Date of Publication
May 4, 2026

Hive Pro

Hiveforce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities, and Actors

27 APRIL to 03 MAY 2026

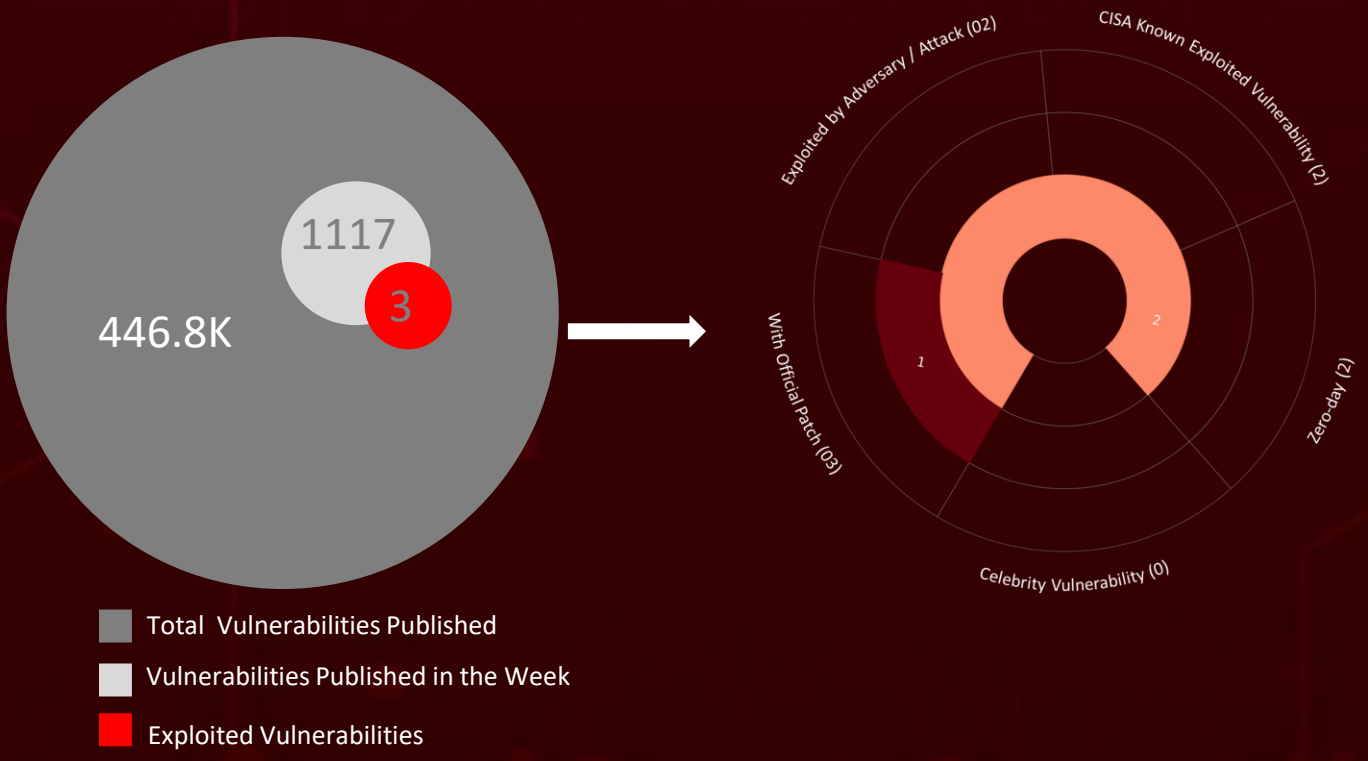
Table Of Contents

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, **four** major attacks were detected, **three** vulnerabilities were exploited, and **two** active threat actor groups were monitored, signaling a concerning escalation in malicious activity.

In one notable intrusion, **UAT-4356** actors abused flaws in Cisco Secure Firewall ASA and FTD VPN web servers to gain unauthenticated access and execute code on exposed systems. Once inside, they deployed the **LINE VIPER** shellcode loader to spin up rogue VPN sessions and quietly siphon off sensitive assets, including configurations, admin credentials, certificates, and private keys. The operation didn't stop there, **FIRESTARTER**, a Linux-based backdoor, was implanted to hook into the LINA process and tamper with system mount configurations, ensuring long-term persistence and stealthy control.

Meanwhile, the threat landscape is also being shaped by scalable cybercrime operations and deceptive social engineering campaigns. The rebranded **VECT 2.0** ransomware group is rapidly expanding its RaaS ecosystem with a purpose-built C++ framework designed for efficiency and impact. Alongside this, **Operation TrustTrap** is leveraging a vast phishing infrastructure of over 16,800 domains, cleverly mimicking government services across multiple countries by manipulating subdomains and trusted naming patterns to evade detection. Together, these developments underscore a shift toward hybrid attack strategies, where technical exploitation and psychological manipulation go hand in hand, making timely patching, vigilant monitoring, and layered defenses more critical than ever.



High Level Statistics

4
Attacks Executed

3
Vulnerabilities Exploited

2
Adversaries in Action

- FIRESTARTER
- LINE VIPER
- RayInitiator
- VECT Ransomware (VECT 2.0)
- CVE-2025-20333
- CVE-2025-20362
- CVE-2026-42208
- UAT-4356
- APT36

Insights

UAT-4356 turns Cisco ASA/FTD VPN flaws into lasting footholds, leveraging LINE VIPER and the FIRESTARTER backdoor to persist even after patches and reboots.

UAT-4356 exploits **CVE-2025-20333** and **CVE-2025-20362** to break into Cisco ASA/FTD, turning exposed VPN gateways into unauthenticated RCE entry points.

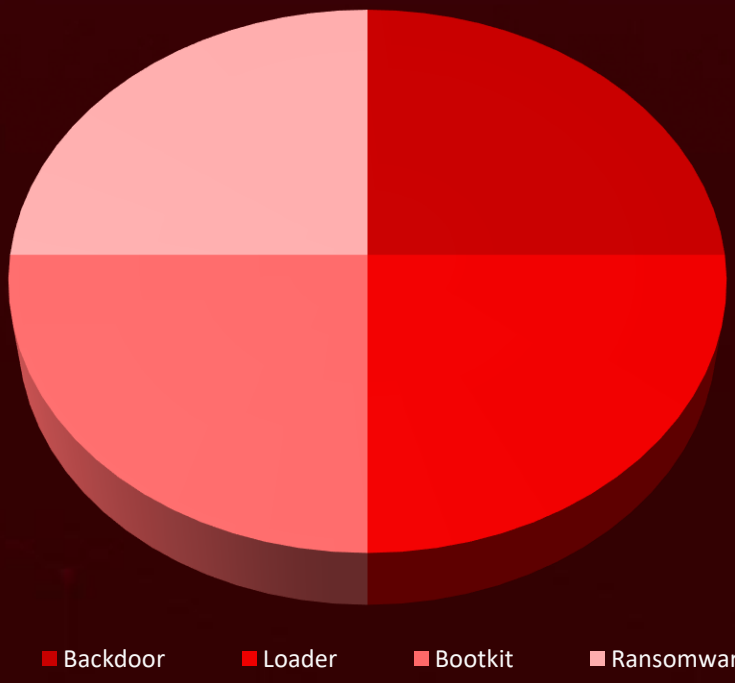
APT36 continues its targeted playbook, using spoofed domains and government impersonation to quietly infiltrate Indian defense and diplomatic circles.

VECT 2.0 is quickly carving out space in the RaaS ecosystem, using a custom C++ locker and aggressive tactics to scale disruption for profit.

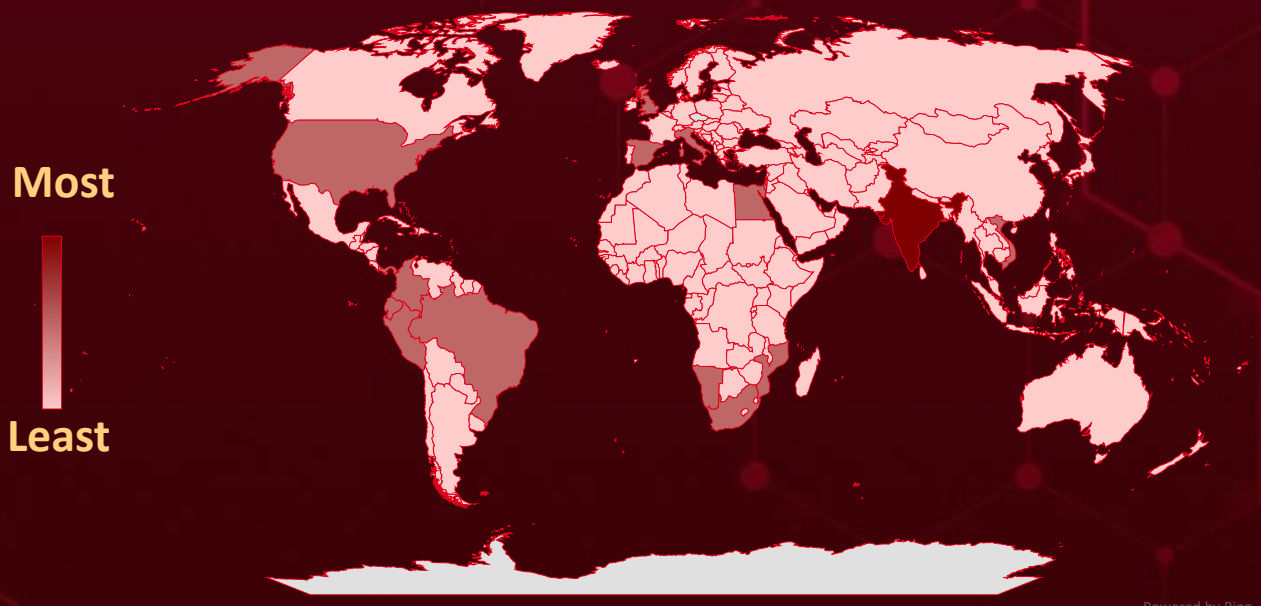
Operation TrustTrap scales deception globally, leveraging 16,800+ spoofed domains to impersonate government services and harvest trust at scale.

CVE-2026-42208 turns LiteLLM's auth check into an attack vector, letting unauthenticated SQL injection expose backend data.

Threat Distribution



Targeted Countries



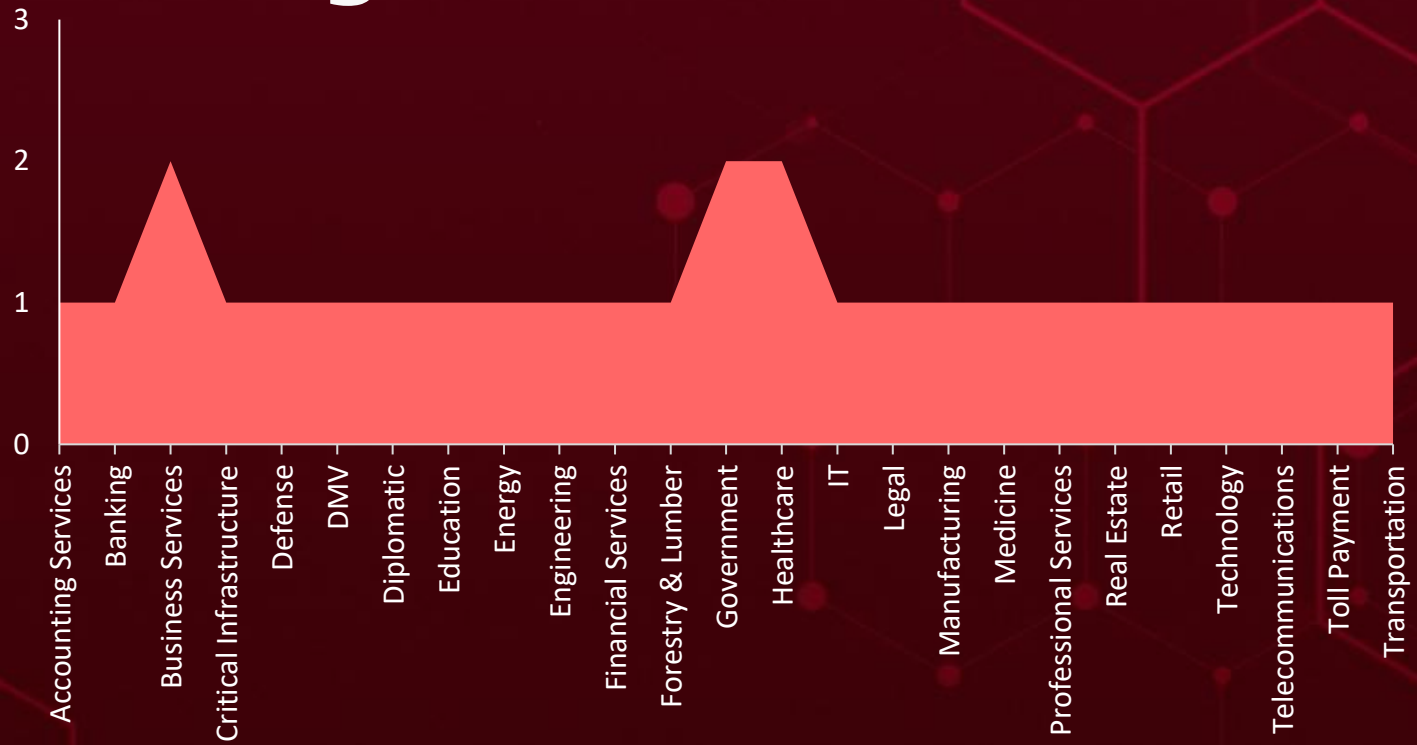
Countries
India
Mozambique
Brazil
Panama
Colombia
United States
Ecuador
Namibia
Egypt
Peru
South Africa
Spain
United Kingdom
Israel
Italy
Vietnam
Russia
Micronesia
Togo
Belize
North Korea
Benin
Solomon Islands
Bhutan
Belgium

Countries
Bolivia
Austria
Bosnia and Herzegovina
Papua New Guinea
Botswana
Saudi Arabia
Albania
Suriname
Brunei
Ukraine
Bulgaria
Marshall Islands
Burkina Faso
Montenegro
Burundi
New Zealand
Cabo Verde
Pakistan
Cambodia
Poland
Cameroon
Saint Vincent and the Grenadines
Canada
Sierra Leone
Central African Republic

Countries
South Sudan
Chad
Tajikistan
Chile
Turkey
China
United States of America
Algeria
Mali
Comoros
Mauritius
Congo (Congo-Brazzaville)
Monaco
Costa Rica
Australia
Côte d'Ivoire
Nepal
Croatia
Niger
Cuba
Norway
Cyprus
Palestine State
Czechia (Czech Republic)
Bahamas

Countries
Denmark
Saint Kitts and Nevis
Djibouti
San Marino
Dominica
Serbia
Dominican Republic
Slovakia
Andorra
Bahrain
Angola
Sri Lanka
El Salvador
Switzerland
Equatorial Guinea
Thailand
Eritrea
Trinidad and Tobago
Estonia
Tuvalu
Barbados
Ethiopia
Uzbekistan

Targeted Industries



TOP MITRE ATT&CK TTPs

T1070.004
File Deletion

T1082
System Information Discovery

T1071.001
Web Protocols

T1005
Data from Local System

T1070
Indicator Removal

T1071
Application Layer Protocol

T1133
External Remote Services

T1562
Impair Defenses

T1552
Unsecured Credentials

T1027
Obfuscated Files or Information

T1059
Command and Scripting Interpreter

T1036
Masquerading

T1547
Boot or Logon Autostart Execution

T1566
Phishing

T1552.001
Credentials In Files

T1036.005
Match Legitimate Resource Name or Location

T1562.001
Disable or Modify Tools

T1078
Valid Accounts

T1046
Network Service Discovery

T1090
Proxy

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
FIRESTARTER	FIRESTARTER is a stealthy backdoor attributed to UAT-4356 that enables remote access and arbitrary code execution within the LINA process, a core component of Cisco ASA and FTD appliances running FXOS. It operates by hijacking a legitimate handler function at a fixed memory offset, replacing it with a malicious routine that inspects incoming WebVPN XML requests. When a specially crafted request containing a predefined prefix is detected, FIRESTARTER extracts and executes the embedded shellcode directly in memory; otherwise, the traffic is passed to the original handler, helping the backdoor remain covert during normal operations.	Exploiting Vulnerabilities	CVE-2025-20333 CVE-2025-20362
		IMPACT	**AFFECTED PRODUCTS**
TYPE		System Compromise, Persistence	Cisco Secure Firewall ASA and FTD Software
Backdoor			**PATCH LINK**
ASSOCIATED ACTOR			https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-CISAED25-03
UAT-4356			

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">LINE VIPER</td><td rowspan="6">LINE VIPER is a user-mode shellcode loader designed to execute and manage malicious tasks within compromised systems. It is typically delivered in memory by the RayInitiator component through a crafted WebVPN authentication request that includes a partial PKCS7 certificate followed by embedded shellcode. The malware supports dual communication methods, via HTTPS WebVPN sessions or ICMP with responses over raw TCP, and relies on victim-specific tokens, a technique also observed in related tools like LINE DANCER and LINE RUNNER. Once active, LINE VIPER enables a wide range of capabilities, including executing CLI commands, capturing network traffic, bypassing authentication controls, suppressing syslog logs, harvesting user command inputs, and even triggering delayed system reboots.</td><td>Exploiting Vulnerabilities</td><td>CVE-2025-20333
CVE-2025-20362</td></tr>
<tr><td>IMPACT</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>TYPE</td><td rowspan="5">Execute Commands, System reboot</td><td rowspan="2">Cisco Secure Firewall ASA and FTD Software</td></tr>
<tr><td>Loader</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td>PATCH LINK</td></tr>
<tr><td>UAT-4356</td><td rowspan="2">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-CISAED25-03</td></tr>
<tr><td>IOC TYPE</td><td colspan="3">VALUE</td></tr>
<tr><td>SHA256</td><td colspan="3">bd82a15394f80c6eb82e439dcec93eb8535e9bbc9b26e991fef8bd92c5ba345f,
e6684678ace298f81aedd140415c74553612bf86b904c11ca059424ef8322e7c</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
RayInitiator	RayInitiator is a persistent, multi-stage bootkit used to deploy the LINE VIPER implant on Cisco ASA 5500-X devices that lack secure boot protections. Implemented as a modified GRUB (GRand Unified Bootloader) component, it is flashed directly onto compromised devices, allowing it to survive both reboots and firmware upgrades. Its primary role is to establish a durable foothold and install a lightweight handler within the LINA process, enabling the execution of LINE VIPER and ensuring continued control over the system.	Exploiting Vulnerabilities	CVE-2025-20333 CVE-2025-20362
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Deploy the LINE VIPER implant	Cisco Secure Firewall ASA and FTD Software
Bootkit			**PATCH LINK**
ASSOCIATED ACTOR			https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-CISAED25-03
UAT-4356			

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
VECT Ransomware (VECT 2.0)	VECT Ransomware is a Ransomware-as-a-Service (RaaS) operation that emerged in December 2025. Its visibility increased further following a reported partnership with TeamPCP, a threat actor linked to multiple supply-chain attacks. Developed in C++, VECT introduced version 2.0 in February 2026, expanding support across Windows, Linux, and ESXi environments, with the group claiming the lockers were built entirely in-house. The operators have also hinted at upcoming “cloud lockers” aimed at targeting cloud storage platforms, which will be selectively offered to affiliates who demonstrate capability through a vetting challenge.		-
		IMPACT	**AFFECTED PLATFORM**
TYPE		Encrypt Data, Data Theft	Windows, Linux, VMware ESXi
Ransomware			**PATCH LINK**
ASSOCIATED ACTOR			-
-			

IOC TYPE	VALUE
SHA256	a7eadcf81dd6fda0dd6affefaffcb33b1d8f64ddec6e5a1772d028ef2a7da0f2, 58e17dd61d4d55fa77c7f2dd28dd51875b0ce900c1e43b368b349e65f27d6fdd

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-2025-20333</td><td>✗</td><td rowspan="2">Cisco ASA Software: 9.16, 9.17, 9.18, 9.19, 9.20, 9.22, 9.23
Cisco FTD Software: 7.0, 7.2, 7.4, 7.6, 7.7</td><td rowspan="2">UAT-4356</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:cisco:firepower_threat_defense:*:*:*:*:*:*:*:*
cpe:2.3:o:cisco:adaptive_security_appliance_software:*:*:*:*:*:*:*:*</td><td rowspan="2">FIRESTARTER, LINE VIPER, RayInitiator</td></tr>
<tr><td rowspan="2">Cisco Secure Firewall Adaptive Security Appliance (ASA) and Secure Firewall Threat Defense (FTD) Buffer Overflow Vulnerability</td><td rowspan="2">✓</td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-120</td><td>T1190: Exploit Public-Facing Application; T1068: Exploitation for Privilege Escalation; T1542.004 Pre-OS Boot: ROMMONkit</td><td>https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-CISAED25-03</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2025-20362	✗	Cisco ASA Software: 9.16, 9.17, 9.18, 9.19, 9.20, 9.22, 9.23 Cisco FTD Software: 7.0, 7.2, 7.4, 7.6, 7.7	UAT-4356
	ZERO-DAY		
	✓	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:a:cisco:firepower_threat_defense:*:*:*:*:*:*:*:* cpe:2.3:o:cisco:adaptive_security_appliance_software:*:*:*:*:*:*:*:*	FIRESTARTER, LINE VIPER, RayInitiator
Cisco Secure Firewall Adaptive Security (ASA) Appliance and Secure Firewall Threat Defense (FTD) Missing Authorization Vulnerability	✓		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-862	T1059: Command and Scripting Interpreter; T1190: Exploit Public-Facing Application; T1068: Exploitation for Privilege Escalation	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-CISAED25-03

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2026-42208	✗	BerriAI LiteLLM (>= 1.81.16, < 1.83.7)	-
	ZERO-DAY		
	✗	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:a:berriai:litellm:*:*:*:*:*:*:*:*	-
BerriAI LiteLLM SQL Injection Vulnerability	✗		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-89	T1190: Exploit Public-Facing Application; T1005: Data from Local System; T1552: Unsecured Credentials	https://github.com/BerriAI/litellm/releases/tag/v1.83.7-stable

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 UAT-4356 (aka Storm-1849)	China	Government, Critical Infrastructure, and Telecommunications (any organization with internet-facing Cisco ASA, FTD, or Firepower VPN web services)	Worldwide
	MOTIVE		
	Espionage		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCT**
	CVE-2025-20333 CVE-2025-20362	FIRESTARTER, LINE VIPER, RayInitiator	Cisco Secure Firewall ASA and FTD Software

TTPs
TA0001: Initial Access; TA0005: Defense Evasion; TA0003: Persistence; TA0007: Discovery; TA0006: Credential Access; TA0011: Command and Control; TA0002: Execution; TA0009: Collection; T1190: Exploit Public-Facing Application; T1133: External Remote Services; T1070: Indicator Removal; T1222: File and Directory Permissions Modification; T1564: Hide Artifacts; T1070: Indicator Removal; T1070.004: File Deletion; T1070.006: Timestomp; T1036: Masquerading; T1036.005: Match Legitimate Resource Name or Location; T1055: Process Injection; T1562: Impair Defenses; T1562.001: Disable or Modify Tools; T1543: Create or Modify System Process; T1078: Valid Accounts; T1546: Event Triggered Execution; T1546.004: Unix Shell Configuration Modification; T1547: Boot or Logon Autostart Execution; T1082: System Information Discovery; T1057: Process Discovery; T1552: Unsecured Credentials; T1552.001: Credentials In Files; T1219: Remote Access Software; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1070.004: File Deletion; T1059: Command and Scripting Interpreter; T1005: Data from Local System

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 APT36 (aka Transparent Tribe, ProjectM, TEMP.Lapis, Mythic Leopard, Copper Fieldstone, Earth Karkaddan, STEPPY-KAVACH, Green Havildar, APT-C-56, Storm-0156, Opaque Draco)	Pakistan	Government, Defense, Diplomatic, Transportation, Department of Motor Vehicles (DMV), Toll Payment, Healthcare	United States, India, Vietnam, United Kingdom
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCT**
	-	-	-

TTPs
TA0042: Resource Development; TA0001: Initial Access; TA0005: Defense Evasion; TA0006: Credential Access; TA0009: Collection; TA0011: Command and Control; T1583: Acquire Infrastructure; T1583.001: Domains; T1583.006: Web Services; T1583.003: Virtual Private Server; T1587: Develop Capabilities; T1608: Stage Capabilities; T1608.001: Upload Malware; T1608.005: Link Target; T1566.002: Spearphishing Link; T1566.003: Spearphishing via Service; T1189: Drive-by Compromise; T1036: Masquerading; T1036.005: Match Legitimate Resource Name or Location; T1027: Obfuscated Files or Information; T1656: Impersonation; T1056: Input Capture; T1056.003: Web Portal Capture; T1185: Browser Session Hijacking; T1071: Application Layer Protocol; T1071.001: Web Protocols

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **three exploited vulnerabilities** and block the indicators related to the threat actors **UAT-4356, APT36,** and malware **FIRESTARTER, LINE VIPER, RayInitiator,** and **VECT Ransomware (VECT 2.0).**

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 **three exploited vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actors **UAT-4356, APT36,** and malware **VECT Ransomware (VECT 2.0)** in Breach and Attack Simulation(BAS).

Threat Advisories

Patched but Not Cured: FIRESTARTER Backdoor Survives Cisco Firewall Upgrades

Operation TrustTrap: APT36 Weaponizes 16,800 Spoofed Domains

VECT Ransomware: Flawed Encryption Turns RaaS Locker into Irreversible File Wiper

CVE-2026-42208: The LiteLLM Flaw Letting Attackers Reach Deep Inside

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
LINE VIPER	SHA256	bd82a15394f80c6eb82e439dcec93eb8535e9bbc9b26e991fef8bd92c5ba345f, e6684678ace298f81aedd140415c74553612bf86b904c11ca059424ef8322e7c, 8dab6e20cfa9ec1445eb32d3ec836e3c17b97cee622caa1b7e6b110b44df769a, 531b619e8b27cfad4628c9539f2707903d129411bd908a0d6f862e382d7ac5a4, 5bf3100c49718b7567acfc5d84606dc010b91e10cedd25aef13e27f0ffc0f997, 27ed8628441ddc88bba8aba5783665b096975d948db92cb8ffc7790ddfa68414, 3a9486da872af184ba250059311f1ee70f46f84b6d92dcdfa4f0396eb83ffb6a, 0bdb8efb72c6566be86963ffb2ec5a135362e18e5e8c6afd3e42b3a761b85428, 0297f9852a70b04cdf2aaf5d66611451d1bde918e8e59ebe8e573e5a0b449af0, 1a4a37df0a6b5ad02b7e91ccbc7c706079761a4e85bebaa09533c3017c9aff71
VECT Ransomware (VECT 2.0)	SHA256	a7eadcf81dd6fda0dd6affefaffcb33b1d8f64ddec6e5a1772d028ef2a7da0f2, 58e17dd61d4d55fa77c7f2dd28dd51875b0ce900c1e43b368b349e65f27d6fdd, e1fc59c7ece6e9a7fb262fc8529e3c4905503a1ca44630f9724b2ccc518d0c06, 8ee4ec425bc0d8db050d13bbff98f483fff020050d49f40c5055ca2b9f6b1c4d, 9c745f95a09b37bc0486bf0f92aad4a3d5548a939c086b93d6235d34648e683f, e512d22d2bd989f35ebaccb63615434870dc0642b0f60e6d4bda0bb89adee27a

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 04, 2026 • 8:30 AM

More at www.hivepro.com