Date of Publication
October 6, 2025

Hive Pro

Hiveforce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities and Actors

29 SEPTEMBER to 5 OCTOBER 2025

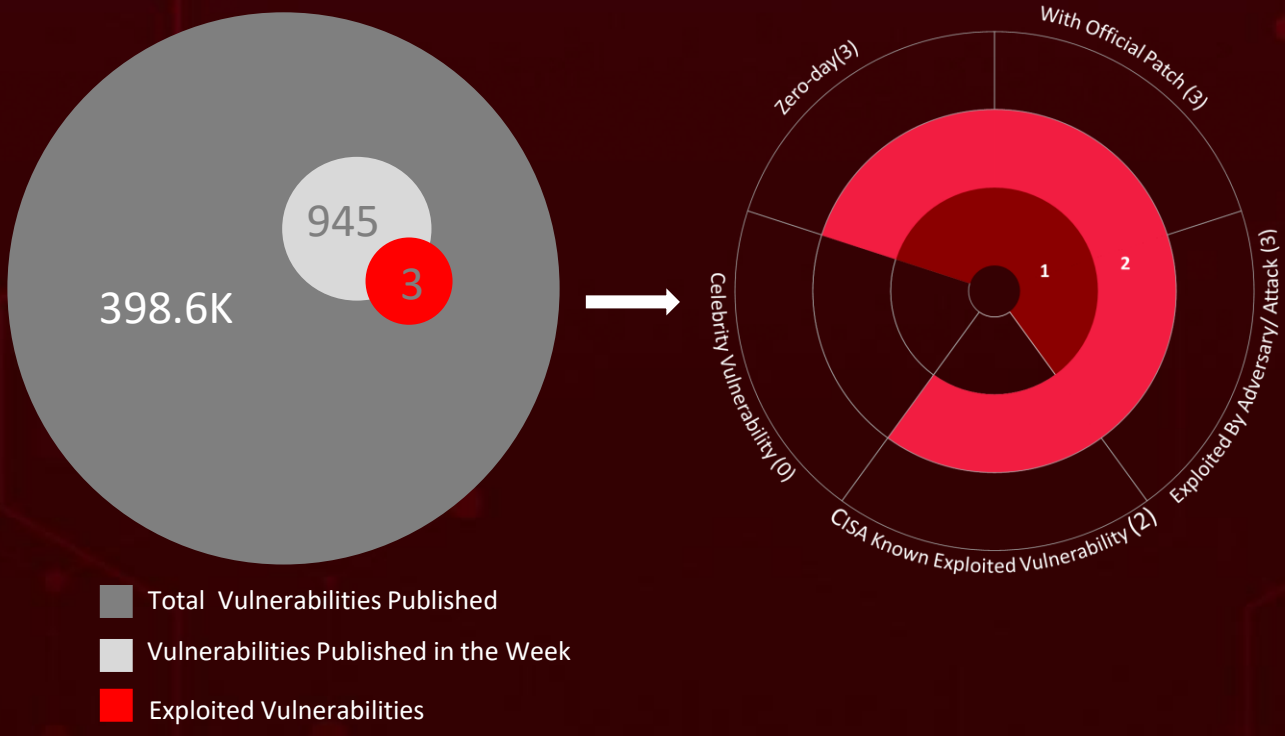
Table Of Contents

Summary

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

Broadcom issued urgent fixes for **VMware flaws**, including the zero-day CVE-2025-41244 exploited by UNC5174 for root escalation on guest VMs. Related bugs (CVE-2025-41245, CVE-2025-41246) enable lateral movement, making immediate patching and tighter vCenter access controls critical.

Additionally, **FunkLocker** is an AI-assisted ransomware from FunkSec that encrypts files with AES-256/RSA-2048, appends .funksec, and demands low ransoms to maximize victim payouts. Cisco ASA/FTD are under active attack via **CVE-2025-20333, CVE-2025-20362**, chained for unauthenticated remote root access, with UAT4356/Storm-1849 deploying persistent RayInitiator bootkit and LINE VIPER loader and tampering logs. These rising threats pose significant and immediate dangers to users worldwide.



High Level Statistics

5
Attacks Executed

3
Vulnerabilities Exploited

3
Adversaries in Action

- RayInitiator
- LINE VIPER
- DarkCloud
- Olymp Loader
- FunkLocker

- CVE-2025-20333
- CVE-2025-20362
- CVE-2025-41244

- UAT4356
- UNC5174
- FunkSec Group

Insights

A spear-phishing email deployed **DarkCloud** info-stealer to capture credentials and crypto wallets, using obfuscation and multi-channel exfiltration to evade detection.

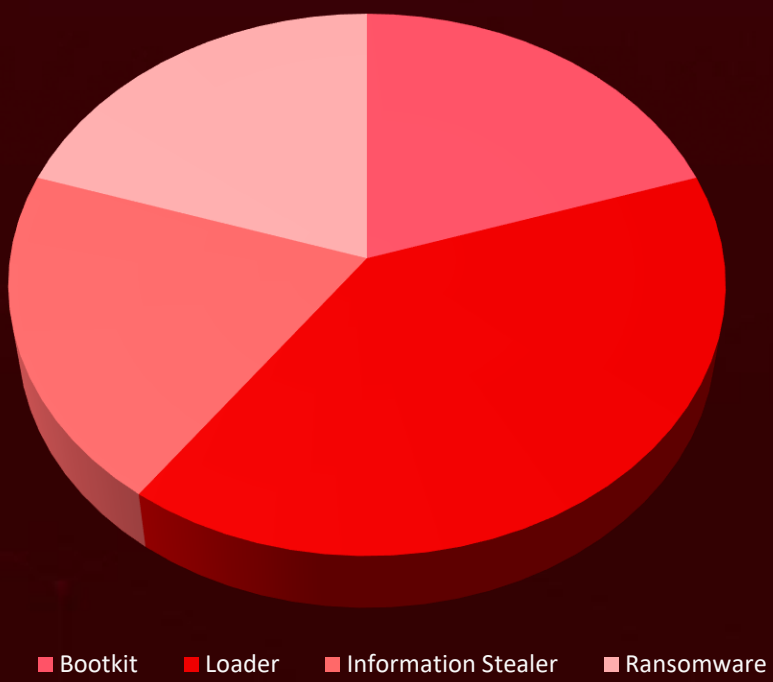
Vmware zero-day **CVE-2025-41244** exploited by **UNC5174** for root access and lateral movement.

Cisco ASA/FTD under active attack via CVE-2025-20333/20362, enabling remote root with persistent RayInitiator and LINE VIPER malware.

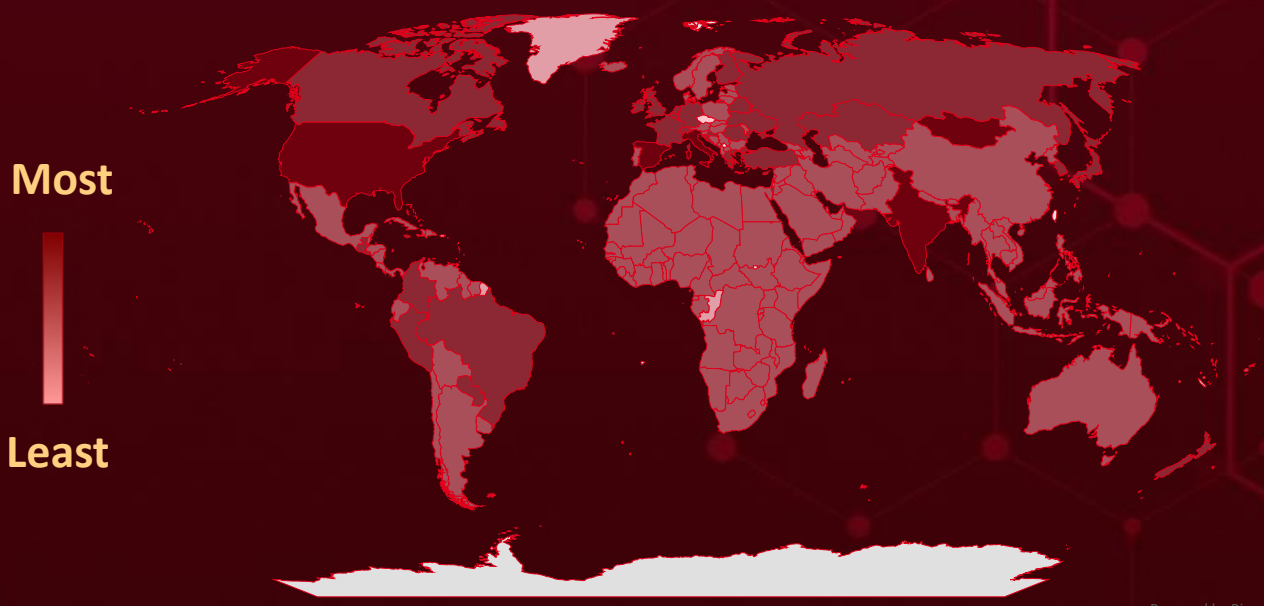
FunkLocker is an AI-powered ransomware from FunkSec that encrypts files with AES-256/RSA-2048, appends .funksec, and demands small ransoms to maximize victim reach.

Olymp Loader a FUD assembly-built loader/crypter seeded via poisoned developer channels that bundles stealers, updates via Telegram, and acts as a turnkey second-stage for RATs.

Threat Distribution



Targeted Countries



Countries	Countries	Countries	Countries
United States	Croatia	Qatar	Eritrea
India	New Zealand	Cuba	Canada
Spain	Cyprus	Slovenia	Estonia
Mongolia	Peru	Austria	Myanmar
Italy	El Salvador	Tanzania	Eswatini
Brazil	Russia	Czech Republic (Czechia)	Angola
Israel	Finland	Moldova	Ethiopia
Japan	South Korea	Denmark	Nigeria
Argentina	France	Nauru	Fiji
Singapore	Switzerland	Djibouti	Oman
Australia	Germany	North Macedonia	Belize
United Kingdom	Greece	Dominica	Papua New Guinea
Barbados	Ukraine	Cambodia	Benin
Mexico	St. Vincent & Grenadines	Dominican Republic	Poland
Belarus	Palau	Saint Kitts & Nevis	Gabon
Romania	Morocco	DR Congo	Albania
Belgium	Congo	Seychelles	Gambia
Netherlands	Sao Tome & Principe	Ecuador	Samoa
Turkey	Costa Rica	Chad	Georgia
Guatemala	Turkmenistan	Egypt	Senegal
Brunei	Côte d'Ivoire	Sweden	Bhutan
Jamaica	Nicaragua	Azerbaijan	Central African Republic
Colombia	Armenia	Tonga	Ghana
Kazakhstan		Equatorial Guinea	Somalia

Targeted Industries

TOP MITRE ATT&CK TTPs

T1059 Command and Scripting Interpreter

T1190 Exploit Public-Facing Application

T1068 Exploitation for Privilege Escalation

T1204 User Execution

T1203 Exploitation for Client Execution

T1566 Phishing

T1566.001 Spearphishing Attachment

T1036 Masquerading

T1588 Obtain Capabilities

T1027 Obfuscated Files or Information

T1204.001 Malicious Link

T1486 Data Encrypted for Impact

T1588.005 Exploits

T1133 External Remote Services

T1059.001 PowerShell

T1082 System Information Discovery

T1588.006 Vulnerabilities

T1105 Ingress Tool Transfer

T1041 Exfiltration Over C2 Channel

T1078 Valid Accounts

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
RayInitiator	RayInitiator is a stealthy bootkit that infects the device's firmware/ROM or ROMMON to insert itself into the boot chain, ensuring early execution before the OS and surviving reboots and many firmware upgrades; it decrypts and stages secondary payloads while evading simple integrity checks.	Firmware / ROM modification	CVE-2025-20333 CVE-2025-20362
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Bootkit		Persistent early-boot compromise	Cisco Secure Firewall Adaptive Security Appliance (ASA) and Secure Firewall Threat Defense (FTD)
ASSOCIATED ACTOR			**PATCH LINK**
UAT4356 (aka Storm-1849)			https://sec.cloudapps.cisco.com/security/center/resources/asa_ftd_continued_attacks

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Line Viper	Line Viper is a user-mode loader that performs in-memory/reflective loading of modules into trusted processes, using process injection, API hooking, and runtime obfuscation to fetch and run plugins for C2, credential harvesting, and lateral movement, together they provide a resilient, layered persistence and post-exploitation framework on compromised network appliances.	Reflective in-memory injection	CVE-2025-20333 CVE-2025-20362
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Loader		Credential theft & lateral movement	Microsoft SharePoint Server
ASSOCIATED ACTOR			**PATCH LINK**
UAT4356 (aka Storm-1849)			https://sec.cloudapps.cisco.com/security/center/resources/asa_ftd_continued_attacks

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
DarkCloud	DarkCloud is a comprehensive, multi-stage Information Stealer malware typically distributed via targeted spear-phishing emails with malicious attachments. Its primary function is to covertly pilfer a wide array of sensitive data, including stored browser credentials, banking details, cookies, and cryptocurrency wallets from a victim's Windows system. The stolen information is then exfiltrated to the attacker's command-and-control server.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Information Stealer		Data theft and exfiltration	Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			-

IOC TYPE	VALUE
SHA256	e013fb82188cb7ea231183197e12c189b4637e7d92e277793d607405e16da1e2, 6a3b4e62a8262a0bf527ad8ea27eb19a0fcb48a76d6fc2868785362e40491432

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>Olymp Loader</td><td rowspan="6">Olymp Loader is an emerging Malware-as-a-Service (MaaS), heavily advertised as "fully undetectable" (FUD) and notably written entirely in assembly language. It functions primarily as a versatile loader to stealthily deliver second-stage malware, such as credential stealers (e.g., LummaC2) and Remote Access Trojans.</td><td>-</td><td>-</td></tr>
<tr><td>TYPE</td><td>IMPACT</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>Loader</td><td rowspan="4">Data theft</td><td>Windows</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td>PATCH LINK</td></tr>
<tr><td>-</td><td>-</td></tr>
<tr><td></td><td></td></tr>
<tr><th>IOC TYPE</th><th colspan="3">VALUE</th></tr>
<tr><td>SHA256</td><td colspan="3">01562cd36b61d517959fdbe5beaef9e1e9462be292c74a49b36a30057d09bc2c, 60f8b5a6c8621e07124fbec4b9253b913056d1279d6c42fdd99a8b6b14c33e9a, 048701ffc9b7ccfe4228bfaaa0b98a0518f02c6325c7f59365f863eccb65aa6d, c465c1ac750e80ffb4020ec085528ca520b4fca587710ae1a5937bc88e5ad22c, dbe4aaef628f4d392fd25946643424334af4ecb9eb2589884112b465f508ca33, 02eb774341d84b8c83b448186f3de8db139c52bea2376fec0ac88c7112186fd2, ee1e27a01b884099a614b8eee78cdb1dd02ffecd6ed9f6a54b7b567b9eab979f</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>FunkLocker</td><td rowspan="6">FunkLocker is an AI-assisted ransomware strain developed by the FunkSec group, which operates under a ransomware-as-a-service model. The group blends cybercrime and hacktivism, targeting a wide range of public and private sector organizations worldwide. Ransom demands are relatively low typically around 0.1 Bitcoin, encouraging faster payments and increasing the number of victims.</td><td>Phishing</td><td>-</td></tr>
<tr><td>TYPE</td><td>IMPACT</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>Ransomware</td><td rowspan="3">Data encryption, Data Exfiltration</td><td>Windows</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td>PATCH LINK</td></tr>
<tr><td>FunkSec Group</td><td>-</td></tr>
<tr><td>IOC TYPE</td><td colspan="3">VALUE</td></tr>
<tr><td>SHA256</td><td colspan="3">c233aec7917cf34294c19dd60ff79a6e0fac5ed6f0cb57af98013c08201a7a1c, e29d95bfb815be80075f0f8bef4fa690abcc461e31a7b3b73106bfcd5cd79033</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-2025-20333		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	UAT4356 (aka Storm-1849)
	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:*:*:*:*:*:*:*:*:*	RayInitiator bootkit, Line Viper loader
Cisco Secure Firewall Adaptive Security Appliance (ASA) and Secure Firewall Threat Defense (FTD) Buffer Overflow Vulnerability			
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-120	T1071.001: Web Protocols, T1071: Application Layer Protocol, T1068: Exploitation for Privilege Escalationn	https://sec.cloudapps.cisco.com/security/center/resources/asa_ftd_continued_attacks

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
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	UAT4356 (aka Storm-1849)
	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:*:*:*:*:*:*:*:*:*	RayInitiator bootkit, Line Viper loader
Cisco Secure Firewall Adaptive Security (ASA) Appliance and Secure Firewall Threat Defense (FTD) Missing Authorization Vulnerability			
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-862	T1068: Exploitation for Privilege Escalation, T1078: Valid Accounts	https://sec.cloudapps.cisco.com/security/center/resources/asa_ftd_continued_attacks

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2025-41244</td><td>  </td><td rowspan="2">VMware Cloud Foundation and VMware vSphere Foundation: VMware Cloud Foundation Operations Version Prior to 9.0.1.0,
VMware Cloud Foundation and VMware vSphere Foundation: VMware Tools Version Prior to 3.0.5.0, Prior to 13.0.5, Prior to
12.5.4,
VMware Cloud Foundation: VMware Aria Operations Version
5.x, 4.x,
VMware Aria Operations Version
Prior to 8.18.5</td><td rowspan="2">UNC5174 (aka Uteus)</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:vmware:vmware_cloud_foundation_operations:*:*:*:*:*:*:*:*
cpe:2.3:a:vmware:vmware_tools:*:*:*:*:*:*:*:*
cpe:2.3:a:vmware:vmware_aria_operations:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td>VMware Aria Operations and VMware Tools Privilege Escalation Vulnerability</td><td>  </td></tr>
<tr><td></td><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td></td><td>CWE-267</td><td>T1068: Exploitation for Privilege Escalation, T1036.005 Masquerading: Match Legitimate Resource Name or Location</td><td>https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/36149</td></tr>
</table>

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGION
 UAT4356 (aka Storm-1849)	China	Government, Critical Infrastructure, Telecommunication, Energy	Worldwide
	MOTIVE		
	Espionage		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOM WARE**	**AFFECTED PRODUCT**
	CVE-2025-20333 CVE-2025-20362	RayInitiator bootkit, Line Viper loader	Cisco ASA and FTD

TTPs
TA0001: Initial Access; TA0005: Defense Evasion; T1190: Exploit Public-Facing Application; T1543: Create or Modify System Process; T1068; TA0002: Execution; TA0040: Impact; T1078: Valid Accounts; T1562; TA0003: Persistence; TA0004: Privilege Escalation; TA0042: Resource Development; T1529: System Shutdown/Reboot; T1542.001: System Firmware; T1070: Impair Defenses; T1068: Exploitation for Privilege Escalation; T1059: Command and Scripting Interpreter; T1588.006: Vulnerabilities; T1588.005: Exploits; T1542: Pre-OS Boot; T1542.003: Bootkit; T1588: Obtain Capabilities

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGION</th></tr>
<tr><td rowspan="4"> 
UNC5174 (aka Uteus)</td><td>China</td><td rowspan="3">Government, defense, research institutes, critical infrastructure (energy, healthcare), non-governmental organizations, technology companies, charities</td><td rowspan="3">United States, Canada, United Kingdom, and Southeast Asia</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Espionage</td></tr>
<tr><td>TARGETED CVE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>CVE-2025-41244</td><td>-</td><td>VMware Aria Operations, VMware Tools, VMware Cloud Foundation, VMware Telco Cloud Platform, VMware Telco Cloud Infrastructure</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0042: Resource Development; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; T1588: Obtain Capabilities; T1588.006: Vulnerabilities; T1036: Masquerading; T1036.005: Match Legitimate Resource Name or Location; T1068: Exploitation for Privilege Escalation; T1552: Unsecured Credentials</td></tr>
</table>

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGION
 FunkSec Group	- **MOTIVE** Financial gain	Government, Defense, Finance, Higher Education	United States, India, Spain, Mongolia, Italy, Brazil, Israel
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOM WARE**	**AFFECTED PRODUCT**
	CVE-2025-20333 CVE-2025-20362	RayInitiator bootkit, Line Viper loader	Cisco ASA and FTD
TTPs			
TA0001: Initial Access; TA0005: Defense Evasion; T1190: Exploit Public-Facing Application; T1543: Create or Modify System Process; T1068; TA0002: Execution; TA0040: Impact; T1078: Valid Accounts; T1562; TA0003: Persistence; TA0004: Privilege Escalation; TA0042: Resource Development; T1036.005: Match Legitimate Name or Location; T1036: Masquerading; T1569: System Services; T1569.002: Service Execution; T1529: System Shutdown/Reboot; T1542.001: System Firmware; T1070: Impair Defenses; T1588.006: Exploitation for Privilege Escalation; T1059: Command and Scripting Interpreter; T1486 : Data Encrypted for Impact; T1588: Obtain Capabilities			

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 actor **UAT4356, UNC5174, FunkSec Group** and malware **RayInitiator, LINE VIPER, DarkCloud, Olymp Loader, FunkLocker.**

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 **three exploited vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actors **UAT4356, UNC5174, FunkSec Group** and malware **DarkCloud, Olymp Loader, FunkLocker,** in Breach and Attack Simulation(BAS).

Threat Advisories

Active Zero-Day Exploitation on Cisco ASA and FTD Devices

DarkCloud Rising: Spear-Phishing Campaign Targets Manufacturing Sector

VMware Aria and Tools Vulnerabilities Fixed Amid Ongoing Exploitation

Olymp Loader: Modular Malware Built for Rapid Exploitation

FunkLocker: Emerging AI-Assisted Ransomware

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
DarkCloud	SHA256	e013fb82188cb7ea231183197e12c189b4637e7d92e277793d607405e16da1e2, 6a3b4e62a8262a0bf527ad8ea27eb19a0fcb48a76d6fc2868785362e40491432
Olymp Loader	SHA256	7bc217f0ee12266d42812af436f494caf599c0705242457a581f64d4eb508904, d36da9c3e5e78aa87bcdcd7fc8d3499d85a60b9dd107bf775d759940fc2f2489, D167a0c6fdba1175b67f10daf4be218b4d8adf2f81280ba5d1510228a4321bca, 446c7b9ff49c7c0b8ae02b720054e4f09ef60475c92a5d7f2e2b2bdb4ca5de23, ff1e159c4c6fcb97c9cb1885796fa4557e1afb92c82ada00f24ae994bffd63e4, 9464a2a1fb53b3a8c783ee4b55bba69cbb74a841f0d06f0cef86a93d607be5ae, 59b143fd884f8450cf5161954ebf38dbd9c951ecdb13de5e1f6aea01a9f92201, 60fec45a29a89c1cb10fd793065e8fc39bdae15daf813e3438e8ff6558fb7e2d, 561809b0c9c67b7d48712ab9e53cf5cc137b94d5a2d8bc65314a2db4c23df99d, 9d5d474791793300a273c5b6e522c7c3acd6fbb26c4da0421d4ef695c82f3fa5, 446c7b9ff49c7c0b8ae02b720054e4f09ef60475c92a5d7f2e2b2bdb4ca5de23,

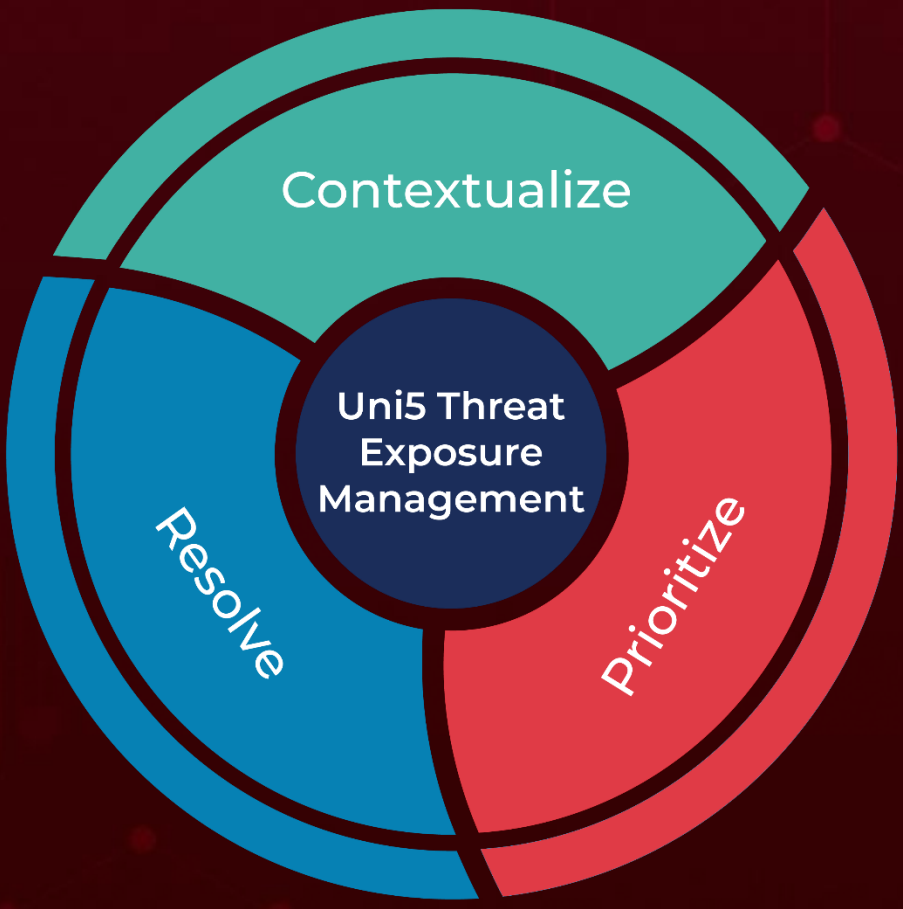
Attack Name	TYPE	VALUE
Olymp Loader	SHA256	14e4884288c1740d5a4b67ac83a890000c3b92f945139b2433bf9746acd14f9b, 01562cd36b61d517959fdbe5beaef9e1e9462be292c74a49b36a30057d09bc2c, 60f8b5a6c8621e07124fbec4b9253b913056d1279d6c42fdd99a8b6b14c33e9a, 048701ffc9b7ccfe4228bfaaa0b98a0518f02c6325c7f59365f863eccb65aa6d, c465c1ac750e80ffb4020ec085528ca520b4fca587710ae1a5937bc88e5ad22c, dbe4aaef628f4d392fd25946643424334af4ecb9eb2589884112b465f508ca33, 02eb774341d84b8c83b448186f3de8db139c52bea2376fec0ac88c7112186fd2, Ee1e27a01b884099a614b8eee78cdb1dd02ffecd6ed9f6a54b7b567b9eab979f
FunkLocker	SHA256	c233aec7917cf34294c19dd60ff79a6e0fac5ed6f0cb57af98013c08201a7a1c, e29d95bfb815be80075f0f8bef4fa690abcc461e31a7b3b73106bfcd5cd79033

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 free demo with **HivePro Uni5**:Threat Exposure Management Platform.



REPORT GENERATED ON

October 6, 2025 . 11:30 AM

More at www.hivepro.com