

Date of Publication
September 28, 2026



HiveForce Labs
WEEKLY
THREAT DIGEST

Attacks, Vulnerabilities, and Actors

21 to 27 SEPTEMBER 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>	19
<u>Recommendations</u>	20
<u>Threat Advisories</u>	21
<u>Appendix</u>	22
<u>What Next?</u>	24

Summary

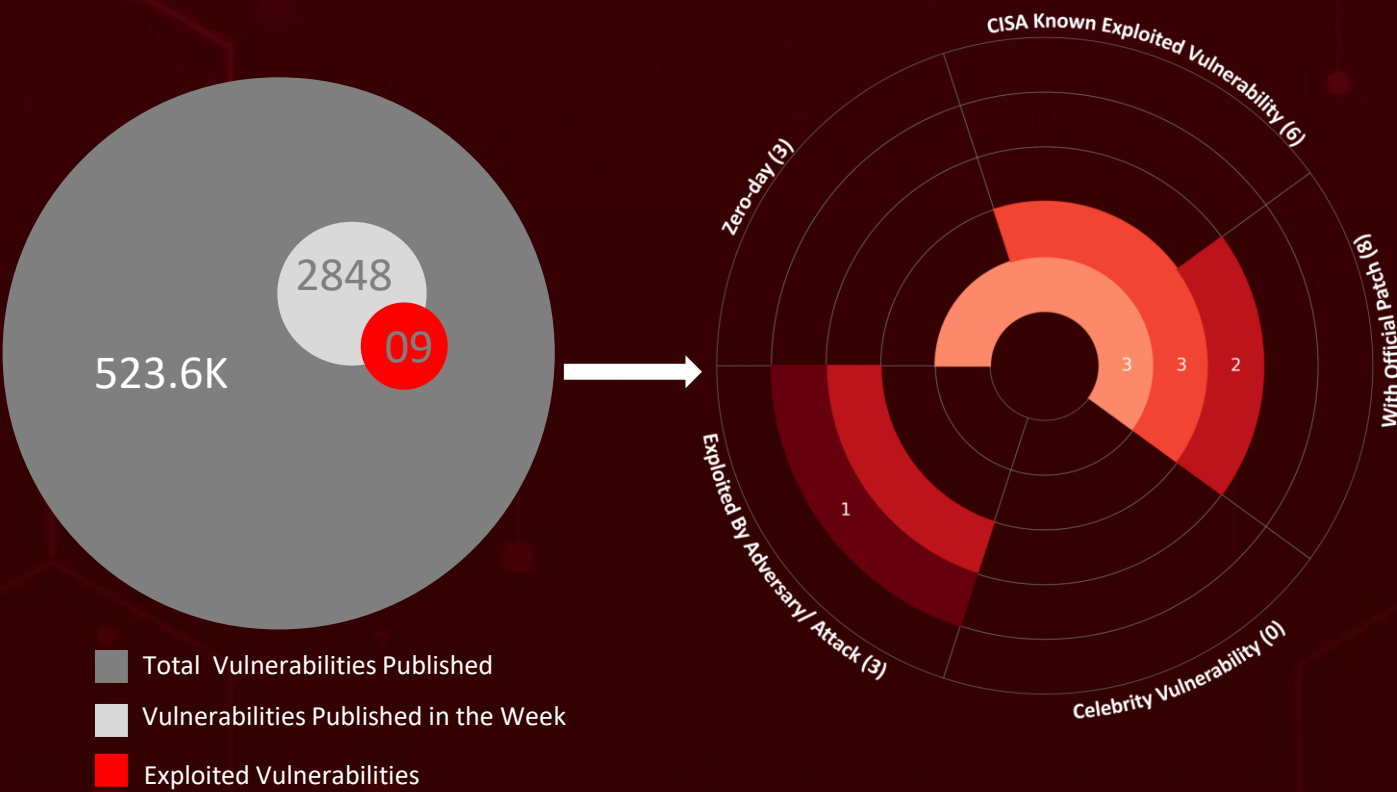
HiveForce Labs has reported a sharp rise in cybersecurity threats, highlighting the growing complexity and frequency of global cyber incidents. Over the past week, **two** major **attacks** were detected, **nine vulnerabilities** were actively exploited, and **one threat actor group** was closely monitored, signaling a concerning escalation in malicious activity worldwide.

Among the most significant developments, **Check Point** is warning that attackers are actively exploiting two critical, no-login-required flaws. One of them, **CVE-2026-93616**, is a zero-day in the Check Point Management web service that gives attackers code execution on the server that controls firewall policy, administration, and logging.

F5 disclosed **CVE-2026-94127**, a critical unauthenticated remote code execution flaw in the OAuth component of BIG-IP Access Policy Manager (APM), and confirmed it is being actively exploited in the wild.

Meowciety403, also tracked as Nekoneko200, is an emerging, financially motivated extortion group that has been active since August 2026. It operates as a data broker rather than as a confirmed encryption-based ransomware operation.

Together, these developments underscore a growing trend of hybrid cyber operations that combine technical exploitation with social engineering, reinforcing the need for timely patching, continuous monitoring, and layered security defenses.



High Level Statistics

2

Attacks
Executed

- [PAYLOAD Ransomware](#)
- [DragonForce Ransomware](#)

9

Vulnerabilities
Exploited

- [CVE-2026-7273](#)
- [CVE-2026-93616](#)
- [CVE-2026-85102](#)
- [CVE-2026-94127](#)
- [CVE-2026-93952](#)
- [CVE-2026-87902](#)
- [CVE-2023-52271](#)
- [CVE-2025-61155](#)
- [CVE-2025-1055](#)

1

Adversaries in
Action

- [Meowciety403](#)



Insights

F5 Confirms Active Exploitation of BIG-IP APM Flaw CVE-2026-94127

996 Zyxel Switches Hacked Across 48 Countries: Patch CVE-2026-7273 Now

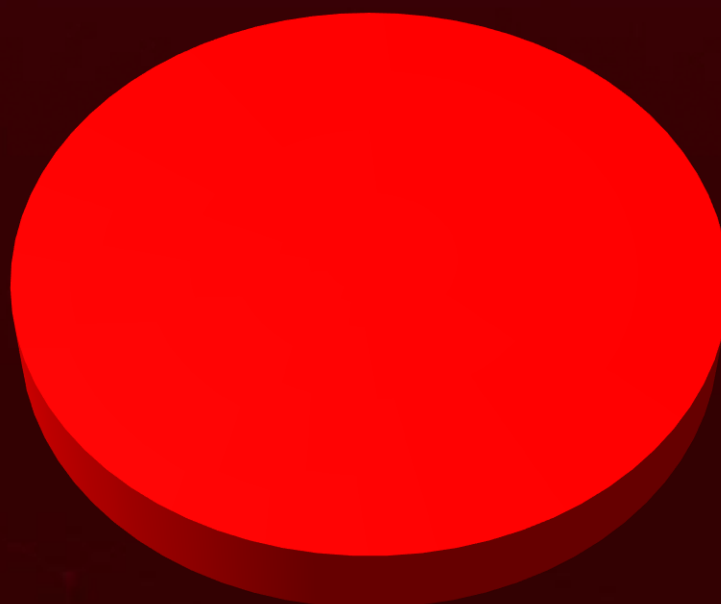
Middle Eastern Manufacturer Hit by PAYLOAD's Encryption-Free Attack

CVE-2026-85102 and CVE-2026-93616: Check Point Warns of Active Attacks on Two Critical Pre-Auth Flaws

CVE-2026-93952: Zero-Day Enables Unauthenticated Privileged Takeover of On-Premises Arista VCO

DragonForce Hides Backdoor Traffic Inside Microsoft Teams Relays

Threat Distribution



■ Ransomware

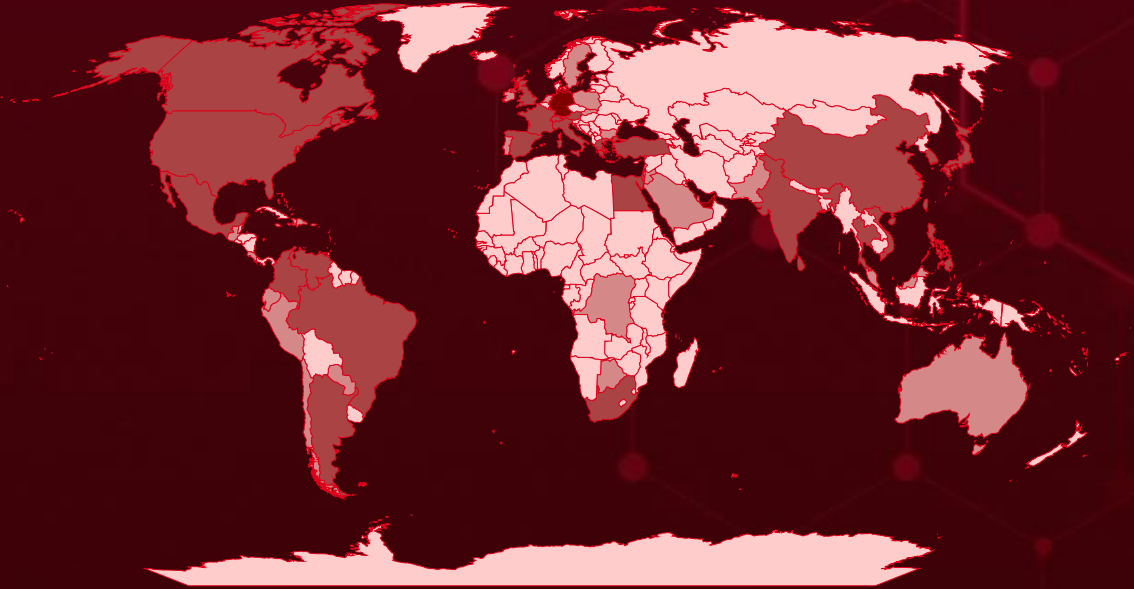


Targeted Countries

Most



Least



Powered by Bing

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

Countries	Countries	Countries	Countries
Germany	Turkey	Saudi Arabia	Georgia
Singapore	Bahrain	Chile	Sierra Leone
United Arab Emirates	United Kingdom	Bulgaria	Barbados
Philippines	Israel	Slovakia	Sudan
Thailand	United States	Jordan	Ghana
Spain	Italy	Lebanon	Tanzania
Brazil	Japan	Armenia	Gibraltar
Vietnam	Costa Rica	Anguilla	Tunisia
Canada	Malaysia	Vanuatu	Belarus
South Africa	Dominican Republic	Bahamas	Denmark
China	Pakistan	Saint Eustatius	Greenland
Switzerland	Guatemala	American Samoa	Zambia
Colombia	Paraguay	Togo	Grenada
Venezuela	Sweden	El Salvador	New Zealand
Egypt	Peru	Niger	Guadeloupe
Mexico	Ecuador	Equatorial Guinea	North Korea
France	Australia	Antigua and Barbuda	Guam
Austria	Netherlands	Estonia	Norway
Argentina	Poland	Scotland	Belgium
South Korea	Haiti	Ethiopia	Panama
Greece	Portugal	Croatia	Guernsey
Sri Lanka	Isle of Man	Faroe Islands	Cambodia
India	Puerto Rico	Uganda	Guinea
Taiwan	Democratic Republic of Congo	Fiji	
	Qatar	Netherland Antilles	
	Jamaica	Finland	
	Republic of Ireland	Northern Cyprus	
	Botswana	Bangladesh	

Targeted Industries



TOP MITRE ATT&CK TTPs

T1059

Command and Scripting Interpreter

T1190

Exploit Public-Facing Application

T1588

Obtain Capabilities

T1588.006

Vulnerabilities

T1027

Obfuscated Files or Information

T1078

Valid Accounts

T1071

Application Layer Protocol

T1562

Impair Defenses

T1068

Exploitation for Privilege Escalation

T1005

Data from Local System

T1021

Remote Services

T1135

Network Share Discovery

T1486

Data Encrypted for Impact

T1489

Service Stop

T1490

Inhibit System Recovery

T1552

Unsecured Credentials

T1499

Endpoint Denial of Service

T1059.003

Windows Command Shell

T1189

Drive-by Compromise

T1204

User Execution

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>PAYLOAD Ransomware</u>	PAYLOAD is a ransomware instead of deploying an encryptor on Windows systems, it turns Active Directory Group Policy into a weapon. The attackers got in through a FortiGate SSL VPN using stolen credentials, gained domain admin-level control, and linked a malicious GPO named "PAYLOAD" at the domain root.	Malicious GPO	-
TYPE		IMPACT	AFFECTED PLATFORM
Ransomware		Wallpaper hijack, Admin lockout, Data exfiltration	Microsoft Active Directory (Group Policy), Fortinet FortiGate SSL VPN, VMware ESXi
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	1CA67AF90400EE6CBBD42175293274A0F5DC05315096CB2E214E4BFE12FFB71F		

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>DragonForce Ransomware</u>	DragonForce, now operating as a ransomware cartel, has deployed Backdoor.Turn, a Go-based backdoor that hides command-and-control inside legitimate Microsoft Teams TURN-relay traffic. It pairs this with multi-driver BYOVD exploitation to terminate security tools at kernel level. Its 32-bit Windows locker then encrypts local files and reachable SMB shares using ChaCha8 and RSA-4096.	DLL sideloading, BYOVD	CVE-2023-52271 CVE-2025-61155 CVE-2025-1055
TYPE		IMPACT	AFFECTED PLATFORM
Ransomware		Data encryption, extortion	Microsoft Windows
ASSOCIATED ACTOR			PATCH DETAILS
-			CVE-2023-52271: Topaz Antifraud (wsftprm.sys) - Fixed in versions above 2.0.0.0. CVE-2025-1055: K7 Security Anti-Malware (K7RKScan.sys) - Fixed in version 23.0.0.10 or later.
IOC TYPE	VALUE		
SHA256	e45b18c93d187aac5c4486f57483bc87580e15def82a312bfb377ff16eb96b22, a4eb9be98d00c961ad8c3329ee80690c1eec98d4c8fa8dd91c371d9ecc451581		

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-2026-7273</u>		Zyxel GS1900-8 (Before 2.90(AAHH.2)C0), GS1900-8HP (Before 2.90(AAHI.2)C0), GS1900-10HP (Before 2.90(AAZI.2)C0), GS1900-16 (Before 2.90(AAHJ.2)C0), GS1900-24 (Before 2.90(AAHL.2)C0), GS1900-24E (Before 2.90(AAHK.2)C0), GS1900-24EP (Before 2.90(ABTO.2)C0), GS1900-24HPv2 (Before 2.90(ABTP.2)C0), GS1900-48 (Before 2.90(AAHN.2)C0), GS1900-48HPv2 (Before 2.90(ABTQ.2)C0)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RAN SOMWARE
NAME	CISA KEV	cpe:2.3:o:zyxel:gs1900-8_firmware:*:*:*:*:*:**,cpe:2.3:o:zyxel:gs1900-8hp_firmware:*:*:*:*:*:**,cpe:2.3:o:zyxel:gs1900-10hp_firmware:*:*:*:*:*:**,cpe:2.3:o:zyxel:gs1900-16_firmware:*:*:*:*:*:**,cpe:2.3:o:zyxel:gs1900-24_firmware:*:*:*:*:*:**,cpe:2.3:o:zyxel:gs1900-24e_firmware:*:*:*:*:*:**,cpe:2.3:o:zyxel:gs1900-24ep_firmware:*:*:*:*:*:**,cpe:2.3:o:zyxel:gs1900-24hpv2_firmware:*:*:*:*:*:**,cpe:2.3:o:zyxel:gs1900-48_firmware:*:*:*:*:*:**,cpe:2.3:o:zyxel:gs1900-48hpv2_firmware:*:*:*:*:*:**	-
Zyxel GS1900 Series Switches Stack-Based Buffer Overflow Vulnerability			
	CWE ID	ASSOCIATED TTPs	
	CWE-121	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-stack-based-buffer-overflow-vulnerability-in-gs1900-series-switches-06-16-2026

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-93616</u>		Check Point Security Management, Multi-Domain Security Management Server, Log Server, Multi-Domain Log Server, SmartEvent (R82.20; R82.10 with Jumbo Hotfix Take 44 or lower; R82 with Take 126 or lower; R81.20 with Take 166 or lower; R81.10 with Take 190 or lower, EoS; R80, R80.10, R80.20, R80.30, R80.40, R81, all EoS)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:checkpoint:security_management:*:*:*:*:*:*	-
Check Point Multiple Products Path Traversal Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-22	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://support.checkpoint.com/results/sk/sk1000171/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-85102</u>		Check Point Security Gateway, Spark Firewall Centrally Managed, Spark Firewall Locally Managed (R81, EoS; R81.10, EoS; R81.10.x; R81.20; R82; R82.00.x; R82.10)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:checkpoint:security_gateway:*.~.*.*.*.*.*.*	-
Check Point Multiple Products Improper Certificate Validation Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	-	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://support.checkpoint.com/results/sk/sk1000117

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-94127</u>		F5 BIG-IP APM (17.1.0 - 17.1.3, 17.5.0 - 17.5.1, 21.1.0)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:f5:big-ip_access_policy_manager:*:*:*:*:*:*	-
F5 BIG-IP APM Heap-based Buffer Overflow Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-122	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://my.f5.com/manage/s/article/K000162605

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-93952</u>		Arista VeloCloud Orchestrator (VCO) On-Prem (5.2.x before 5.2.3.16, 6.1.x through 6.1.3.7, 6.4.x before 6.4.2.8, 7.0.x through 7.0.0.2)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:arista:velocloud_orchestrator:*:*:*:*:*.*	-
Arista VeloCloud Orchestrator Improper Input Validation Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://www.arista.com/en/support/advisories-notices/security-advisory/24765-security-advisory-0183

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-87902</u>		WordPress WordPress Core (4.7.0 – 7.1.1)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:wordpress:wordpress:*.~*~*~*~*~*~*	-
WordPress Unauthenticated Path Traversal Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-98	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://wordpress.org/download/releases/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2023-52271</u>		Topaz Antifraud (wsftprm.sys driver)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:topazevolution:antifraud:*:*:*:*:*:*	DragonForce Ransomware
Topaz Antifraud Improper Access Control Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	-	T1068: Exploitation for Privilege Escalation	Update to the latest version above 2.0.0.0.

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2025-61155</u>		Tower of Fantasy (Gamedriverx64.sys driver)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:hotta_studio:gamedriverx64.sys:*:*:*:*:*:*	DragonForce Ransomware
Hotta Studio GameDriverX64 Improper Access Control Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-400	T1068: Exploitation for Privilege Escalation	

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2025-1055</u>		K7 Security (K7RKScan.sys driver)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	-	DragonForce Ransomware
K7 Computing K7 Security Anti-Malware Missing Authorization Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-862	T1068: Exploitation for Privilege Escalation	K7 Security Anti-Malware (K7RKScan.sys) - Fixed in version 23.0.0.10 or later.



Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 <u>Meowciety403</u> (aka <u>Nekoneko200</u>)	-	Financial Services, Financial Brokerage and Foreign Exchange, Information Technology, IT Consulting, Technology	United Arab Emirates, Singapore, Germany
	MOTIVE		
	Financial Gains, Information Theft		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	-	-	-
TTPs			
TA0001: Initial Access, TA0002: Execution, TA0003: Persistence, TA0005: Defense Evasion, TA0008: Lateral Movement, TA0040: Impact, T1078: Valid Accounts, T1059: Command and Scripting Interpreter, T1547: Boot or Logon AutoStart Execution, T1562: Impair Defenses, T1021: Remote Services, T1021.001: Remote Desktop Protocol, T1080: Taint Shared Content, T1657: Financial Theft			

Recommendations

Security Teams

This digest can be utilized as a driver to force security teams to prioritize the **nine exploited vulnerabilities** and block the indicators related to the threat actor **Meowciety403**, malware **PAYLOAD**, and **DragonForce**.

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 **nine exploited vulnerabilities**.
- Test the efficacy of their security controls by simulating the attacks related to the threat actor **Meowciety403** and malware **PAYLOAD** and **DragonForce** in Breach and Attack Simulation(BAS).

Threat Advisories

[September 2026 Linux Patch Roundup](#)

[Zyxel GS1900 Switches Under Active Attack](#)

[Paws on the Payroll: The Rise of Meowciety403](#)

[Check Point Rushes Fixes as Two Critical Flaws Come Under Active Attack](#)

[CVE-2026-94127: Critical F5 BIG-IP APM Flaw Under Active Exploitation](#)

[Critical Zero-Day in Arista VeloCloud Orchestrator Under Active Attack](#)

[PAYLOAD Ransomware Emerges as a Fast-Growing Extortion Threat](#)

[Race Against the Patch: Critical WordPress RCE Exploited Within Hours](#)

[DragonForce Evolves: Teams-Relayed C2 and BYOVD Kernel Evasion](#)

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>PAYLOAD Ransomware</u>	SHA256	1CA67AF90400EE6CBBD42175293274A0F5DC05315096CB2E214E4BFE12FFB71F
	MD5	E0FD8FF6D39E4C11BDAF860C35FD8DC0, 0108656A3E1ADE6CA4F21B084F5E1208, BEA5E267F24D7DA59F6821BFFDBFF293
	TOR Address	payloadrz5yw227brtbvdqpnlhq3rdcdekdn3rgucbcdeawq2v6vuyd[.]onion, payload6eualw6kni6v2lqn7ovjcl76ojx25z5unsyvqo3lbqy3bo5qd[.]onion, payloadynyvabjacbun4uwhmx7yvdzorycslnleguxjn7glahsvqd[.]onion
<u>DragonForce Ransomware</u>	SHA256	e45b18c93d187aac5c4486f57483bc87580e15def82a312bfb377ff16eb96b22, a4eb9be98d00c961ad8c3329ee80690c1eec98d4c8fa8dd91c371d9ecc451581
	SHA1	55acb53f348c9f6b89343dc8d96522aa75e4cfdb

Attack Name	TYPE	VALUE
<u>DragonForce Ransomware</u>	MD5	bd47ae24b03e5ba0f1ab2e95e7acb989
	File Path	C:\Users\Public\log.log
	TOR Address	3pktcrbcmssvrnwe5skburdwe2h3v6ibdn5kbjqihsg6eu6s6b7ryqd[.]onion, z3wqggtxft7id3ibr7srivv5gjof5fwg76slewnzwwakjuf3nlhukdid[.]onion
	TOX ID	1C054B722BCBF41A918EF3C485712742088F5C3E81B2FDD91ADEA6BA55F4A856D90A65E99D20

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

September 28, 2026 • 6:30 AM

© 2026 All Rights are Reserved by Hive Pro



More at www.hivepro.com