

Date of Publication
October 5, 2026



HiveForce Labs
WEEKLY
THREAT DIGEST

Attacks, Vulnerabilities, and Actors

28 SEPTEMBER to 4 OCTOBER 2026

Table Of Contents

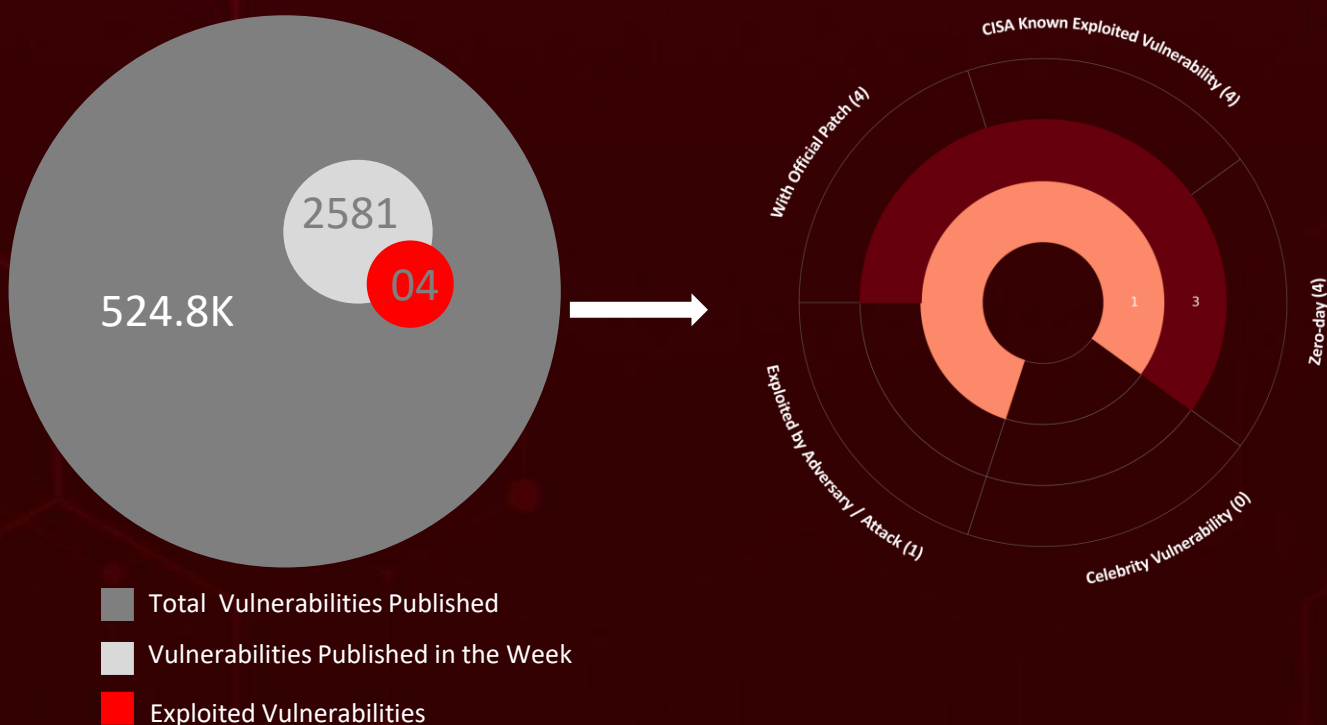
<u>Summary</u>	03
<u>High Level Statistics</u>	04
<u>Insights</u>	05
<u>Targeted Countries</u>	06
<u>Targeted Industries</u>	07
<u>Top MITRE ATT&CK TTPs</u>	07
<u>Attacks Executed</u>	08
<u>Vulnerabilities Exploited</u>	10
<u>Adversaries in Action</u>	14
<u>Recommendations</u>	16
<u>Threat Advisories</u>	17
<u>Appendix</u>	18
<u>What Next?</u>	19

Summary

HiveForce Labs reports a sharp rise in cyber threats over the past week. **Two** major attacks were detected, **four** vulnerabilities were actively exploited, and **two** threat actor groups were closely tracked. Together, they point to growing malicious activity worldwide.

Citrix has confirmed two critical remote code execution flaws in NetScaler ADC and NetScaler Gateway, [CVE-2026-88771](#) and [CVE-2026-88772](#). Attackers exploited both as zero-days before any fix existed. The first flaw lets an unauthenticated attacker run commands on the device, even in the default setup. The second is a memory overflow that can cause code execution or a denial of service when DTLS is enabled, which is the default for VPN virtual servers. Since NetScaler sits at the network edge and handles VPN, remote access, and user logins, a hacked device gives attackers a way into internal systems.

ShinyHunters (UNC6240) is again mass-exploiting the critical Oracle PeopleSoft PeopleTools flaw [CVE-2026-35273](#). The group bypasses WAF rules by URL-encoding a single character in the PSEMHub path, which lets it reach unpatched systems. It has dropped web shells, the [SIDEYE](#) backdoor, Neo-reGeorg tunnels, and MeshAgent across education, healthcare, government, and other sectors to steal data and demand ransom. Organizations should patch immediately and not rely on WAF rules alone. These incidents show a rising trend of attacks that mix technical exploits with social engineering, so timely patching, constant monitoring, and layered defenses remain essential.



High Level Statistics

2

Attacks
Executed

- [SIDEEYE](#)
- [NeedyMantis](#)

4

Vulnerabilities
Exploited

- [CVE-2026-88771](#)
- [CVE-2026-88772](#)
- [CVE-2026-86950](#)
- [CVE-2026-35273](#)

2

Adversaries in
Action

- [ShinyHunters](#)
- [Storm-3069](#)



Insights

Attackers are walking in through things we trust, from **edge devices** and built-in **Apple tools** to everyday software and a WAF we assumed was enough.

Getting in is just step one. The real damage comes from how long they stay, so **patch fast**, then check who's already inside.

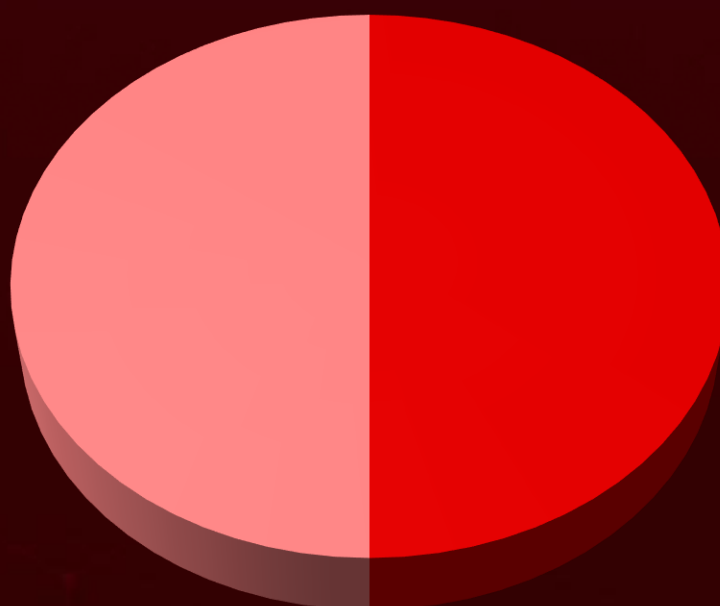
Attackers used **CVE-2026-88771** and **CVE-2026-88772** before any fix existed, so every unpatched day is a day of exposure.

Apple's **CVE-2026-86950** can run an attacker's code just from opening a crafted file, so one tap is all it takes.

ShinyHunters has renewed mass exploitation of Oracle's **CVE-2026-35273**, so patch immediately and hunt for web shells and tunnels.

NeedyMantis reaches telecom, education, healthcare, nonprofit, and government networks, so **Storm-3069** can be in any of them.

Threat Distribution



■ Multi-stage backdoor

■ Modular Backdoor

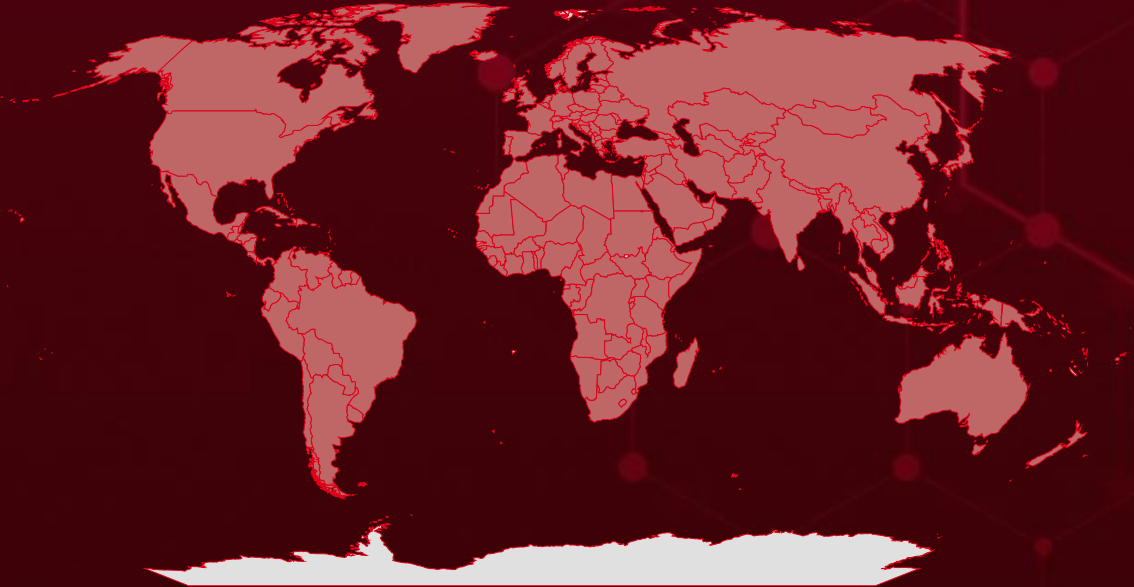


Targeted Countries

Most



Least

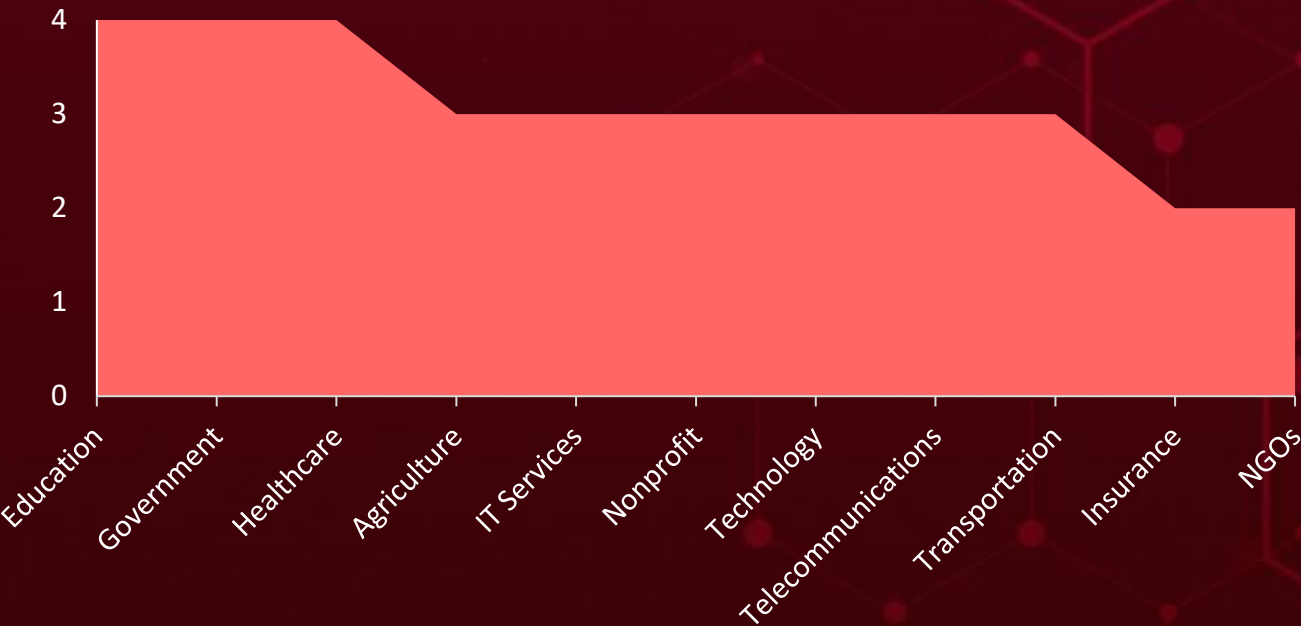


Powered by Bing

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

Countries	Countries	Countries	Countries
Ukraine	Belgium	Uruguay	Denmark
Oman	Togo	Cambodia	Switzerland
Moldova	Belize	Madagascar	Djibouti
Brazil	Lithuania	Cameroon	Thailand
Romania	Benin	Mali	Dominica
Guinea	Marshall Islands	Canada	Trinidad and Tobago
Afghanistan	Bhutan	Mauritius	Dominican Republic
Venezuela	Montenegro	Central African Republic	Tuvalu
Papua New Guinea	Bolivia	Monaco	Ecuador
Malaysia	New Zealand	Chad	United Kingdom
Suriname	Bosnia and Herzegovina	Mozambique	Egypt
Austria	Pakistan	Chile	Australia
Namibia	Botswana	Nepal	El Salvador
Azerbaijan	Poland	China	Luxembourg
Saudi Arabia	Albania	Niger	Malawi
Bahamas	Saint Vincent and the Grenadines	Colombia	Eritrea
Armenia	Brunei	Norway	Maldives
Bahrain	Sierra Leone	Comoros	Estonia
Micronesia	Bulgaria	Palestine State	Malta
Bangladesh	South Sudan	Congo (Congo-Brazzaville)	Mauritania
North Korea	Burkina Faso	Peru	Ethiopia
Barbados	Tajikistan	Costa Rica	
Russia	Burundi	Qatar	
Belarus	Turkey	Côte d'Ivoire	
Solomon Islands	Cabo Verde		

Targeted Industries



TOP MITRE ATT&CK TTPs

T1059 Command and Scripting Interpreter	T1105 Ingress Tool Transfer	T1071 Application Layer Protocol	T1021 Remote Services	T1082 System Information Discovery
T1027 Obfuscated Files or Information	T1190 Exploit Public-Facing Application	T1140 Deobfuscate/D ecode Files or Information	T1588 Obtain Capabilities	T1071.001 Web Protocols
T1588.006 Vulnerabilities	T1543 Create or Modify System Process	T1083 File and Directory Discovery	T1036 Masquerading	T1041 Exfiltration Over C2 Channel
T1570 Lateral Tool Transfer	T1574 Hijack Execution Flow	T1573 Encrypted Channel	T1057 Process Discovery	T1132 Data Encoding

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>SIDEEYE</u>	A multi-stage C++ backdoor delivered in-memory on compromised Windows PeopleSoft servers, capable of stealing browser and desktop-application credentials, file/process management, interactive reverse shell, and reverse-proxy tunneling.	Trojanized Ple64.exe installer	CVE-2026-35273
TYPE		IMPACT	AFFECTED PLATFORM
Multi-stage backdoor		Credential theft, remote control	Oracle PeopleSoft PeopleTools
ASSOCIATED ACTOR			PATCH LINK
ShinyHunters			https://www.oracle.com/security-alerts/alert-cve-2026-35273.html
IOC TYPE	VALUE		
SHA256	3ba215692665513abfffd4e815c5c45f2d41e5dcc4283a2a3b740930c5c417c3		

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
<u>NeedyMantis</u>	NeedyMantis is a modular, post-compromise backdoor used by the China-based threat actor Storm-3069 to keep hidden, long-term access to networks it has already broken into. It is delivered through : the attackers place a trusted program such as Poedit, curl, Vim, or TightVNC next to a malicious DLL and an encrypted archive, so the trusted program loads the malware without raising suspicion. They then spread the same bundle to other machines with the Impacket toolkit.	DLL sideloading	-
TYPE		IMPACT	AFFECTED PLATFORM
Modular Backdoor		Persistent Access, System Reconnaissance, Defense Evasion, Remote Control	Windows
ASSOCIATED ACTOR			PATCH LINK
Storm-3069			-
IOC TYPE	VALUE		
SHA256	e842dd7642c8e04b5ec20b6393848a9c904e4832930950c16664fe7800ba382e, 9cb68f986043a576e19d32184c583b7d8f571c7219d8dc0065dced1c13f077ef		

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
<u>CVE-2026-88771</u>		Citrix NetScaler ADC & NetScaler Gateway (14.1 before 14.1-73.37; 13.1 before 13.1-64.23; 14.1-FIPS before 14.1-73.37 FIPS; 13.1-FIPS & 13.1-NDcPP before 13.1-37.279)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:*:* *, cpe:2.3:a:citrix:netscaler_gateway:*:*:*:*:*:* :*	-
Citrix NetScaler Improper Input Validation Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX697096

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-88772</u>		Citrix NetScaler ADC & NetScaler Gateway (ADC: before 14.1-73.37, before 13.1-64.23, before 14.1-73.37 FIPS, and before 13.1.37.279 FIPS and NDcPP; Gateway: before 14.1-73.37 and before 13.1-64.23)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:*:* *, cpe:2.3:a:citrix:netscaler_gateway:*:*:*:*:*:* :*	-
Citrix NetScaler Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-119	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1499: Endpoint Denial of Service	https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX697096

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-86950</u>		Apple iOS and iPadOS (Before 26.7.1), Apple macOS Tahoe (Before 26.7.1), Apple macOS Sequoia (Before 15.8.1)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:apple:iphone_os:*.~*~*~*~*~*~*~*, cpe:2.3:o:apple:ipados:*:*:*~*~*~*~*~*~*~*, cpe:2.3:o:apple:macos:*:*:*~*~*~*~*~*~*~*	-
Apple Multiple Products Out-of-Bounds Write Vulnerability		CWE ID	ASSOCIATED TTPs
	CWE-787	T1059: Command and Scripting Interpreter, T1203: Exploitation for Client Execution	https://support.apple.com/en-us/149226 , https://support.apple.com/en-us/149228 , https://support.apple.com/en-us/149229

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-35273</u>		Oracle PeopleSoft Enterprise PeopleTools (versions 8.61, 8.62)	ShinyHunters
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:oracle:peoplesoft_enterprise_peopletools:*.*:*:*:*:*.*	SIDEEYE
Oracle PeopleSoft Enterprise PeopleTools Missing Authentication for Critical Function Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-306	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://www.oracle.com/security-alerts/alert-cve-2026-35273.html



Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 ShinyHunters (aka UNC6240)	-	Higher education, technology, IT services, healthcare, agriculture, transportation, government	Worldwide
	MOTIVE		
	Financial gain		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	CVE-2026-35273	SIDEEYE	Oracle PeopleSoft
TTPs			
TA0043:Reconnaissance, T1595:Active Scanning, T1595.002:Vulnerability Scanning, T1596:Search Open Technical Databases, T1596.003:Digital Certificates, T1596.005:Scan Databases, TA0001:Initial Access, T1190:Exploit Public-Facing Application, TA0002:Execution, T1059:Command and Scripting Interpreter, T1059.003:Windows Command Shell, T1059.004:Unix Shell, TA0003:Persistence, T1505:Server Software Component, T1505.003:Web Shell, TA0005:Defense Evasion, T1027:Obfuscated Files or Information, T1140:Deobfuscate/Decode Files or Information, T1553:Subvert Trust Controls, T1553.002:Code Signing, TA0006:Credential Access, T1552:Unsecured Credentials, T1552.001:Credentials In Files, T1110:Brute Force, T1110.003:Password Spraying, T1555:Credentials from Password Stores, T1555.003:Credentials from Web Browsers, TA0007:Discovery, T1082:System Information Discovery, T1016:System Network Configuration Discovery, TA0008:Lateral Movement, T1021:Remote Services, T1021.004:SSH, TA0011:Command and Control, T1105:Ingress Tool Transfer, T1071:Application Layer Protocol, T1071.001:Web Protocols, T1572:Protocol Tunneling, T1090:Proxy, T1219:Remote Access Software, TA0009:Collection, T1560:Archive Collected Data, T1560.001:Archive via Utility, TA0010:Exfiltration, T1048:Exfiltration Over Alternative Protocol, TA0040:Impact, T1491:Defacement, T1491.001:Internal Defacement			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 Storm-3069	China	Telecommunications, Education, Healthcare, Nonprofits, Government	Worldwide
	MOTIVE		
	Information Theft, Espionage		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	-	NeedyMantis	-
TTPs			
TA0002: Execution, TA0003: Persistence, TA0005: Defense Evasion, TA0007: Discovery, TA0008: Lateral Movement, TA0011: Command and Control, TA0010: Exfiltration, T1129: Shared Modules, T1543: Create or Modify System Process, T1574: Hijack Execution Flow, T1036: Masquerading, T1027: Obfuscated Files or Information, T1140: Deobfuscate/Decode Files or Information, T1622: Debugger Evasion, T1082: System Information Discovery, T1033: System Owner/User Discovery, T1057: Process Discovery, T1083: File and Directory Discovery, T1570: Lateral Tool Transfer, T1021: Remote Services, T1071: Application Layer Protocol, T1573: Encrypted Channel, T1132: Data Encoding, T1105: Ingress Tool Transfer, T1041: Exfiltration Over C2 Channel, T1543.003: Windows Service, T1574.002: DLL, T1036.005: Match Legitimate Resource Name or Location, T1036.008: Masquerade File Type, T1027.013: Encrypted/Encoded File, T1027.015: Compression, T1027.007: Dynamic API Resolution, T1021.002: SMB/Windows Admin Shares, T1071.001: Web Protocols, T1573.001: Symmetric Cryptography, T1132.001: Standard Encoding			

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **four exploited vulnerabilities** and block the indicators related to the threat actors **ShinyHunters** and **Storm-3069**, and the malware **SIDEYE** and **NeedyMantis**.

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 exploited vulnerabilities**.
- Testing the efficacy of their security controls by simulating attacks related to the threat actor **ShinyHunters** and the malware **SIDEYE** and **NeedyMantis** in Breach and Attack Simulation(BAS).

Threat Advisories

[Citrix NetScaler Zero-Days Under Active Exploitation](#)

[Apple CoreGraphics Flaw Exploited in Targeted Attacks](#)

[From Zero-Day to N-Day: ShinyHunters Renews Oracle PeopleSoft Mass Exploitation](#)

[NeedyMantis: The Patient Predator Hiding in Plain Sight](#)

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
<u>SIDE EYE</u>	SHA256	3ba215692665513abfffd4e815c5c45f2d41e5dcc4283a2a3b740930c5c417c3
	IPv4	162[.]219[.]30[.]165
<u>NeedyMantis</u>	SHA256	e842dd7642c8e04b5ec20b6393848a9c904e4832930950c16664fe7800ba382e, 9cb68f986043a576e19d32184c583b7d8f571c7219d8dc0065dced1c13f077ef, c82520eb03c084226be4eafbff46f56dca0aa8804a2a7f23a085a96afe71ef77

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

October 05, 2026 • 08:00 AM

© 2026 All Rights are Reserved by Hive Pro



More at www.hivepro.com