Date of Publication
May 11, 2026

Hive Pro

Hiveforce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities and Actors

04 to 10 May 2026

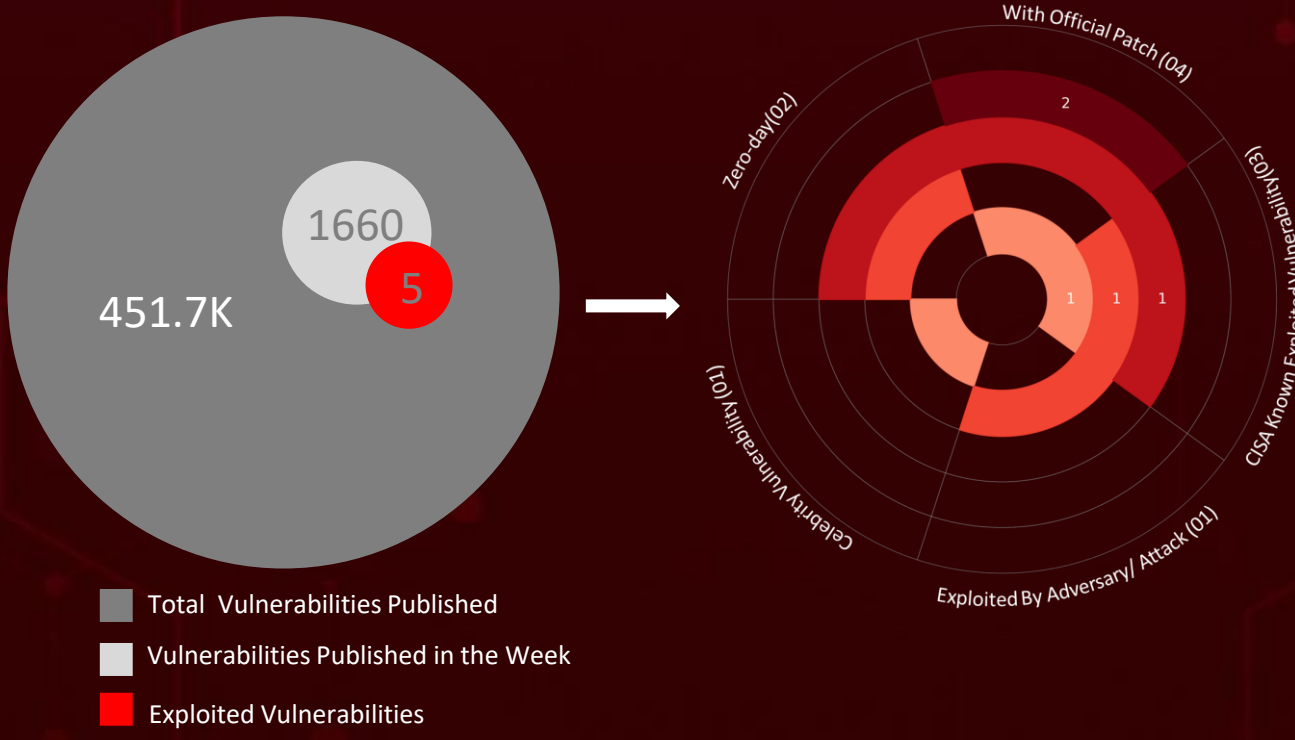
Table Of Contents

Summary

HiveForce Labs has recently made significant advancements in identifying cybersecurity threats. Over the past week, **five** major attacks were detected, **five** critical vulnerabilities were actively exploited, and **two** threat actors were closely monitored, reflecting an alarming escalation in malicious activities.

CVE-2026-31431 "Copy Fail" a critical Linux kernel privilege-escalation flaw in the algif_aead crypto module that lets an unprivileged user gain root via a 732-byte Python exploit, affecting virtually every major Linux distribution shipped since 2017. **Silver Fox APT** Tax-Themed Campaign China-based threat group ran a large-scale phishing operation against organizations in India and Russia, distributing over 1,600 malicious emails impersonating tax authorities to deploy ValleyRAT and the newly discovered Python-based ABCDoor backdoor through a customized RustSL loader, hitting industrial, consulting, retail, and transportation sectors.

Meanwhile, **CVE-2026-0300** PAN-OS Zero-Day, a likely state-sponsored cluster tracked as **CL-STA-1132** exploited an unauthenticated buffer overflow in the User-ID Authentication Portal since April 9, gaining root on internet-exposed firewalls, injecting shellcode into nginx, deploying EarthWorm and ReverseSocks5 tunnels, enumerating Active Directory, and systematically destroying forensic evidence. These rising threats pose significant and immediate dangers to users worldwide.



High Level Statistics

5
Attacks Executed

5
Vulnerabilities Exploited

2
Adversaries in Action

- ValleyRAT
- ABCDoor
- RustSL
- EarthWorm
- ReverseSocks5

- CVE-2026-31431
- CVE-2026-22679
- CVE-2026-0300
- CVE-2026-40982
- CVE-2026-6973

- Silver Fox
- CL-STA-1132

Insights

CL-STA-1132 State-sponsored actor roots PAN-OS firewalls via Captive Portal overflow, deploys EarthWorm/ReverseSocks5 tunnels.

CVE-2026-22679 Weaver E-cology Unauthenticated RCE via exposed Dubbo debug endpoint, exploited with stealthy PowerShell payloads.

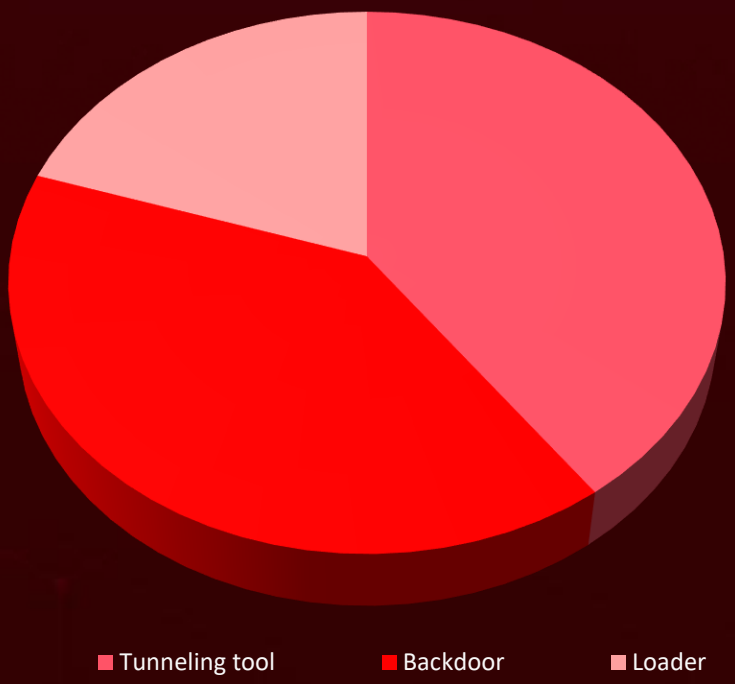
CVE-2026-6973 Ivanti EPMM Actively exploited admin RCE on on-prem EPMM.

Silver Fox APT China-based group used fake Indian and Russian tax emails to drop ValleyRAT, ABCDoor, and RustSL loader.

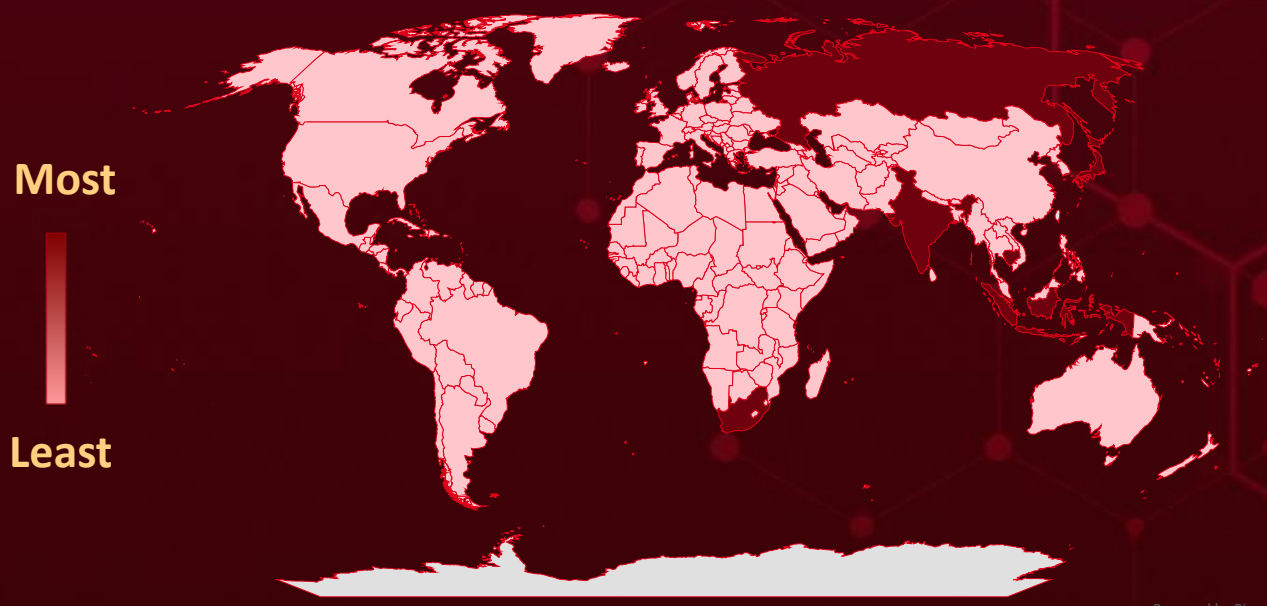
CVE-2026-31431 "Copy Fail“ 732-byte Python exploit roots nearly every Linux distro since 2017 via algif_aead crypto flaw.

CVE-2026-40982 Spring Cloud Unauthenticated path traversal in Config Server leaks secrets, tokens, and credentials from microservices.

Threat Distribution



Targeted Countries



Countries
Indonesia
South Africa
Russia
Cambodia
India
Japan
United Arab Emirates
United States
Mexico
France
Oman
Germany
Qatar
Italy
Spain
Kuwait
United Kingdom
Romania
Azerbaijan
Thailand

Countries
Benin
Nigeria
Bhutan
Solomon Islands
Bolivia
Malawi
Bosnia and Herzegovina
Myanmar
Botswana
Papua New Guinea
Brazil
Belarus
Brunei
State of Palestine
Bulgaria
Tuvalu
Burkina Faso
Malta
Burundi
Mongolia
Cabo Verde
Netherlands
Syria

Countries
Albania
Cameroon
Bangladesh
Andorra
Saint Lucia
Central African Republic
Sierra Leone
Chad
South Sudan
Chile
China
Trinidad and Tobago
Colombia
Luxembourg
Comoros
Maldives
Congo
Mauritania
Costa Rica
Moldova
Côte d'Ivoire
Morocco
Croatia

Countries
Nauru
Cuba
Nicaragua
Cyprus
North Macedonia
Czech Republic
Palau
Denmark
Peru
Djibouti
Barbados
Dominica
Rwanda
Dominican Republic
San Marino
DR Congo
Serbia
Ecuador
Slovakia
Egypt
South Korea
El Salvador
Sri Lanka
Equatorial Guinea

Targeted Industries

TOP MITRE ATT&CK TTPs

T1059 Command and Scripting Interpreter	**T1566** Phishing	**T1190** Exploit Public-Facing Application	**T1204** User Execution	**T1588** Obtain Capabilities
T1105 Ingress Tool Transfer	**T1068** Exploitation for Privilege Escalation	**T1555** Credentials from Password Stores	**T1071** Application Layer Protocol	**T1082** System Information Discovery
T1078 Valid Accounts	**T1027** Obfuscated Files or Information	**T1071.001** Web Protocols	**T1083** File and Directory Discovery	**T1566.001** Spearphishing Attachment
T1059.001 PowerShell	**T1204.001** Malicious Link	**T1588.006** Vulnerabilities	**T1021** Remote Services	**T1041** Exfiltration Over C2 Channel

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
ValleyRAT	ValleyRat is a sophisticated multi-stage Remote Access Trojan attributed to the China-based Silver Fox APT group, targeting Chinese-speaking users and now expanding globally. It uses staged shellcode loading, multiple UAC bypasses, and AV/Defender disabling to remain stealthy. Once installed, it grants attackers full remote control with keylogging, screen capture, and arbitrary plugin deployment.	Phishing	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		Espionage, full system compromise	Windows
Backdoor			
ASSOCIATED ACTOR			**PATCH LINK**
Silver Fox			-

IOC TYPE	VALUE
IPv4	108[.]187[.]37[.]85, 108[.]187[.]42[.]63, 207[.]56[.]138[.]28
MD5	4A5195A38A458CDD2C1B5AB13AF3B393, E66BAE6E8621DB2A835FA6721C3E5BBE

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 rowspan="2">ABCDoor</td><td rowspan="6">ABCDoor is a previously undocumented Python-based backdoor used by the Silver Fox group since at least December 2024, delivered as a custom ValleyRAT plugin. It communicates with C2 servers over HTTPS using a distinctive "abc" subdomain pattern. Capabilities include persistence, screenshot capture, remote mouse/keyboard control, file system operations, and clipboard exfiltration.</td><td>Phishing</td><td>-</td></tr>
<tr><td rowspan="2">TYPE</td><td>IMPACT</td><td>AFFECTED PRODUCT</td></tr>
<tr><td rowspan="2">Backdoor</td><td rowspan="3">Remote control, data exfiltration</td><td>Windows</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td>PATCH LINK</td></tr>
<tr><td>Silver Fox</td><td>-</td></tr>
<tr><td>IOC TYPE</td><td colspan="3">VALUE</td></tr>
<tr><td>MD5</td><td colspan="3">04194F8DDD0518FD8005F0E87AE96335,
F15A67899CFE4DECFF76D4CD1677C254,
11705121F64FA36F1E9D7E59867B0724,
13669B8F2BD0AF53A3FE9AC0490499E5,
5B998A5BC5AD1C550564294034D4A62C</td></tr>
</table>

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 rowspan="2">RustSL</td><td rowspan="5">RustSL is a modified Rust-based shellcode loader derived from a public GitHub project, weaponized by Silver Fox for stealthy payload delivery. It uses custom modules for steganography-based unpacking and country-based geofencing before executing payloads. Establishes "Phantom Persistence" and serves as the initial stage for dropping ValleyRAT while evading antivirus detection.</td><td>Phishing</td><td>-</td></tr>
<tr><td>IMPACT</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>TYPE</td><td rowspan="3">Stealthy payload delivery, AV bypass</td><td>Windows</td></tr>
<tr><td>Loader</td><td>PATCH LINK</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td>-</td></tr>
<tr><td>Silver Fox</td><td colspan="3"></td></tr>
<tr><td>IOC TYPE</td><td colspan="3">VALUE</td></tr>
<tr><td>MD5</td><td colspan="3">039E93B98EF5E329F8666A424237AE73,
B6DF7C59756AB655CA752B8A1B20CFFA,
5390E8BF7131CAAAA98A5DD63E27B2BC,
44299A368000AE1EE9E9E584377B8757,
E5E8EF65B4D265BD5FB77FE165131C2F</td></tr>
</table>

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 rowspan="2">EarthWorm</td><td rowspan="5">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.</td><td>-</td><td>CVE-2026-0300</td></tr>
<tr><td rowspan="2">TYPE</td><td>IMPACT</td><td>AFFECTED PRODUCT</td></tr>
<tr><td rowspan="3">Covert tunneling, lateral movement</td><td rowspan="2">Palo Alto Networks PAN-OS</td></tr>
<tr><td>Tunneling tool</td><td>ASSOCIATED ACTOR</td><td>PATCH LINK</td></tr>
<tr><td>CL-STA-1132</td><td>✕</td></tr>
<tr><td>IOC TYPE</td><td colspan="3">VALUE</td></tr>
<tr><td>URL</td><td colspan="3">hxxp[:]//146[.]70[.]100[.]69[:]8000/php_sess</td></tr>
<tr><td>SHA256</td><td colspan="3">e11f69b49b6f2e829454371c31ebf86893f82a042dae3f2faf63dcd84f97a584</td></tr>
</table>

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 rowspan="2">ReverseSocks5</td><td rowspan="6">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.</td><td>-</td><td>CVE-2026-0300</td></tr>
<tr><td>TYPE</td><td>IMPACT</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>Tunneling tool</td><td rowspan="3">Firewall bypass, internal pivoting</td><td rowspan="2">Palo Alto Networks PAN-OS</td></tr>
<tr><td>ASSOCIATED ACTOR</td></tr>
<tr><td>CL-STA-1132</td><td>PATCH LINK</td></tr>
<tr><td>IOC TYPE</td><td colspan="3">VALUE</td></tr>
<tr><td>URL</td><td colspan="3">hxxps[:]//github[.]com/Acebond/ReverseSocks5/releases/download/v2.2.0/ReverseSocks5-v2.2.0-linux-amd64.tar[.]gz</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 PRODUCTS	ASSOCIATED ACTOR
CVE-2026-31431	Copy Fail	Linux Kernel versions shipped from 2017 through 6.18.21 and 6.19.11; fixed in 6.18.22, 6.19.12, and 7.0)	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*	-
Linux Kernel Incorrect Resource Transfer Between Spheres Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-669	T1068: Exploitation for Privilege Escalation, T1059.006 Command and Scripting Interpreter: Python	https://git.kernel.org/pub/scm/linux/kernel/git/stable/linux.git/commit/?id=893d22e0135fa394db81df88697fba6032747667

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-22679	✗	Weaver (Fanwei) E-cology 10.0 versions prior to 20260312	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:weaver:e-cology:*:*:*:*:*:*:*:*	-
Weaver (Fanwei) E-cology Remote Code Execution Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-306	T1190: Exploit Public-Facing Application, T1059.001: Command and Scripting Interpreter: PowerShell, T1105: Ingress Tool Transfer, T1036: Masquerading	https://www.weaver.com.cn/cs/securityDownload.html#

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	✗

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-40982		VMware Spring Cloud Config Server 3.1.0 through 3.1.13; 4.1.0 through 4.1.9; 4.2.0 through 4.2.6; 4.3.0 through 4.3.2; 5.0.0 through 5.0.2; and older unsupported versions	-
	ZERO-DAY		
		**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:a:vmware:spring_cloud_config:*:*:*:*:*:*:*:*	-
VMware Spring Cloud Config Server Path Traversal Vulnerability			
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-22	T1190: Exploit Public-Facing Application, T1083: File and Directory Discovery, T1005: Data from Local System	https://github.com/spring-cloud/spring-cloud-config/releases

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2026-6973	 ZERO-DAY	Ivanti EPMM (Before 12.6.1.1, 12.7.0.1, 12.8.0.1)	-
		**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:a:ivanti:endpoint_manager_mobile:*:*:*:*:*:*:*:*	-
Ivanti Endpoint Manager Mobile (EPMM) Improper Input Validation Vulnerability			
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-20	T1078: Valid Accounts, T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://hub.ivanti.com/s/article/May-2026-Security-Advisory-Ivanti-Endpoint-Manager-Mobile-EPMM-Multiple-CVEs?language=en_US

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 Silver Fox (aka Void Arachne)	China	Industrial, Consulting, Retail, Transportation	India, Russia, Indonesia, South Africa, Cambodia, Japan
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCT**
	-	ValleyRAT, ABCDoor, RustSL	Windows

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, TA0011: Command and Control, TA0010: Exfiltration, TA0040: Impact, T1566: Phishing, T1566.001: Spearphishing Attachment, T1566.002: Spearphishing Link, T1204: User Execution , T1204.002: Malicious File, T1059: Command and Scripting Interpreter, T1059.001: PowerShell, T1059.003: Windows Command Shell, T1059.007: JavaScript, T1059.006: Python, T1547: Boot or Logon Autostart Execution, T1547.001: Registry Run Keys /Startup Folder, T1053: Scheduled Task/Job , T1053.005: Scheduled Task, T1027: Obfuscated Files or Information, T1027.013: Encrypted/Encoded File, T1497: Virtualization/Sandbox Evasion , T1497.001: System Checks, T1036: Masquerading, T1036.005: Match Legitimate Name or Location, T1036.008: Masquerade File Type, T1140: Deobfuscate/Decode Files or Information, T1622: Debugger Evasion, T1016: System Network Configuration Discovery, T1016.001: Internet Connection Discovery, T1082: System Information Discovery Collection, T1115: Clipboard Data, T1113: Screen Capture, T1071: Application Layer Protocol , T1071.001: Web Protocols, T1105: Ingress Tool Transfer, T1571: Non-Standard Port Exfiltration , T1041: Exfiltration Over C2 Channel

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			

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **five exploited vulnerabilities** and block the indicators related to the threat actor **Silver Fox, CL-STA-1132,** and malware **ValleyRAT, ABCDoor, RustSL, EarthWorm, ReverseSocks5.**

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

- Running a Scan to discover the assets impacted by the **five exploited vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to the malware **ValleyRAT, ABCDoor, RustSL** in Breach and Attack Simulation(BAS).

Threat Advisories

One Script, Every Distro, Full Root: Copy Fail Vulnerability Rewriting Linux Threat Models

Tax Trap to Full Takeover: Inside the Silver Fox Multi-Stage Intrusion Chain

Unauthenticated RCE in Weaver E-cology Actively Exploited

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

Is Your Spring Config Server an Open Door? CVE-2026-40982 Says Yes

Ivanti EPMM Flaws Threaten Enterprise Device Management Systems

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
ValleyRAT	IPv4	108[.]187[.]37[.]85, 108[.]187[.]42[.]63, 207[.]56[.]138[.]28
	MD5	4A5195A38A458CDD2C1B5AB13AF3B393, E66BAE6E8621DB2A835FA6721C3E5BBE
ABCDoor	IPv4:Port	45[.]118[.]133[.]203[:]5000
	Domains	abc[.]fetish-friends[.]com, abc[.]3mkorealtd[.]com, abc[.]sudsmama[.]com, abc[.]woopami[.]com, abc[.]ilptour[.]com, abc[.]petitechanson[.]com, abc[.]doublemobile[.]com
	MD5	04194F8DDD0518FD8005F0E87AE96335, F15A67899CFE4DECFF76D4CD1677C254, 11705121F64FA36F1E9D7E59867B0724, 13669B8F2BD0AF53A3FE9AC0490499E5, 5B998A5BC5AD1C550564294034D4A62C, C50C980D3F4B7ED970F083B0D37A6A6A,

Attack Name	TYPE	VALUE
ABCDoor	MD5	DE8F0008B15F2404F721F76FAC34456A, 9BF9F635019494C4B70FB0A7C0FB53E4, A543B96B0938DE798DD4F683DD92A94A, FA08B243F12E31940B8B4B82D3498804
RustSL	MD5	039E93B98EF5E329F8666A424237AE73, B6DF7C59756AB655CA752B8A1B20CFFA, 5390E8BF7131CAAAA98A5DD63E27B2BC, 44299A368000AE1EE9E9E584377B8757, E5E8EF65B4D265BD5FB77FE165131C2F, 3279307508F3E5FB3A2420DEC645F583, 1020497BEF56F4181AEFB7A0A9873FB4, B23D302B7F23453C98C11CA7B2E4616E, A234850DFDFD7EE128F648F9750DD2C4, 4FC5EC1DE89CE3FCDD3E70DB4A9C39D1, A0D1223CA4327AA5F7674BDA8779323F, 70AE9CA2A285DA9005A8ACB32DD31ACE, DD0114FFACC6610B5A4A1CB0E79624CC, 891DE2FF486A1824F2DB01C1BDF1D2E9, B0E06925DB5416DFC90BABF46402CD6F, AD39A5790B79178D02AC739099B8E1F4, D1D78CD1436991ADB9C005CC7C6B5B98, 2C5A1DD4CB53287FE0ED14E0B7B7B1B7, E6362A81991323E198A463A8CE255533, CB3D86E3EC2736EE1C883706FCA172F8, A083C546DC66B0F2A5E0E2E68032F62C, 70016DDBCB8543BDB06E0F8C509EE980, 8FC911CA37F9F451A213B967F016F1F8, 202A5BCB87C34993318CFA3FA0C7ECB0, 06130DC648621E93ACB9EFB9FABB9651, F7037CC9A5659D5A1F68E88582242375, 8AC5BEE89436B29F9817E434507FEF55, 5ED84B2099E220D645934E1FD552AE3A, 27A3C439308F5C4956D77E23E1AAD1A9, 53B68CA8D7A54C15700CF9500AE4A4E2, 1D1F71936DB05F67765F442FEB95F3FD, 3C6AEC25EBB2D51E1F16C2EEF181C82A, 7F27818E4244310A645984CCC41EA818, A75713F0310E74FFD24D91E5731C4D31, 4FC8C78516A8C2130286429686E200ED, 3417B9CF7ACB22FAE9E24603D4DE1194, 933F1CB8ED2CED5D0DD2877C5EA374E8, B5CA812843570DCF8E7F35CACAB36D4A

Attack Name	TYPE	VALUE
EarthWorm	URL	hxxp[:]//146[.]70[.]100[.]69[:]8000/php_sess
	SHA256	e11f69b49b6f2e829454371c31ebf86893f82a042dae3f2faf63dcd84f97a584
ReverseSocks5	URL	hxxps[:]//github[.]com/Acebond/ReverseSocks5/releases/download/v2.2.0/ReverseSocks5-v2.2.0-linux-amd64.tar[.]gz

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 11, 2026 • 9:30 AM

More at www.hivepro.com