Date of Publication
May 18, 2026

Hive Pro

Hiveforce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities, and Actors

11 to 17 MAY 2026

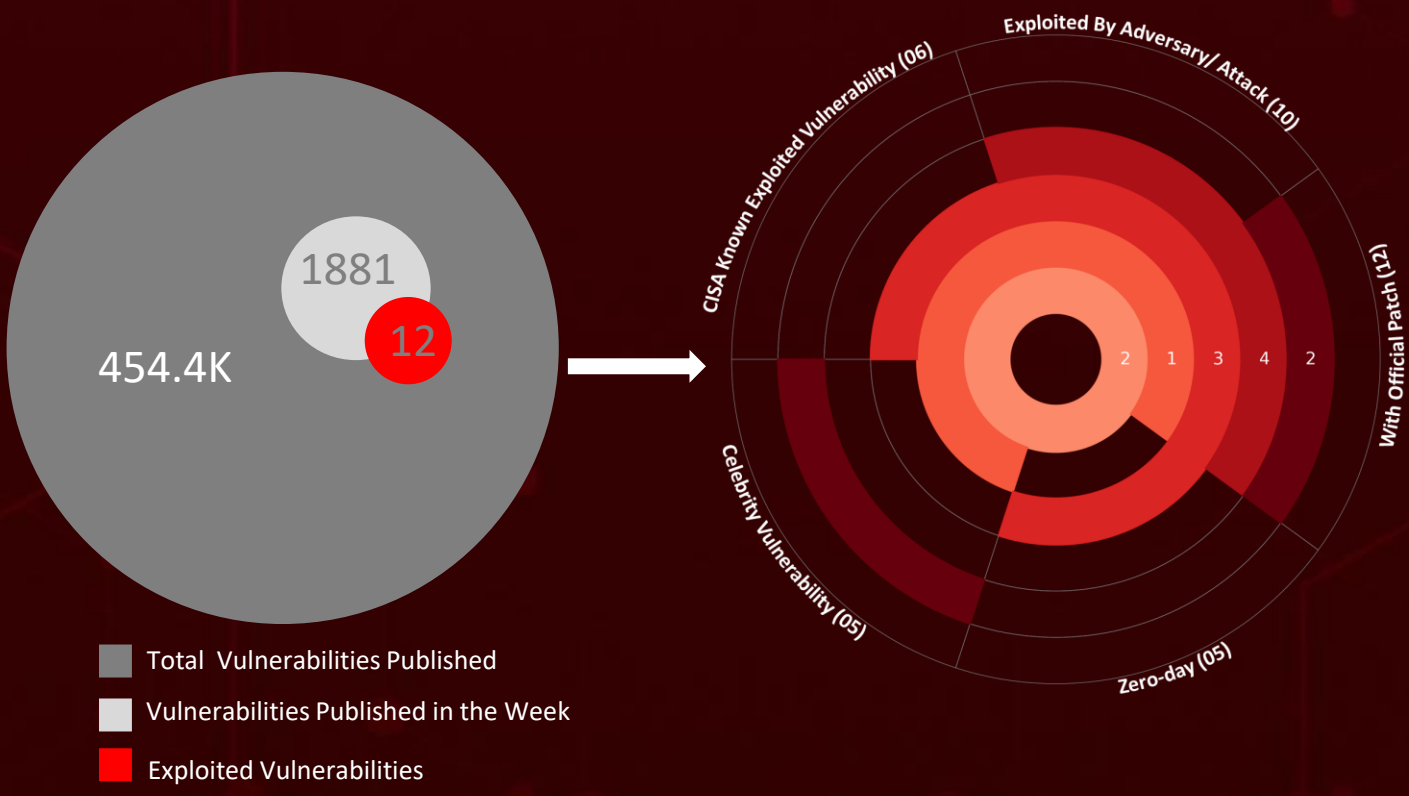
Table Of Contents

Summary

HiveForce Labs has reported a sharp rise in cybersecurity threats, highlighting the increasing complexity and frequency of global cyber incidents. Over the past week, **nine** major attacks were detected, **twelve** critical vulnerabilities were publicly disclosed, and **four** active threat actor groups were monitored, signaling a concerning escalation in malicious activity.

Dirty Frag (CVE-2026-43284/43500) Kernel-level privilege escalation in Linux networking enables unprivileged users to gain instant root access. **Quasar Linux** is a full-featured RAT targeting developers and DevOps workstations with rootkit, PAM backdoor, and credential harvesting to compromise publishing pipelines and orchestrate supply chain attacks.

GemStuffer is a campaign that injects malicious Ruby scripts into CI/CD pipelines to extract UK government intelligence through trojanized RubyGems packages, disguising theft as legitimate developer activity. These underscore the need for disciplined security updates and sustained monitoring in response to rapidly evolving attack methodologies.



High Level Statistics

9
Attacks Executed

12
Vulnerabilities Exploited

4
Adversaries in Action

- TCLBANKER
- Quasar Linux
- PCPJack
- Mini Shai-Hulud
- EarthWorm
- ReverseSocks5
- Deed RAT
- Terndoor
- Mofu Loader

- CVE-2026-43284
- CVE-2026-43500
- CVE-2025-29927
- CVE-2025-55182
- CVE-2026-1357
- CVE-2025-9501
- CVE-2025-48703
- CVE-2026-45321
- CVE-2026-0300
- CVE-2026-20182
- CVE-2022-41040
- CVE-2022-41082

- TeamPCP
- CL-STA-1132
- UAT-8616
- FamousSparrow

Insights

Brazilian Banks Under Siege: TCLBANKER Targets 59 Institutions via Trusted Vendor

CopyFail 2 is Here: Dirty Frag Joins the Second Universal Linux Kernel LPE in 8 Days

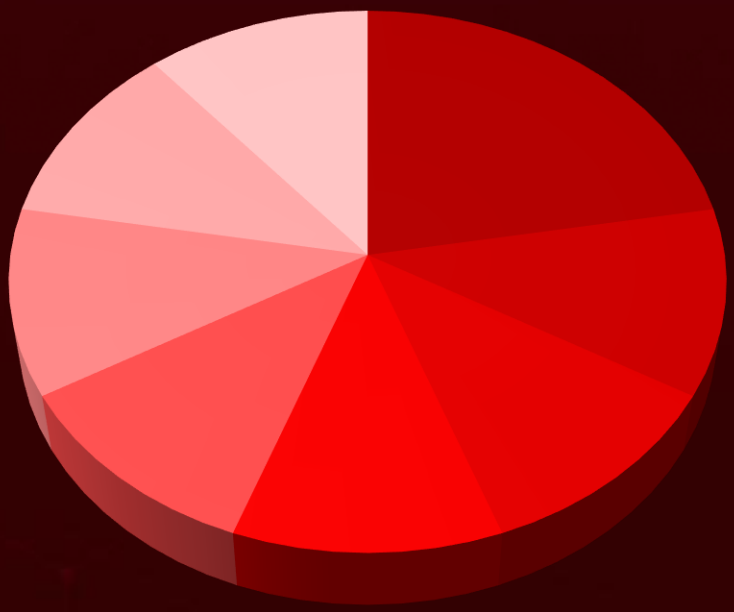
Quasar Linux: Full-Featured RAT Weaponizes Developer Workstations Into Supply Chain Attack Engines

TeamPCP's Supply Chain Weapon: 84 Malicious Packages Across TanStack Compromise 170+ npm Libraries

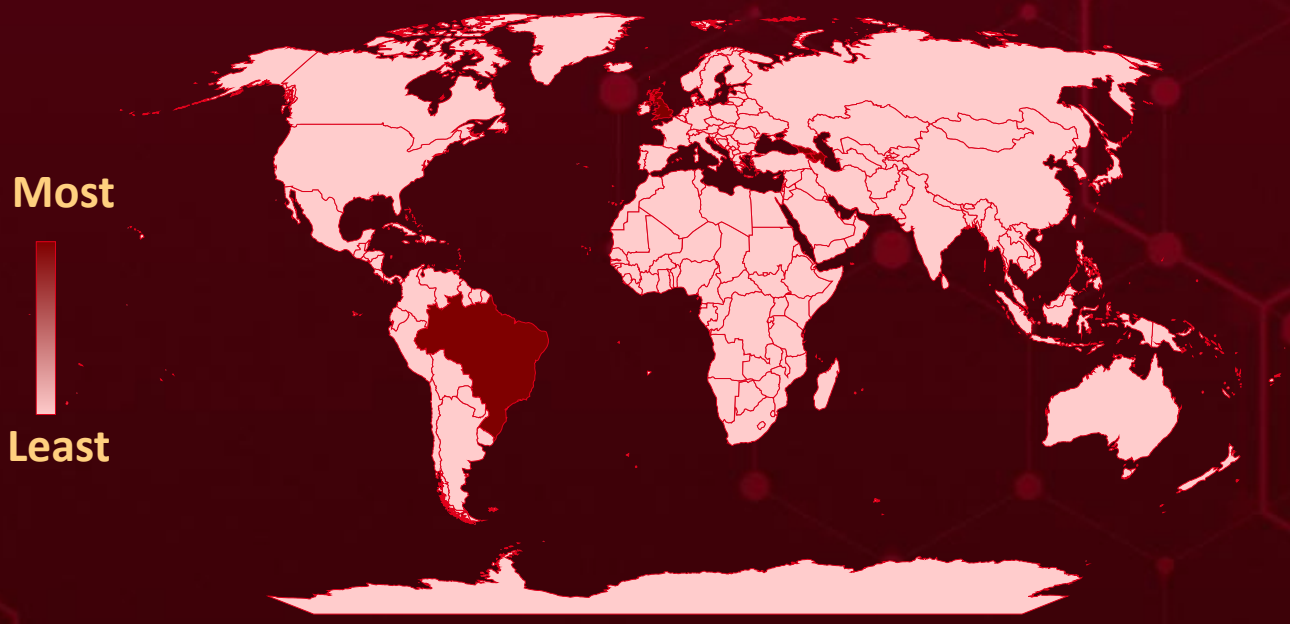
Government Data Heist: GemStuffer Campaign Exfiltrates UK Local Government Intelligence Through RubyGems

The Credential Black Market Feeder: PCPJack's Monetization Model Enables Industrial-Scale Credential Resale

Threat Distribution

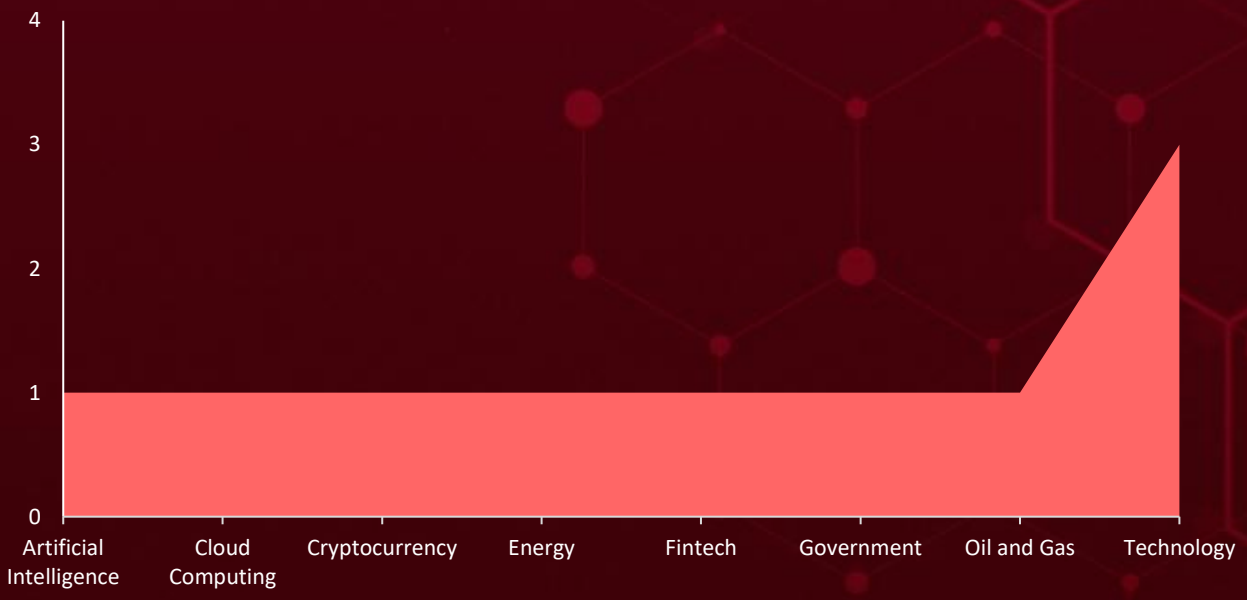


Targeted Countries



Countries	Countries	Countries	Countries
Brazil	Belgium	Cambodia	Cuba
Azerbaijan	Moldova	Mexico	Suriname
United Kingdom	Belize	Cameroon	Cyprus
Armenia	Nauru	Mongolia	Tajikistan
Georgia	Benin	Canada	Czechia
Peru	Antigua and Barbuda	Myanmar	Togo
Luxembourg	Bhutan	Central African Republic	Democratic Republic of the Congo
Switzerland	Qatar	Netherlands	Turkey
Argentina	Bolivia	Chad	Denmark
Morocco	San Marino	Nigeria	Ukraine
Albania	Bosnia and Herzegovina	Chile	Djibouti
Serbia	Slovakia	Papua New Guinea	Uruguay
Australia	Botswana	China	Dominica
Angola	Sri Lanka	Poland	Vietnam
Austria	Andorra	Colombia	Dominican Republic
Mauritania	Thailand	Russia	Afghanistan
Algeria	Brunei	Comoros	Ecuador
Nicaragua	Tuvalu	Saint Vincent and the Grenadines	Lithuania
Bahamas	Bulgaria	Congo	Egypt
Saint Kitts and Nevis	Vanuatu	Saudi Arabia	Madagascar
Bahrain	Burkina Faso	Costa Rica	El Salvador
South Africa	Liechtenstein	Sierra Leone	Malaysia
Bangladesh	Burundi	Côte d'Ivoire	Equatorial Guinea
Trinidad and Tobago	Malawi	Solomon Islands	Mali
Barbados	Cabo Verde	Croatia	Eritrea
Zambia	Malta	South Sudan	Marshall Islands
Belarus			Estonia
Maldives			

Targeted Industries



TOP MITRE ATT&CK TTPs

T1059 Command and Scripting Interpreter	**T1552** Unsecured Credentials	**T1190** Exploit Public-Facing Application	**T1071** Application Layer Protocol	**T1027** Obfuscated Files or Information
T1036 Masquerading	**T1071.001** Web Protocols	**T1021** Remote Services	**T1036.005** Match Legitimate Resource Name or Location	**T1543** Create or Modify System Process
T1057 Process Discovery	**T1041** Exfiltration Over C2 Channel	**T1070.004** File Deletion	**T1567** Exfiltration Over Web Service	**T1053** Scheduled Task/Job
T1068 Exploitation for Privilege Escalation	**T1070** Indicator Removal	**T1543.002** Systemd Service	**T1546** Event Triggered Execution	**T1059.001** PowerShell

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
TCLBANKER	TCLBANKER is a banking trojan delivered via trojanized Logitech Logi AI Prompt Builder MSI installers bundled inside ZIP files. It uses DLL side-loading to execute a malicious loader that deploys two .NET Reactor-protected modules: a banking trojan using WPF-based fraud overlays and WebSocket C2, and a worm module that self-propagates via WhatsApp session hijacking and Outlook COM-automated phishing emails.	Trojanized MSI Installer	-
		IMPACT	**AFFECTED PLATFORM**
TYPE		Malware self-propagation, Supply chain contamination, System compromise and resource hijacking	Windows
Banking Trojan			**PATCH LINK**
ASSOCIATED ACTOR			-
-			

IOC TYPE	VALUE
SHA256	701d51b7be8b034c860bf97847bd59a87dca8481c4625328813746964995b626

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Quasar Linux	Quasar Linux (QLNX) is a sophisticated Linux malware targeting developer workstations and DevOps environments. It employs the memfd_create syscall to load itself into memory, re-execute from the in-memory image, and delete the original binary from disk to erase its on-disk footprint. The malware uses the MFD_RE environment variable to prevent re-execution loops and includes fallback mechanisms for systems lacking memfd_create support via /proc/self/fd.	-	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		Persistence establishment, Sandbox/monitoring bypass	npm, PyPI, GitHub, AWS, Docker, Kubernetes, Git, HashiCorp Vault, Terraform
RAT			**PATCH LINK**
ASSOCIATED ACTOR			-
-			

IOC TYPE	VALUE
SHA256	ea1d34b21b739a6bbf89b3f7e67978005cf7f3eda612cefc7eac1c8ead7c5545

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>PCPJack</td><td rowspan="6">PCPJack is a modular credential theft framework that worms across exposed cloud infrastructure, harvesting credentials from cloud, container, developer, productivity, and financial services. The toolset actively evicts and replaces artifacts associated with the TeamPCP threat actor before establishing its own persistence and exfiltrating stolen data through attacker-controlled Telegram channels. Unlike typical cloud-focused malware, PCPJack does not deploy cryptominers, suggesting monetization through credential theft, fraud, spam, extortion, or resale of stolen access.</td><td>Dropper</td><td>CVE-2025-29927
CVE-2025-55182
CVE-2026-1357
CVE-2025-9501
CVE-2025-48703</td></tr>
<tr><td rowspan="2">TYPE</td><td>IMPACT</td><td>AFFECTED PRODUCT</td></tr>
<tr><td rowspan="3">Credential Loss, Infrastructure Compromise, Data Exfiltration</td><td>Docker, Kubernetes, Redis, MongoDB, RayML, Next.js, React, WordPress (WPVivid Backup, W3 Total Cache), CentOS Web Panel (CWP)</td></tr>
<tr><td>Framework</td><td>PATCH LINK</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td>https://github.com/vercel/next.js/releases, https://github.com/facebook/react/security/advisories/GHSA-fv66-9v8q-g76r, https://wordpress.org/plugins/wpvivid-backuprestore/, https://wordpress.org/plugins/w3-total-cache/, http://centos-webpanel.com/</td></tr>
<tr><td>-</td><td colspan="2"></td></tr>
<tr><td>IOC TYPE</td><td colspan="3">VALUE</td></tr>
<tr><td>SHA256</td><td colspan="3">b1d8149e5c7b6312f40c220e89b1913762f9aa416ff491540b3b7b7040260eb5</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 CVE
Mini Shai-Hulud	Mini Shai-Hulud is a self-propagating supply chain worm that compromises npm and PyPI packages to steal credentials from developer machines and CI/CD runners. The malware uses stolen credentials to automatically publish additional malicious package versions, enabling worm-like propagation across the software supply chain. Payloads are heavily obfuscated and execute during package installation.	Exploiting Vulnerability	CVE-2026-45321
		IMPACT	AFFECTED PRODUCT
TYPE		Credential Theft, Destructive Capabilities	TanStack Router npm Packages
Worm			PATCH LINK
ASSOCIATED ACTOR			https://github.com/TanStack/router/releases
TeamPCP			
IOC TYPE	VALUE		
SHA256	ab4fcadaec49c03278063dd269ea5eef82d24f2124a8e15d7b90f2fa8601266c		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
EarthWorm	EarthWorm is an open-source network tunneling utility frequently abused by adversaries for post-exploitation pivoting, including by APT groups like UAT-5918. It provides SOCKS5 proxy and port-forwarding features with forward, reverse, and multi-transfer modes across Windows, Linux, and macOS. Enables attackers to traverse segmented networks and reach internal assets shielded by firewalls.	-	CVE-2026-0300
		IMPACT	AFFECTED PRODUCT
TYPE		Covert tunneling, lateral movement	Palo Alto Networks PAN-OS
Tunneling tool			PATCH LINK
ASSOCIATED ACTOR			https://security.paloaltonetworks.com/CVE-2026-0300
CL-STA-1132			
IOC TYPE	VALUE		
SHA256	e11f69b49b6f2e829454371c31ebf86893f82a042dae3f2faf63dcd84f97a584		

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
ReverseSocks5	ReverseSocks5 is an open-source networking tool used to bypass firewalls or NAT by establishing an outbound connection from a target machine to a controller, rather than the other way around. Once the connection is established, it creates a SOCKS5 proxy tunnel that allows the controller to route traffic into the target's internal network. Used in the recent PAN-OS firewall zero-day campaign attributed to a suspected Chinese state actor, alongside Cavalry Werewolf operations.	-	CVE-2026-0300
		IMPACT	AFFECTED PRODUCT
TYPE		Firewall bypass, internal pivoting	Palo Alto Networks PAN-OS
Tunneling tool			PATCH LINK
ASSOCIATED ACTOR			https://security.paloaltonetworks.com/CVE-2026-0300
CL-STA-1132			
IOC TYPE	VALUE		
URL	hxxps[:]//github[.]com/Acebond/ReverseSocks5/releases/download/v2.2.0/ReverseSocks5-v2.2.0-linux-amd64.tar[.]gz		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Deed RAT	Deed RAT is a modular backdoor uses multi-stage AES-CBC/RC4-encrypted payloads and LZNT1/Deflate compression. The malware patches Windows API to trigger execution during the host application's natural control flow, evading sandbox analysis. Plugins provide command execution, process injection, network communication, and persistence. Lateral movement occurs via RDP and Impacket SMB utilities. HTTPS C2 exfiltration via masqueraded security vendor domains.	Exploiting Vulnerabilities	CVE-2022-41040 CVE-2022-41082
		IMPACT	AFFECTED PRODUCT
TYPE		Initial Access, Persistence, Credential & Data Theft	Windows
Modular Backdoor			PATCH LINKS
ASSOCIATED ACTOR			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41040, https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2022-41082
FamousSparrow			
IOC TYPE	VALUE		
SHA256	25b9fdef3061c7dfea744830774ca0e289dba7c14be85f0d4695d382763b409b		

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
Terndoor	Terndoor is a kernel-mode backed deployed as a redundant persistence mechanism. Delivered via Mofu shellcode loader using DLL sideloading, Terndoor stages a Windows kernel driver to achieve system-level persistence and evasion. The malware uses LZNT1 compression, RC4 encryption with hardcoded keys, and one-byte XOR string obfuscation. Payloads target msdt.exe for process injection and establish C2 via service creation.	Exploiting Vulnerabilities	CVE-2022-41040 CVE-2022-41082
TYPE		**IMPACT**	**AFFECTED PRODUCT**
Backdoor		Kernel & Driver Persistence, Evasion & Detection Bypass	Windows
ASSOCIATED ACTOR			**PATCH LINK**
FamousSparrow			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41040, https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2022-41082
IOC TYPE	**VALUE**		
SHA256	711d9427ee43bc2186b9124f31cba2db5f54ec9a0d56dc2948e1a4377bada289		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Mofu Loader	Mofu Loader is a position-independent shellcode loader used to deliver kernel-mode and userland payloads. The loader uses NOP+CALL prologue for PIC execution, subtract-XOR-add (SXA) transformation for decryption, and LZNT1 compression. Payloads are prefixed with 12-byte headers containing seed and size values; MZ/PE headers are stripped to evade signature detection. Execution occurs entirely in memory with no disk footprint, making it ideal for covert payload staging in multi-stage intrusions.	Exploiting Vulnerabilities	CVE-2022-41040 CVE-2022-41082
TYPE		**IMPACT**	**AFFECTED PRODUCT**
Loader		Fileless Execution, Lateral Movement, & Persistence	Windows
ASSOCIATED ACTOR			**PATCH LINKS**
FamousSparrow			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41040, https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2022-41082

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

Vulnerabilities Exploited

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCT</th><th>ASSOCIATED ACTORS</th></tr>
<tr><td rowspan="3">CVE-2026-43284</td><td>Dirty Frag</td><td rowspan="2">Linux kernel (xfrm-ESP / Ipsec subsystem) kernel versions 4.10 through 7.0 (vulnerable code introduced January 2017 by commit cac2661c53f3)</td><td rowspan="2">-</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td>✗</td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>CISA KEV</td><td rowspan="2">cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">Linux Kernel xfrm-ESP In-Place Decrypt Page-Cache Write Vulnerability</td><td>✗</td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-123</td><td>T1068 - Exploitation for Privilege Escalation, T1078 - Valid Accounts, T1059 - Command and Scripting Interpreter</td><td>https://git.kernel.org/pub/scm/linux/kernel/git/stable/linux.git/commit/?id=8253aab4659ca16116b522203c2a6b18dccacea7</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2026-43500	Dirty Frag	Linux kernel (RxRPC subsystem) kernel versions 4.10 through 7.0 (vulnerable code introduced June 2023)	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*	-
Linux Kernel RxRPC In-Place Decrypt Page-Cache Write Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-123	T1068 - Exploitation for Privilege Escalation, T1611 - Escape to Host	https://git.kernel.org/pub/scm/linux/kernel/git/stable/linux.git/commit/?id=d45179f8795222ce858770dc619abe51f9d24411

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2025-29927	✗	Next.js versions prior to 12.3.5 and after 11.1.4, prior to 14.2.25 and after 14.0, prior to 15.2.3 and after 15.0, prior to 13.5.9 and after 13.0.0	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:vercel:next.js:-:*:*:*:*:*:*:*	PCPJack
Next.js Middleware Bypass Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-863 CWE-285	T1059: Command and Scripting Interpreter	https://github.com/vercel/next.js/releases

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2025-55182	React2Shell ZERO-DAY	react-server-dom-webpack, react-server-dom-parcel, react-server-dom-turbopack versions: 19.0.0, 19.1.0, 19.1.1, 19.2.0 Next.js versions: 14.3.0- canary.77+, 15.x, 16.x (before 16.0.7) React Router, Waku, RedwoodSDK, @parcel/rsc, @vitejs/plugin-rsc	-
	✗	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:a:facebook:react:*:*:*:*:*:*:*:* cpe:2.3:a:vercel:next.js:*:*:*:*:*:node.js:*:* cpe:2.3:a:remix:react_router:*:*:*	PCPJack
Meta React Server Components Remote Code Execution Vulnerability	✓		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-502	T1190: Exploit Public-Facing Application, T1059.007: JavaScript, T1059: Command and Scripting Interpreter	https://github.com/facebook/react/security/advisories/GHSA-fv66-9v8q-g76r

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2026-1357	✗ ZERO-DAY	WordPress WPVivid Backup & Migration	-
	✗	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:a:wpvivid:wpvivid_backup_plugin:*:*:*:*:*:wordpress:*:*	PCPJack
WordPress WPVivid Backup & Migration Unauthenticated Arbitrary File Upload Vulnerability	✗		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-434	T1190 - Exploit Public-Facing Application, T1505 - Server Software Component, T1505.003 - Web Shell	https://wordpress.org/plugins/wpvivid-backuprestore/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2025-9501		WordPress W3 Total Cache plugin before 2.8.13	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:boldgrid:w3_total_cache:*:*:*:*:*:wordpress:*:*	PCPJack
WordPress W3 Total Cache Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1190 - Exploit Public-Facing Application, T1059 - Command and Scripting Interpreter	https://wordpress.org/plugins/w3-total-cache/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2025-48703		CWP (aka Control Web Panel or CentOS Web Panel) before 0.9.8.1205	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:control-webpanel:webpanel:*:*:*:*:*:*:*:*	PCPJack
CWP Control Web Panel OS Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter	https://control-webpanel.com/changelog

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2026-45321		TanStack Router npm Packages	TeamPCP
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:tanstack:tanstack\/arktype-adapter:*:*:*:*:*:*:*:*	Mini Shai-Hulud Worm
TanStack Router npm Packages Embedded Malicious Code Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-506	T1583 - Acquire Infrastructure, T1583.001 - Domains, T1587 - Develop Capabilities, T1587.001 - Malware	https://github.com/TanStack/router/releases

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2026-0300		Palo Alto Networks PAN-OS (PA-Series, VM-Series) Versions 10.2.x, 11.1.x, 11.2.x, 12.1.x	CL-STA-1132
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:palo_alto_networks:pan-os:*:*:*:*:*:*:*:*	EarthWorm, ReverseSocks5
Palo Alto Networks PAN-OS Out-of-bounds Write Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-787	T1190: Exploit Public-Facing Application, T1068: Exploitation for Privilege Escalation, T1090: Proxy, T1070: Indicator Removal	https://security.paloaltonetworks.com/CVE-2026-0300

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2026-20182	✗	Cisco Catalyst SD-WAN before 20.9.9.1, before 20.12.7.1, before 20.12.7.1, before 20.12.5.4, 20.12.6.2, 20.12.7.1, before 20.15.5.2, before 20.15.5.2, before 20.15.4.4, 20.15.5.2, before 20.18.2.2, before 20.18.2.2, before 26.1.1.1	UAT-8616
	ZERO-DAY		
	✓	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOM WARE**
NAME	**CISA KEV**	cpe:2.3:a:cisco:catalyst_sd-wan_controller:*:*:*:*:*:*:*:*, cpe:2.3:a:cisco:catalyst_sd-wan_manager:*:*:*:*:*:*:*:*	-
Cisco Catalyst SD-WAN Controller Authentication Bypass Vulnerability	✓		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-287	T1190 - Exploit Public-Facing Application, T1059 - Command and Scripting Interpreter, T1098 - Account Manipulation, T1098.004 - SSH Authorized Keys, T1068 - Exploitation for Privilege Escalation, T1588 - Obtain Capabilities, T1588.006 - Vulnerabilities	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-rpa2-v69WY2SW

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2022-41040	ProxyNotShell	Microsoft Exchange Server	FamousSparrow
	ZERO-DAY		
	✓	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:a:microsoft:exchange_server:*:*:*:*:*:*:*:*	Deed RAT (aka Snappybee), Terndoor, Mofu loader
Microsoft Exchange Server Server-Side Request Forgery Vulnerability	✓		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-918	T1552.005: Cloud Instance Metadata API	https://msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41040

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2022-41082	ProxyNotShell	Microsoft Exchange Server	CL-STA-1132
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:exchange_server:*:*:*:*:*:*:*:*	Deed RAT (aka Snappybee), Terndoor, Mofu loader
Microsoft Exchange Server Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502	T1059: Command and Scripting Interpreter	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2022-41082

Adversaries in Action

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="3"> 

TeamPCP (aka PCPcat, ShellForce, DeadCatx3, UNC6780, PersyPCP)</td><td>-</td><td rowspan="2">Software Development, Enterprise Automation, Artificial Intelligence, Cloud Computing, CI/CD Pipelines</td><td rowspan="2">Global (excludes systems configured with Russian language locale)</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Espionage, Sabotage, Disruption, Financial Gains</td></tr>
<tr><td></td><td>TARGETED CVE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCT</td></tr>
<tr><td></td><td>CVE-2026-45321</td><td>Mini Shai-Hulud Worm</td><td>TanStack Router npm Packages</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0001: Initial Access, T1195: Supply Chain Compromise, T1204: User Execution, 1195.002: Compromise Software Supply Chain, T1195.001: Compromise Software Dependencies and Development Tools, T1204.002: Malicious File, TA0002: Execution, T1059: Command and Scripting Interpreter, 1059.007: JavaScript, T1059.006: Python, TA0003: Persistence, T1543: Create or Modify System Process, T1546: Event Triggered Execution, 1543.001: Launch Agent, T1543.002: Systemd Service, TA0005: Defense Evasion, T1027: Obfuscated Files or Information, T1036: Masquerading, 1036.005: Match Legitimate Name or Location, TA0006: Credential Access, T1552: Unsecured Credentials, T1528: Steal Application Access Token, 1552.001: Credentials In Files, T1552.005: Cloud Instance Metadata API, TA0007: Discovery, T1526: Cloud Service Discovery, TA0009: Collection, T1005: Data from Local System, TA0010: Exfiltration, T1567: Exfiltration Over Web Service, T1041: Exfiltration Over C2 Channel, 1567.001: Exfiltration to Code Repository, TA0040: Impact, T1485: Data Destruction, TA0008: Lateral Movement, T1072: Software Deployment Tools</td></tr>
</table>

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 CL-STA-1132	- **MOTIVE** Espionage	-	-
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCT**
	CVE-2026-0300	EarthWorm, ReverseSocks5	Palo Alto Networks PAN-OS
TTPs			
TA0042: Resource Development, TA0001: Initial Access, TA0003: Persistence, TA0004: Privilege Escalation, TA0005: Defense Evasion, TA0006: Credential Access, TA0007: Discovery, TA0008: Lateral Movement, TA0009: Collection, T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1548: Abuse Elevation Control Mechanism , T1548.001: Setuid and Setgid Defense Evasion , T1070: Indicator Removal T1070.004: File Deletion, T1003: OS Credential Dumping Discovery , T1018: Remote System Discovery, T1090: Proxy, T1572: Protocol Tunneling , T1588: Obtain Capabilities , T1588.006: Vulnerabilities			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 UAT-8616	-	-	-
	MOTIVE		
	Information theft and Espionage		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCT
	CVE-2026-20182	-	Cisco Catalyst SD-WAN Controller / Manager
TTPs			
TA0001: Initial Access, T1190: Exploit Public-Facing Application Execution, T1059: Command and Scripting Interpreter , TA0002: Persistence, T1098: Account Manipulation, T1098.004: SSH Authorized Keys, TA0004: Privilege Escalation, T1068: Exploitation for Privilege Escalation, TA0042: Resource Development, T1588: Obtain Capabilities, T1588.006: Vulnerabilities			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 FamousSparrow (aka UNC2286, GhostEmperor, RedMike, Operator Panda, Earth Estries, Salt Typhoon)	China	Oil and Gas, Energy	Armenia, Azerbaijan, Georgia
	MOTIVE		
	Information Theft, Espionage		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCT**
	CVE-2022-41040 CVE-2022-41082	Malware: Deed RAT (aka Snappybee), Terndoor, Mofu loader	Microsoft Exchange Server
TTPs			
TA0001: Initial Access, T1190: Exploit Public-Facing Application, TA0003: Persistence, T1505: Server Software Component, T1543: Create or Modify System Process, T1547: Boot or Logon Autostart Execution, T1505.003: Web Shell, T1543.003: Windows Service, T1547.001: Registry Run Keys / Startup Folder, TA0002: Execution, T1569: System Services, T1059: Command and Scripting Interpreter, T1569.002: Service Execution, T1059.001: PowerShell, TA0005: Defense Evasion, T1574: Hijack Execution Flow, T1140: Deobfuscate/Decode Files or Information, T1562: Impair Defenses, T1027: Obfuscated Files or Information, T1055: Process Injection, T1014: Rootkit, T1036: Masquerading, T1574.002: DLL Side-Loading, T1036.005: Match Legitimate Resource Name or Location, TA0006: Credential Access, T1078: Valid Accounts, T1078.002: Domain Accounts, TA0007: Discovery, T1016: System Network Configuration Discovery, TA0008: Lateral Movement, T1021: Remote Services, T1021.001: Remote Desktop Protocol, T1021.002: SMB/Windows Admin Shares, TA0024: Resource Development, T1583: Acquire Infrastructure, T1583.001: Domains, TA0011: Command and Control, T1071: Application Layer Protocol, T1573: Encrypted Channel, T1071.001: Web Protocols, T1573.002: Asymmetric Cryptography		

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **twelve exploitable vulnerabilities** and block the indicators related to the threat actors **TeamPCP, CL-STA-1132, UAT-8616, FamousSparrow,** and malware **TCLBANKER, Quasar Linux, PCPJack, Mini Shai-Hulud, EarthWorm, ReverseSocks5, Deed RAT, Terndoor, and Mofu Loader.**

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 **twelve exploitable vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **TeamPCP, CL-STA-1132, UAT-8616, FamousSparrow,** and malware **TCLBANKER, Quasar Linux, PCPJack, Mini Shai-Hulud, EarthWorm, Deed RAT** in Breach and Attack Simulation(BAS).

Threat Advisories

TCLBanker: Trojanized Logitech Installer Fuels Banking Malware Campaign

Dirty Frag A 2017 Optimization That Aged Into a Root Exploit

QLNX Unmasked: Advanced Linux Malware Targets Developers and Cloud Infrastructure

PCPJack Hijacks Vulnerable Servers With Worm-Like Cloud Propagation Tactics

Microsoft's May 2026 Patch Tuesday

Malicious Ruby Gems Fuel GemStuffer Data Theft Campaign

Mini Shai-Hulud npm Supply Chain Worm: TanStack and Multi-Ecosystem Compromise

PAN-OS Buffer Overflow Flaw Under Active State-Sponsored Exploitation

Cisco SD-WAN Authentication Bypass Exploited in Zero-Day Attacks

FamousSparrow's Persistent Hold on Azerbaijani Oil & Gas

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
TCLBANKER	SHA256	701d51b7be8b034c860bf97847bd59a87dca8481c462532881 3746964995b626, 8a174aa70a4396547045aef6c69eb0259bae1706880f4375af7 1085eeb537059, 668f932433a24bbae89d60b24eee4a24808fc741f62c5a3043b b7c9152342f40
	Domains	campanha1-api[.]ef971a42[.]workers[.]dev, mxtestacionamentos[.]com
Quasar Linux	MD5	70f70743f287a837d17c56933152a8a6
	SHA1	b0f2c668cbdd63a871c90592b6c93e931115872e
	SHA256	ea1d34b21b739a6bbf89b3f7e67978005cf7f3eda612cefc7eac1c 8ead7c5545
PCPJack	Domain	cdn[.]cloudfront-js[.]com
	SHA256	b1d8149e5c7b6312f40c220e89b1913762f9aa416ff491540b3 b7b7040260eb5
Mini Shai-Hulud	SHA256	ab4fcadaec49c03278063dd269ea5eef82d24f2124a8e15d7b9 0f2fa8601266c
EarthWorm	URL	hxxp[:]//146[.]70[.]100[.]69[:]8000/php_sess
	SHA256	e11f69b49b6f2e829454371c31ebf86893f82a042dae3f2faf63dc d84f97a584

Attack Name	TYPE	VALUE
ReverseSocks5	URL	hxxps[:]//github[.]com/Acebond/ReverseSocks5/releases/download/v2.2.0/ReverseSocks5-v2.2.0-linux-amd64.tar[.]gz
Deed RAT	SHA256	25b9fdef3061c7dfea744830774ca0e289dba7c14be85f0d4695d382763b409b
Terndoor	SHA256	711d9427ee43bc2186b9124f31cba2db5f54ec9a0d56dc2948e1a4377bada289

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 Demo of **HivePro**.

REPORT GENERATED ON

May 18, 2026 • 1:00 PM

More at www.hivepro.com