Date of Publication
April 14, 2026

Hive Pro

Hiveforce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities, and Actors

06 to 12 APRIL 2026

Table Of Contents

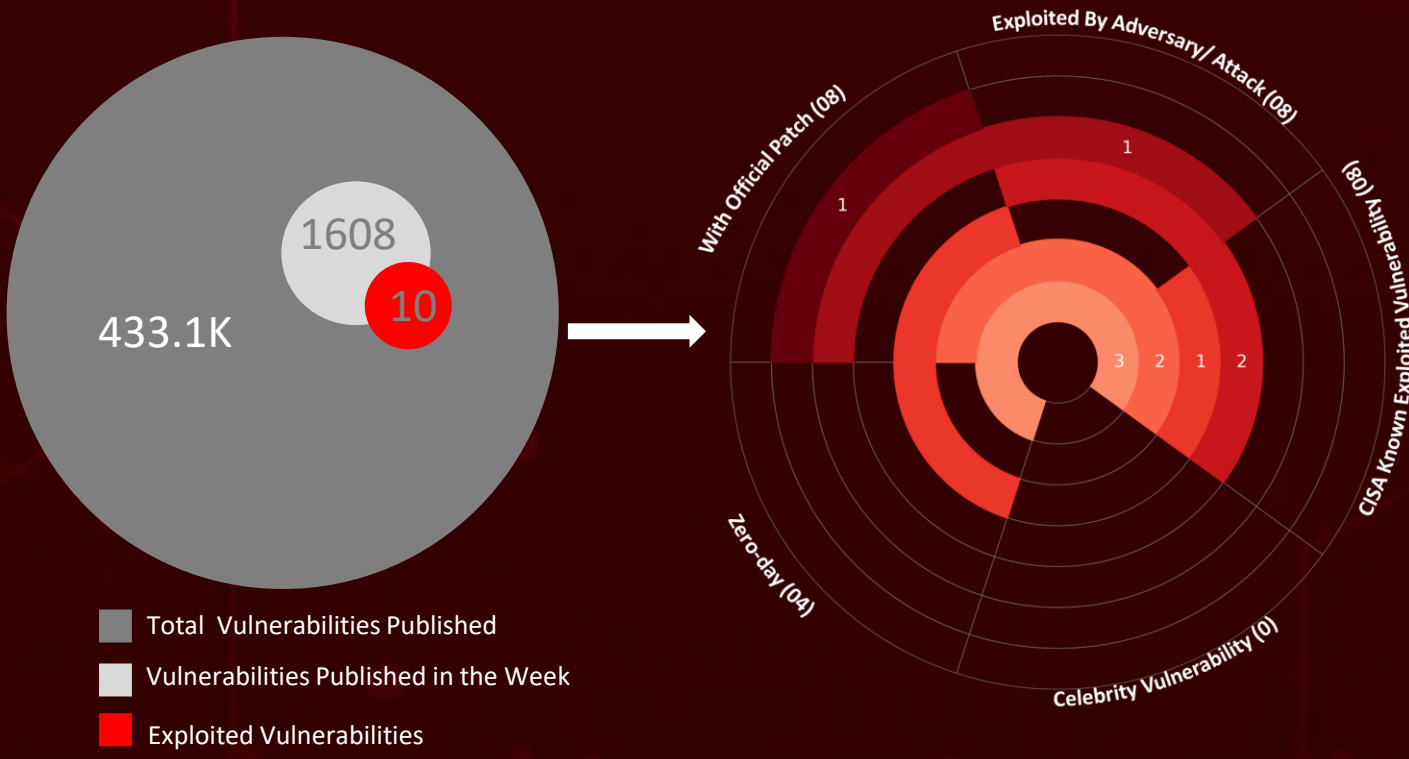
Summary

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

Fortinet has released emergency patches for a critical vulnerability in **FortiClient EMS**, confirming that the flaw is already under active exploitation. Tracked as **CVE-2026-35616**, the issue affects the system's API that handles communication between the EMS server and managed endpoints, raising serious concerns that centralized security control could become an attack surface.

At the same time, multiple zero-day campaigns are unfolding in parallel. The TrueConf Windows client vulnerability (**CVE-2026-3502**) is being exploited in **Operation TrueChaos**, a targeted campaign against government entities in Southeast Asia. In a separate but equally sophisticated effort, **Pawn Storm (APT28)** is leveraging chained zero-day exploits to transform a single user interaction into a full-scale breach, silently infiltrating high-value **Ukrainian and NATO-linked networks**.

Beyond targeted intrusions, large-scale threats continue to expand. **Masjesu**, a commercially operated IoT botnet, is being actively marketed as a DDoS-for-hire service via Telegram. These underscore the need for disciplined security updates and sustained monitoring in response to rapidly evolving attack methodologies.



High Level Statistics

9
Attacks Executed

10
Vulnerabilities Exploited

3
Adversaries in Action

- Havoc
- PrismexDrop
- PrismexLoader
- PrismexStager
- PrismexSheet
- LucidRook
- LucidPawn
- LucidKnight
- Masjesu

- CVE-2026-35616
- CVE-2026-21643
- CVE-2026-3502
- CVE-2023-50224
- CVE-2021-22681
- CVE-2026-21513
- CVE-2026-21509
- CVE-2018-10561
- CVE-2018-10562
- CVE-2024-12847

- APT28
- CyberAv3ngers
- UAT-10362

Insights

Pawn Storm's Hidden Entry: The Zero-Day Chain That Slips Past Every Defense

CVE-2026-35616's Silent Takeover: The Master Key Vulnerability Lurking in FortiClient EMS

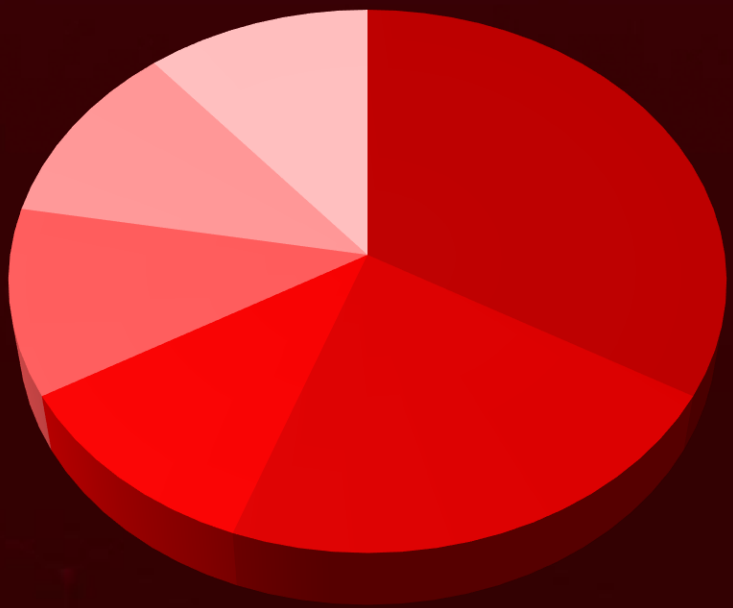
UAT-10362: Precision Phishing With Minimal Footprint

Operation TrueChaos: The TrueConf CVE-2026-3502 Zero-Day That Turned Against Its Users

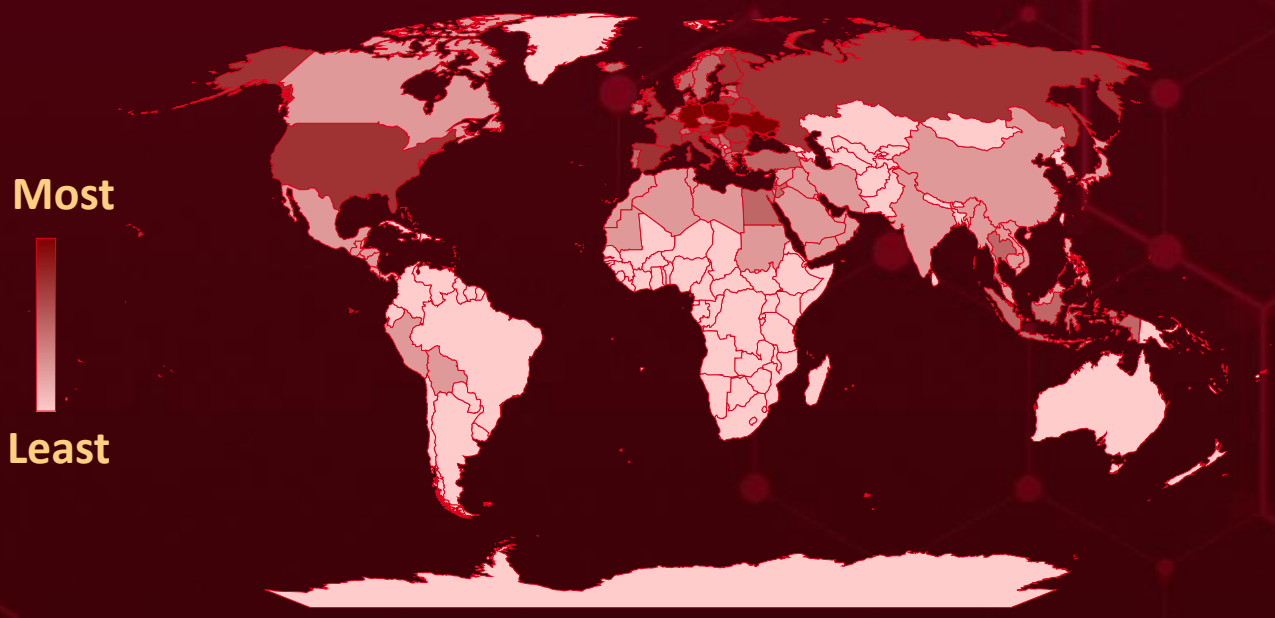
CyberAv3ngers Unleashed: The PLC Attacks Hitting Critical Infrastructure

Masjesu Unmasked: The IoT Botnet Powering DDoS-for-Hire

Threat Distribution

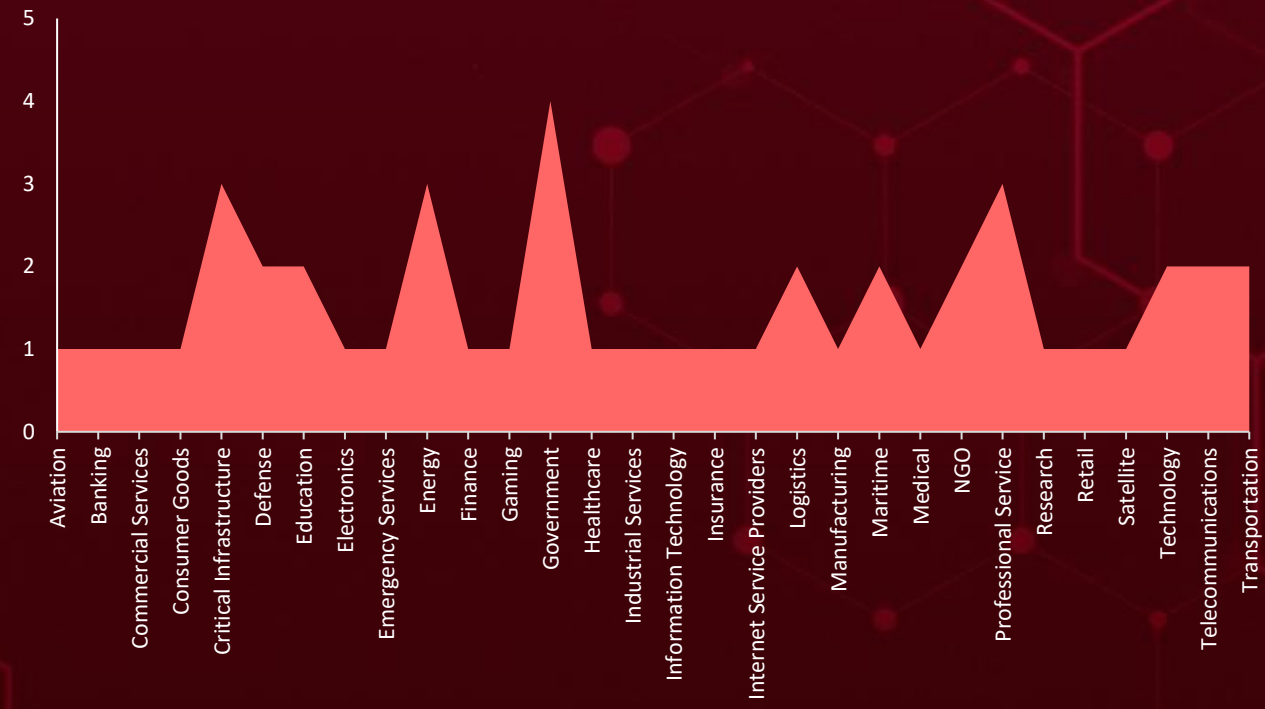


Targeted Countries



Countries	Countries	Countries	Countries
Poland	Jordan	Tunisia	China
Ukraine	Greece	El Salvador	Lebanon
Slovakia	Denmark	Peru	Costa Rica
Germany	Switzerland	Bahrain	Libya
Hungary	Egypt	Cyprus	Sudan
Moldova	Indonesia	Guatemala	Brunei
Croatia	Luxembourg	Morocco	Syria
Romania	Bosnia and Herzegovina	Honduras	Malaysia
France		Oman	Timor-Leste
Finland	Malta	Belize	Mauritania
Austria	San Marino	Qatar	Algeria
Bulgaria	Estonia	India	Mexico
Spain	Singapore	South Korea	Vietnam
Russia	Monaco	Iran	Cambodia
Belarus	Holy See	Czechia	Yemen
Slovenia	Montenegro	Iraq	Congo
United Kingdom	Sweden	United Arab Emirates	Australia
Lithuania	Netherlands		Brazil
Italy	Thailand	Bolivia	South Africa
United States	North Macedonia	Myanmar	Georgia
Portugal	Iceland	Israel	Tonga
Andorra	Norway	Canada	Liberia
Serbia	Belgium	Japan	Comoros
Ireland	Latvia	Panama	Barbados
Turkey	Liechtenstein	Kuwait	Afghanistan
Czech Republic	Saudi Arabia	Philippines	Sri Lanka
Albania	Nicaragua	Laos	Ghana

Targeted Industries



TOP MITRE ATT&CK TTPs

T1059
Command and Scripting Interpreter

T1071
Application Layer Protocol

T1190
Exploit Public-Facing Application

T1036
Masquerading

T1574
Hijack Execution Flow

T1036.005
Match Legitimate Resource Name or Location

T1102
Web Service

T1027
Obfuscated Files or Information

T1204
User Execution

T1059.001
PowerShell

T1078
Valid Accounts

T1547.001
Registry Run Keys / Startup Folder

T1574.001
DLL

T1573
Encrypted Channel

T1048
Exfiltration Over Alternative Protocol

T1547
Boot or Logon Autostart Execution

T1048.003
Exfiltration Over Unencrypted Non-C2 Protocol

T1566
Phishing

T1114
Email Collection

T1057
Process Discovery

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Havoc	Havoc is an open-source command-and-control framework designed for post-exploitation, penetration testing, and adversary simulation. Despite its legitimate purpose, it is frequently repurposed by threat actors to manage and sustain real-world intrusions.	Exploiting vulnerabilities	CVE-2026-3502
		IMPACT	**AFFECTED PLATFORM**
TYPE		Persistent remote access, Surveillance, Privilege escalation	TrueConf Client
Framework			**PATCH LINK**
ASSOCIATED ACTOR			https://trueconf.com/downloads/windows.html
-			
IOC TYPE	**VALUE**		
MD5	248a4d7d4c48478dcbeade8f7dba80b3		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
PrismexDrop	PrismexDrop is a native dropper that initializes the environment for later-stage payloads and establishes persistence through COM hijacking.	Exploiting vulnerabilities	CVE-2026-21513 CVE-2026-21509
		IMPACT	**AFFECTED PRODUCT**
TYPE		Bypasses standard security mechanisms, maintains stealthy persistence	Microsoft Office, Microsoft Windows (MSHTML Framework)
Dropper			**PATCH LINKS**
ASSOCIATED ACTOR			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21509, https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21513
Pawn Storm			
IOC TYPE	**VALUE**		
SHA256	969d2776df0674a1cca0f74c2fccbc43802b4f2b62ecccecc26ed538e9565eae		

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
PrismexLoader	PrismexLoader is a proxy DLL that retrieves embedded payloads from steganographic PNG images using a proprietary “Bit Plane Round Robin” extraction algorithm.	Exploiting vulnerabilities	CVE-2026-21513 CVE-2026-21509
		IMPACT	**AFFECTED PRODUCT**
TYPE		Malware staging, Stealth execution	Microsoft Office, Microsoft Windows (MSHTML Framework)
Loader			**PATCH LINKS**
ASSOCIATED ACTOR			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21509, https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21513
Pawn Storm			
IOC TYPE	**VALUE**		
SHA256	8c1dc9732884c6078b23953b78314a8d0d8b8d9fe42e5f97a7cd09b8ace943a9		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
PrismexStager	PrismexStager is a Covenant Grunt stager that leverages Filen.io cloud storage as a covert command-and-control channel.	Exploiting vulnerabilities	CVE-2026-21513 CVE-2026-21509
		IMPACT	**AFFECTED PRODUCT**
TYPE		Remote control, Data exfiltration	Microsoft Office, Microsoft Windows (MSHTML Framework)
Stager			**PATCH LINKS**
ASSOCIATED ACTOR			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21509, https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21513
Pawn Storm			
IOC TYPE	**VALUE**		
SHA256	57357655a62e3a8b1f4b78e1d3ed7e0f6d59a9bac213087294f91bb7847b2a8f		

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
PrismexSheet	PrismexSheet is a malicious Excel-based dropper that leverages VBA macros to extract steganographically embedded payloads from within the file itself.	Exploiting vulnerabilities	CVE-2026-21513 CVE-2026-21509
		IMPACT	**AFFECTED PRODUCT**
TYPE		Payload extraction, Malware delivery	Microsoft Office, Microsoft Windows (MSHTML Framework)
Dropper			**PATCH LINKS**
ASSOCIATED ACTOR			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21509, https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21513
Pawn Storm			

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
LucidRook	LucidRook is an advanced stager that integrates a Lua interpreter and Rust-compiled libraries within a DLL to retrieve and execute staged Lua bytecode payloads.	Spear-phishing	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		Payload execution, Modular staging	Microsoft Windows
Stager			**PATCH LINK**
ASSOCIATED ACTOR			-
UAT-10362			
IOC TYPE	**VALUE**		
SHA256	edb25fed9df8e9a517188f609b9d1a030682c701c01c0d1b5ce79cba9f7ac809		

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
LucidPawn	LucidPawn is a dropper that employs region-specific anti-analysis checks, manages decoy documents by identifying targeted file extensions, and embeds two AES-encrypted binaries.	Spear-phishing	-
		IMPACT	AFFECTED PRODUCT
TYPE		Anti-analysis evasion, Payload concealment	Microsoft Windows
Dropper			PATCH LINK
ASSOCIATED ACTOR			-
UAT-10362			
IOC TYPE	VALUE		
SHA256	d8bc6047fb3fd4f47b15b4058fa482690b5b72a5e3b3d324c21d7da4435c9964		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
LucidKnight	LucidKnight is a companion reconnaissance tool that profiles targets by exfiltrating system information via Gmail. Implemented as a 64-bit Windows DLL, it incorporates Rust-compiled components to support staged escalation toward full payload deployment.	Spear-phishing	-
		IMPACT	AFFECTED PRODUCT
TYPE		System profiling, Data exfiltration	Microsoft Windows
Reconnaissance tool			PATCH LINK
ASSOCIATED ACTOR			-
UAT-10362			
IOC TYPE	VALUE		
SHA256	d8bc6047fb3fd4f47b15b4058fa482690b5b72a5e3b3d324c21d7da4435c9964		

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 rowspan="2">Masjesu</td><td rowspan="5">Masjesu is a commercially operated IoT botnet that initiates infection by binding to a hardcoded TCP port (55988), enabling direct attacker access. It maintains persistence by creating a cron job that repeatedly executes a renamed, masqueraded process at 15-minute intervals.</td><td>Exploiting Vulnerabilities</td><td>CVE-2018-10561
CVE-2018-10562
CVE-2024-12847</td></tr>
<tr><td>TYPE</td><td>IMPACT</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>Botnet</td><td rowspan="3">Remote access, Persistent control</td><td>Dasan GPON Routers, NETGEAR DGN1000</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td>PATCH LINK</td></tr>
<tr><td>-</td><td>https://www.netgear.com/support/product/dgn1000</td></tr>
<tr><td>IOC TYPE</td><td colspan="3">VALUE</td></tr>
<tr><td>SHA256</td><td colspan="3">f39b67fff1f106fb1b4fa9beb386427c8e7eb010f306ad0445da70bffc855f2e</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 PRODUCT	ASSOCIATED ACTORS
CVE-2026-35616		Fortinet FortiClient EMS version 7.4.5 through 7.4.6	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:fortinet:forticlientems:*:*:*:*:*:*:*:*	-
Fortinet FortiClient EMS Improper Access Control Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-284	T1562.001: Disable or Modify Tools, T1059: Command and scripting interpreter	https://fortiguard.fortinet.com/psirt/FG-IR-26-099

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2026-21643	✗	Fortinet FortiClient EMS 7.4.4	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:fortinet:forticlientems:*:*:*:*:*:*:*:*	-
Fortinet FortiClient EMS Sql Injection Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-89	T1059: Command and scripting interpreter	https://fortiguard.fortinet.com/psirt/FG-IR-25-1142

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2026-3502	✗	TrueConf Client for Windows (versions 8.1.0 through 8.5.2)	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:trueconf:trueconf_client:*:*:*:*:*:windows:*:*	Havoc
TrueConf Client Download of Code Without Integrity Check Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-494	T1195.002: Supply Chain Compromise, T1072: Software Deployment Tools	https://trueconf.com/downloads/windows.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2023-50224		TP-Link WR841N	APT28
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:h:tp-link:tl-wr841n:12:*:*:*:*:*:*:*	-
TP-Link TL-WR841N Authentication Bypass by Spoofing Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-290	T1190: Exploit Public-Facing Application, T1040: Network Sniffing	https://www.tp-link.com/en/support/download/tl-wr841n/v12/#Firmware

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2021-22681		Rockwell Automation Multiple Products: Studio 5000 Logix Designer, Logix Controllers (multiple)	CyberAv3ngers
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:rockwellautomation:factorytalk_services_platform:*:*:*:*:*:*:*:*	-
Rockwell Multiple Products Insufficient Protected Credentials Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-522	T0862: Supply Chain Compromise, T0859: Valid Accounts, T1552.004: Unsecured Credentials: Private Keys	https://www.rockwellautomation.com/es-es/trust-center/security-advisories/advisory.PN1550.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2026-21513	 ZERO-DAY	Windows 10, 11 26H1 Windows Server 2012, 2016, 2025, 2022, 2019	Pawn Storm
		**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	PrismexDrop, PrismexLoader, PrismexStager, PrismexSheet
Microsoft MSHTML Framework Protection Mechanism Failure Vulnerability			
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-693	T1204: User Execution, T1059: Command and Scripting Interpreter	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2026-21513

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2026-21509	 ZERO-DAY	Microsoft Office 2016, 2019 (64-bit edition, 32-bit edition); Microsoft Office LTSC 2024, 2021 (64-bit editions, 32-bit editions); Microsoft 365 Apps for Enterprise (64-bit Systems, 32-bit Systems)	Pawn Storm
		**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:a:microsoft:office:*:*:*:*:*:*:*:* cpe:2.3:a:microsoft:365_apps:*:*:*:*:enterprise:*:*:*	PrismexDrop, PrismexLoader, PrismexStager, PrismexSheet
Microsoft Office Security Feature Bypass Vulnerability			
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-807	T1566: Phishing, T1204: User Execution, T1204.002: Malicious File, T1055: Process Injection	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21509

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2018-10561	✗	Dasan GPON home routers	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:dasannetworks:gpon_router_firmware:*:*:*:*:*:*:*:*	Masjesu botnet (aka XorBot)
Dasan GPON Routers Authentication Bypass Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1556: Modify Authentication, T1059: Command and Scripting Interpreter	✗

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2018-10562	✗	Dasan GPON home routers	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:dasannetworks:gpon_router_firmware:*:*:*:*:*:*:*:*	Masjesu botnet (aka XorBot)
Dasan GPON Routers Command Injection Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter	✗

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2024-12847		NETGEAR DGN1000 before 1.1.00.48	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:h:netgear:dgn1000:-:*:*:*:*:*:*:*	Masjesu botnet (aka XorBot)
NETGEAR DGN1000 authentication bypass vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-306, CWE-78	T1190: Exploit Public-Facing Application, T1040: Network Sniffing	https://www.netgear.com/support/product/dgn1000

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
APT28(aka Sofacy, Fancy Bear, Sednit, Group 74, TG-4127, Pawn Storm, Tsar Team, Strontium, Swallowtail, SIG40, Snakemackerel, Iron Twilight, ATK 5, T-APT-12, ITG05, TAG-0700, UAC-0028, FROZENLAKE, Grey-Cloud, Forest Blizzard, GruesomeLarch, BlueDelta, TA422, Fighting Ursa, Blue Athena, UAC-0063, TAG-110)	Russia	Government, Critical Infrastructure, Information Technology, Telecommunications, Energy, Third-party Email and Cloud Service Providers, Government, Military, Critical Infrastructure, Defense, Emergency Services, Hydrometeorology, Rail Logistics, Maritime and Transport, Humanitarian Aid Organizations	North Africa, Central America, Southeast Asia, Europe, Ukraine, United States, Turkey, Central and Eastern Europe
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCT**
	CVE-2023-50224 CVE-2026-21513 CVE-2026-21509	PrismexDrop, PrismexLoader, PrismexStager, PrismexSheet	TP-Link WR841N, Windows

TTPs

TA0001: Initial Access, T1190: Exploit Public-Facing Application, T1078: Valid Accounts, TA0042: Resource Development, T1583: Acquire Infrastructure, T1583.002: DNS Server, T1583.003: Virtual Private Server, T1588: Obtain Capabilities, T1588.006: Vulnerabilities, T1586: Compromise Accounts, TA0006: Credential Access, T1528: Steal Application Access Token, T1556: Modify Authentication Process, TA0009: Collection, T1557: Adversary-in-the-Middle, TA0003: Persistence, T1584: Compromise Infrastructure T1584.008: Network Devices, TA0043: Reconnaissance, T1595: Active Scanning, TA0011: Command and Control, T1071: Application Layer Protocol, T1071.004: DNS, TA0005: Defense Evasion, T1036: Masquerading

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="4"> 
CyberAv3ngers (aka Hydro Kitten, Shahid Kaveh Group, UNC5691, Storm-0784)</td><td>Iran</td><td rowspan="3">Government, Water and Wastewater Systems (WWS), Energy</td><td rowspan="3">United States</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Sabotage and destruction</td></tr>
<tr><td>TARGETED CVE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>CVE-2021-22681</td><td>-</td><td>Rockwell Automation CompactLogix PLCs, Micro850 PLCs, Rockwell Automation Studio 5000 Logix Designer, RSLogix 5000</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0001: Initial Access, T1190: Exploit Public-Facing Application, T1078: Valid Accounts, TA0002: Execution, T1059: Command and Scripting Interpreter, T1059.001: PowerShell, T1059.007: JavaScript, TA0003: Persistence, T1133: External Remote Services, TA0011: Command and Control, T1102: Web Service, T1571: Non-Standard Port, TA0009: Collection, T1005: Data from Local System, TA0040: Impact, T1565: Data Manipulation, T1565.001: Stored Data Manipulation, T1489: Service Stop</td></tr>
</table>

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="4"> 
UAT-10362</td><td>-</td><td rowspan="2">Non-Governmental Organizations (NGOs), Education (Universities)</td><td rowspan="2">Taiwan</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information Theft, Espionage</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>TARGETED CVE</td><td>-</td><td>LucidRook, LucidPawn, LucidKnight</td><td>Windows</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0001: Initial Access, T1566: Phishing T1566.002: Spearphishing Link, TA0002: Execution, T1059: Command and Scripting Interpreter, T1059.001: PowerShell, T1204: User Execution, T1204.002: Malicious File, TA0003: Persistence, T1547: Boot or Logon Autostart Execution, T1547.001: Registry Run Keys / Startup Folder, TA0005: Defense Evasion, T1574: Hijack Execution Flow, T1574.001: DLL, T1027: Obfuscated Files or Information, T1036: Masquerading, T1036.005: Match Legitimate Name or Location, T1497: Virtualization/Sandbox Evasion, T1140: Deobfuscate/Decode Files or Information, TA0007: Discovery, T1082: System Information Discovery, T1057: Process Discovery, T1614: System Location Discovery, T1614.001: System Language Discovery, TA0009: Collection, T1560: Archive Collected Data, T1560.001: Archive via Utility, TA0011: Command and Control, T1071: Application Layer Protocol, T1071.002: File Transfer Protocols, T1105: Ingress Tool Transfer, T1102: Web Service, TA0010: Exfiltration, T1048: Exfiltration Over Alternative Protocol, T1048.003: Exfiltration Over Unencrypted Non-C2 Protocol, T1041: Exfiltration Over C2 Channel</td></tr>
</table>

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **ten exploitable vulnerabilities** and block the indicators related to the threat actors **APT28, CyberAv3ngers, UAT-10362,** and malware **Havoc, PrismexDrop, PrismexLoader, PrismexStager, PrismexSheet, LucidRook, LucidPawn, LucidKnight, Masjesu.**

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 **ten exploitable vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **APT28, CyberAv3ngers, UAT-10362,** and malware **PrismexDrop, PrismexLoader, PrismexStager, LucidRook, LucidPawn, and Masjesu** in Breach and Attack Simulation(BAS).

Threat Advisories

Fortinet EMS Left Defenseless by CVE-2026-35616

TrueConf Zero-Day Abused in Operation TrueChaos to Weaponize Software Updates

Spraying for Access: Iran-Aligned Actors Turn Weak Credentials into Intelligence

APT28 Exploits SOHO Routers for Large-Scale DNS Hijacking and Credential Theft

Iranian-Affiliated CyberAv3ngers Exploits Internet-Exposed PLCs in U.S.

Pawn Storm's Dual Zero-Day Exploit Unleashed

UAT-10362 Deploys LucidRook Malware Against Taiwanese NGOs

Masjesu: Exploit-Driven Botnet with Stealth, Scale, and Staying Power

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
Havoc	MD5	248a4d7d4c48478dcbeade8f7dba80b3
	IPv4	43[.]134[.]90[.]60, 43[.]134[.]52[.]221, 47[.]237[.]15[.]197
PrismexDrop	SHA256	969d2776df0674a1cca0f74c2fccbc43802b4f2b62ecccecc26ed538e9565eae
PrismexLoader	SHA256	8c1dc9732884c6078b23953b78314a8d0d8b8d9fe42e5f97a7cd09b8ace943a9
PrismexStager	SHA256	57357655a62e3a8b1f4b78e1d3ed7e0f6d59a9bac213087294f91bb7847b2a8f
LucidRook	SHA256	11ae897d79548b6b44da75f7ab335a0585f47886ce22b371f6d340968dbed9ae, edb25fed9df8e9a517188f609b9d1a030682c701c01c0d1b5ce79cba9f7ac809, 0305e89110744077d8db8618827351a03bce5b11ef5815a72c64eea009304a34
LucidPawn	SHA256	6aba7b5a9b4f7ad4203f26f3fb539911369aeef502d43af23aa3646d91280ad9, bdc5417ffba758b6d0a359b252ba047b59aacf1d217a8b664554256b5adb071d, d8bc6047fb3fd4f47b15b4058fa482690b5b72a5e3b3d324c21d7da4435c9964

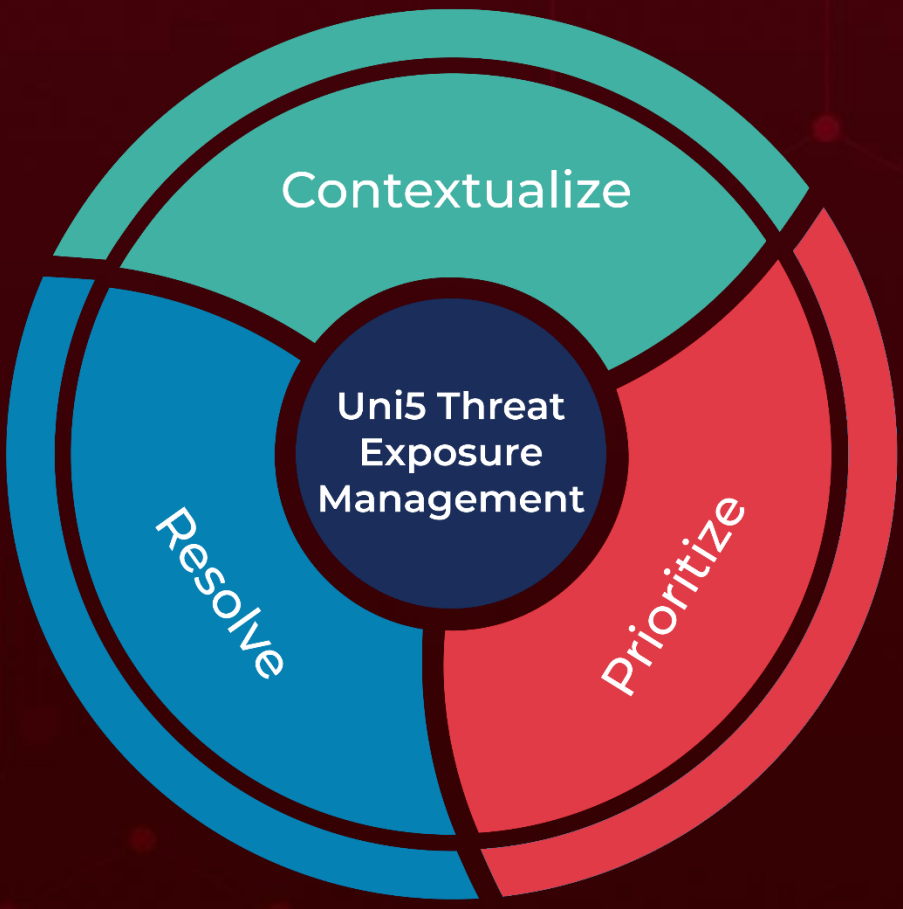
Attack Name	TYPE	VALUE
LucidKnight	SHA256	d8bc6047fb3fd4f47b15b4058fa482690b5b72a5e3b3d324c21d7da4435c9964, aa7a3e8b59b5495f6eebc19f0654b93bb01fd2fa2932458179a8ae85fb4b8ec1
Masjesu	SHA256	f39b67fff1f106fb1b4fa9beb386427c8e7eb010f306ad0445da70bffc855f2e, dfd830368724f6abcc542bc8b85e3d5fa2aedf8282d3805d0d6d53f45c7e0937, de5fb68023465cb5d8ace412e11032d98a41bd6af2a83245c046020530130496, d8018e31b77b135ed300a988757f409347d013b76f9c9a4972e48cb715f45967, cb4a3665ebd12bdb094b9fc188793c67ec3008363a49b1dde00d488b54df984b, b53d4781bbadb17014da280e274e11f2de9063a35f2eabd32d4596707b147306, 4190491b9006404cab256d66125bd77b1c3a0e63451fbb3d829617d7e87acc9b, 85758df12964024af3ae829e3630f9ad5de7c55dae00181198033da8816e3293, 8340ff8920412a70f0c29cdf72f6f218e61142b3f210e70e24811c413971a8ed, 620f6949b82f9ef987b7511fbbb09c2da57d8be47b019fa6a9686ce08b4c3e70, 87f11a3ee2486bc4845a28465c2e70d2d9f98725edf4a73c3359c23a43ed74b7, 9c683b0be86d4cd274a7a16073bdf092218f259b055a72f848d589574e9b8084, 8ce9145fee0d3d2444554d901b334c36e71bb1346280ada7ff366cf9d25c5938

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

April 14, 2026 • 3:00 AM

More at www.hivepro.com