

Date of Publication  
January 06, 2025



HiveForce Labs

WEEKLY

# THREAT DIGEST

**Attacks, Vulnerabilities and Actors**

30 DECEMBER 2024 to 05 JANUARY 2025

# Table Of Contents

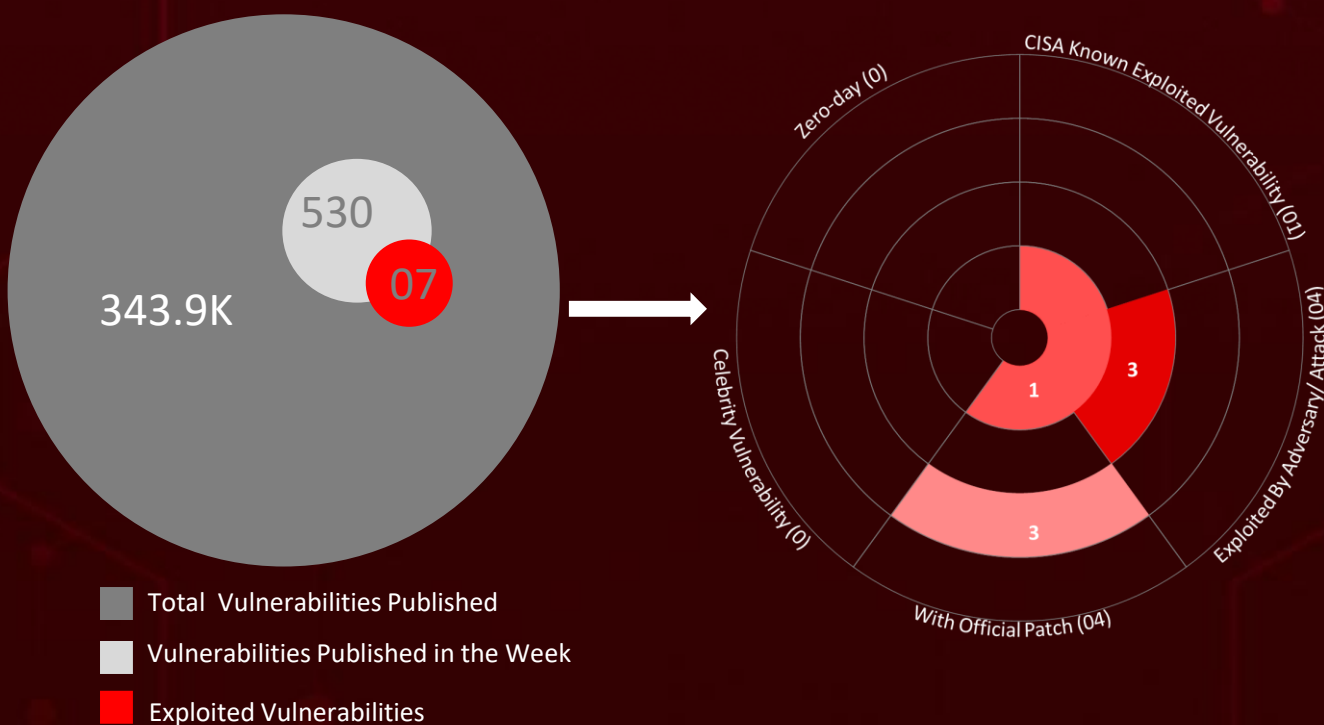
<u>Summary</u>	03
<u>High Level Statistics</u>	04
<u>Insights</u>	05
<u>Targeted Countries</u>	06
<u>Targeted Industries</u>	07
<u>Top MITRE ATT&amp;CK TTPs</u>	07
<u>Attacks Executed</u>	08
<u>Vulnerabilities Exploited</u>	14
<u>Adversaries in Action</u>	18
<u>Recommendations</u>	19
<u>Threat Advisories</u>	20
<u>Appendix</u>	21
<u>What Next?</u>	24

# Summary

HiveForce Labs has identified a surge in cybersecurity threats, highlighting the increasing complexity and frequency of cyber incidents. Over the past week, **seven** major attacks were detected, **seven** critical vulnerabilities were actively exploited, and **one** threat actor group was closely monitored, reflecting a relentless rise in malicious activities.

Recent botnet activity highlights the increasing threat to cybersecurity, with FICORA (a Mirai variant) and CAPSAICIN (a Kaiten variant) **exploiting vulnerabilities in D-Link routers** via the Home Network Administration Protocol (HNAP). Concurrently, the **Paper Werewolf** cyberespionage group, active since 2022, has been targeting Russian organizations using phishing emails embedded with malicious macros to deploy PowerRAT for unauthorized access and data exfiltration.

Adding to the concern, a malicious npm package named 'ethereumvulncontracthandler' poses as a tool for identifying Ethereum smart contract vulnerabilities but instead delivers the **Quasar Remote Access Trojan** (RAT). These developments highlight the advanced techniques employed by threat actors and reinforce the critical need for robust, proactive cybersecurity strategies to address the rapidly evolving global threat landscape.



# High Level Statistics

7

Attacks  
Executed

7

Vulnerabilities  
Exploited

1

Adversaries in  
Action

- [FICORA](#)
- [CAPSAICIN](#)
- [Quasar](#)
- [NonEuclid](#)
- [PowerRAT](#)
- [PowerTaskel](#)
- [QwakMyAgent](#)

- [CVE-2024-52046](#)
- [CVE-2015-2051](#)
- [CVE-2019-10891](#)
- [CVE-2022-37056](#)
- [CVE-2024-33112](#)
- [CVE-2024-49112](#)
- [CVE-2024-49113](#)

- [Paper Werewolf](#)

# Insights

Protect Against Botnet Infiltration: Update Your **D-Link Router** Firmware Today

**CVE-2024-52046**: Stop RCE Threats Patch **Apache MINA** Before It's Too Late

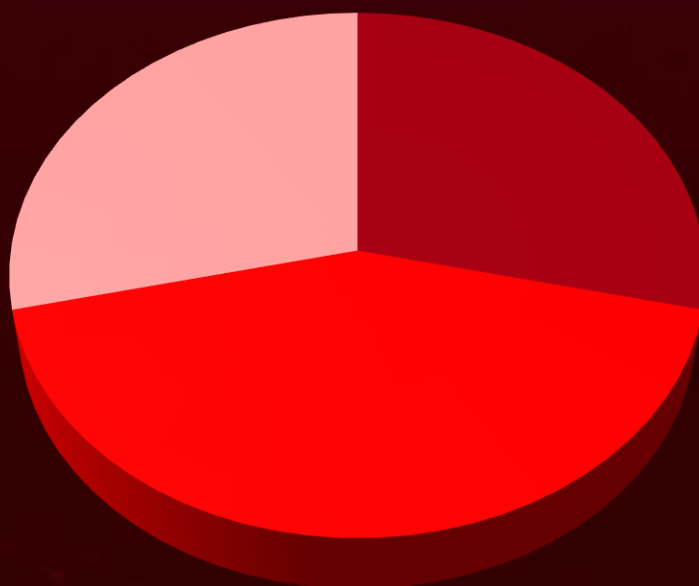
Persistence Perfected **NonEuclid RAT** Evades Detection with Ease

**FICORA** Botnet Brute Forces Routers **CAPSAICIN** Wipes Out Rivals

**Paper Werewolf's** Destructive Cyberattacks Shake **Russian Organizations**

Beware Fake **npm** Tools **Quasar RAT** Hidden in **Ethereum** Package

### Threat Distribution



■ Botnet

■ RAT

■ Hack Tool

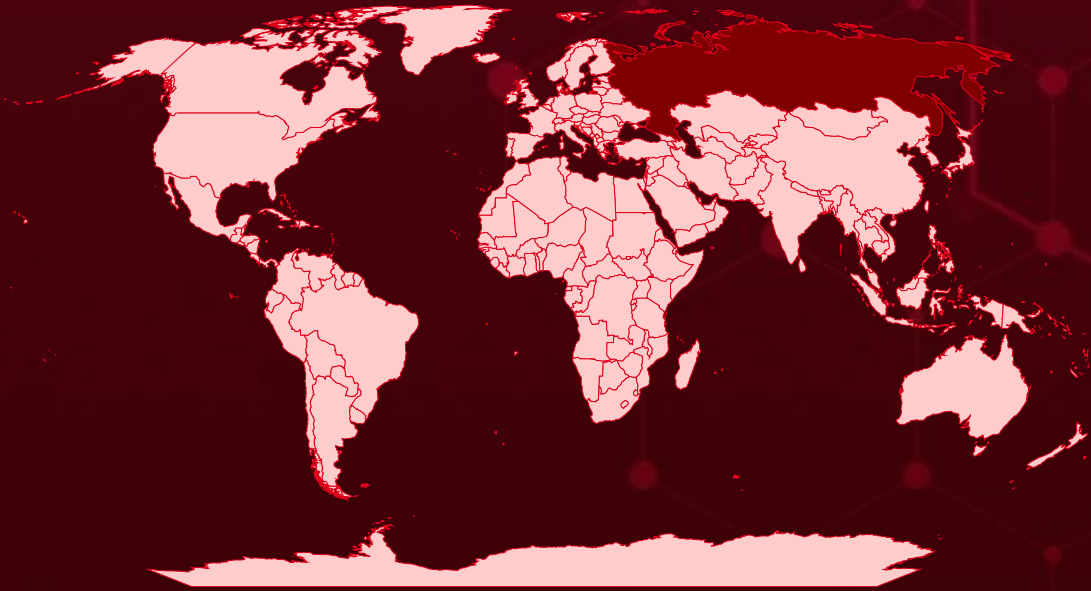


# Targeted Countries

Most



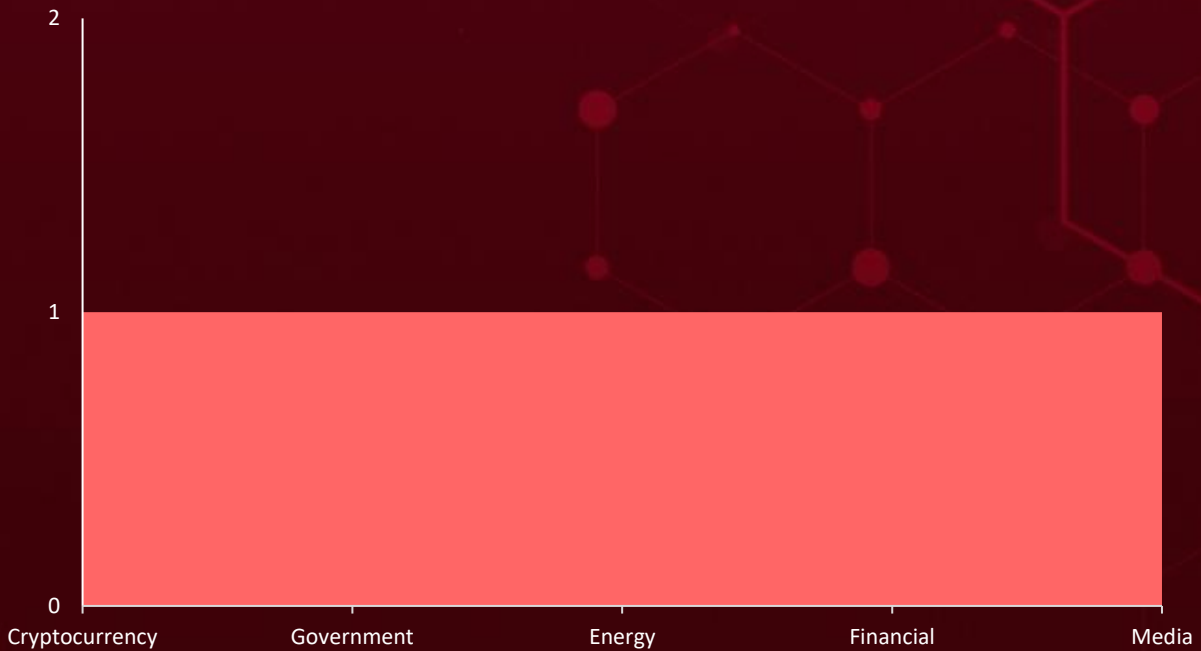
Least



Powered by Bing  
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

Countries	Countries	Countries	Countries
Russia	Morocco	Burundi	Suriname
North Macedonia	Barbados	Mongolia	Croatia
Zambia	Nicaragua	Cabo Verde	Tajikistan
South Sudan	Belarus	Myanmar	Cuba
Algeria	Palau	Cambodia	Togo
Moldova	Belgium	Netherlands	Cyprus
Andorra	Qatar	Cameroon	Turkey
Saint Lucia	Belize	Nigeria	Czech Republic
Angola	Saudi Arabia	Canada	Ukraine
Trinidad and Tobago	Benin	Oman	Denmark
Antigua and Barbuda	Solomon Islands	Central African Republic	Uruguay
Maldives	Bhutan	Papua New Guinea	Djibouti
Argentina	State of Palestine	Chad	Vietnam
Nauru	Bolivia	Poland	Dominica
Armenia	Thailand	Chile	Afghanistan
Peru	Bosnia and Herzegovina	Rwanda	Dominican Republic
Australia	Tuvalu	China	Lithuania
Sierra Leone	Botswana	San Marino	DR Congo
Austria	Vanuatu	Colombia	Madagascar
Switzerland	Brazil	Serbia	Ecuador
Azerbaijan	Liechtenstein	Comoros	Malaysia
United Kingdom	Brunei	Slovakia	Egypt
Bahamas	Malawi	Congo	Mali
Luxembourg	Bulgaria	South Africa	El Salvador
Bahrain	Malta	Costa Rica	Marshall Islands
Mauritania	Burkina Faso	Sri Lanka	Equatorial Guinea
Bangladesh	Mexico	Côte d'Ivoire	Mauritius
			Eritrea

# Targeted Industries



## TOP MITRE ATT&CK TTPs

### T1059

Command and Scripting Interpreter

### T1071

Application Layer Protocol

### T1027

Obfuscated Files or Information

### T1071.001

Web Protocols

### T1547.001

Registry Run Keys / Startup Folder

### T1588

Obtain Capabilities

### T1203

Exploitation for Client Execution

### T1033

System Owner/User Discovery

### T1505

Server Software Component

### T1068

Exploitation for Privilege Escalation

### T1059.001

PowerShell

### T1070

Indicator Removal

### T1498

Network Denial of Service

### T1041

Exfiltration Over C2 Channel

### T1547

Boot or Logon Autostart Execution

### T1588.006

Vulnerabilities

### T1562

Impair Defenses

### T1562.001

Disable or Modify Tools

### T1056

Input Capture

### T1082

System Information Discovery

# ✂ Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<b><u>FICORA</u></b>	<p>The FICORA botnet employs a shell script called "multi" to initiate its attacks. This script uses multiple download methods, to retrieve the FICORA malware, executing and then removing itself to evade detection. Beyond delivery, the script incorporates brute-force capabilities with hard-coded credentials to compromise additional Linux systems, expanding the botnet's reach. Once deployed, FICORA is primed for disruption, conducting distributed denial-of-service (DDoS) attacks through techniques like UDP flooding, TCP flooding, and DNS amplification.</p>	Exploiting Vulnerabilities	CVE-2015-2051 CVE-2019-10891 CVE-2022-37056 CVE-2024-33112
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
Botnet		System Compromise, DDoS	Multiple D-Link Routers
<b>ASSOCIATED ACTOR</b>			<b>PATCH LINK</b>
-	-	-	Patch Link for CVE-2015-2051: <a href="https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10051">https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10051</a>
<b>IOC TYPE</b>	<b>VALUE</b>		
SHA256	9b161a32d89f9b19d40cd4c21d436c1daf208b5d159ffe1df7ad5fd1a57610e5, faeea9d5091384195e87caae9dd88010c9a2b3b2c88ae9cac8d79fd94f250e9f, 10d7aedc963ea77302b967aad100d7dd90d95abcbdb099c5a0a2df309c52c32b8		

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
<b><u>CAPSAICIN</u></b>	The CAPSAICIN is a botnet that begins its operations with a downloader script named "bins.sh", designed to retrieve its malicious payload and establish a connection to its command-and-control (C2) server. Upon compromising a system, CAPSAICIN transmits system information back to the C2 server and waits for further instructions. These commands enable it to perform various functions, including launching distributed denial-of-service (DDoS) attacks, making it a versatile and potentially disruptive threat.	Exploiting Vulnerabilities	CVE-2015-2051 CVE-2019-10891 CVE-2022-37056 CVE-2024-33112
		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
		System Compromise, DDoS	Multiple D-Link Routers
			<b>PATCH LINK</b>
<b>TYPE</b> Botnet			
<b>ASSOCIATED ACTOR</b>			
-			Patch Link for CVE-2015-2051: <a href="https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10051">https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10051</a>
<b>IOC TYPE</b>	<b>VALUE</b>		
SHA256	8349ba17f028b6a17aaa09cd17f1107409611a0734e06e6047ccc33e8ff669b0, b3ad8409d82500e790e6599337abe4d6edf5bd4c6737f8357d19edd82c88b064, Ec87dc841af77ec2987f3e8ae316143218e9557e281ca13fb954536aa9f9caf1		

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
<u>Quasar</u>	<p>Quasar RAT is a remote access trojan (RAT) written in .NET, designed to target Windows devices. Known for being open-source and fully functional, it has become a popular tool among attackers due to its accessibility and flexibility. While its open-source nature allows legitimate use, cybercriminals frequently pack the malware to obfuscate its source code and hinder analysis.</p> <p>Once deployed, Quasar RAT enables attackers to gain unauthorized remote control of infected systems. Its capabilities include spying on victims, stealing sensitive information, and deploying additional malware.</p>	Masqueraded as Malicious npm package	-
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
RAT			Windows
<b>ASSOCIATED ACTOR</b>			<b>PATCH LINK</b>
-			-
<b>IOC TYPE</b>	<b>VALUE</b>		
SHA256	9c3d53c7723bfdd037df85de4c26efcd5e6f4ad58cc24f7a38a774bf22de3876		
IPv4	154[.]216[.]17[.]47		

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
<u>NonEuclid</u>	<p>NonEuclid Remote Access Trojan (RAT) is a powerful C# malware designed to grant unauthorized control over victim computers while evading detection. This stealthy RAT employs advanced tactics, including antivirus bypass, privilege escalation, AES encryption, and anti-virtual machine checks, to ensure persistence and resilience.</p>	-	-
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
RAT		<p>Unauthorized Remote Control, Privilege Escalation, Data Theft, and Exfiltration</p>	-
<b>ASSOCIATED ACTOR</b>			<b>PATCH LINK</b>
-			-
<b>IOC TYPE</b>	<b>VALUE</b>		
SHA256	d32585b207fd3e2ce87dc2ea33890a445d68a4001ea923daa750d32b5de52bf0, 0521aeba49554242674994b1a8881e819c24f0047870d7e1d120deed76895b55		

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
<u>PowerRAT</u>	PowerRAT is a PowerShell-based reverse shell that facilitates remote control over a compromised system and employs various techniques to evade detection, such as hiding malicious files using environment variables and encrypting payloads.	Phishing emails	-
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
RAT		System Compromise and Control, Malware Persistence	Windows
<b>ASSOCIATED ACTOR</b>			<b>PATCH LINK</b>
Paper Werewolf			-
<b>IOC TYPE</b>	<b>VALUE</b>		
SHA256	13252199b18d5257a60f57de95d8c6be7d7973df7f957bca8c2f31e15fcc947b		
IPv4	94[.]103[.]85[.]47		




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
<a href="#"><u>PowerTaskel</u></a>	<p>PowerTaskel is a PowerShell-based tool used by the Paper Werewolf cyberespionage group for remote command execution, data collection, and maintaining persistence on compromised systems. It integrates seamlessly with post-exploitation frameworks, enabling stealthy operations and evasion of detection mechanisms. Designed for flexibility, it supports advanced tasks such as file manipulation, process management, and network reconnaissance.</p>	Phishing emails	-
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
Hack Tool		<p>Compromise of Sensitive Data, Persistence on Target Systems</p>	Windows
<b>ASSOCIATED ACTOR</b>			<b>PATCH LINK</b>
Paper Werewolf			-




NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<a href="#"><u>QwakMyAgent</u></a>	<p>QwakMyAgent is a PowerShell script, previously undetected, that functions as a non-public Mythic modular agent. During execution, the script sends information about the infected system and cyclically receives and processes commands from the server.</p>	Phishing emails	-
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
Hack Tool		<p>Data Exfiltration, Remote Command Execution</p>	Windows
<b>ASSOCIATED ACTOR</b>			<b>PATCH LINK</b>
Paper Werewolf			-

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
<a href="#">CVE-2024-52046</a>		Apache MINA 2.0 through 2.0.26, Apache MINA 2.1 through 2.1.9, Apache MINA 2.2 through 2.2.3	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:apache:mina:*:*:*:*:*:*	-
Apache MINA Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-94	T1059: Command and Scripting Interpreter	<a href="https://mina.apache.org/downloads-mina_2_0.html">https://mina.apache.org/downloads-mina_2_0.html</a>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u><a href="#">CVE-2015-2051</a></u>		D-Link DIR-645 Router	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:dlink:dir-645_firmware:*:*:*:*:*:*:*	FICORA and CAPSAICIN
D-Link DIR-645 Router Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-77	T1059: Command and Scripting Interpreter	<a href="https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10051">https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10051</a>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u><a href="#">CVE-2019-10891</a></u>		D-Link DIR-806 Router	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:dlink:dir-806_firmware:-:*:*:*:*:*:*	FICORA and CAPSAICIN
D-Link DIR-806 Router Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter	EOL

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#"><u>CVE-2022-37056</u></a>		D-Link Go-RT-AC750 Router	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:dlink:go-rt-ac750_firmware:reva_1.01b03:*.~.*.*.*.*.*.*	FICORA and CAPSAICIN
D-Link Go-RT-AC750 Command Injection Vulnerability		cpe:2.3:o:dlink:go-rt-ac750_firmware:revb_2.00b02:*.~.*.*.*.*.*.*	
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter	EOL


CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#"><u>CVE-2024-33112</u></a>		D-Link DIR-845L router	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:d-link:dir-845l:*.~.*.*.*.*.*.*	FICORA and CAPSAICIN
D-Link DIR-845L router Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-77	T1059: Command and Scripting Interpreter	EOL



CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#"><u>CVE-2024-49112</u></a>		Windows: 10 - 11 24H2 Windows Server: 2008 – 2025	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows :*:*:*:*:*:*:*	-
Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability		cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*	-
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-190	T1059: Command and Scripting Interpreter	<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49112">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49112</a>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#"><u>CVE-2024-49113</u></a>		Windows: 10 - 11 24H2 Windows Server: 2008 – 2025	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows :*:*:*:*:*:*:*	-
Windows Lightweight Directory Access Protocol (LDAP) Denial of Service Vulnerability		cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*	-
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-125	T1498: Network Denial of Service	<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49113">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49113</a>

# Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRY
 <u>Paper Werewolf (aka GOFFEE)</u>	-	Government, Energy, Financial, and Media	Russia
	<b>MOTIVE</b> Espionage and Destruction		
	<b>TARGETED CVEs</b>	<b>ASSOCIATED ATTACKS/RANSOM WARE</b>	<b>AFFECTED PRODUCTS</b>
	-	PowerRAT, PowerTaskel and QwakMyAgent	Windows

## TTPs

TA0005: Defense Evasion; TA0007: Discovery; TA0042: Resource Development; TA0008: Lateral Movement; TA0002: Execution; TA0001: Initial Access; TA0040: Impact; TA0011: Command and Control; TA0003: Persistence; TA0006: Credential Access; T1583: Acquire Infrastructure; T1583.001: Domains; T1008: Fallback Channels; T1583.003: Virtual Private Server; T1105: Ingress Tool Transfer; T1587: Develop Capabilities; T1587.001: Malware; T1608.001: Upload Malware; T1588: Obtain Capabilities; T1566: Phishing; T1588.002: Tool; T1059.001: PowerShell; T1059.005: Visual Basic; T1204: User Execution; T1505: Server Software Component; T1564: Hide Artifacts; T1204.002: Malicious File; T1547: Boot or Logon Autostart Execution; T1505.004: IIS Components; T1027.009: Embedded Payloads; T1056: Input Capture; T1529: System Shutdown/Reboot; T1485: Data Destruction; T1564.001: Hidden Files and Directories; T1027.011: Fileless Storage; T1082: System Information Discovery; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1027.007: Dynamic API Resolution; T1027.013: Encrypted/Encoded File; T1033: System Owner/User Discovery; T1573: Encrypted Channel; T1608: Stage Capabilities; T1059: Command and Scripting Interpreter; T1547.001: Registry Run Keys / Startup Folder; T1140: Deobfuscate/Decode Files or Information; T1027: Obfuscated Files or Information; T1056.003: Web Portal Capture; T1570: Lateral Tool Transfer; T1573.002: Asymmetric Cryptography

# Recommendations

## Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **seven exploited vulnerabilities** and block the indicators related to the threat actor **Paper Werewolf**, and malware **FICORA, CAPSAICIN, Quasar, NonEuclid, PowerRAT, PowerTaskel, QwakMyAgent**.

## 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 **seven exploited vulnerabilities**.
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **Paper Werewolf**, and malware **FICORA, CAPSAICIN, Quasar RAT, PowerRAT, Owowa Infostealer** in Breach and Attack Simulation(BAS).

# Threat Advisories

[Critical Apache MINA Flaw Exposes Systems to Remote Code Execution](#)

[FICORA and CAPSAICIN Botnets Target Unpatched D-Link Devices](#)

[Quasar RAT Hidden in npm Package Targets Ethereum Developers](#)

[Ransomware Meets RAT NonEuclid's Destructive Capabilities Revealed](#)

[Paper Werewolf: A Cyberespionage Group Turning to Destruction](#)

[Microsoft's December 2024 Patch Tuesday Addresses 72 Vulnerabilities](#)

# 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
<b><u>FICORA</u></b>	SHA256	9b161a32d89f9b19d40cd4c21d436c1daf208b5d159ffe1df7ad5fd1a57610e5, faeea9d5091384195e87caae9dd88010c9a2b3b2c88ae9cac8d79fd94f250e9f, 10d7aedc963ea77302b967aad100d7dd90d95abcdb099c5a0a2df309c52c32b8, 7f6912de8bef9ced5b9018401452278570b4264bb1e935292575f2c3a0616ec4, a06fd0b8936f5b2370db5f7ec933d53bd8a1bf5042cdc5c052390d1ecc7c0e07, 764a03bf28f9eec50a1bd994308e977a64201fbe5d41337bdcc942c74861bcd3, df176fb8cfbc7512c77673f862e73833641ebb0d43213492c168f99302dcd5e3, ac2df391ede03df27bcf238077d2dddcd24cd86f16202c5c51ecd31b7596a68, ca3f6dce945ccad5a50ea01262b2d42171f893632fc5c5b8ce4499990e978e5b, afee245b6f999f6b9d0dd997436df5f2abfb3c8d2a8811ff57e3c21637207d62, ec508df7cb142a639b0c33f710d5e49c29a5a578521b6306bee28012aadde4a8
	URLs	hxxp[://]103[.]149[.]87[.]69/multi, hxxp[://]103[.]149[.]87[.]69/la[.]bot[.]arc, hxxp[://]103[.]149[.]87[.]69/la[.]bot[.]arm, hxxp[://]103[.]149[.]87[.]69/la[.]bot[.]arm5, hxxp[://]103[.]149[.]87[.]69/la[.]bot[.]arm6, hxxp[://]103[.]149[.]87[.]69/la[.]bot[.]arm7, hxxp[://]103[.]149[.]87[.]69/la[.]bot[.]m68k,

Attack Name	TYPE	VALUE
<b><u>FICORA</u></b>	URLs	hxxp[:]//[103[.]149[.]87[.]69/la[.]bot[.]mips, hxxp[:]//[103[.]149[.]87[.]69/la[.]bot[.]mipsel, hxxp[:]//[103[.]149[.]87[.]69/la[.]bot[.]powerpc, hxxp[:]//[103[.]149[.]87[.]69/la[.]bot[.]sh4, hxxp[:]//[103[.]149[.]87[.]69/la[.]bot[.]sparc
<b><u>CAPSAICIN</u></b>	SHA256	8349ba17f028b6a17aaa09cd17f1107409611a0734e06e6047ccc33e 8ff669b0, b3ad8409d82500e790e6599337abe4d6edf5bd4c6737f8357d19edd 82c88b064, ec87dc841af77ec2987f3e8ae316143218e9557e281ca13fb954536a a9f9caf1, 784c9711eadceb7fedf022b7d7f00cff7a75d05c18ff726e257602e3a3 ccccc1, bde6ef047e0880ac7ef02e56eb87d5bc39116e98ef97a5b1960e9a55 cea5082b, c7be8d1b8948e1cb095d46376ced64367718ed2d9270c2fc99c7052 a9d1ffed7, 4600703535e35b464f0198a1fa95e3668a0c956ab68ce7b719c2803 1d69b86ff, 6e3ef9404817e168c974000205b27723bc93abd7fbf0581c16bb5d2e 1c5c6e4a, 32e66b87f47245a892b102b7141d3845540b270c278e221f5028077 58a4e5dee, 540c00e6c0b53332128b605b0d5e0926db0560a541bb13448d0947 64844763df, b74dbd02b7ebb51700f3c5900283e46570fe497f9b415d25a029623 118073519, 148f6b990fc1f1903287cd5c20276664b332dd3ba8d58f2bf8c26334c 93c3af5, 464e2f1faab2a40db44f118f7c3d1f9b300297fe6ced83fabe87563fc8 2efe95, b699cd64b9895cdcc325d7dd96c9eca623d3ec0247d20f393235471 32c8fa63b, 1007f5613a91a5d4170f28e24bfa704c8a63d95a2b4d033ff2bff7e2f e3dcffe, 7a815d4ca3771de8a71cde2bdacf951bf48ea5854eb0a2af5db7d13a d51c44ab, d6a2a2200d68d79caae482d8cf092c2d84d55dccee05e179a961c7 2f77b1ba, 7ab36a93f009058e60c8a45b900c1c7ae38c96005a43a39e45be9dc7 af9d6da8, 803abfe19cdc6c0c41acfeb210a2361cab96d5926b2c43e5eb3b589a 6ed189ad, 7b29053306f194ca75021952f97f894d8eae6d2e1d02939df37b62d3 845bfd7b, 59704cf55b9fa439d6f7a36821a50178e9d73ddc5407ff340460c054 d7defc54, aaa49b7b4f1e71623c42bc77bb7aa40534bcb7312da511b041799bf 0e1a63ee7,

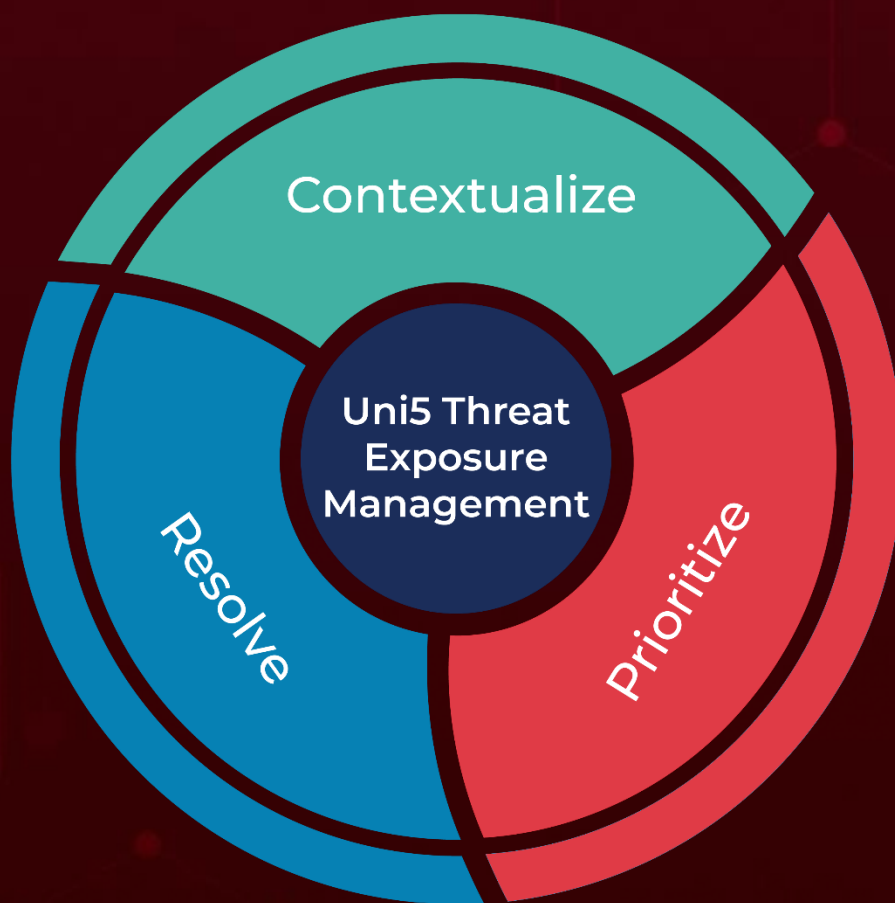
Attack Name	TYPE	VALUE
<b><u>CAPSAICIN</u></b>	SHA256	1ca1d5a53c4379c3015c74af2b18c1d9285ac1a48d515f9b7827e4f900a61bde
	URLs	hxxp://[87[.]11[.]174[.]141/bins[.]sh, hxxp://pirati[.]abuser[.]eu/yakuza[.]yak[.]sh, hxxp://pirati[.]abuser[.]eu/yakuza[.]arm5, hxxp://pirati[.]abuser[.]eu/yakuza[.]arm6, hxxp://pirati[.]abuser[.]eu/yakuza[.]arm7, hxxp://pirati[.]abuser[.]eu/yakuza[.]i586, hxxp://pirati[.]abuser[.]eu/yakuza[.]i686, hxxp://pirati[.]abuser[.]eu/yakuza[.]m68k, hxxp://pirati[.]abuser[.]eu/yakuza[.]mips, hxxp://pirati[.]abuser[.]eu/yakuza[.]mipsel, hxxp://pirati[.]abuser[.]eu/yakuza[.]ppc, hxxp://pirati[.]abuser[.]eu/yakuza[.]sparc, hxxp://pirati[.]abuser[.]eu/yakuza[.]x86, hxxp://[87[.]10[.]220[.]221/bins[.]sh, hxxp://[87[.]10[.]220[.]221/yakuza[.]sh, hxxp://[87[.]10[.]220[.]221/yakuza[.]arm4, hxxp://[87[.]10[.]220[.]221/yakuza[.]arm5, hxxp://[87[.]10[.]220[.]221/yakuza[.]arm6, hxxp://[87[.]10[.]220[.]221/yakuza[.]arm7, hxxp://[87[.]10[.]220[.]221/yakuza[.]i586, hxxp://[87[.]10[.]220[.]221/yakuza[.]i686, hxxp://[87[.]10[.]220[.]221/yakuza[.]m68k, hxxp://[87[.]10[.]220[.]221/yakuza[.]mips, hxxp://[87[.]10[.]220[.]221/yakuza[.]mipsel, hxxp://[87[.]10[.]220[.]221/yakuza[.]ppc, hxxp://[87[.]10[.]220[.]221/yakuza[.]sparc, hxxp://[87[.]10[.]220[.]221/yakuza[.]x86
<b><u>Quasar</u></b>	SHA256	9c3d53c7723bfdd037df85de4c26efcd5e6f4ad58cc24f7a38a774bf22de3876
	URL	hxxps[://]jujuju[.]lat/files/kk[.]cmd
	Domain	captchacdn[.]com[:]7000
	IPv4	154[.]216[.]17[.]47
<b><u>NonEuclid</u></b>	SHA256	d32585b207fd3e2ce87dc2ea33890a445d68a4001ea923daa750d32b5de52bf0, 0521aeba49554242674994b1a8881e819c24f0047870d7e1d120deed76895b55
<b><u>PowerRAT</u></b>	SHA256	13252199b18d5257a60f57de95d8c6be7d7973df7f957bca8c2f31e15fcc947b
	IPv4	94[.]103[.]85[.]47
	Domain	disk-yanbex[.]ru

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

**January 06, 2025 • 9:00 PM**

© 2025 All Rights are Reserved by Hive Pro



More at [www.hivepro.com](http://www.hivepro.com)