Date of Publication
May 25, 2026

Hive Pro

Hiveforce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities, and Actors

18 MAY to 24 MAY 2026

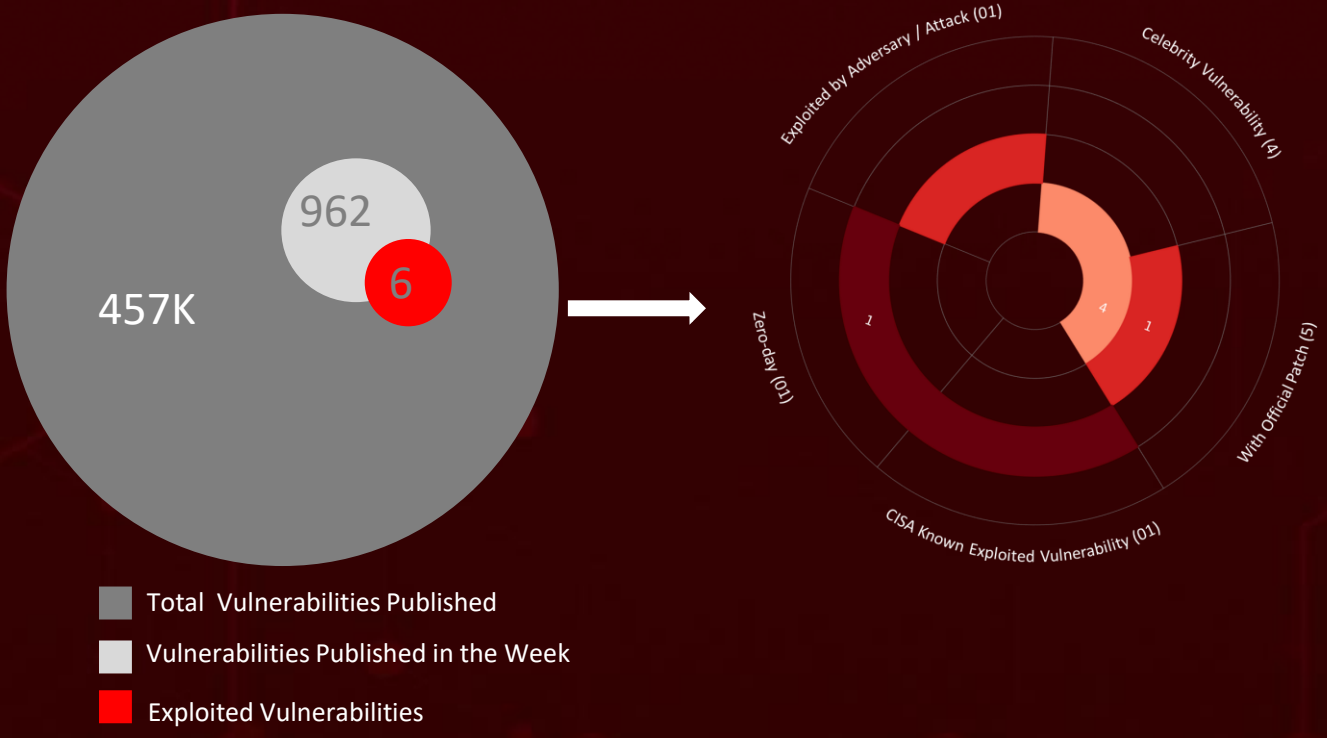
Table Of Contents

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, **one** major attack was detected, **six** vulnerabilities were actively exploited, and **three** threat actor groups were closely monitored, signaling a concerning escalation in malicious activity worldwide.

Among the most significant incidents, Microsoft confirmed the active exploitation of **CVE-2026-42897**, a newly disclosed spoofing flaw impacting on-premises Exchange Server deployments. The vulnerability stems from a cross-site scripting (XSS) issue in Outlook Web Access (OWA), enabling attackers to inject malicious JavaScript through specially crafted emails and hijack authenticated user sessions. At the same time, F5 issued emergency patches for six NGINX vulnerabilities, including **CVE-2026-42945**, a critical heap-based buffer overflow hidden in the ngx_http_rewrite_module for nearly 18 years since 2008. Adding to the growing threat landscape, **Storm-2949** executed a sophisticated cloud intrusion campaign by abusing Microsoft's Self-Service Password Reset (SSPR) process through targeted social engineering attacks aimed at privileged users, including IT administrators and senior executives.

Meanwhile, financially motivated threat groups are becoming increasingly aggressive and innovative. **TeamPCP** intensified its supply chain attacks throughout May 2026, evolving from package poisoning to ecosystem-wide worm propagation, ultimately culminating in a breach of GitHub itself. The group allegedly exfiltrated nearly 3,800 internal GitHub repositories through a poisoned VS Code extension and later open-sourced the worm with a $1,000 underground bounty, rapidly fueling copycat campaigns. In parallel, **Fox Tempest** continued operating its SignSpace malware-signing-as-a-service platform, abusing Microsoft Artifact Signing to generate fraudulent short-lived certificates that made malware appear as trusted software such as AnyDesk, Microsoft Teams, PuTTY, and Webex. Together, these incidents highlight a dangerous shift toward hybrid cyberattacks that blend technical exploitation with psychological manipulation, reinforcing the urgent need for timely patching, continuous monitoring, and layered security defenses.



High Level Statistics

1
Attacks Executed

6
Vulnerabilities Exploited

3
Adversaries in Action

- Mini Shai-Hulud Worm

- CVE-2026-45321
- CVE-2026-42897
- CVE-2026-42945
- CVE-2026-46300
- CVE-2026-31635
- CVE-2026-45185

- TeamPCP
- Storm-2949
- Fox Tempest

Insights

CVE-2026-45185 “Dead.Letter” exposes Exim servers to critical unauthenticated RCE attacks.

Fragnesia (CVE-2026-46300) and **DirtyDecrypt (CVE-2026-31635)** expose multi-tenant Linux and cloud environments to high-risk attacks that can be triggered by untrusted local users and shared workloads.

Fox Tempest abused Microsoft signing services to disguise malware as trusted Windows software using fraudulently issued short-lived certificates.

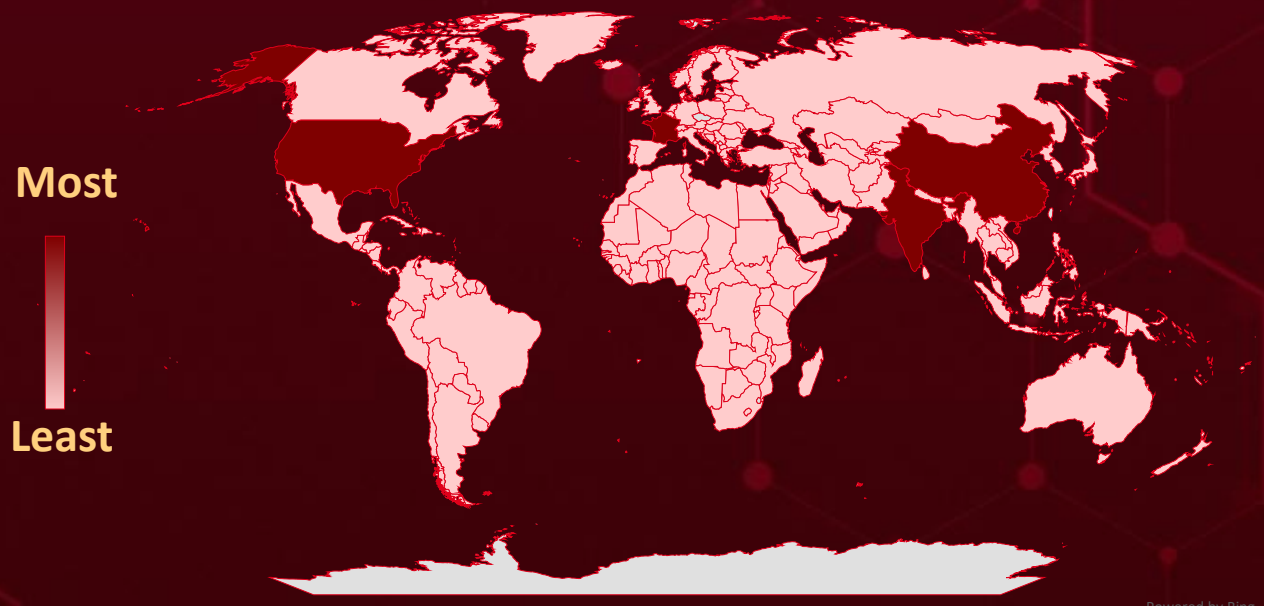
CVE-2026-42945 exposes an 18-year-old flaw in NGINX’s rewrite module, enabling heap-based buffer overflow attacks from code that remained hidden since 2008.

CVE-2026-42897 is being actively exploited to weaponize malicious emails that execute attacker-controlled scripts inside authenticated Microsoft Exchange OWA sessions.

TeamPCPs’ rampage evolves from package poisoning to worm-driven ecosystem compromise and a direct GitHub breach, marking a new phase in supply chain attacks.

Threat Distribution

Targeted Countries



Powered by Bing

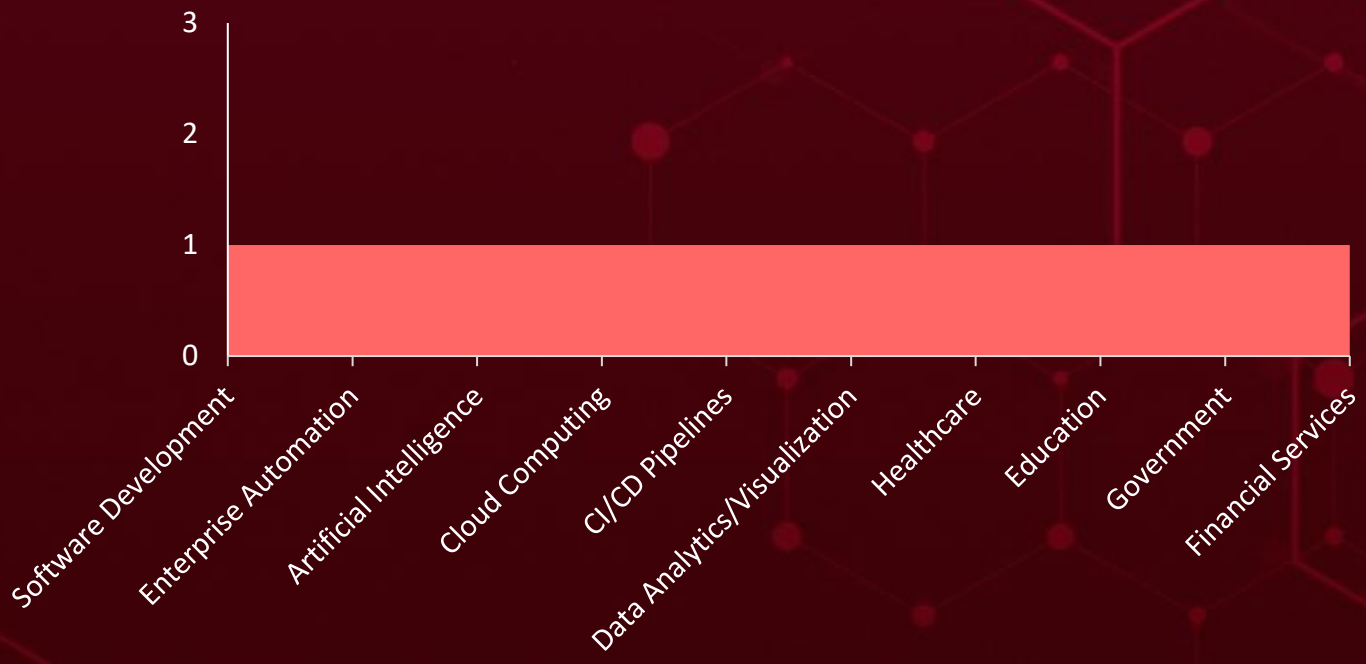
Countries
United States
France
China
India
Norway
Afghanistan
Spain
Antigua and Barbuda
Monaco
Argentina
Rwanda
Armenia
Turkmenistan
Australia
Mali
Austria
Nepal
Azerbaijan
Peru
Bahamas
Senegal
Bahrain
Tanzania
Bangladesh
Uzbekistan

Countries
Barbados
Madagascar
Belarus
Mauritius
Belgium
Mozambique
Belize
Niger
Benin
Palestine State
Bhutan
Qatar
Bolivia
Samoa
Bosnia and Herzegovina
Singapore
Botswana
Sweden
Brazil
Tonga
Brunei
United Arab Emirates
Bulgaria
Yemen
Burkina Faso

Countries
South Korea
Cuba
Sudan
Cyprus
Syria
Czechia (Czech Republic)
Timor-Leste
Democratic Republic of the Congo
Tunisia
Denmark
Uganda
Djibouti
Andorra
Dominica
Venezuela
Dominican Republic
Zimbabwe
Ecuador
Liechtenstein
Egypt
Luxembourg
El Salvador
Malawi
Maldives

Countries
Iran
South Sudan
Iraq
Sri Lanka
Ireland
Suriname
Israel
Switzerland
Italy
Tajikistan
Jamaica
Thailand
Japan
Togo
Jordan
Trinidad and Tobago
Kazakhstan
Turkey
Kenya
Tuvalu
Kiribati
Ukraine
Kuwait

Targeted Industries



TOP MITRE ATT&CK TTPs

T1059 Command and Scripting Interpreter	**T1036** Masquerading	**T1588.006** Vulnerabilities	**T1588** Obtain Capabilities	**T1071** Application Layer Protocol
T1528 Steal Application Access Token	**T1588.005** Exploits	**T1567** Exfiltration Over Web Service	**T1068** Exploitation for Privilege Escalation	**T1204** User Execution
T1070 Indicator Removal	**T1552** Unsecured Credentials	**T1041** Exfiltration Over C2 Channel	**T1036.005** Match Legitimate Resource Name or Location	**T1078** Valid Accounts
T1059.007 JavaScript	**T1190** Exploit Public-Facing Application	**T1204.002** Malicious File	**T1543.001** Launch Agent	**T1567.001** Exfiltration to Code Repository

Attacks Executed

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 PRODUCTS**
TYPE		Credential Theft, Destructive Capabilities	TanStack Router npm Package
Worm			**PATCH LINK**
ASSOCIATED ACTOR			https://github.com/TanStack/router/releases
TeamPCP			

IOC TYPE	VALUE
SHA256	ab4fcadaec49c03278063dd269ea5eef82d24f2124a8e15d7b90f2fa8601266c

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-2026-45321</td><td>✕</td><td rowspan="2">TanStack Router npm Packages</td><td rowspan="2">TeamPCP</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="3">cpe:2.3:a:tanstack:tanstack\/arktype-adapter:*:*:*:*:*:*:*:*</td><td rowspan="3">Mini Shai-Hulud Worm</td></tr>
<tr><td rowspan="3">TanStack Router npm Packages Embedded Malicious Code Vulnerability</td><td>✕</td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-506</td><td>T1583: Acquire Infrastructure, T1583.001: Domains, T1587: Develop Capabilities, T1587.001: Malware</td><td>https://github.com/TanStack/router/releases</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2026-42897		Microsoft Exchange Server 2016 (all update levels), Microsoft Exchange Server 2019 (all update levels), Microsoft Exchange Server Subscription Edition (all update levels)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:exchange_server:2016:-:*:*:*:*:*:*:* cpe:2.3:a:microsoft:exchange_server:2019:*:*:*:*:*:*:* cpe:2.3:a:microsoft:exchange_server:-:*:*:*:subscription:*:*:*	-
Microsoft Exchange Server Cross-Site Scripting Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-79	T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter; T1059.007: JavaScript	

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCT</th><th>ASSOCIATED ACTORS</th></tr>
<tr><td rowspan="3">CVE-2026-42945</td><td>NGINX Rift</td><td rowspan="2">NGINX Plus: R32 – R36NGINX Open Source: 1.0.0 – 1.30.0, 0.6.27 – 0.9.7
NGINX Instance Manager: 2.16.0 – 2.22.0F5
WAF for NGINX: 5.9.0 – 5.12.1
NGINX App Protect WAF: 5.1.0 – 5.8.0, 4.9.0 – 4.16.0F5 DoS for NGINX: 4.8.0
NGINX App Protect DoS: 4.3.0 – 4.7.0
NGINX Gateway Fabric: 2.0.0 – 2.6.0, 1.3.0 – 1.6.2
NGINX Ingress Controller: 5.0.0 – 5.4.2, 4.0.0 – 4.0.1, 3.5.0 – 3.7.2</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:a:f5:nginx:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">F5 NGINX ngx_http_rewrite_module Heap-Based Buffer Overflow Vulnerability</td><td>✗</td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-122</td><td>T1059: Command and Scripting Interpreter, T1190: Exploit Public-Facing Application, T1203: Exploitation for Client Execution</td><td>https://my.f5.com/manage/s/article/K000161019</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2026-46300	Fragnesia	Linux Kernel (XFRM ESP-in-TCP / `esp4`, `esp6`, `rxrpc` modules) – impacts AlmaLinux 8/9/10, AlmaLinux Kitten 10, Amazon Linux, CloudLinux, Debian, Fedora, Gentoo, openSUSE, Red Hat Enterprise Linux, SUSE, Ubuntu, and OpenShift	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*	-
Linux Kernel XFRM ESP-in-TCP Page-Cache Corruption Local Privilege Escalation Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-123	T1068: Exploitation for Privilege Escalation, T1059: Command and Scripting Interpreter	Alma Linux, Redhat, Ubuntu, SUSE, Debian, Amazon, Gentoo, Openwall, Kernel

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2026-31635	DirtyDecrypt	Linux Linux Kernel (6.16; 7.0-rc1 through 7.0-rc7; 6.19 before 6.19.13; 6.16.1 up to but excluding 6.18.23) — requires `CONFIG_RXGK` enabled	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*	-
Linux Kernel Local Privilege Escalation Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-130	T1068: Exploitation for Privilege Escalation, T1059: Command and Scripting Interpreter	https://git.kernel.org/pub/scm/linux/kernel/git/stable/linux.git/commit/?id=e2f1a80d8b1ed6a5ae585a399c2b46500bdcc305

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCT</th><th>ASSOCIATED ACTORS</th></tr>
<tr><td rowspan="3">CVE-2026-45185</td><td>Dead.Letter</td><td rowspan="2">Exim Internet Mailer 4.97 through 4.99.2 (GnuTLS builds only)</td><td>-</td></tr>
<tr><td>ZERO-DAY</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:a:exim:exim:*:*:*:*:*:*:*:*</td><td>-</td></tr>
<tr><td rowspan="2">Exim Internet Mailer Use-After-Free Vulnerability</td><td>✗</td><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-416</td><td>T1059: Command and Scripting Interpreter, T1190: Exploit Public- Facing Application, T1203: Exploitation for Client Execution, T1082: System Information Discovery</td><td>https://exim.org/static/doc/security/EXIM-Security-2026-05-01.1/</td></tr>
</table>

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 Storm-2949	-	Worldwide	All
	MOTIVE		
	Information Theft and Espionage		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCT**
	-	-	-
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0009: Collection; TA0007: Discovery; TA0006: Credential Access; TA0008: Lateral Movement; TA0011: Command and Control; TA0010: Exfiltration; T1078: Valid Accounts; T1078.004: Cloud Accounts; T1566: Phishing; T1566.003: Spearphishing via Service; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1059.006: Python; T1098: Account Manipulation; T1098.005: Device Registration; T1562: Impair Defenses; T1562.001: Disable or Modify Tools; T1070: Indicator Removal; T1070.001: Clear Windows Event Logs; T1036: Masquerading; T1036.004: Masquerade Task or Service; T1530: Data from Cloud Storage; T1087: Account Discovery; T1087.004: Cloud Account; T1580: Cloud Infrastructure Discovery; T1528: Steal Application Access Token; T1552: Unsecured Credentials; T1552.001: Credentials In Files; T1021: Remote Services; T1021.007: Cloud Services Dashboard; T1219: Remote Access Software; T1567: Exfiltration Over Web Service			

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="4"> 
TeamPCP (aka PCPcat, ShellForce, DeadCatx3, CipherForce, Persy_PCP, UNC6780)</td><td>-</td><td rowspan="2">Software Development, AI/ML, Cloud Computing, CI/CD Pipelines, Data Analytics/Visualization, Enterprise Automation, Source Code Hosting Platforms</td><td rowspan="2">Worldwide</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Espionage, Sabotage, Disruption, Financial Gains</td><td>TARGETED CVE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCT</td></tr>
<tr><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; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0009: Collection; TA0008: Lateral Movement; TA0011: Command and Control; TA0010: Exfiltration; TA0040: Impact; T1195: Supply Chain Compromise; T1195.002: Compromise Software Supply Chain; T1195.001: Compromise Software Dependencies and Development Tools; T1078: Valid Accounts; T1204: User Execution; T1204.002: Malicious File; T1059: Command and Scripting Interpreter; T1059.007: JavaScript; T1106: Native API; T1176: Browser Extensions; T1543: Create or Modify System Process; T1543.001: Launch Agent; T1543.002: Systemd Service; T1546: Event Triggered Execution; T1027: Obfuscated Files or Information; T1036: Masquerading; T1036.005: Match Legitimate Name or Location; T1070: Indicator Removal; T1070.006: Timestomp; T1656: Impersonation; T1552: Unsecured Credentials; T1552.001: Credentials In Files; T1552.004: Private Keys; T1555: Credentials from Password Stores; T1555: Credentials from Password Stores; T1555.005: Password Managers; T1528: Steal Application Access Token; T1539: Steal Web Session Cookie; T1526: Cloud Service Discovery; T1083: File and Directory Discovery; T1005: Data from Local System; T1213: Data from Information Repositories; T1213.003: Code Repositories; T1072: Software Deployment Tools; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1102: Web Service; T1102.002: Bidirectional Communication; T1132: Data Encoding; T1567: Exfiltration Over Web Service; T1567.001: Exfiltration to Code Repository; T1041: Exfiltration Over C2 Channel; T1657: Financial Theft; T1485: Data Destruction; T1204: User Execution; T1204.002: Malicious File; T1059.006: Python; T1552: Unsecured Credentials; T1552.001: Credentials In Files; T1552.005: Cloud Instance Metadata API</td></tr>
</table>

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="4"> 
Fox Tempest</td><td>-</td><td rowspan="2">Healthcare, Education, Government, Financial Services</td><td rowspan="2">United States, France, India, China</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Financial Gains</td><td>TARGETED CVE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>-</td><td>-</td><td>AnyDesk, Microsoft Teams, PuTTY, Webex (impersonated as lures)</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0006: Credential Access; TA0011: Command and Control; TA0040: Impact; T1583: Acquire Infrastructure; T1583.001: Domains; T1583.003: Virtual Private Server; T1583.008: Malvertising; T1585: Establish Accounts; T1585.001: Social Media Accounts; T1585.003: Cloud Accounts; T1586: Compromise Accounts; T1587: Develop Capabilities; T1587.002: Code Signing Certificates; T1608: Stage Capabilities; T1608.006: SEO Poisoning; T1189: Drive-by Compromise; T1204: User Execution; T1204.002: Malicious File; T1053: Scheduled Task/Job; T1053.005: Scheduled Task; T1136: Create Account; T1136.001: Local Account; T1553: Subvert Trust Controls; T1553.002: Code Signing; T1036: Masquerading; T1036.005: Match Legitimate Resource Name or Location; T1082: System Information Discovery; T1555: Credentials from Password Stores; T1071: Application Layer Protocol; T1105: Ingress Tool Transfer; T1486: Data Encrypted for Impact</td></tr>
</table>

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **six exploited vulnerabilities** and block the indicators related to the threat actors **TeamPCP, Storm-2949, Fox Tempest,** and malware **Mini Shai-Hulud Worm.**

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 **six exploited vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **TeamPCP,** and malware **Mini Shai-Hulud Worm** in Breach and Attack Simulation(BAS).

Threat Advisories

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

Active Exploitation of CVE-2026-42897 Targets Microsoft Exchange Servers

Critical NGINX Vulnerabilities Including 18-Year-Old RCE Flaw Actively Exploited

Three Strikes in Two Weeks: Fragnesia Joins the Dirty Frag Family

One Million WordPress Sites at Risk: Avada Builder Flaws Expose Sensitive Data

Dead.Letter Walking: Unauthenticated RCE Stalks Exim Mail Servers

Inside Storm-2949's Cloud Takeover Campaign Targeting Microsoft 365 and Azure

From npm to GitHub: TeamPCP's May 2026 Escalation Reaches the Source Code Platform

72-Hour Window of Trust: Fox Tempest's Abuse of Microsoft Artifact Signing

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
Mini Shai-Hulud	SHA256	ab4fcadaec49c03278063dd269ea5eef82d24f2124a8e15d7b90f2fa8601266c, e7347d90653efc565f03733a95e9209d78f9cfa81e31ff2b2dd9d48d75a4b8b1

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 25, 2026 • 10:00 AM

More at www.hivepro.com