Date of Publication
June 29, 2026

Hive Pro

Hiveforce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities, and Actors

22 to 28 JUNE 2026

Table Of Contents

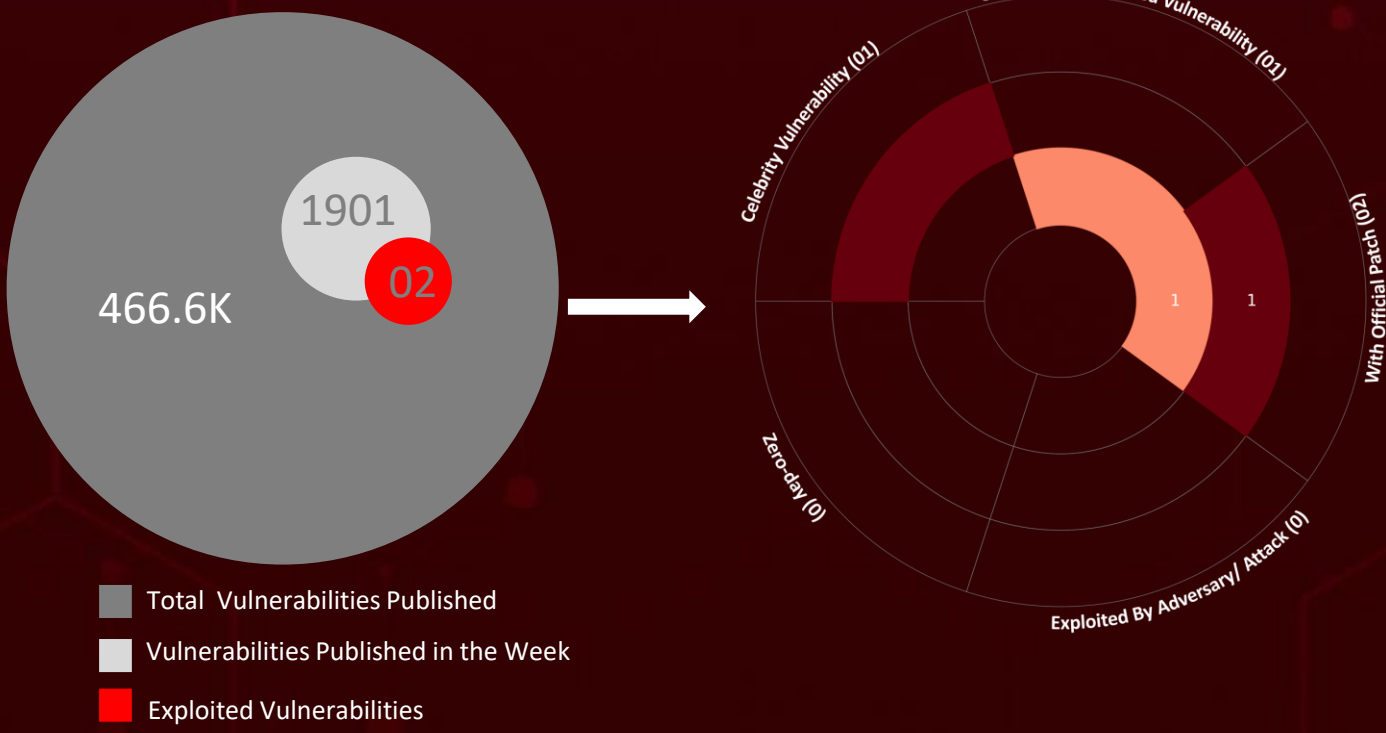
Summary

HiveForce Labs has reported a sharp rise in cybersecurity threats, highlighting the growing complexity and frequency of global cyber incidents. Over the past week, **seven** major attacks were detected, **two** vulnerabilities were identified, and **one** threat actor group was closely monitored, signaling a concerning escalation in malicious activity worldwide.

A newly disclosed information disclosure vulnerability, **CVE-2026-47729**, dubbed **Squidbleed**, affects the widely used Squid web proxy. Rooted in a decades-old parsing bug in Squid's FTP gateway, the flaw allows a malicious FTP server to trigger an out-of-bounds memory read, potentially exposing sensitive fragments of previously processed data, such as HTTP requests and authentication headers, to remote attackers.

A critical unauthenticated remote code execution vulnerability, **CVE-2026-12569**, has been identified in PTC Windchill PDMLink and FlexPLM, stemming from unsafe deserialization of untrusted input. Active exploitation has been confirmed in the wild and given the platform's deep integration into manufacturing and supply-chain environments, immediate remediation is strongly advised.

The **Edgecution** campaign represents a sophisticated browser-based intrusion chain targeting enterprise environments through social engineering. Threat actors impersonate IT support staff via Microsoft Teams, directing victims to a fake Outlook update portal that silently deploys a malicious Microsoft Edge browser extension. 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

7
Attacks Executed

2
Vulnerabilities Exploited

1
Adversaries in Action

- Potemkin
- RMMProject
- EtherRAT
- BabaDeda Loader
- Lorem Ipsum Loader
- Edgecution
- Gaslight

- CVE-2026-47729
- CVE-2026-12569

- Rapid Brigantine

Insights

WhatsApp as a Weapon: Inside the VBScript Campaign Hijacking Business Conversations

ClickFix Under the Microscope: Potemkin, BabaDeda, and Lorem Ipsum Unpacked

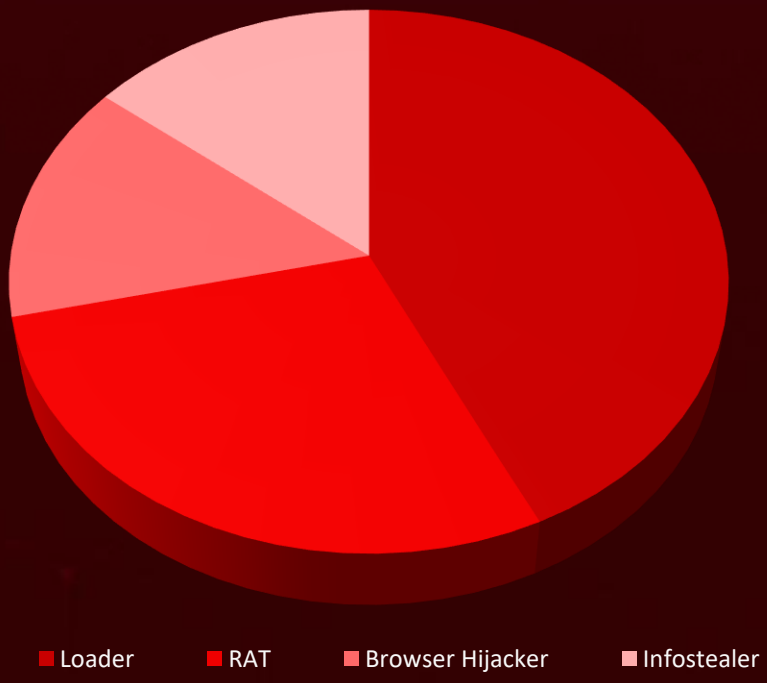
13 Linux Flaws That Attackers Are Already Eyeing This June

North Korea Built Malware That Gaslights Your AI Security Tools

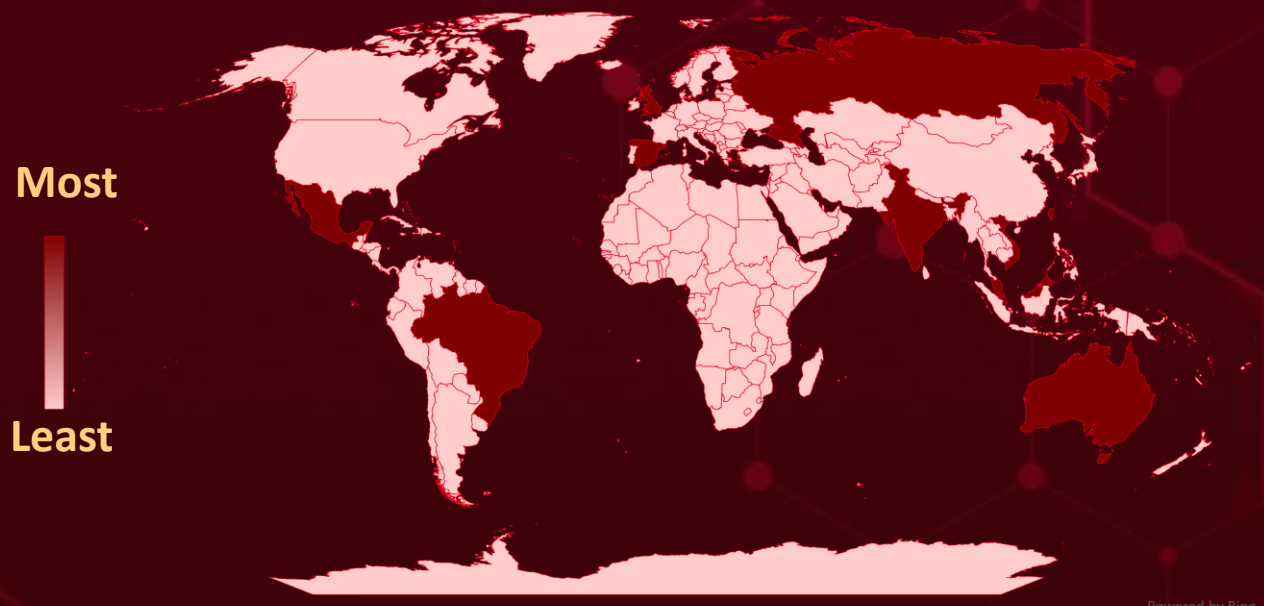
Supply Chain Attack Surface Expanded: CVE-2026-12569's Reach Into Integrated Environments

Edgecution Weaponizes a Trusted Browser Protocol to Bypass Endpoint Defenses

Threat Distribution

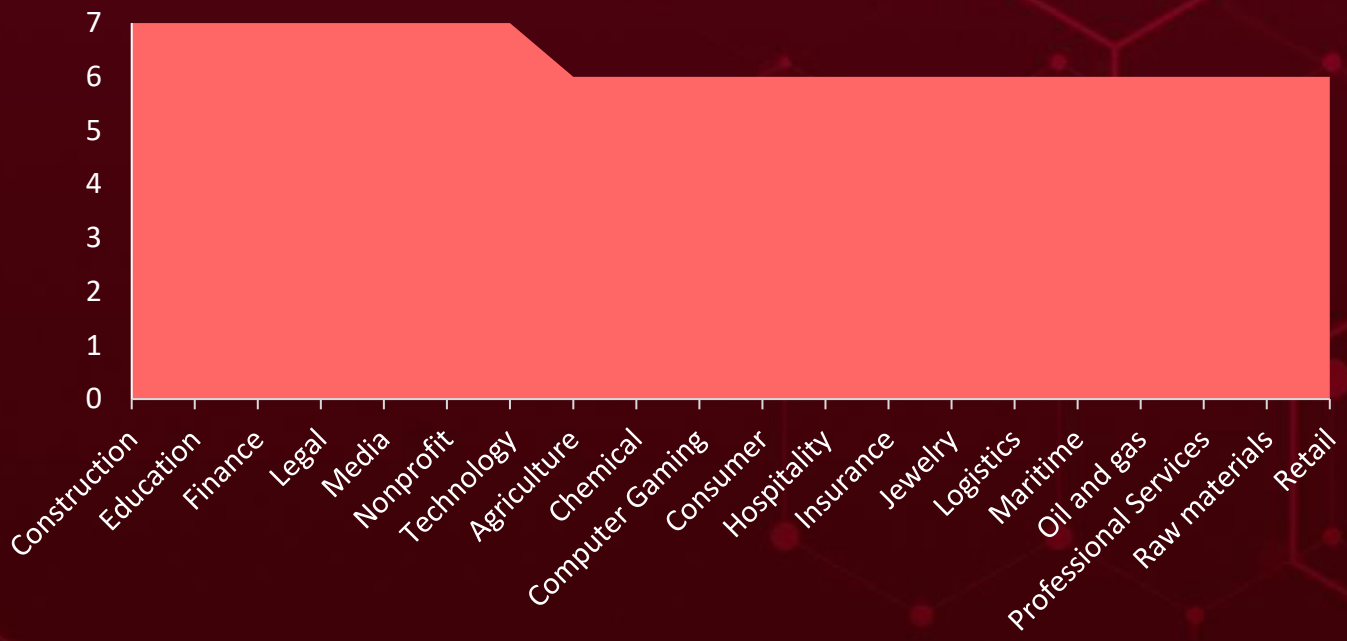


Targeted Countries



	Countries		Countries		Countries		Countries
	Russia		Nigeria		Suriname		Comoros
	Malaysia		Barbados		Bulgaria		Poland
	Spain		Puerto Rico		Thailand		Congo-Brazzaville
	Australia		Belarus		Burkina Faso		Republic of Ireland
	Mexico		Senegal		Turkey		Costa Rica
	Brazil		Belgium		Burundi		Saba
	Singapore		Syria		Lesotho		Croatia
	India		Belize		Cambodia		Saint Maarten
	Taiwan		Ukraine		Lithuania		Cuba
	Vietnam		Benin		Cameroon		Saudi Arabia
	United Kingdom		Macau		Madagascar		Curacao
	Namibia		Bermuda		Canada		Seychelles
	Tokelau		Martinique		Mali		Cyprus
	Saint Kitts and Nevis		Bhutan		Canada Quebec		Slovenia
	Akrotiri and Dhekelia		Montserrat		Mauritius		Czech Republic
	Andorra		Bolivia		Cape Verde		Sri Lanka
	Austria		Netherlands		Mongolia		Democratic Republic of Congo
	Palestine		Bonaire		Cayman Islands		Sweden
	Azerbaijan		Northern Ireland		Mozambique		Denmark
	South Korea		Bosnia and Herzegovina		Central African Republic		Tajikistan
	Bahamas		Peru		Nepal		Djibouti
	Libya		Botswana		Chad		Timor-Leste
	Bahrain		Anguilla		Nicaragua		Dominica
	Moldova		Albania		Chile		Trinidad and Tobago
	Bangladesh		Samoa		North Macedonia		
			British Virgin Islands		China		
			Antigua and Barbuda		Oman		
			Brunei		Colombia		
					Papua New Guinea		

Targeted Industries



TOP MITRE ATT&CK TTPs

T1059
Command and Scripting Interpreter

T1204
User Execution

T1036
Masquerading

T1071
Application Layer Protocol

T1112
Modify Registry

T1057
Process Discovery

T1102
Web Service

T1027
Obfuscated Files or Information

T1082
System Information Discovery

T1140
Deobfuscate/ Decode Files or Information

T1036.005
Match Legitimate Name or Location

T1071.001
Web Protocols

T1059.006
Python

T1218
System Binary Proxy Execution

T1564
Hide Artifacts

T1212
Exploitation for Credential Access

T1588
Obtain Capabilities

T1105
Ingress Tool Transfer

T1573
Encrypted Channel

T1566
Phishing

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Potemkin	Potemkin loader which is a purpose-built loader with a deterministic Domain Generation Algorithm (DGA), a custom byte cipher, and a reflective module loader, but its entire command vocabulary is a single task code.	ClickFix	-
TYPE		**IMPACT**	**AFFECTED PLATFORM**
Loader		Resilient C2 communication, Modular extensibility	Microsoft Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
SHA256	2abe5dd3a057fdef935722e50e9251c272d29fd26113187b853a1f9a9cb89d9b, 79f7b67ce8b39070f3e1c2b90fce0ce84134782a7dedcccc1edac197ee9e089b		

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
RMMProject	RMMProject is a remote access trojan (RAT) built around an embedded LuaJIT scripting engine, giving operators a flexible, programmable platform for executing malicious tasks. It supports 15 distinct task types, making it a versatile tool for a wide range of intrusion activities.	ClickFix	-
TYPE		**IMPACT**	**AFFECTED PLATFORM**
RAT		Full remote compromise, Browser credential and cookie theft	Microsoft Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
SHA256	3b7ae925e2d64522b4f69b56285b05aeca8c5aab5ab46a9c02c4fafb69d881ce		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
EtherRAT	EtherRAT serves as the resilient backbone of an intrusion: a blockchain-anchored backdoor designed to survive domain takedowns and other disruption efforts that would typically sever an attacker's foothold.	ClickFix	-
TYPE		**IMPACT**	**AFFECTED PLATFORM**
RAT		Takedown-resistant C2, Persistent remote access	Microsoft Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			-

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
BabaDeda Loader	BabaDeda was previously known for hiding malicious payloads inside legitimate-looking installer packages, disguising its activity as trustworthy software. This new framework preserves that same underlying code lineage but evolves it into a far more capable loader—engineered for stealth, evasion, and flexible payload delivery.	ClickFix	-
TYPE		**IMPACT**	**AFFECTED PLATFORM**
Loader		Deceptive delivery, Stealth and evasion	Microsoft Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
SHA256	0098b2c38a69132bfde02d329d6c1c6e2b529d32d7b775a2ac78a369c0d10853, 062f019515bff366fcbf49cca3f776c21e2beb81c043a45eea81044a9391fd97		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Lorem Ipsum Loader	The Lorem Ipsum Loader is a multi-stage malware loader operated by the financially motivated threat group Rapid Brigantine (a.k.a. Vanilla Tempest). Its defining technical signature is a substitution-cipher routine that reconstructs executable payloads at runtime from encoded text strings of innocuous-looking words mapped to byte values making static and signature-based detection difficult.	ClickFix	-
TYPE		**IMPACT**	**AFFECTED PLATFORM**
Loader		Registry persistence, Backdoor deployment, Credential theft	Microsoft Windows
ASSOCIATED ACTOR			**PATCH LINK**
Rapid Brigantine			-

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
Edgecution	Edgecution is a malicious Microsoft Edge browser extension that abuses the Chrome native messaging protocol to escape the browser sandbox and interact directly with the host system. It has two components: the Edge extension, which beacons to a C2 server over WebSockets, and a Python-based backdoor that handles privileged host-level operations including filesystem access, arbitrary code execution, and PowerShell command execution.	Social Engineering	-
TYPE		**IMPACT**	**AFFECTED PLATFORM**
Browser Hijacker		Sandbox escape, Code execution, Credential harvesting	Microsoft Edge, Microsoft Teams, Microsoft Outlook
ASSOCIATED ACTOR			**PATCH LINK**
-			-

IOC TYPE	VALUE
SHA256	a08d8e63b0cd3638fb40b8e6da546e26da69439597565827f9cec87915f78568, 3d1158884fb339b3328bd330fcc27598e1f1c94bcac39e75d1a272afa4deee1a

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 CVE</th></tr>
<tr><td>Gaslight</td><td rowspan="6">Gaslight is a Rust-based macOS implant and information stealer attributed with high confidence to DPRK-aligned activity. Its defining feature is an embedded 3.5 KB Markdown-fenced payload of 38 fabricated "system" messages designed as a prompt-injection cascade that targets LLM-assisted malware triage pipelines rather than conventional sandboxes, attempting to make the analyst's AI tooling abort, truncate, or refuse analysis.</td><td>-</td><td>-</td></tr>
<tr><td>TYPE</td><td>IMPACT</td><td>AFFECTED PLATFORM</td></tr>
<tr><td>Infostealer</td><td rowspan="3">Persistent backdoor, Browser harvesting, Credential exfiltration</td><td>macOS</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td>PATCH LINK</td></tr>
<tr><td>-</td><td>-</td></tr>
<tr><td>IOC TYPE</td><td colspan="3">VALUE</td></tr>
<tr><td>SHA256</td><td colspan="3">6328567511d88fdc2ae0939c5ef17b7a63d2a833881900de018a4f12f4982525</td></tr>
</table>

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
CVE-2026-47729	Squidbleed	Squid Web Proxy (all versions in default configuration prior to the upstream fix)	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:squid-cache:squid:*:*:*:*:*:*:*:*	-
Squid Proxy Memory Leak Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-125	T1212: Exploitation for Credential Access, T1528: Steal Application Access Token, T1588: Obtain Capabilities, T1588.006: Vulnerabilities	https://github.com/squid-cache/squid/releases

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCT</th><th>ASSOCIATED ACTORS</th></tr>
<tr><td rowspan="3">CVE-2026-12569</td><td>  </td><td rowspan="2">PTC Windchill PDMLink and FlexPLM - all CPS (Critical Patch Set) versions, including releases prior to 11.0 M030</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:ptc:windchill_pdmlink:*:*:*:*:*:*:*:*
cpe:2.3:a:ptc:flexplm:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">PTC Windchill and FlexPLM Improper Input Validation Vulnerability</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-20
CWE-502</td><td>T1190: Exploit Public-Facing Application,T1059: Command and Scripting Interpreter,T1505: Server Software Component,T1505.003: Web Shell</td><td>https://www.ptc.com/en/support/article/CS473270, https://support.ptc.com/appserver/cs/view/solution.jsp?n=CS473270</td></tr>
</table>

Adversaries in Action

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="4"> 
Rapid Brigantine (aka Vanilla Tempest, Vice Society, Vice Spider, DEV-0832)</td><td>-</td><td rowspan="2">Education, Financial Services, Architecture, Legal Services, Non-profit, Construction Technology, Content Publishing</td><td rowspan="2">Worldwide</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Financial Gains</td><td>ASSOCIATED ATTACKS/RANSOM WARE</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>TARGETED CVE</td><td>Lorem Ipsum Loader, Oyster, Supper, MeowBackConn, Rhysida Ransomware</td><td>Google Chrome, Mozilla Firefox, Microsoft Edge, Microsoft Defender, WordPress</td></tr>
<tr><td>-</td><td colspan="2"></td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0043: Resource Development; 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; TA0040: Impact; T1584: Compromise Infrastructure; T1584.006: Web Services; T1608: Stage Capabilities; T1608.004: Drive-by Target; T1608.001: Upload Malware; T1583: Acquire Infrastructure; T1583.008: Malvertising; T1588: Obtain Capabilities; T1588.003: Code Signing Certificates; T1189: Drive-by Compromise; T1204: User Execution; T1204.004: Malicious Copy and Paste; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1059.007: JavaScript; T1059.003: Windows Command Shell; T1218: System Binary Proxy Execution; T1218.005: Mshta; T1218.007: Msiexec; T1106: Native API; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys / Startup Folder; T1053: Scheduled Task/Job; T1053.005: Scheduled Task; T1134: Access Token Manipulation; T1134.001: Token Impersonation/Theft; T1562: Impair Defenses T1562.001: Disable or Modify Tools; T1112: Modify Registry; T1140: Deobfuscate/Decode Files or Information; T1027: Obfuscated Files or Information; T1620: Reflective Code Loading; T1574: Hijack Execution Flow; T1574.001: DLL; T1055: Process Injection; T1055.001: Dynamic-link Library Injection; T1218: System Binary Proxy Execution; T1218.011: Rundll32; T1036: Masquerading; T1036.005: Match Legitimate Name or Location; T1497: Virtualization/Sandbox Evasion; T1480: Execution Guardrails; T1555: Credentials from Password Stores; T1555.003: Credentials from Web Browsers; T1539: Steal Web Session Cookie; T1518: Software Discovery; T1518.001: Security Software Discovery; T1082: System Information Discovery; T1087: Account Discovery; T1057: Process Discovery; T1021: Remote Services; T1021.002: SMB/Windows Admin Shares; T1021.006: Windows Remote Management; T1047: Windows Management Instrumentation; T1570: Lateral Tool Transfer; T1113: Screen Capture; T1560: Archive Collected Data; T1005: Data from Local System; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1568: Dynamic Resolution; T1568.002: Domain Generation Algorithms; T1102: Web Service; T1102.001: Dead Drop Resolver; T1102.002: Bidirectional Communication; T1572: Protocol Tunneling; T1090: Proxy; T1573: Encrypted Channel; 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 **two exploited vulnerabilities** and block the indicators related to the threat actor **Rapid Brigantine** and malware **Potemkin, RMMProject, EtherRAT, BabaDeda Loader, Lorem Ipsum Loader, Edgecution,** and **Gaslight.**

Uni5 Users

This is an actionable threat digest for HivePro Uni5 customers, and they can get comprehensive insights into their threat exposure and can take action on it effortlessly over the HivePro Uni5 dashboard by

- Run a Scan to discover the assets impacted by the **two exploited vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **Rapid Brigantine** and malware **Potemkin Loader, RMMProject, Edgecution,** and **Gaslight** in Breach and Attack Simulation(BAS).

Threat Advisories

WhatsApp Campaign Turns Victims into Remotely Managed Hosts

Squidbleed: Decades-Old Parser Flaw Exposes Sensitive Proxy Data

ClickFix Campaigns Deliver BabaDeda, Lorem Ipsum, and Potemkin Loaders

June 2026 Linux Patch Roundup

Edgecution: Malicious Edge Extension Opens the Door to Host Compromise

Gaslight: The Rust-Powered macOS Implant Designed to Mislead AI Tools

Critical PTC Windchill and FlexPLM Deserialization RCE Actively Exploited

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
Potemkin	SHA256	2abe5dd3a057fdef935722e50e9251c272d29fd26113187b853a1f9a9cb89d9b, 79f7b67ce8b39070f3e1c2b90fce0ce84134782a7dedcccc1edac197ee9e089b
RMMProject	SHA256	3b7ae925e2d64522b4f69b56285b05aeca8c5aab5ab46a9c02c4fafb69d881ce
BabaDeda Loader	SHA256	0098b2c38a69132bfde02d329d6c1c6e2b529d32d7b775a2ac78a369c0d10853, 062f019515bff366fcbf49cca3f776c21e2beb81c043a45eea81044a9391fd97
Edgecution	SHA256	a08d8e63b0cd3638fb40b8e6da546e26da69439597565827f9cec87915f78568, 3d1158884fb339b3328bd330fcc27598e1f1c94bcac39e75d1a272afa4deee1a
Gaslight	SHA256	6328567511d88fdc2ae0939c5ef17b7a63d2a833881900de018a4f12f4982525

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

June 29, 2026 • 7:30 AM

More at www.hivepro.com