Date of Publication
December 2, 2025

Hive Pro

HiveForce Labs

WEEKLY
THREAT DIGEST

Attacks, Vulnerabilities and Actors

24 to 30 NOVEMBER 2025

Table Of Contents

Summary 03

High Level Statistics 04

Insights 05

Targeted Countries 06

Targeted Industries 07

Top MITRE ATT&CK TTPs 07

Attacks Executed 08

Vulnerabilities Exploited 12

Adversaries in Action 15

Recommendations 16

Threat Advisories 17

Appendix 18

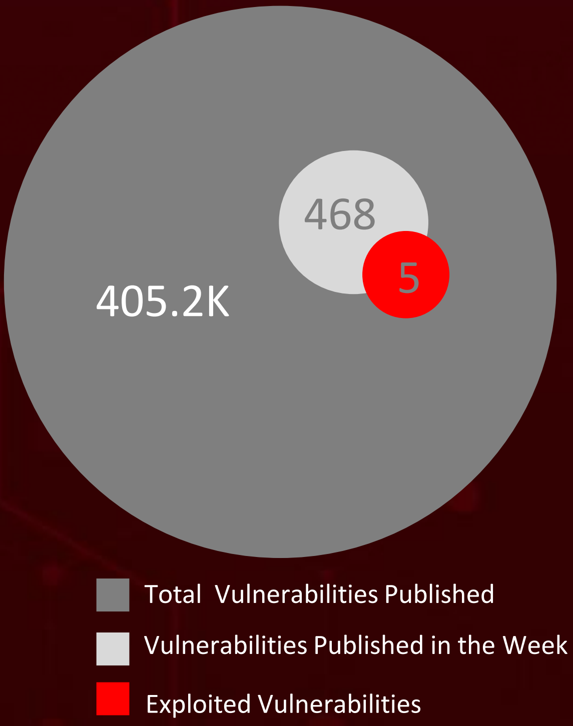
What Next? 22

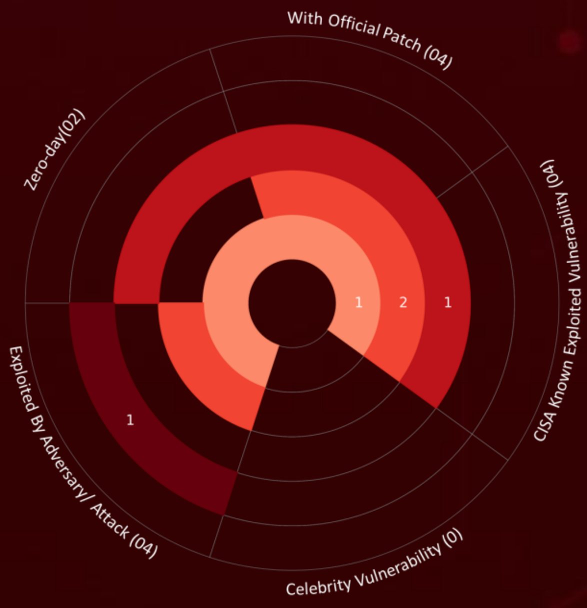
Summary

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

Cl0p ransomware has evolved into 2025’s most aggressive extortion force, weaponizing zero-days for rapid, automated data theft at massive scale, forcing defenders to prioritize fast patching, tight segmentation, and rigorous exfiltration monitoring. **ShadowRay 2.0** exposes how rapidly cybercriminals are weaponizing AI-era infrastructure, turning misconfigured Ray clusters into stealthy, self-spreading engines for cryptomining, data theft, and botnet expansion, underscoring the urgency of hardening access and visibility across modern AI stacks.

Additionally, **ClickFix** turns a single misguided “update” click into a stealthy, steganography-driven infection chain, proving that even advanced attacks still rely on basic user trust to succeed. **Shai-Hulud 2.0** weaponizes npm’s supply chain at scale, using poisoned preinstall scripts and stolen tokens to self-propagate, turning routine package installs into a destructive breach that demands urgent secret rotation and dependency audits. These rising threats pose significant and immediate dangers to users worldwide.





High Level Statistics

8
Attacks Executed

5
Vulnerabilities Exploited

1
Adversaries in Action

- XMRig
- Cl0p ransomware
- LummaC2
- Rhadamanthys
- Stego Loader
- StealC V2
- Sha1-Hulud 2.0
- ShadowPad

- CVE-2023-48022
- CVE-2025-61882
- CVE-2025-61884
- CVE-2025-59287
- CVE-2025-61757

- TA505

Insights

ShadowRay 2.0 reveals how fast attackers can weaponize AI infrastructure, turning exposed Ray clusters into stealthy engines for cryptomining, data theft, and botnet spread.

Cl0p has become 2025's dominant extortion threat, weaponizing zero-days for lightning-fast data theft at massive scale, underscoring the need for rapid patching and tighter zero-trust defenses.

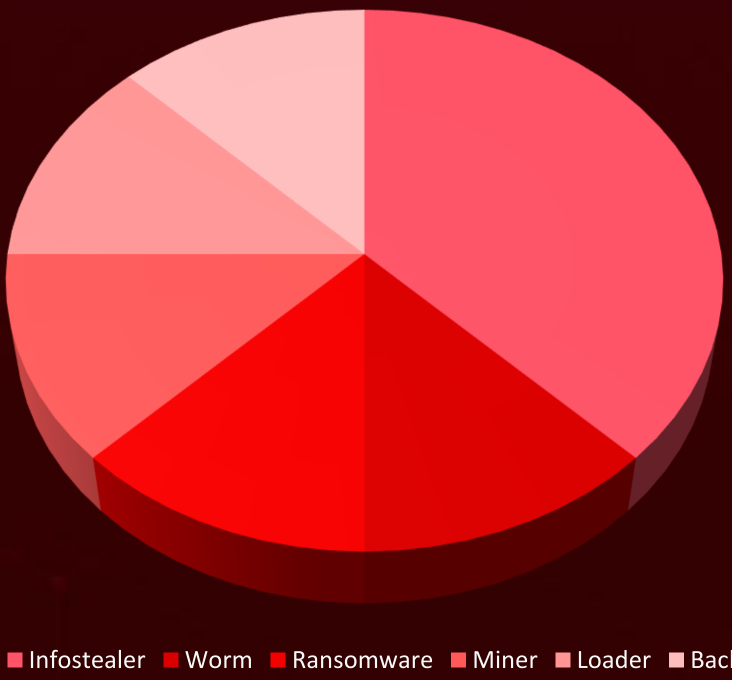
Attackers are weaponizing Blender assets to silently deliver **StealC V2**, turning creative 3D workflows into an unexpected entry point for high-impact data theft.

Shai-Hulud 2.0 turns the npm ecosystem into a propagation engine, stealing tokens, auto-reinfecting packages, and even deploying a destructive wipe fail-safe.

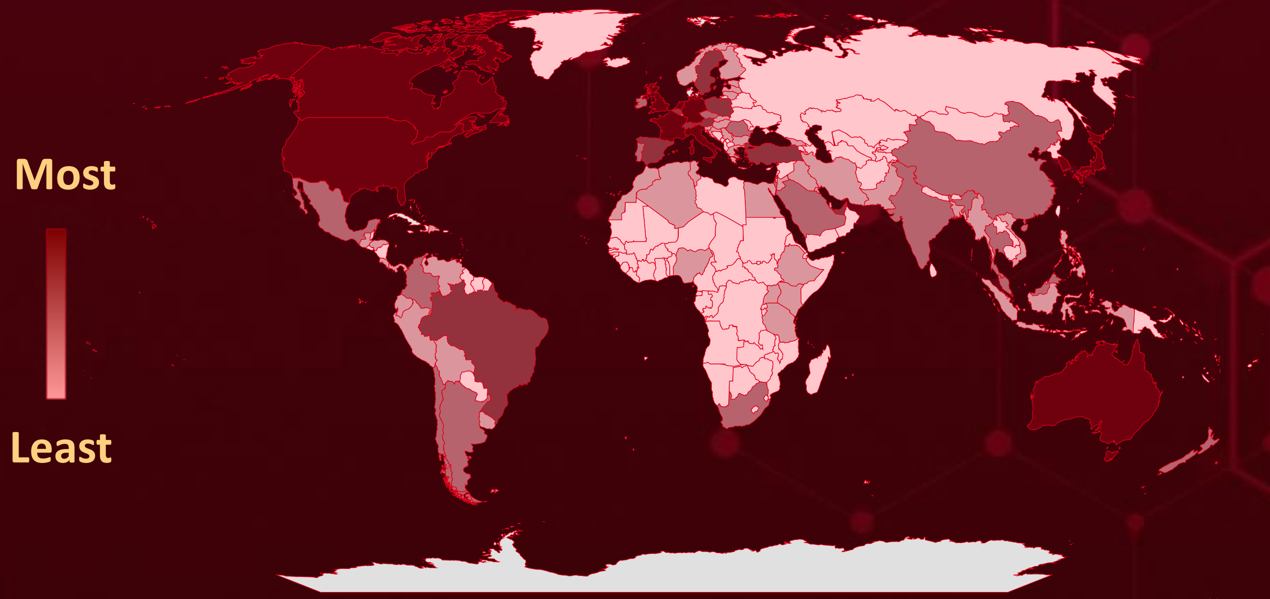
The rapid weaponization of **CVE-2025-59287** shows how quickly attackers can turn a WSUS flaw into a **ShadowPad** foothold, pairing a critical vuln with one of the most persistent state-aligned backdoors.

CVE-2025-61757 shows how a simple URI trick can bypass Oracle Identity Manager's authentication entirely, enabling RCE and exposing organizations to full compromise months before a patch arrived.

Threat Distribution



Targeted Countries



Powered by Bing

© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, Overture Maps Fundation, TomTom, Zenrin

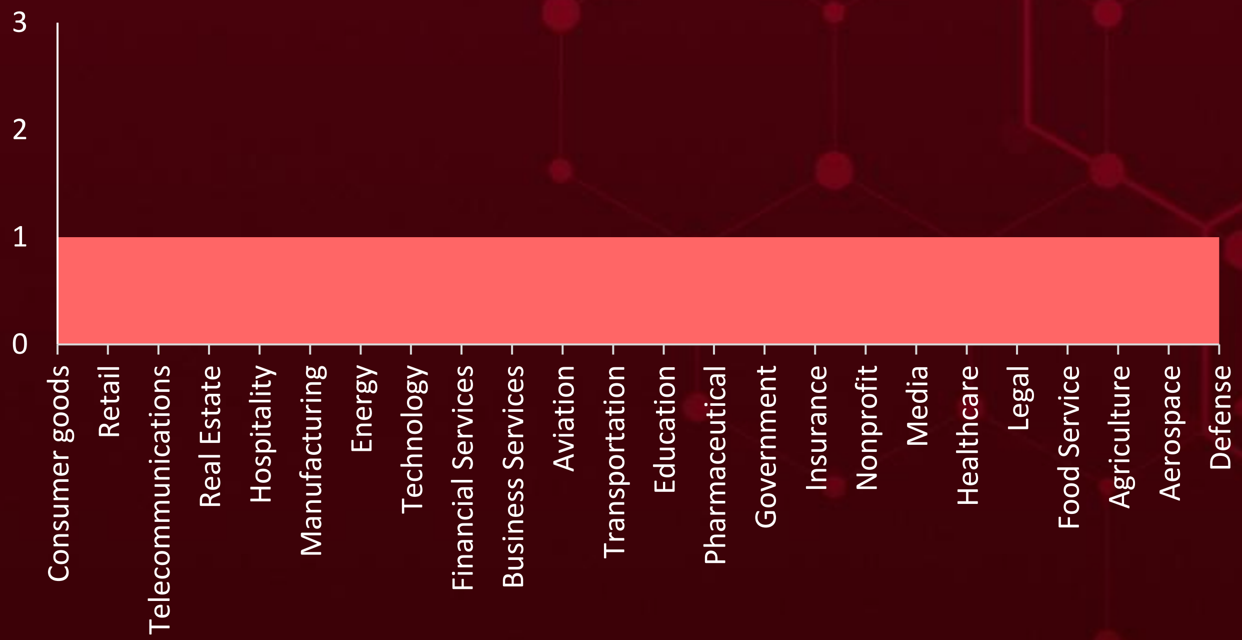
Countries
United States
United Kingdom
Germany
France
Italy
Canada
Australia
Japan
South Korea
Netherlands
Brazil
Spain
Poland
Belgium
Sweden
Switzerland
Austria
Singapore
United Arab Emirates
Turkey
India
China
Mexico

Countries
South Africa
Argentina
Chile
Colombia
Malaysia
Thailand
Israel
Ireland
Portugal
Czech Republic
Romania
New Zealand
Saudi Arabia
Indonesia
Pakistan
Nigeria
Bangladesh
Ethiopia
Philippines
Vietnam
Egypt
Iraq
Peru

Countries
Morocco
Kenya
Myanmar
Tanzania
Uganda
Algeria
Venezuela
Bolivia
Tunisia
Ecuador
Guatemala
Dominican Republic
Jordan
Honduras
Panama
Croatia
Georgia
Uruguay
Costa Rica
Kuwait
Qatar
Bulgaria
Serbia
Greece

Countries
Hungary
Finland
Norway
Slovakia
Slovenia
Lithuania
Latvia
Estonia
DR Congo
Afghanistan
Yemen
Angola
Mozambique
Ghana
Madagascar
Côte d'Ivoire
Cameroon
Nepal
Niger
North Korea
Syria
Mali
Burkina Faso
Sri Lanka
Malawi

Targeted Industries



TOP MITRE ATT&CK TTPs

T1059
Command and Scripting Interpreter

T1190
Exploit Public-Facing Application

T1068
Exploitation for Privilege Escalation

T1566
Phishing

T1204
User Execution

T1203
Exploitation for Client Execution

T1059.001
PowerShell

T1195
Supply Chain Compromise

T1082
System Information Discovery

T1027
Obfuscated Files or Information

T1588
Obtain Capabilities

T1562
Impair Defenses

T1078
Valid Accounts

T1133
External Remote Services

T1566.001
Spearphishing Attachment

T1588.006
Vulnerabilities

T1204.001
Malicious Link

T1105
Ingress Tool Transfer

T1041
Exfiltration Over C2 Channel

T1036
Masquerading

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
XMRig	XMRig is a legitimate open-source cryptocurrency miner often embedded into malware.Threat actors deploy it to hijack system CPU/GPU resources for unauthorized mining.It typically runs silently to avoid user detection and maximize profit.	Phishing	CVE-2023-48022
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Miner		Resource hijacking, system slowdown	Anyscale Ray
ASSOCIATED ACTOR			**PATCH LINK**
-			☒

IOC TYPE	VALUE
SHA256	6f445252494a0908ab51d526e09134cebc33a199384771acd58c4a87f1ffc063

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Cl0p	Cl0p is a prominent ransomware strain used in large-scale data extortion attacks. It encrypts systems and steals data for double-extortion operations. The group often exploits vulnerabilities to infiltrate enterprise networks.	Exploiting vulnerabilities	CVE-2025-61882 CVE-2025-61884
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Data encryption, data theft, extortion, operational disruption	Oracle E-Business Suite
ASSOCIATED ACTOR			**PATCH LINK**
TA505			✓

IOC TYPE	VALUE
SHA256	76b6d36e04e367a2334c445b51e1ecce97e4c614e88dfb4f72b104ca0f31235d, aa0d3859d6633b62bccfb69017d33a8979a3be1f3f0a5a4bf6960d6c73d41121, 6fd538e4a8e3493dda6f9fcdc96e814bdd14f3e2ef8aa46f0143bff34b882c1b, 10f0a21b688a30d4f3f827edca45316c3b1bd2b86edd58f0f3629d7b58ebd37b, ebf9282f9535f2094765735 89a7026a52285cb366d075591618895896187ad03

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 CVEs</th></tr>
<tr><td>LummaC2</td><td rowspan="5">LummaC2 is a rapidly evolving information-stealer sold as Malware-as-a-Service.It targets browser data, cryptocurrency wallets, and authentication tokens.It communicates with a C2 panel for exfiltration and victim tracking.</td><td>Cracked software, phishing</td><td>-</td></tr>
<tr><td><b>TYPE</b></td><td><b>IMPACT</b></td><td><b>AFFECTED PRODUCTS</b></td></tr>
<tr><td>Infostealer</td><td rowspan="3">Credential theft</td><td>-</td></tr>
<tr><td><b>ASSOCIATED ACTOR</b></td><td><b>PATCH LINK</b></td></tr>
<tr><td>-</td><td>-</td></tr>
<tr><td><b>IOC TYPE</b></td><td colspan="3"><b>VALUE</b></td></tr>
<tr><td>SHA256</td><td colspan="3">91a294d07f52493df4a8f8ad3de0500d23c11cce2c927a6ef478b8de2912258e,
f54959731594f2cda943820c67a276668577679eb2f3e22d835e4df2b55feca1,
b732a9865a227ad9bf76a2d0c3b7459f3cac838741bbe00e133b583ebf644391,
a57026e831135c49e6867d177c367608584e3653c57e2fe28859af0674369f07,
2dca3205e60ebe5d748309db91e2debc240beb15eef80667165d06b080563866</td></tr>
</table>

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVE</th></tr>
<tr><td>Rhadamanthys</td><td rowspan="5">Rhadamanthys is an advanced infostealer distributed via multi-stage loaders.It collects credentials, system data, financial information, and browser data.It uses obfuscation and underground updates to bypass defenses.</td><td>Malvertising, phishing</td><td>-</td></tr>
<tr><td><b>TYPE</b></td><td><b>IMPACT</b></td><td><b>AFFECTED PRODUCT</b></td></tr>
<tr><td>Infostealer</td><td rowspan="3">Credential theft</td><td>-</td></tr>
<tr><td><b>ASSOCIATED ACTOR</b></td><td><b>PATCH LINK</b></td></tr>
<tr><td>-</td><td>-</td></tr>
<tr><td><b>IOC TYPE</b></td><td colspan="3"><b>VALUE</b></td></tr>
<tr><td>SHA256</td><td colspan="3">9e7f2e72d5812dcd3f965039efbd9d47170a99b9a03cd72970650bed8d8402d7,
067171ca88daa1c9816c657e21464421225630a7d2f6ae5d05d82a11ae3e16fa,
e5f99a53b6f99bf112db4bf4a513cee89f8b424ade4e7198a14755124cb8af5c,
60b156ea82325d3caf7fa04ef4346b6ee1019b030bd2bfc3654c99b69229edd3,
4eaf0c8a00e69948c2a66fd954389eb7e294d631f4ee179987429fb409d64070</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 CVEs
Stego Loader	Stego Loader is a stealthy loader known for hiding malicious code inside images.It extracts embedded payloads via steganography to evade detection.Once executed, it deploys secondary malware onto the victim system.	Steganographic images, phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Loader		Malware delivery, stealthy payload execution	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

IOC TYPE	VALUE
SHA256	8c2e9aa5e926e55dbb33b7c07997a81d5a297b5e2c1c0fa18bf496445602210f, 5fd746de2643a000d36f0aeff42ceed4c35068c0c4a6bdb6c58966e91e9c4fab, 6a11145b4ccd6c05c2ee4fbb32a6468272863e22a8376ee85d10c558d3f09207

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
StealC V2	StealC V2 is an updated information-stealer with improved evasion and data theft.It targets browsers, crypto wallets, messaging apps, and system information.The malware communicates with a C2 server for automated exfiltration.	phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCT**
Infostealer		Credential theft	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

IOC TYPE	VALUE
SHA256	FC16AB400800B3D6A05B6FB3884D5BA52ED097B8F50A2BEAB25442961B8FB8D0 , AD278E48574CB10FE84B9B46C8B7BEF4F71C25B29F3EDAC93829B675B736BD69

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
Sha1-Hulud 2.0	Shai-Hulud 2.0 is a self-replicating worm targeting the npm ecosystem.It harvests cloud tokens, API keys, repository credentials, and CI/CD secrets.It propagates automatically by republishing altered npm packages using stolen credentials.	Trojanized npm packages with malicious preinstall scripts	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Worm		Credential theft, supply-chain compromise, CI/CD pipeline exposure	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
SHA256	62ee164b9b306250c1172583f138c9614139264f889fa99614903c12755468d0, e0250076c1d2ac38777ea8f542431daf61fcbaab0ca9c196614b28065ef5b918, cbb9bc5a8496243e02f3cc080efbe3e4a1430ba0671f2e43a202bf45b05479cd, f1df4896244500671eb4aa63ebb48ea11cee196fafaa0e9874e17b24ac053c02, f099c5d9ec417d4445a0328ac0ada9cde79fc37410914103ae9c609cbc0ee068		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
ShadowPad	ShadowPad is a modular backdoor platform used in advanced espionage operations. It offers plugin-based capabilities for persistence, lateral movement, and C2.Often attributed to state-aligned actors, it is used in long-term intrusions.	Exploiting vulnerabilities	CVE-2025-59287
TYPE		**IMPACT**	**AFFECTED PRODUCT**
Backdoor		Long-term remote access, data exfiltration	Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-59287
IOC TYPE	**VALUE**		
SHA256	d429934b06de67c156dc559b33c34db5e02bc56ac2c1cd45ee03e6a21cf003af		

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-2023-48022	⊗	Anyscale Ray 2.6.3 and 2.8.0	-
	ZERO-DAY		
	⊗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:anyscale:ray:2.6.3:*:*:*:*:*:*:*	XMRig
Anyscale Ray Remote Code Execution Vulnerability	⊗		
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-918	T1190 : Exploit Public-Facing Application, T1203 : Exploitation for Client Execution, T1068: Exploitation for Privilege Escalation	⊗

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2025-61882	✗	Oracle E-Business Suite versions 12.2.3-12.2.14	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:oracle:concurrent_processing:*:*:*:*:*:*:*:*	Cl0p Ransomware
Oracle E-Business Suite Unspecified Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-22 CWE-444	T1203: Exploitation for Client Execution, T1059: Command and Scripting Interpreter	https://www.oracle.com/security-alerts/alert-cve-2025-61882.html, https://www.oracle.com/security-alerts/, https://support.oracle.com/rs?type=doc&id=3106344.1

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2025-61884	✗	Oracle E-Business Suite versions 12.2.3-12.2.14	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:oracle:concurrent_processing:*:*:*:*:*:*:*:*	Cl0p Ransomware
Oracle E-Business Suite Server-Side Request Forgery (SSRF) Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-444, CWE-501, CWE-287, CWE-22, CWE-918, CWE-93	T1190 - Exploit Public-Facing Application, T1555 - Credentials from Password Stores	https://www.oracle.com/security-alerts/alert-cve-2025-61884.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-59287	✗	Windows Server 2012, 2016, 2019, 2022, 2025	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	ShadowPad
Microsoft Windows Server Update Service (WSUS) Deserialization of Untrusted Data Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502	T1059: Command and Scripting Interpreter, T1190: Exploit Public-Facing Application	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-59287

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-61757	✗	Oracle Identity Manager Versions 12.2.1.4.0 and 14.1.2.1.0	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:oracle:identity_manager:*:*:*:*:*:*:*:*	-
Oracle Fusion Middleware Missing Authentication for Critical Function Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-306	T1068: Exploitation for Privilege Escalation, T1059: Command and Scripting Interpreter, T1552 : Unsecured Credentials	https://www.oracle.com/security-alerts/cpuoct2025.html

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
TA505 (Graceful Spider, Lace Tempest , Spandex Tempest, DEV-0950, FIN11, Evil Corp, GOLD TAHOE, GOLD EVERGREEN, Chimborazo, Hive0065, ATK103, TEMP.Warlock)	Russia	Consumer goods and services, Retail, Telecommunications, Real Estate, Hospitality, Manufacturing, Energy, Technology, Financial Services, Business Services & Consulting, Aviation, Transportation, Education, Pharmaceutical, Government, Insurance, Charitable Organizations, Media, Associations, Healthcare, Legal, Food Service, Agriculture, Aerospace and Defense	Worldwide
	MOTIVE		
	Financial crime, Financial gain		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCT**
	CVE-2025-61882 CVE-2025-61884	Cl0p ransomware	Oracle EBS, Cleo Harmony, other enterprise file transfer/ERP solutions
TTPs			
TA0003: Persistence; TA0007: Discovery; TA0002: Execution; T1190: Exploit Public-Facing Application; T1105: Ingress Tool Transfer; T1203: Exploitation for Client Execution; T1210: Exploitation of Remote Services; T1218: System Binary Proxy Execution; TA0005: Defense Evasion; TA0004: Privilege Escalation; TA0010: Exfiltration; T1059: Command and Scripting Interpreter; T1505.003: Web Shell; T1588.006; TA0001: Initial Access; TA0011: Command and Control; T1588: Obtain Capabilities; T1071; TA0040: Impact; TA0009: Collection; T1562: Impair Defenses; T1071.001: Application Layer Protocol; T1505: Server Software Component; T1588.005: Vulnerabilities; T1041: Exfiltration Over C2 Channel; T1005: Data from Local System: Exploits; T1486: Data Encrypted for Impact; T1083: File and Directory Discovery: Web Protocols; T1068: Exploitation for Privilege Escalation; T1078: Valid Accounts; T1027: Obfuscated Files or Information; T1490: Inhibit System Recovery			

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 **TA505** and malware **XMRig, Cl0p ransomware, LummaC2, Rhadamanthys, Stego Loader, StealC V2, Sha1-Hulud 2.0, ShadowPad.**

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 threat actor **TA505** and malware **XMRig, Cl0p ransomware, Sha1-Hulud 2.0, ShadowPad** in Breach and Attack Simulation(BAS).

Threat Advisories

November 2025 Linux Patch Roundup

ShadowRay Strikes Back: Inside the Multi-Purpose Ray Cluster Takeover Threat Level: Red

Cl0p Ransomware Surge 2025: Operational Patterns and Key Mitigations

The Windows Update Deception: How ClickFix Lures Unleash Stealthy Stealers

StealC V2 Spreads via Malicious Blender Files

Shai-Hulud 2.0 Fuels Global NPM Supply-Chain Compromise

ShadowPad Gatecrashes the Enterprise by Hijacking WSUS Vulnerability

CVE-2025-61757: Oracle Identity Manager Pre-Auth RCE Under Active Attack

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
XMRig	IPv4	18[.]230[.]118[.]147
	URL	hxxps[:]//github[.]com/xmrig/xmrig/releases/download/v6.16.4/xmrig-6.16.4-linux-static-x64[.]tar[.]gz
	SHA256	6f445252494a0908ab51d526e09134cebc33a199384771acd58c4a87f1ffc063
Cl0p ransomware	SHA256	76b6d36e04e367a2334c445b51e1ecce97e4c614e88dfb4f72b104ca0f31235d, aa0d3859d6633b62bccfb69017d33a8979a3be1f3f0a5a4bf6960d6c73d41121, 6fd538e4a8e3493dda6f9fcdc96e814bdd14f3e2ef8aa46f0143bff34b882c1b, 10f0a21b688a30d4f3f827edca45316c3b1bd2b86edd58f0f3629d7b58ebd37b, ebf9282f9535f209476573589a7026a52285cb366d075591618895896187ad03, 3b7b604a5ee94a6ac25db7703e0479680a682f634346bf21545cdbd50f2fd968, 155697cb84bd5c5f44f8f0f76a3488f9f87dcfc6fd8413ede27aed2c07d00585, 9dd79b92be7d5908e55aaddeb9273274bfd2beffc6e60ed14beb451465a0d5b9, 4b6d5a907ce85779880018e5b8060105001275 3d0b4b3182963614887fe3ca0d,

Attack Name	TYPE	VALUE
Cl0p ransomware	SHA256	987b083305afb0cc223246c6053b3b755a30537da9df54ff41fed1935d22cc16, 30d53349fa2a642ee1717dd70b4951247136cfce3fc1995d51646814a017fbe, e2fef8904d4e51e3ad5b8186b62be06e1fc58d43583c8c72778f3dab482249af, 177053d18a425d2ea075502e6f75bfe00dc9d15ee85c89128f3ea17c0cbd3a6, 658e273a62c76fa2a9ad95d4d2d48fead83777040feacc851721e70e741a9458
LummaC2	SHA256	91a294d07f52493df4a8f8ad3de0500d23c11cce2c927a6ef478b8de2912258e, f54959731594f2cda943820c67a276668577679eb2f3e22d835e4df2b55feca1, b732a9865a227ad9bf76a2d0c3b7459f3cac838741bbe00e133b583ebf644391, a57026e831135c49e6867d177c367608584e3653c57e2fe28859af0674369f07, 2dca3205e60ebe5d748309db91e2debc240beb15eef80667165d06b080563866, 3068bbe62e5dbba9631d54af3d687fd67caf43b433f3304972366e3633657eb2, 08943eeb93052c706ec4331827e48bd8405c7ec6d980604dd52272e6efcf258b, f3e4c368a31ea5872f85e7e94e4fc58bf9a50ff839ea696f4fe602301f4a8b92, 6d07ace8512cb823f910bbb8cc9d16e54c04289c142b4b687815805e4ed0c52e, e60f84b8061804f4dfd5115dfb8a56b50b670a9a8650878160a45f22487d077c, e45f7df294a5bd06a40140e1f89788ac86fcbbebe7627a6b21c5819024369959
Rhadamanthys	SHA256	9e7f2e72d5812dcd3f965039efbd9d47170a99b9a03cd72970650bed8d8402d7, 067171ca88daa1c9816c657e21464421225630a7d2f6ae5d05d82a11ae3e16fa, e5f99a53b6f99bf112db4bf4a513cee89f8b424ade4e7198a14755124cb8af5c, 60b156ea82325d3caf7fa04ef4346b6ee1019b030bd2bfc3654c99b69229edd3, 4eaf0c8a00e69948c2a66fd954389eb7e294d631f4ee179987429fb409d64070,

Attack Name	TYPE	VALUE
Rhadamanthys	SHA256	ac2ae93520ecd4108c945e39ed1954f86ce5385b717bc9536d5ccb23f6e8eb86, 47150fa819c6d9ce7c5bdf9d54b128378946cab79eb621cd5b38280bf77d6bcd, 0639bf90ccf30d0f3c0764fc9a39f074d493ee5fd0eafddf32ab1ee54a0cf07d, fed2d796c6e9518d6220377972597e4ff223a885520e737d143d9d04afacc450, db8a254ca5916cd4824747505acc6e9c87af6ed68f8babca0fdee896b994b733
Stego Loader	SHA256	8c2e9aa5e926e55dbb33b7c07997a81d5a297b5e2c1c0fa18bf496445602210f, 5fd746de2643a000d36f0aeff42ceed4c35068c0c4a6bdb6c58966e91e9c4fab, 6a11145b4ccd6c05c2ee4fbb32a6468272863e22a8376ee85d10c558d3f09207
StealC V2	SHA256	FC16AB400800B3D6A05B6FB3884D5BA52ED097B8F50A2BEAB25442961B8FB8D0, AD278E48574CB10FE84B9B46C8B7BEF4F71C25B29F3EDAC93829B675B736BD69
Sha1_Hulud 2.0	SHA256	62ee164b9b306250c1172583f138c9614139264f889fa99614903c12755468d0, e0250076c1d2ac38777ea8f542431daf61fcbaab0ca9c196614b28065ef5b918, cbb9bc5a8496243e02f3cc080efbe3e4a1430ba0671f2e43a202bf45b05479cd, f1df4896244500671eb4aa63ebb48ea11cee196fafaa0e9874e17b24ac053c02, f099c5d9ec417d4445a0328ac0ada9cde79fc37410914103ae9c609cbc0ee068, 46faab8ab153fae6e80e7cca38eab363075bb524edd79e42269217a083628f09, b74caeaa75e077c99f7d44f46daaf9796a3be43ecf24f2a1fd381844669da777, dc67467a39b70d1cd4c1f7f7a459b35058163592f4a9e8fb4dffcbba98ef210c, 4b2399646573bb737c4969563303d8ee2e9ddbd1b271f1ca9e35ea78062538db, a3894003ad1d293ba96d77881ccd2071446dc3f65f434669b49b3da92421901a,

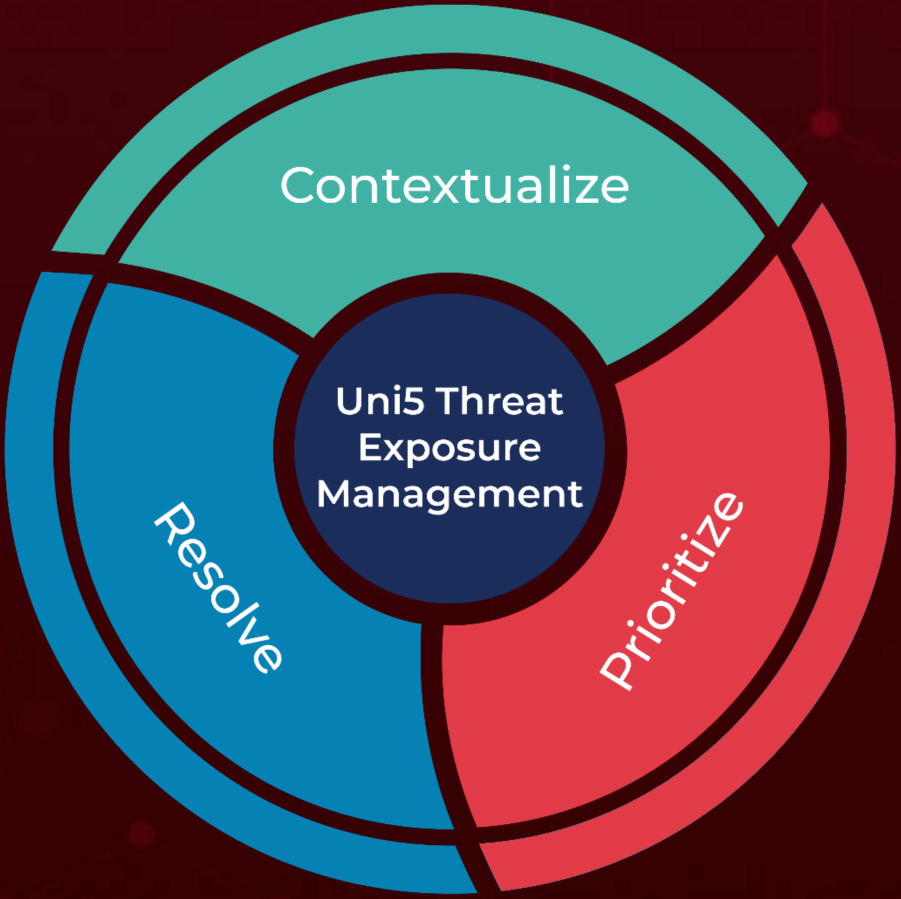
Attack Name	TYPE	VALUE
ShadowPad	SHA256	d429934b06de67c156dc559b33c34db5e02bc56ac2c1cd45ee03e6a21cf003af
	File Name	ETDApix.dll
	MD5	27e00b5594530e8c5e004098eef2ec50

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

December 2, 2025 • 1:45 AM

More at www.hivepro.com