Date of Publication
October 14, 2025

Hive Pro

Hiveforce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities, and Actors

06 to 12 OCTOBER 2025

Table Of Contents

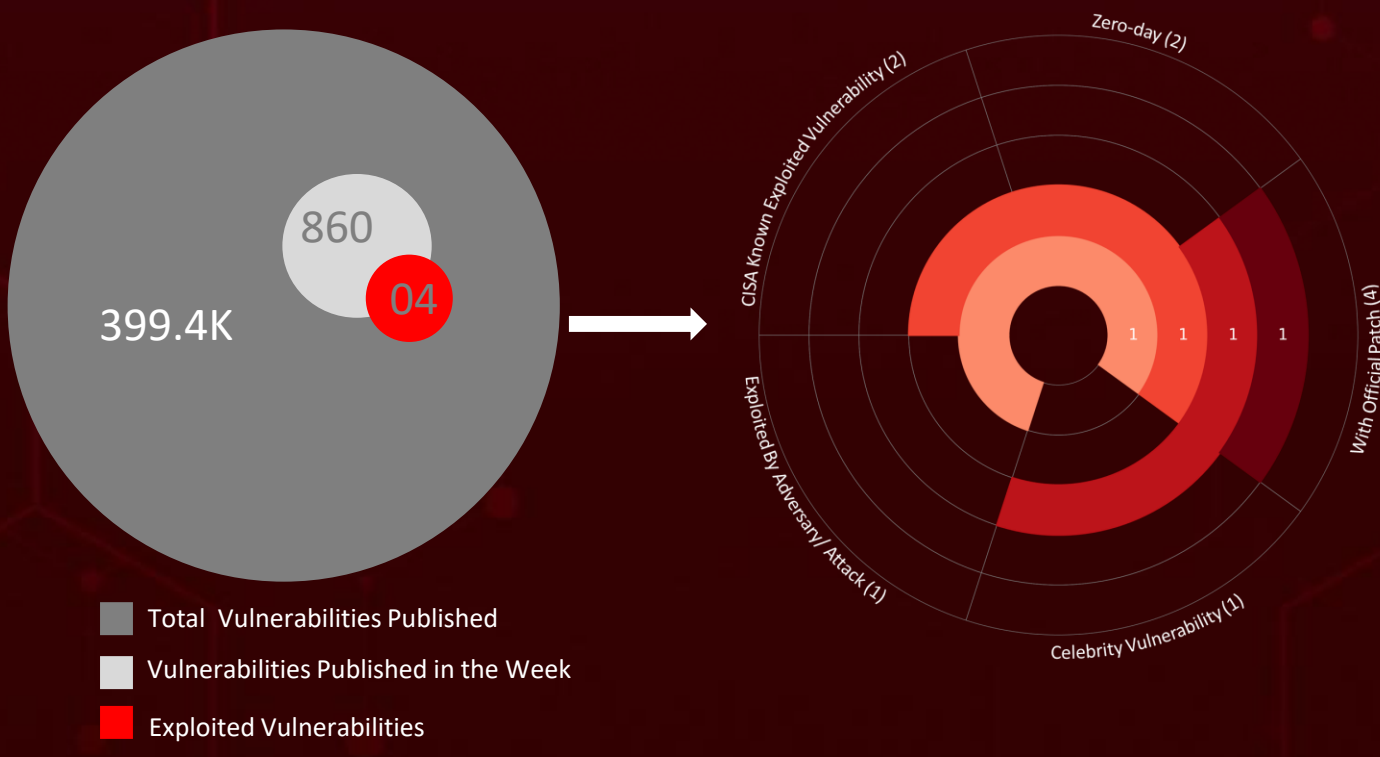
Summary

HiveForce Labs has reported a sharp rise in cybersecurity threats, highlighting the increasing complexity and frequency of global cyber incidents. Over the past week, **six** major attacks were detected, **four** critical vulnerabilities were publicly disclosed, and **five** active threat actor groups were monitored, signaling a concerning escalation in malicious activity.

One of the most severe vulnerabilities, **CVE-2025-61882**, is an unauthenticated remote code execution flaw in Oracle E-Business Suite (EBS). This weakness has been actively exploited by the **Cl0p ransomware** group since August 2025, with attack frequency surging after a proof-of-concept exploit was leaked in October 2025 by the collective known as **Scattered Lapsus$ Hunters**.

Earlier in 2025, an unidentified actor posing as the Libyan Navy's Office of Protocol targeted Brazil's military through a malicious calendar file exploiting a **zero-day** vulnerability in the Zimbra Collaboration Suite (**CVE-2025-27915**).

Another campaign tracked **Water Saci**, which spreads the **SORVEPOTEL** malware through WhatsApp, demonstrating the expanding reach of social engineering tactics. This underscores the growing importance of proactive security updates and robust monitoring to defend against sophisticated, rapidly evolving attacks.



High Level Statistics

6
Attacks Executed

4
Vulnerabilities Exploited

5
Adversaries in Action

- WooperStealer
- AnonDoor
- SORVEPOTEL
- Cl0p
- GOVERSHELL
- Ghost RAT

- CVE-2025-61882
- CVE-2025-49844
- CVE-2025-5947
- CVE-2025-27915

- Confucius
- Scattered Spider
- ShinyHunters
- LAPSUS$
- UTA0388

Insights

China-Aligned UTA0388 Uses **ChatGPT** to Craft Deceptive **Multilingual Phishing Campaigns**

Government and Defense Under Watch: Confucius Group Upgrades Espionage Capabilities with Python-Driven Persistence

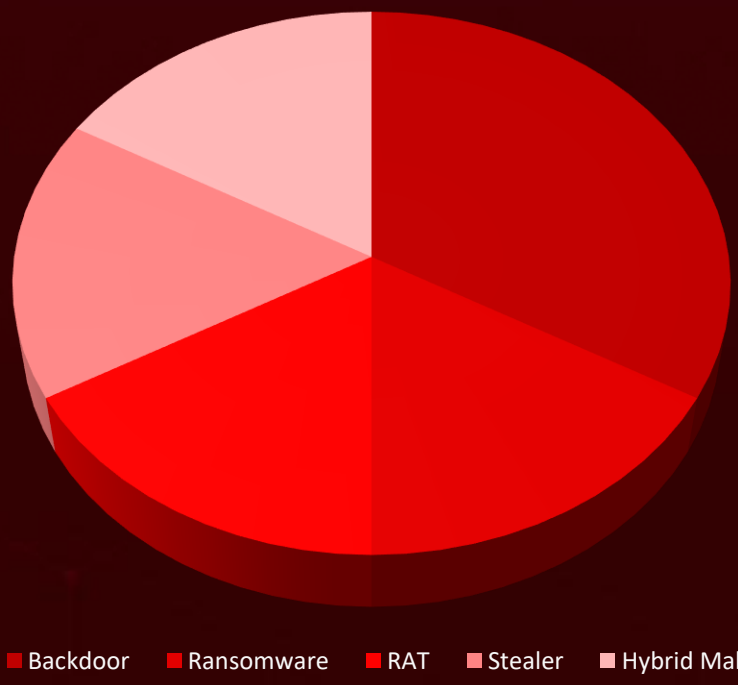
Nezha Monitoring Tool Weaponized to Deploy **Ghost RAT Across 100+ Machines**

RediShell Vulnerability (CVE-2025-49844): 13-Year-Old Bug Puts Redis at Risk of Remote Code Execution

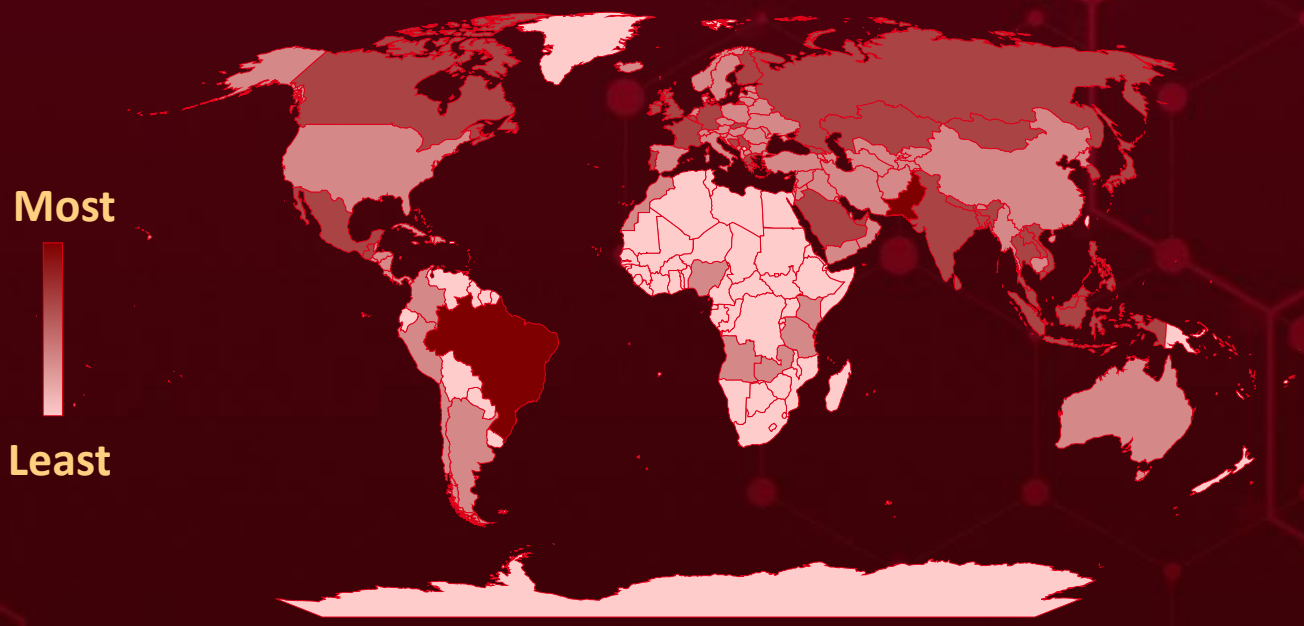
Cl0p Turns **Oracle E-Business Suite** Flaw Into Enterprise-Scale Ransomware Entry Point

Hackers Exploit Service Finder Plugin Bug to Control **WordPress Sites**

Threat Distribution

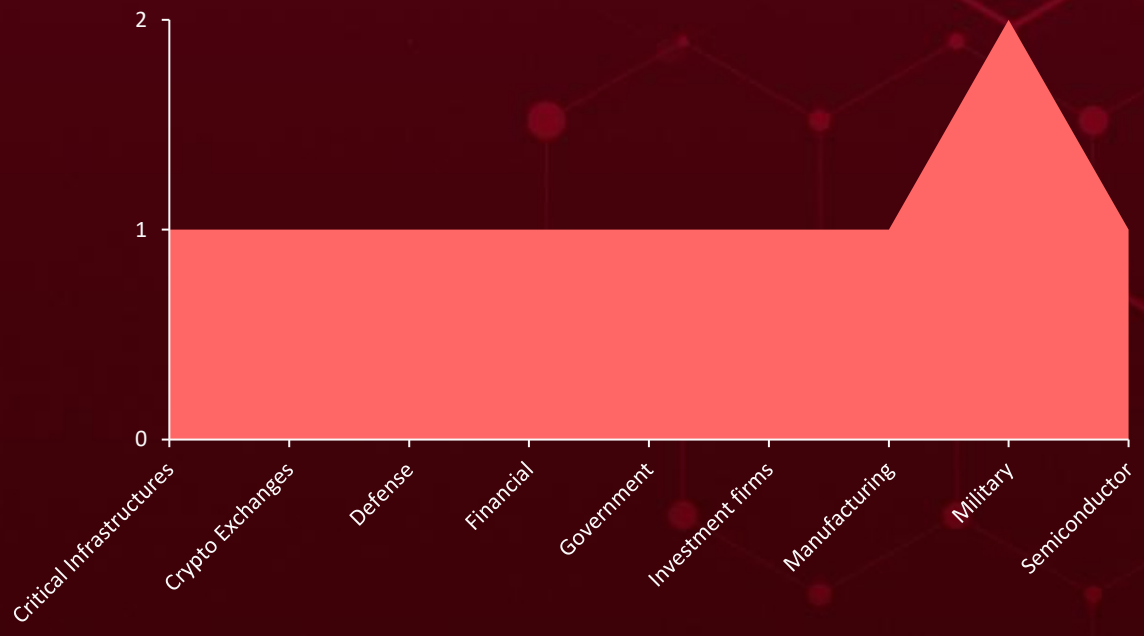


Targeted Countries



Countries	Countries	Countries	Countries
Brazil	Serbia	Holy See	North Macedonia
Pakistan	Indonesia	Nicaragua	Belize
Malaysia	Slovakia	Honduras	Oman
South Korea	Ireland	Norway	United States
Saudi Arabia	Sri Lanka	Hungary	Panama
Bosnia and Herzegovina	Japan	Peru	Bhutan
United Arab Emirates	Trinidad and Tobago	Iceland	Chile
Mongolia	United Kingdom	Qatar	Zambia
Belgium	Vietnam	Albania	China
Bangladesh	Kazakhstan	Saint Lucia	Angola
Portugal	Costa Rica	Barbados	Romania
Canada	North Korea	Cuba	Latvia
Singapore	Dominican Republic	Iran	Saint Kitts & Nevis
Finland	Armenia	Spain	Lebanon
Thailand	Poland	Iraq	San Marino
France	Australia	Switzerland	Afghanistan
Laos	Austria	Belarus	Croatia
Georgia	Cambodia	Dominica	Lithuania
Mexico	Azerbaijan	Israel	Cyprus
Germany	Argentina	Turkmenistan	Luxembourg
Nepal	Bahamas	Italy	Czech Republic
Greece	Colombia	Myanmar	Antigua and Barbuda
Philippines	Grenada	Jamaica	Denmark
Guatemala	Slovenia	Netherlands	Maldives
Russia	Bahrain	Andorra	Sweden
India	Tajikistan	Nigeria	Malta
	Haiti	Jordan	
	El Salvador		

Targeted Industries



TOP MITRE ATT&CK TTPs

T1059 Command and Scripting Interpreter	**T1071.001** Web Protocols	**T1071** Application Layer Protocol	**T1027** Obfuscated Files or Information	**T1588** Obtain Capabilities
T1574.001 DLL	**T1190** Exploit Public-Facing Application	**T1574** Hijack Execution Flow	**T1041** Exfiltration Over C2 Channel	**T1036** Masquerading
T1078 Valid Accounts	**T1068** Exploitation for Privilege Escalation	**T1082** System Information Discovery	**T1566** Phishing	**T1203** Exploitation for Client Execution
T1588.006 Vulnerabilities	**T1204** User Execution	**T1204.002** Malicious File	**T1105** Ingress Tool Transfer	**T1566.001** Spearphishing Attachment

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
WooperStealer	WooperStealer is a type of information-stealing malware that is configured to enumerate and collect files with specific extensions across an infected host. After gathering this data, it transmits the stolen files to a designated remote endpoint	Spear-phishing	-
		IMPACT	AFFECTED PLATFORM
TYPE		Data Exfiltration and Confidentiality Loss	Windows
Stealer			PATCH LINK
ASSOCIATED ACTOR			-
Confucius			
IOC TYPE	VALUE		
SHA256	8603b9fa8a6886861571fd8400d96a705eb6258821c6ebc679476d1b92dcd09e		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
AnonDoor	AnonDoor is a Python-based persistent backdoor that also serves as a centralized loader for modular payloads. It facilitates sustained access and detailed host profiling, including screenshots and enumeration of files and disk volumes. Heavier operations are throttled to run no more than once every six minutes, minimizing observable activity and redundant data transfers.	Spear-phishing	-
		IMPACT	AFFECTED PLATFORM
TYPE		Sustained Remote Access, Host Profiling & Reconnaissance	Windows
Backdoor			PATCH LINK
ASSOCIATED ACTOR			-
Confucius			
IOC TYPE	VALUE		
SHA256	abefd29c85d69f35f3cf8f5e6a2be76834416cc43d87d1f6643470b359ed4b1b		

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
SORVEPOTEL	Water Saci is a malicious campaign that spreads SORVEOTEL, a hybrid malware. It uses deceptive messages with ZIP attachments that execute PowerShell commands to load additional payloads directly into memory. SORVEOTEL can hijack active WhatsApp Web sessions to propagate infected files to contacts and deploy convincing banking overlays to harvest credentials.	Spear-phishing via WhatsApp	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		Credential Theft, Financial Loss	Windows
Hybrid Malware			
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Cl0p	The Cl0p ransomware group has escalated its attacks, particularly after the October 2025 leak of a proof-of-concept exploit for an Oracle EBS zero-day. The group has been involved in campaigns that combine data theft with double extortion tactics. Key indicators of compromise include unauthorized web shells, outbound command-and-control traffic, and stolen application credentials.	Exploiting vulnerabilities	CVE-2025-61882
		IMPACT	**AFFECTED PRODUCT**
TYPE		Information Theft, Financial Loss	Oracle E-Business Suite
Ransomware			
ASSOCIATED ACTOR			**PATCH LINKS**
-			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
IOC TYPE	**VALUE**		
SHA256	76b6d36e04e367a2334c445b51e1ecce97e4c614e88dfb4f72b104ca0f31235d, aa0d3859d6633b62bccfb69017d33a8979a3be1f3f0a5a4bf6960d6c73d41121		

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
GOVERSHELL	GOVERSHELL is a sophisticated backdoor malware that leverages search-order hijacking to deploy itself through malicious archives. Once executed, it establishes persistent access to compromised systems, allowing attackers to control the target remotely.	Spear-phishing	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		Persistent Remote Access, Data Exfiltration	Windows
Backdoor			
ASSOCIATED ACTOR			**PATCH LINK**
UTA0388			-
IOC TYPE	**VALUE**		
SHA256	2ffe1e4f4df34e1aca3b8a8e93eee34bfc4b7876cedd1a0b6ca5d63d89a26301, 4c041c7c0d5216422d5d22164f83762be1e70f39fb8a791d758a816cdf3779a9, 53af82811514992241e232e5c04e5258e506f9bc2361b5a5b718b4e4b5690040		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Ghost RAT	The Ghost RAT attack began when a phpMyAdmin panel was accidentally exposed online due to a DNS misconfiguration. The attacker, using an AWS IP from Hong Kong, quickly changed the interface to Simplified Chinese and executed SQL commands. They exploited a logging misconfiguration and directory traversal flaw to inject a PHP web shell into the MariaDB logs, creating a hidden backdoor. The malware used multiple stages to evade detection and maintained persistence by masquerading as a Windows service called SQLlite.	Compromised Web Server	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		Sustained Remote Access, Operational Disruption	Windows
RAT			
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
SHA256	7b2599ed54b72daec0acfd32744c7a9a77b19e6cf4e1651837175e4606dbc958		

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-2025-61882	✗	Oracle E-Business Suite versions 12.2.3-12.2.14	Scattered Spider, ShinyHunters, and LAPSUS$
	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 ACTOR
CVE-2025-49844	RediShell	All Versions of Redis with Lua Scripting (Before 8.2.2)	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:redis:redis:*:*:*:*:*:*:*:*	-
Redis Remote Code Execution Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-416	T1059: Command and Scripting Interpreter, T1497: Virtualization/Sandbox Evasion	https://github.com/redis/redis/releases/tag/8.2.2, https://redis.io/blog/security-advisory-cve-2025-49844/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2025-5947	✗	WordPress Service Finder Bookings Plugin Version Prior to 6.1	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:service_finder_bookings_plugin:service_finder_bookings_plugin:*:*:*:*:*:*:*:*	-
WordPress Service Finder Bookings Plugin Authentication Bypass Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-639	T1068: Exploitation for Privilege Escalation, T1078: Valid Accounts	https://themeforest.net/item/service-finder-service-and-business-listing-wordpress-theme/15208793?srsltid=AfmBOoq5ifHWqLc8b5o0Q7gjSz6HEpbHfquXWh-KhP0FWnFBTCFLaBzH

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTOR
CVE-2025-27915	✗	Zimbra Collaboration (ZCS) 9.0, 10.0, and 10.1	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:zimbra:collaboration:*:*:*:*:*:*:*:*	-
Synacor Zimbra Collaboration Suite (ZCS) Cross-site Scripting Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-79	T1203: Exploitation for Client Execution, T1059: Command and Scripting Interpreter	https://wiki.zimbra.com/wiki/Zimbra_Releases/10.0.13, https://wiki.zimbra.com/wiki/Zimbra_Releases/10.1.5, https://wiki.zimbra.com/wiki/Zimbra_Releases/9.0.0/P44

Adversaries in Action

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGION</th></tr>
<tr><td rowspan="4"> 
Confucius (aka G0142)</td><td>South Asia-based</td><td rowspan="3">Government Agencies, Military Organizations, Defense Contractors, Critical Infrastructures</td><td rowspan="3">Pakistan</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information Theft and Espionage</td></tr>
<tr><td>TARGETED CVE</td><td>ASSOCIATED ATTACKS/RANSOM WARE</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>-</td><td>WooperStealer, AnonDoor</td><td>Microsoft Windows</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; T1204: User Execution; T1204.002: Malicious File; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1059.006: Python; T1053: Scheduled Task/Job; T1053.005: Scheduled Task; T1218: System Binary Proxy Execution; T1218.011: Rundll32; T1082: System Information Discovery; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1566: Phishing; T1566.001: Spearphishing Attachment; T1574: Hijack Execution Flow; T1574.001: DLL; T1041: Exfiltration Over C2 Channel; T1112: Modify Registry; T1005: Data from Local System; T1083: File and Directory Discovery; T1087: Account Discovery; T1113: Screen Capture; T1027: Obfuscated Files or Information</td></tr>
</table>

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="3"> 

Scattered Spider (Starfraud, UNC3944, 0ktapus, Storm-0875, LUCR-3, Scatter Swine, Muddled Libra, Octo Tempest and 0ktapus)</td><td>Suspected UK and US</td><td rowspan="3">All</td><td rowspan="3">Worldwide</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Financial gain</td></tr>
<tr><td>TARGETED CVE</td><td>ASSOCIATED ATTACKS/RANSOM WARE</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>CVE-2025-61882</td><td>-</td><td>Oracle E-Business Suite</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0042: Resource Development; TA0005: Defense Evasion; TA0040: Impact; TA0010: Exfiltration; TA0004: Privilege Escalation; TA0006: Credential Access; TA0008: Lateral Movement; TA0011: Command and Control; TA0007: Discovery; T1190: Exploit Public-Facing Application; T1203: Exploitation for Client Execution; T1071.001: Web Protocols; T1071: Application Layer Protocol; T1105: Ingress Tool Transfer; T1059: Command and Scripting Interpreter; T1505.003: Web Shell; T1505: Server Software Component; T1588.006: Vulnerabilities; T1588.005: Exploits; T1588: Obtain Capabilities; T1068: Exploitation for Privilege Escalation; T1078: Valid Accounts; T1210: Exploitation of Remote Services; T1041: Exfiltration Over C2 Channel; T1486: Data Encrypted for Impact</td></tr>
</table>

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 ShinyHunters	-	All	Worldwide
	MOTIVE		
	Financial gain		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCT
	CVE-2025-61882	-	Oracle E-Business Suite
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0042: Resource Development; TA0005: Defense Evasion; TA0040: Impact; TA0010: Exfiltration; TA0004: Privilege Escalation; TA0006: Credential Access; TA0008: Lateral Movement; TA0011: Command and Control; TA0007: Discovery; T1190: Exploit Public-Facing Application; T1203: Exploitation for Client Execution; T1071.001: Web Protocols; T1071: Application Layer Protocol; T1105: Ingress Tool Transfer; T1059: Command and Scripting Interpreter; T1505.003: Web Shell; T1505: Server Software Component; T1588.006: Vulnerabilities; T1588.005: Exploits; T1588: Obtain Capabilities; T1068: Exploitation for Privilege Escalation; T1078: Valid Accounts; T1210: Exploitation of Remote Services; T1041: Exfiltration Over C2 Channel; T1486: Data Encrypted for Impact			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 LAPSUS$ (aka DEV-0537, Strawberry Tempest, Slippy Spider, G1004)	Brazil	All	Worldwide
	MOTIVE		
	Financial gain		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOM WARE**	**AFFECTED PRODUCT**
	CVE-2025-61882	-	Oracle E-Business Suite

TTPs
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0042: Resource Development; TA0005: Defense Evasion; TA0040: Impact; TA0010: Exfiltration; TA0004: Privilege Escalation; TA0006: Credential Access; TA0008: Lateral Movement; TA0011: Command and Control; TA0007: Discovery; T1190: Exploit Public-Facing Application; T1203: Exploitation for Client Execution; T1071.001: Web Protocols; T1071: Application Layer Protocol; T1105: Ingress Tool Transfer; T1059: Command and Scripting Interpreter; T1505.003: Web Shell; T1505: Server Software Component; T1588.006: Vulnerabilities; T1588.005: Exploits; T1588: Obtain Capabilities; T1068: Exploitation for Privilege Escalation; T1078: Valid Accounts; T1210: Exploitation of Remote Services; T1041: Exfiltration Over C2 Channel; T1486: Data Encrypted for Impact

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 UTA0388 (aka UNK_DropPitch)	China	Manufacturing, Investment firms, Semiconductor	North America, Asia, and Europe
	MOTIVE		
	Information Theft and Espionage		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCT**
	-	GOVERSHELL	Windows
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0011: Command and Control; TA0005: Defense Evasion; TA0040: Impact; T1574.001: DLL Search Order Hijacking; T1574: Hijack Execution Flow; T1053.005: Scheduled Task; T1053: Scheduled Task/Job; T1036: Masquerading; T1027: Obfuscated Files or Information; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1071.004: DNS; T1203: Exploitation for Client Execution; T1588.007: Artificial Intelligence; T1588: Obtain Capabilities; T1598.003: Spearphishing Link; T1566.001: Spearphishing Attachment; T1566: Phishing; T1204: User Execution; T1204.002: Malicious File; T1486: Data Encrypted for Impact; T1059: Command and Scripting Interpreter			

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **four exploitable vulnerabilities** and block the indicators related to the threat actors **Confucius, Scattered Spider, ShinyHunters, LAPSUS$, UTA0388,** and malware **WooperStealer, AnonDoor, SORVEPOTEL, Cl0p, GOVERSHELL, Ghost RAT.**

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 **four exploitable vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actors **Confucius, Scattered Spider, LAPSUS$,** and malware **WooperStealer, GOVERSHELL, Ghost RAT** in Breach and Attack Simulation(BAS).

Threat Advisories

Confucius Hackers Spy on Critical Sectors Using AnonDoor

Water Saci: Brazil's WhatsApp-Borne Malware Storm

CVE-2025-61882: Oracle EBS Zero-Day Actively Exploited in the Wild

Redis Under Siege: RediShell Flaw Opens Door to Remote Code Execution

Service Finder Plugin Flaw Opens Door to Full Site Compromise

Zimbra Zero-Day Hidden in "Harmless" ICS File Targets Military

UTA0388: AI-Powered Targeted Operations Leveraging GOVERSHELL

Hidden in Plain Sight: The Abuse of Nezha and the Ghost RAT That Followed

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
WooperStealer	SHA256	8603b9fa8a6886861571fd8400d96a705eb6258821c6ebc679476d1b92dcd09e
AnonDoor	SHA256	abefd29c85d69f35f3cf8f5e6a2be76834416cc43d87d1f6643470b359ed4b1b
Cl0p	SHA256	76b6d36e04e367a2334c445b51e1ecce97e4c614e88dfb4f72b104ca0f31235d, aa0d3859d6633b62bccfb69017d33a8979a3be1f3f0a5a4bf6960d6c73d41121, 6fd538e4a8e3493dda6f9fcdc96e814bdd14f3e2ef8aa46f0143bff34b882c1b
GOVERSHELL	IPv4:Port	80[.]85[.]154[.]48[:]443, 80[.]85[.]157[.]117[:]443, 82[.]118[.]16[.]173[:]443
	IPv4	104[.]194[.]152[.]137, 104[.]194[.]152[.]152, 185[.]144[.]28[.]68, 31[.]192[.]234[.]22, 45[.]141[.]139[.]222, 74[.]119[.]193[.]175, 80[.]85[.]156[.]234, 80[.]85[.]154[.]48, 80[.]85[.]157[.]117, 82[.]118[.]16[.]173

Attack Name	TYPE	VALUE
GOVERSHELL	Hostname	azure-app[.]store, twmoc[.]info, windows-app[.]store, cdn-apple[.]info, sliddeshare[.]online, doccloude[.]info
	URLs	hxxp[:]//1drv[.]ms/u/c/F703BC98FAB44D61/ER_XG5FDkURHtsmna8vOQrIBRODKiQBKYJVKnI-kGKwX0A, hxxp[:]//1drv[.]ms/u/c/F703BC98FAB44D61/ESz4UV9JeOhOp8kiWd0Ie10ByH7eUdSRlBy2NCiNeo2LYw, hxxp[:]//1drv[.]ms/u/c/f9e3b332ce488781/Eap6_fxYFP5Eh1ZKDZaf8lMBjJNcfdba4MVcr4YfKj674w?e=fgNIj4, hxxp[:]//1drv[.]ms/u/c/F703BC98FAB44D61/ERpeLpJlb7FAkbfyuffpFJYBZ-8u2MmQH6LW5xH86B4M8w, hxxp[:]//aesthetic-donut-1af43s2[.]netlify[.]app/file/rar, hxxp[:]//aesthetic-donut-1af43s2[.]netlify[.]app/file/zip, hxxp[:]//animated-dango-0fa8c8[.]netlify[.]app/file/Taiwan%20Intro[.]zip, hxxp[:]//aquamarine-choux-46cb43[.]netlify[.]app/file/rar hxxp[:]//aquamarine-choux-46cb43[.]netlify[.]app/file/zip hxxp[:]//aquamarine-choux-46cb43[.]netlify[.]app/index/file/[PDF]202507_Please_check_the_document[.]zip hxxp[:]//dainty-licorice-db2b1e[.]netlify[.]app/file/zip hxxp[:]//dulcet-mooncake-36558c[.]netlify[.]app/file/zip hxxp[:]//harmonious-malabi-a8ebfa[.]netlify[.]app/file/Taiwan%20Intro[.]rar hxxp[:]//hllowrodcanlhelipme[.]netlify[.]app/file/zip hxxp[:]//jazzy-biscotti-68241f[.]netlify[.]app/files/Intro-Doc[.]rar hxxp[:]//ln5[.]sync[.]com/4[.]0/dl/100016f90#3d5wrb4z-hfb4iz3m-qmjzsqnq-39rn3vjv hxxp[:]//loveusa[.]netlify[.]app/file/rar hxxp[:]//pulicwordfiledownlos[.]netlify[.]app/file/rar hxxp[:]//spontaneous-selkie-d3346f[.]netlify[.]app/file/zip hxxp[:]//statuesque-unicorn-09420f[.]netlify[.]app/r hxxp[:]//subtle-klepon-d73b9b[.]netlify[.]app/file/rar hxxp[:]//subtle-klepon-d73b9b[.]netlify[.]app/file/zip hxxp[:]//vocal-crostata-86ebbf[.]netlify[.]app/files/zip wss[:]//api[.]twmoc[.]info/ws wss[:]//onedrive[.]azure-app[.]store/ws wss[:]//outlook[.]windows-app[.]store/ws www[.]twmoc[.]info hxxp[:]//app-site-association[.]cdn-apple[.]info[:]443/updates[.]rss

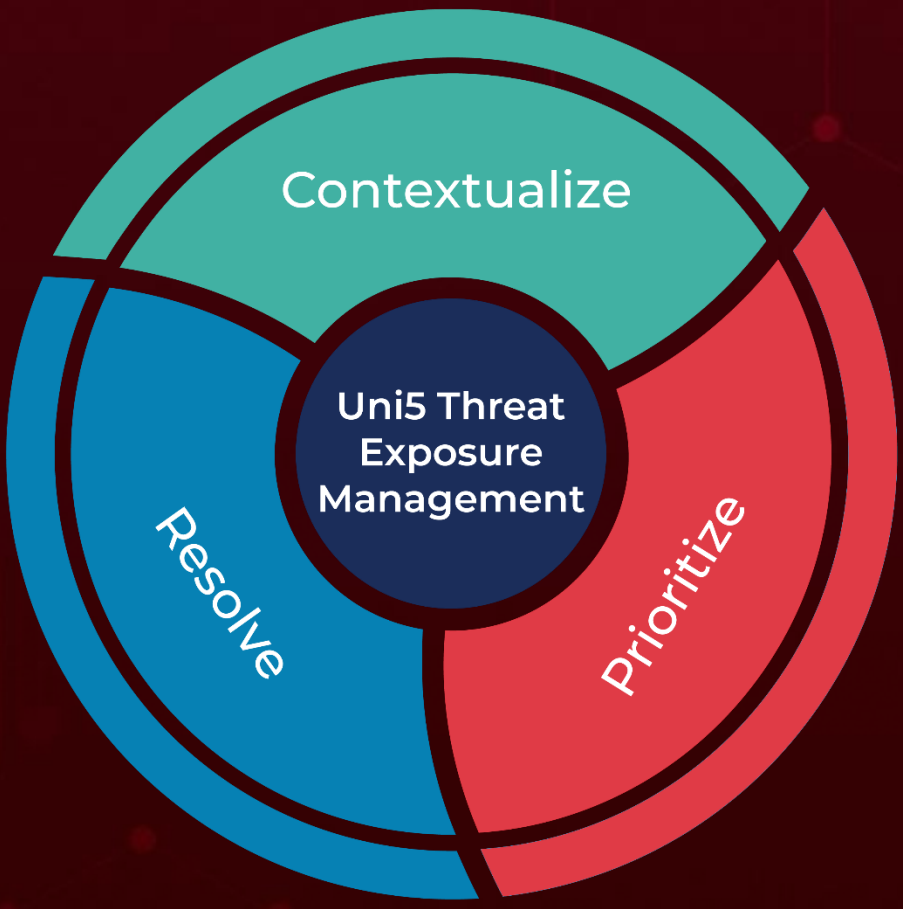
Attack Name	TYPE	VALUE
GOVERSHELL	SHA256	2ffe1e4f4df34e1aca3b8a8e93eee34bfc4b7876cedd1a0b6ca5d63d89a26301 4c041c7c0d5216422d5d22164f83762be1e70f39fb8a791d758a816cdf3779a9 53af82811514992241e232e5c04e5258e506f9bc2361b5a5b718b4e4b5690040 88782d26f05d82acd084861d6a4b9397d5738e951c722ec5afed8d0f6b07f95e 998e314a8babf6db11145687be18dc3b8652a3dd4b36c115778b7ca5f240aae4 a5ee55a78d420dbba6dec0b87ffd7ad6252628fd4130ed4b1531ede960706d2d ad5718f6810714bc6527cc86d71d34d8c556fe48706d18b5d14f0261eb27d942 fbade9d8a040ed643b68e25e19cba9562d2bd3c51d38693fe4be72e01da39861 7d7d75e4d524e32fc471ef2d36fd6f7972c05674a9f2bac909a07dfd3e19dd18 0414217624404930137ec8f6a26aebd8a3605fe089dbfb9f5aaaa37a9e2bad2e 126c3d21a1dae94df2b7a7d0b2f0213eeeec3557c21717e02ffaed690c4b1dbd, 53af82811514992241e232e5c04e5258e506f9bc2361b5a5b718b4e4b5690040
Ghost RAT	SHA256	7b2599ed54b72daec0acfd32744c7a9a77b19e6cf4e1651837175e4606dbc958
	File Path	C:\Windows\Cursors\x.exe

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 14, 2025 . 1:00 AM

More at www.hivepro.com