.0.0 - 7.0.16; FortiProxy 7.0.0 - 7.0.19, 7.2.0 - 7.2.12	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:fortinet:fortiproxy:*:*:*:*:* cpe:2.3:o:fortinet:fortios:*:*:*:*:*	Gunra Ransomware
Fortinet FortiOS and FortiProxy Authentication Bypass Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-288	T1190: Exploit Public-Facing Application, T1078: Valid Accounts , T1068 : Exploitation for Privilege Escalation	https://fortiguard.fortinet.com/psirt/FG-IR-24-535

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2024-6387</u>	regreSSHion	OpenSSH server	APT36
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:openssh:openssh:*.*.*:*.*.*.*	PATCHCORD SHEETCORD HACKERAI C2 Agent
regreSSHion (OpenSSH Unauthenticated Remote Code Execution Vulnerability)			PATCH LINKS
	CWE ID	ASSOCIATED TTPs	
	CWE-362, CWE-364	T1059: Command and Scripting Interpreter, T1190: Exploit Public-Facing Application	https://www.openssh.org/txt/release-9.8 , https://www.openssh.org/releasenotes.html



Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGION
 Head Mare	-	Instrumentation, Electronics, Transportation, Energy, IT, Software Development	Russia
	MOTIVE		
	Information Theft, Espionage, Financial Gain		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	-	PhantomCore, PhantomGraph	TrueConf Server, TrueConf Client
TTPs			
TA0001: Initial Access, TA0002: Execution, TA0003: Persistence, TA0004: Privilege Escalation, TA0005: Defense Evasion, TA0006: Credential Access, TA0007: Discovery, TA0011: Command and Control, TA0010: Exfiltration, T1190: Exploit Public-Facing Application, T1199: Trusted Relationship, T1566: Phishing, T1059: Command and Scripting Interpreter, T1059.001: PowerShell, T1059.003: Windows Command Shell, T1505: Server Software Component, T1505.003: Web Shell, T1543: Create or Modify System Process, T1543.003: Windows Service, T1546: Event Triggered Execution, T1546.015: Component Object Model Hijacking, T1068: Exploitation for Privilege Escalation, T1027: Obfuscated Files or Information, T1036: Masquerading, T1003: OS Credential Dumping, T1003.001: LSASS Memory, T1082: System Information Discovery, T1033: System Owner/User Discovery, T1102: Web Service, T1102.002: Bidirectional Communication, T1572: Protocol Tunneling, T1041: Exfiltration Over C2 Channel			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 <u>Payroll Pirates</u> <u>(aka Storm-2755)</u>	-	Healthcare, Education, Manufacturing, Government, Professional Services	United States, Canada, Europe
	MOTIVE		
	Financial Gains		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	-	-	Microsoft 365, Microsoft Outlook, Microsoft Graph API, Microsoft Entra ID
TTPs			
TA0042: Resource Development, TA0001: Initial Access, TA0006: Credential Access, TA0005: Defense Evasion, TA0011: Command and Control, TA0007: Discovery, TA0009: Collection, T1583: Acquire Infrastructure, T1583.001: Domains, T1566: Phishing, T1566.002: Spearphishing Link, T1557: Adversary-in-the-Middle, T1111: Multi-Factor Authentication Interception, T1539: Steal Web Session Cookie, T1550: Use Alternate Authentication Material, T1550.004: Web Session Cookie, T1036: Masquerading, T1036.005: Match Legitimate Name or Location, T1684: Social Engineering, T1684.001: Impersonation, T1090: Proxy, T1090.002: External Proxy, T1087: Account Discovery, T1087.004: Cloud Account, T1114: Email Collection, T1114.002: Remote Email Collection			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 <u>Lazarus (aka 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, UNC2970, UNC4034, UNC4736, UNC4899, Diamond Sleet, Citrine Sleet, Jade Sleet, TraderTraitor, Gleaming Pisces, Slow Pisces, G0032)</u>	North Korea	Defense, Aerospace, and Aviation	Europe (France, Germany), India, and South America (Brazil)
	MOTIVE		
	Information theft and espionage, Sabotage and destruction, Financial crime		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	CVE-2026-68820 CVE-2025-49113	Troy, FudModule, RelayShell, MISTPEN, ForestTiger	Microsoft Windows, Roundcube Webmail
TTPs			
TA0042: Resource Development, TA0001: Initial Access, TA0002: Execution, TA0003: Persistence, TA0004: Privilege Escalation, TA0005: Defense Evasion, TA0006: Credential Access, TA0007: Discovery, TA0009: Collection, TA0011: Command and Control, TA0010: Exfiltration, T1583: Acquire Infrastructure, T1583.001: Domains, T1584: Compromise Infrastructure, T1584.004: Server, T1608: Stage Capabilities, T1608.001: Upload Malware, T1608.006: SEO Poisoning, T1586: Compromise Accounts, T1586.002: Email Accounts, T1566: Phishing, T1566.003: Spearphishing via Service, T1566.001: Spearphishing Attachment, T1190: Exploit Public-Facing Application, T1204: User Execution, T1204.002: Malicious File, T1059: Command and Scripting Interpreter, T1059.003: Windows Command Shell, T1505: Server Software Component, T1505.003: Web Shell, T1068: Exploitation for Privilege Escalation, T1574: Hijack Execution Flow, T1574.002: DLL Side-Loading, T1014: Rootkit, T1562: Impair Defenses, T1562.001: Disable or Modify Tools, T1055: Process Injection, T1055.001: Dynamic-link Library Injection, T1684: Social Engineering, T1684.001: Impersonation, T1027: Obfuscated Files or Information, T1140: Deobfuscate/Decode Files or Information, T1036: Masquerading, T1036.005: Match Legitimate Resource Name or Location, T1070: Indicator Removal, T1070.004: File Deletion, T1078: Valid Accounts, T1057: Process Discovery, T1082: System Information Discovery, T1113: Screen Capture, T1560: Archive Collected Data, T1560.001: Archive via Utility, T1071: Application Layer Protocol, T1071.001: Web Protocols, T1102: Web Service, T1041: Exfiltration Over C2 Channel			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 <u>APT36 (aka Transparent Tribe, ProjectM, TEMP.Lapis, Mythic Leopard, Copper Fieldstone, Earth Karkaddan, STEPPY-KAVACH, Green Havildar, APT-C-56, Storm-0156, Opaque Draco)</u>	Pakistan	Telecommunications, Government, Defense, Energy, Critical Infrastructure	Afghanistan, India, South Asia
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	CVE-2024-6387	PATCHCORD, SHEETCORD, HACKERAI C2 Agent	OpenSSH server
TTPs			
TA0042: Resource Development, TA0001: Initial Access, TA0002: Execution, TA0003: Persistence, TA0005: Defense Evasion, TA0007: Discovery, TA0006: Credential Access, TA0011: Command and Control, TA0010: Exfiltration, T1583: Acquire Infrastructure, T1583.001: Domains, T1583.006: Web Services, T1566: Phishing, T1566.001: Spearphishing Attachment, T1566.002: Spearphishing Link, T1190: Exploit Public-Facing Application, T1204: User Execution, T1204.002: Malicious File, T1059: Command and Scripting Interpreter, T1059.003: Windows Command Shell, T1059.001: PowerShell, T1059.005: Visual Basic, T1620: Reflective Code Loading, T1547: Boot or Logon Autostart Execution, T1547.001: Registry Run Keys / Startup Folder, T1547.009: Shortcut Modification, T1564: Hide Artifacts, T1564.003: Hidden Window, T1497: Virtualization/Sandbox Evasion, T1497.001: System Checks, T1622: Debugger Evasion, T1140: Deobfuscate/Decode Information, T1057: Process Discovery, T1082: System Information Discovery, T1555: Credentials from Password Stores, T1071: Application Layer Protocol, T1071.001: Web Protocols, T1102: Web Service, T1102.002: Bidirectional Communication, T1132: Data Encoding, T1132.001: Standard Encoding, T1571: Non-Standard Port, T1041: Exfiltration Over C2 Channel			

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **nine exploited vulnerabilities** and block the indicators related to the threat actors **Head Mare, Payroll Pirates, Lazarus, and APT36**, and malware **PhantomCore, PhantomGraph, Troy, FudModule, RelayShell, MISTPEN, ForestTiger, DeadLock, Gunra, PATCHCORD, SHEETCORD**, and **HACKERAI C2 Agent**.

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 **nine exploited vulnerabilities**.
- Testing the efficacy of their security controls by simulating the attacks related to the threat actors **Head Mare, Lazarus, and APT36**, and malware **PhantomCore, PhantomGraph, Troy Backdoor, MISTPEN, DeadLock Ransomware, Gunra Ransomware, PATCHCORD, SHEETCORD** in Breach and Attack Simulation(BAS).

Threat Advisories

[CVE-2026-64638 \(XSS2Shell\): Pre-Auth XSS in the WordPress Login Screen](#)

[Head Mare Chains TrueConf Server Flaws to Drop PhantomCore and PhantomGraph](#)

[Payroll Pirates Abuse AiTM Phishing to Compromise Microsoft 365](#)

[Microsoft Patch Tuesday August 2026 - Priority Fixes](#)

[Operation Dream Job: Lazarus Exploits a Windows Zero-Day to Deploy Backdoor](#)

[DeadLock Ransomware Anchors Extortion to the Polygon Blockchain](#)

[Gunra Ransomware Evolves into Full RaaS Operation Targeting Global Critical Infrastructure](#)

[PATCHCORD Cluster Targets South Asian Infrastructure](#)

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>PhantomCore</u>	MD5	c5a460e4e68a088f6e51b2c6474642ec, 129462164a7d52e9ea8560b60f0412c5, ec0bf4a2186a88874e9f26f07cfeb532, b348642146ea34771e5785c5857950f5, c915cb6c2aeb863ee8479238e1644217, 0e79996d9483d1e44fea32b0a48c2c19, 2bb75c20e778eb5c416965bd4d4259b1, b3a6fee3307f1c26841fd5c603e2b013, 8fcc3e4ccbf1725d9989fb464abf3561
	SHA256	b9e4052b310f9451eca9784a4a33bf5282d1bd07e3359eba9648be625e2e40dd
<u>PhantomGraph</u>	MD5	489f43be558b2679284ceabed7adc4f3, dd1fd2b459b97b7d59375cb8383cd19a, 0e4541c3153ec5ed01497f19cf4f63d0, 12d4e8f5295f2ef7e0f9bfc0f4830939, 7f267006cac10f341c356b62fe493527, ee2861d5965e8730708cd1da8a93fa4c
	SHA256	0fce4b732ce10c72093587e82ca9747a885430e366934ddc27e437443ff0cc0e
<u>Troy</u>	SHA256	590fb6ae19480d694e08ee85859cad8066f2f87e7e5abba2960c6d115e1615d6, 68d4fba7b1300a59cd6212c08910a260cd71b40cd9f51cac933030a68faac0bb, a738059ce07c951c31ab2da3d93d8f69bff32f9b7d933dbf5943441b9cc99075

Attack Name	TYPE	VALUE
<u>FudModule</u>	SHA256	3b6378df8442e63a6ed7317075913e4720847a510d95022d4a8347b2637c245d
<u>RelayShell</u>	SHA256	21c3ad4838c4324bc5f081021da5fb2e9073d0c9304087811c21eb47c9e22762, cc4e06aa378a190f71384c03023bb3d18a6d66e297d46701220e132963d2e222
<u>MISTPEN</u>	SHA256	2db25ac41a66aa523c79e23e00443573530dd7bd82b8371bcc87bd7232e141eb, 5278ee922838352f1480a73e971161017d643a80b7ec22bf725897dfd088696d, b4082d21070d9ddf53fde4ea22524d09e41ec9826ce63cef3c6235e458d21afb, fb3fc5626f68677fb1269a2fefbe70e719211b4065e836ab92e06a8210139a2d, ea7056f2bf36c66a61ff787ff5be975a85f534c3c5ca178791dac2504db2c619, 13d10bc99f7f7abe7ee0902be87920b73b2ea41bd9683dbfcad340dacbcdef79, 4fd32432341dfcf54d0517a6bbc38e5d265be70933493e4183c2a340cdde9a2d, 4dd792c9f672bbdcc8d363d745994efe90f4ffc5fdc2c059c8e379a48ad6a68a, ba96c603e44046de703c67b2c3b7e4ca974afef7b437a0244418bc4edc781bb7
<u>ForestTiger</u>	SHA256	72dcca85e062f541fecad9ec7a18a3123e7ae5ac5d53c91709b53a46dbbd289, 231b1ef8b95bf77887d5377e2a60f649035e78f543af1b82877db36a5759d858, 6da9b1e6f3315ceb77dd14a937a26cc3602bf6a7e2c2ecafb3c65ce5319837be, a0578a2b7821d7e2c573530648f26d7a0d98b373ab24fb7f0c792736761e542d, 82268052f94df6f4870d02e57b18d4c54136cc7a8c8d80ad162631f99462c943
<u>DeadLock</u>	SHA256	a1fdf65020ce4a0f0940c793c6425baf8a0b994ec48b9baaf72788661a9d29f4, 3c1b9df801b9abbb3684670822f367b5b8cda566b749f457821b6481606995b3, 3cd5703d285ed2753434f14f8da933010ecfdc1e5009d0e438188aaf85501612,

Attack Name	TYPE	VALUE
<u>DeadLock</u>	SHA256	c9cc95ff8f2998229394dfd31c2bd6b723e826a3ca5e008d2b5be19ba419ae2c, 2d89fb7455ff3ebf6b965d8b1113857607f7fbda4c752ccb591dbc1dc14ba0da
	TOR Address	deadblogdbdu5wprek7wa2o4ce7rnt6u6ntqeud3hzjjcveosgpsqqqd[.]]onion
<u>Gunra</u>	SHA256	75e5621756e9d19efeac2bcbb2ac4711fb85243c03b0a19c05b18e31a780691e, 25c8cb27947042de89d634b3e260e614e5b1425a89494fa4e4295bcabfa8ee48, 2dc70a12d158d437e45a55b1d52f3d61c6082a1e1667573302ba3b62813e2751, 834efe9b392c6c000877ea5613a079445affc16fe8af5997d68c55cafc95e5d1, 91f8fc7a3290611e28a35a403fd815554d9d856006cc2ee91ccdb64057ae53b0, a82e496b7b5279cb6b93393ec167dd3f50aff1557366784b25f9e51cb23689d9
<u>PATCHCORD</u>	SHA256	d46ee94d6a27ff9f02cff6fb57780acac2833ce48c95e63042a6274e24a040bb, 50fc220347f9e281037e831c3755dc70a8ba7f663025aea35b301226918b016b, 0f4073d3c866bc3daf55b25f71250b96ec120db94a4f9cc8fe85b7c9f9d346b3
<u>SHEETCORD</u>	SHA256	959bbb09cd86ce3930406bf1cf32776ca477dfefe3fd63e90bf0017fccd90587
<u>HACKERAI C2 Agent</u>	SHA256	74d347785dc47f8cda3876826cdd3fb3935ac55dc8e9e0c0f96d5ef4e00089a2

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 demo of HivePro.

REPORT GENERATED ON

August 17, 2026 • 7:00 AM

© 2026 All Rights are Reserved by Hive Pro



More at www.hivepro.com