Date of Publication
August 18, 2025

Hive Pro

HiveForce Labs

WEEKLY
THREAT DIGEST

Attacks, Vulnerabilities, and Actors

11 to 17 AUGUST 2025

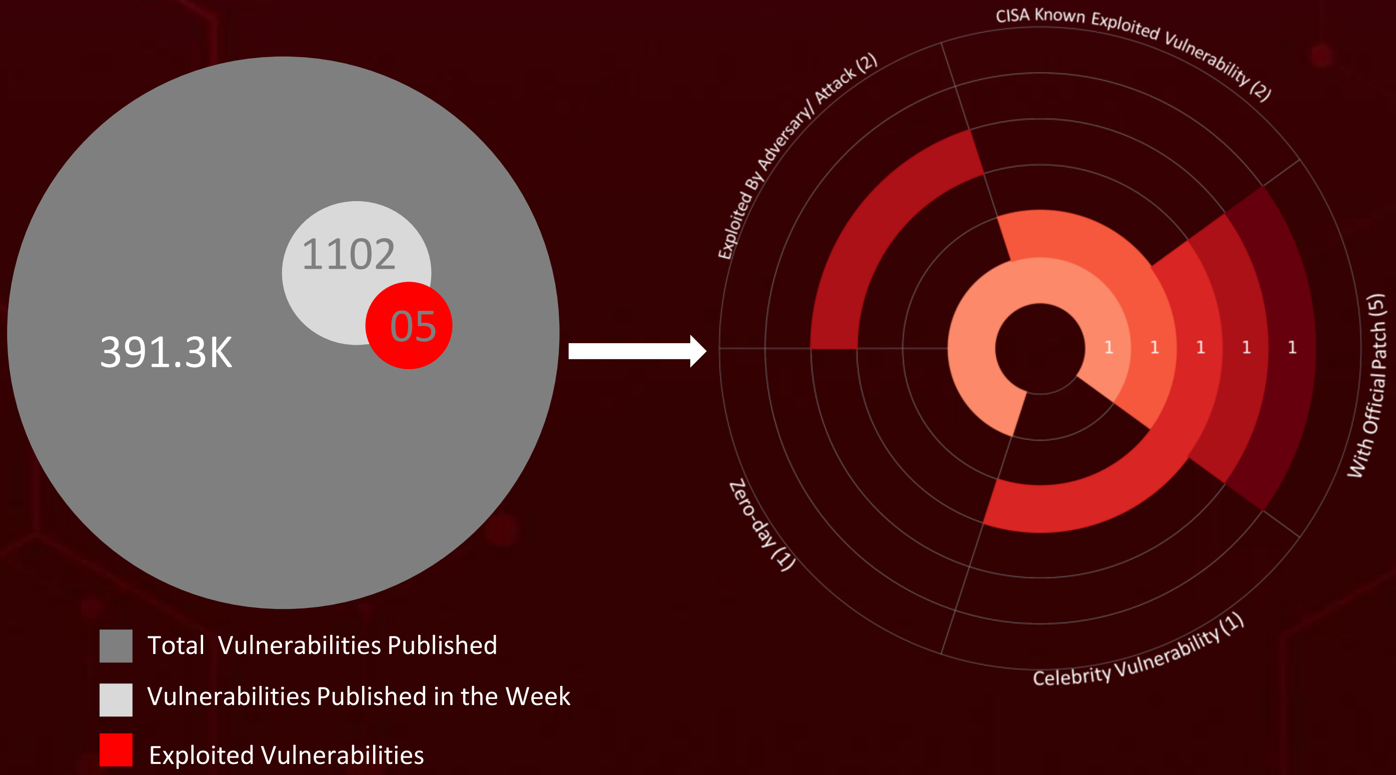
Table Of Contents

Summary

HiveForce Labs has observed a significant surge in cybersecurity threats, underscoring the growing complexity and frequency of cyber incidents. Over the past week, **eight** major attacks were detected, **five** critical vulnerabilities were actively exploited, and **two** threat actor groups were closely monitored, reflecting an alarming escalation in malicious activities.

Among the key developments, **CVE-2025-32433** is a critical unauthenticated remote code execution vulnerability in the Erlang/OTP SSH server, already being exploited in the wild. This flaw presents a significant risk to OT networks and industries such as education, healthcare, and telecommunications, with proof-of-concept code publicly available.

A newly discovered zero-day vulnerability in WinRAR (**CVE-2025-8088**) has been actively exploited by advanced threat groups like **RomCom** and **Paper Werewolf**. The **Charon ransomware** strain has been linked to APT-style attacks targeting the aviation and public sectors in the **Middle East**. These escalating threats highlight the increasing sophistication of cyber adversaries and reinforce the urgent need for proactive, resilient cybersecurity measures to combat the rapidly evolving global threat landscape.



High Level Statistics

8
Attacks Executed

5
Vulnerabilities Exploited

2
Adversaries in Action

- CastleBot
- DarkCloud
- Efimer
- Charon
- SWORDLDR
- Mythic
- SnipBot
- RustyClaw

- CVE-2025-8088
- CVE-2025-6218
- CVE-2025-25256
- CVE-2025-53779
- CVE-2025-32433

- RomCom
- Paper Werewolf

Insights

Efimer Trojan: **Cryptocurrency** Theft Powered by Phishing Emails, WordPress Hacks, and Fake Downloads

Erlang/OTP SSH Bug CVE-2025-32433: A Publicly Known Exploit Putting **Education** and **Healthcare** at Risk

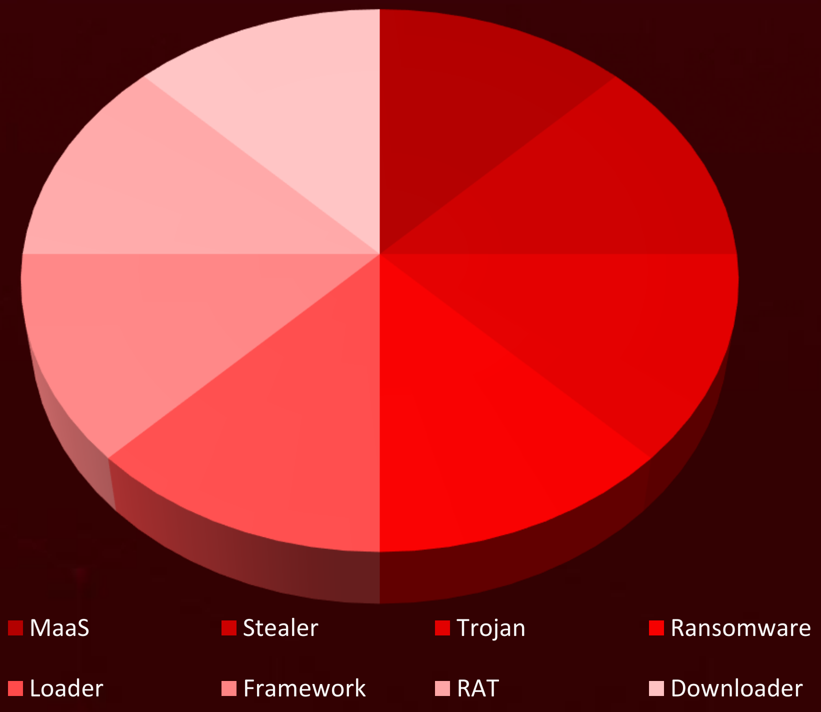
CastleBot's Modular Design is Revolutionizing Cybercrime Tactics

WinRAR CVE-2025-8088: Exploit Code Bought for **$80,000** on the Dark Web to Target **European**, **Canadian**, and **Russian** Companies

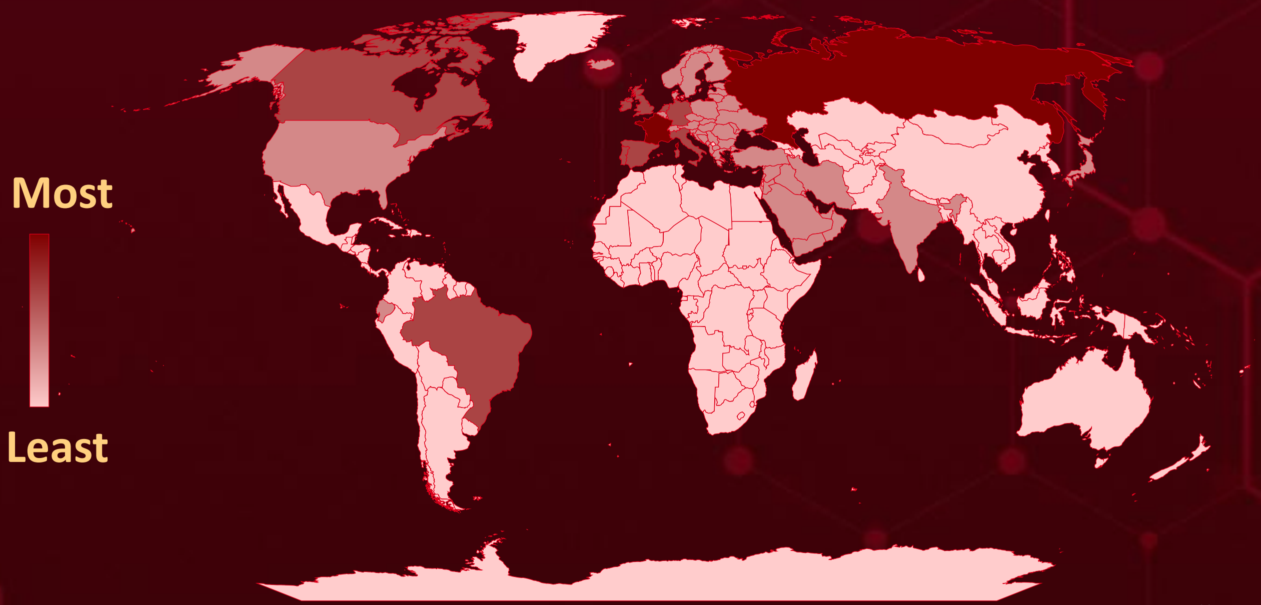
Remote Code Execution Without Login? That's CVE-2025-25256 in FortiSIEM

Charon Ransomware Puts **Middle East Aviation and Public Sectors** on High Alert

Threat Distribution



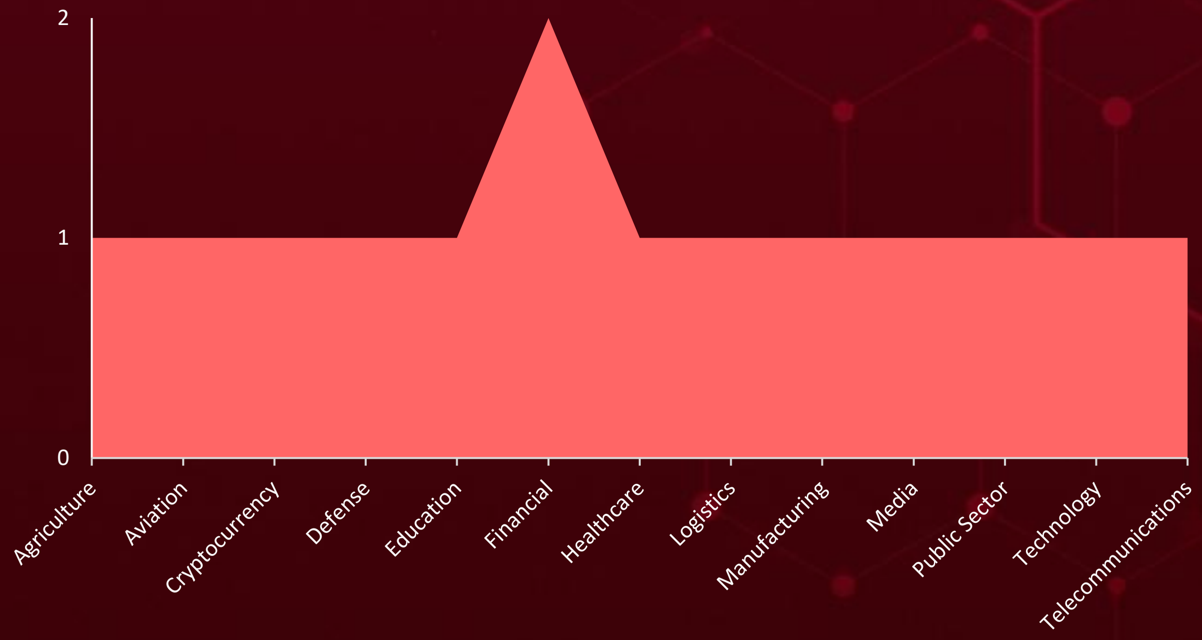
Targeted Countries



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

	Countries		Countries		Countries		Countries
🟥	Russia	▨	Albania	▨	United States	⬜	Dominica
🟥	France	▨	Bahrain	▨	Andorra	⬜	Bolivia
🟥	Ireland	▨	San Marino	▨	Latvia	⬜	Egypt
🟥	Netherlands	▨	Greece	▨	Switzerland	⬜	Honduras
🟥	Italy	▨	Slovenia	▨	Yemen	⬜	Eritrea
🟥	Portugal	▨	Holy See	▨	Turkey	⬜	Argentina
🟥	Canada	▨	Syria	▨	Liechtenstein	⬜	Sri Lanka
🟥	Brazil	▨	Hungary	▨	Croatia	⬜	Botswana
🟥	Spain	▨	Luxembourg	▨	Lithuania	⬜	Tanzania
🟥	Germany	▨	Iceland	▨	Jordan	⬜	Armenia
🟥	United Kingdom	▨	Moldova	▨	Kuwait	⬜	Turkmenistan
▨	Bosnia and Herzegovina	▨	India	▨	Lebanon	⬜	Indonesia
▨	Sweden	▨	Montenegro	⬜	Cuba	⬜	Uzbekistan
▨	Romania	▨	Iran	⬜	South Africa	⬜	Brunei
▨	Cyprus	▨	North Macedonia	⬜	Rwanda	⬜	Akrotiri and Dhekelia
▨	Malta	▨	Iraq	⬜	Bhutan	⬜	Australia
▨	Czech Republic	▨	Oman	⬜	Tonga	⬜	Panama
▨	Palestine	▨	Belarus	⬜	Grenada	⬜	Burkina Faso
▨	Denmark	▨	Poland	⬜	Paraguay	⬜	Philippines
▨	Serbia	▨	Israel	⬜	Guatemala	⬜	Burundi
▨	Ecuador	▨	Qatar	⬜	Equatorial Guinea	⬜	DR Congo
▨	Ukraine	▨	Belgium	⬜	Guinea	⬜	Cabo Verde
▨	Estonia	▨	Bulgaria	⬜	Ethiopia	⬜	Saint Lucia
▨	Monaco	▨	Japan	⬜	Guinea-Bissau	⬜	Jamaica
▨	Finland	▨	Saudi Arabia	⬜	Gambia	⬜	El Salvador
▨	Norway	▨	United Arab Emirates	⬜	Guyana	⬜	Cambodia
▨	Austria	▨	Slovakia	⬜	Palau	⬜	Sierra Leone
				⬜	Haiti		

Targeted Industries



TOP MITRE ATT&CK TTPs

T1059
Command and Scripting Interpreter

T1082
System Information Discovery

T1027
Obfuscated Files or Information

T1204
User Execution

T1566
Phishing

T1068
Exploitation for Privilege Escalation

T1071
Application Layer Protocol

T1036
Masquerading

T1574.001
DLL

T1588
Obtain Capabilities

T1588.006
Vulnerabilities

T1588.005
Exploits

T1071.001
Web Protocols

T1574
Hijack Execution Flow

T1566.001
Spearphishing Attachment

T1055
Process Injection

T1059.001
PowerShell

T1204.002
Malicious File

T1021
Remote Services

T1555.003
Credentials from Web Browsers

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
CastleBot	CastleBot is a malware framework offered as part of a Malware-as-a-Service operation. It operates in multiple stages: starting with a lightweight "stager," followed by a "loader," and finishing with a core backdoor. The core backdoor can steal information, install additional malware, and set up the system for potential ransomware attacks.	Fake software installers via SEO poisoning	-
TYPE		IMPACT	AFFECTED PLATFORM
MaaS		Remote Access, Installation of Additional Malware	-
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	202f6b6631ade2c41e4762e5877ce0063a3beabce0c3f8564b6499a1164c1e04, d6eea6cf20a744f3394fb0c1a30431f1ef79d6992b552622ad17d86490b7aa7b, cbaf513e7fd4322b14adcc34b34d793d79076ad310925981548e8d3cff886527		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
DarkCloud	DarkCloud, a Windows-based information stealer first spotted in 2022, reappeared in 2025 with enhanced delivery and obfuscation techniques, including ConfuserEx-protected files and a VB6 payload. It uses JavaScript and PowerShell to deploy a fileless .NET DLL, maintain persistence, and inject its payload into MSBuild.exe. DarkCloud then steals browser credentials and payment information, exfiltrating the data via FTP or SMTP.	Phishing Emails	-
TYPE		IMPACT	AFFECTED PLATFORM
Stealer		Information Theft, Persistence on the System, Decreased System Performance	Microsoft Windows
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	bd8c0b0503741c17d75ce560a10eeeaa0cdd21dff323d9f1644c62b7b8eb43d9, 9588c9a754574246d179c9fb05fea9dc5762c855a3a2a4823b402217f82a71c1, 6b8a4c3d4a4a0a3aea50037744c5fec26a38d3fb6a596d006457f1c51bbc75c7		

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
Efimer	The Efimer Trojan is a highly evasive cryptocurrency-stealing malware. It monitors clipboard activity to intercept and replace wallet addresses, captures recovery phrases, and uses the Tor network to conceal its communications. Efimer silently executes in the background. When run with administrative privileges, it bypasses security, establishes persistence through Windows registry modifications.	Phishing Emails, Compromised WordPress sites, fake torrent downloads	-
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Cryptocurrency Theft, Bypasses Windows Defender, Persistence through Windows Registry	-
Trojan			
ASSOCIATED ACTOR			**PATCH LINK**
-			-

IOC TYPE	VALUE
SHA256	6199960f2ec96d4851e4f36d5a5095922e422e3b4265bdb537ccdbb8d44ac8dc, 3e9e666b06d3708ab9591454ac119e276bcaea7f7e6c4b8e5c349c9baa3c0faa, 006c397ec5b65e0c646598ee6014813ff601802d927fb90571e5ad1204d7f70f

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Charon	Charon is a ransomware strain linked to advanced APT-style attacks. The attackers used DLL sideloading, a technique also seen in Earth Baxia campaigns. While DLL sideloading is widely used, its execution here shows high-level sophistication, with coordinated toolchains and encrypted payloads. Charon's deployment involves a multi-stage process for extracting and delivering its payload.	-	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		Data Encryption, Disruption of Operations, Financial Loss	Microsoft Windows
Ransomware			
ASSOCIATED ACTOR			**PATCH LINK**
-			-

IOC TYPE	VALUE
SHA256	80711e37f226ef1dc86dc80a8cbc0b2ec895b361e9ade85da793d94b1d876be8, 739e2cac9e2a15631c770236b34ba569aad1d1de87c6243f285bf1995af2cdc2

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 CVE</th></tr>
<tr><td rowspan="2">SWORDLDR</td><td rowspan="6">SWORDLDR is a loader used in the attack chain to sideload a malicious DLL. It begins by leveraging the legitimate Edge.exe process, which is a browser-related executable, to load msedge.dll, the payload containing SWORDLDR. By disguising itself as a legitimate Windows service, the malware successfully bypasses standard security defenses, allowing it to execute undetected.</td><td>-</td><td>-</td></tr>
<tr><td><b>IMPACT</b></td><td><b>AFFECTED PRODUCT</b></td></tr>
<tr><td><b>TYPE</b></td><td rowspan="4">Bypassing Security Defenses, Increased Privileges, Malicious Payload Injection</td><td rowspan="2">Microsoft Windows</td></tr>
<tr><td>Loader</td></tr>
<tr><td><b>ASSOCIATED ACTOR</b></td><td><b>PATCH LINK</b></td></tr>
<tr><td>-</td><td>-</td></tr>
<tr><td><b>IOC TYPE</b></td><td colspan="3"><b>VALUE</b></td></tr>
<tr><td>SHA256</td><td colspan="3">e0a23c0d99c45d40f6ef99c901bacf04bb12e9a3a15823b663b392abadd2444e</td></tr>
</table>

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVE</th></tr>
<tr><td rowspan="2">Mythic</td><td rowspan="6">Mythic is a cross-platform post-exploitation framework that, while originally built for legitimate red-teaming operations, has been weaponized by threat actors like RomCom to control compromised systems. It provides a flexible, plug-and-play command-and-control (C2) platform, allowing operators to easily add new agents, communication channels, and custom payloads on the fly. Mythic enables attackers to coordinate tasks, maintain persistence, and expand their capabilities across victim environments with remarkable efficiency.</td><td>Exploiting Vulnerability</td><td>CVE-2025-8088</td></tr>
<tr><td><b>IMPACT</b></td><td><b>AFFECTED PRODUCT</b></td></tr>
<tr><td><b>TYPE</b></td><td rowspan="4">Remote Command and Control, Persistence, Exposure of Confidential Business Information</td><td rowspan="2">RARLAB WinRAR</td></tr>
<tr><td>Framework</td></tr>
<tr><td><b>ASSOCIATED ACTOR</b></td><td><b>PATCH LINK</b></td></tr>
<tr><td>RomCom</td><td>https://www.win-rar.com/download.html?&L=0</td></tr>
<tr><td><b>IOC TYPE</b></td><td colspan="3"><b>VALUE</b></td></tr>
<tr><td>SHA256</td><td colspan="3">e0cbe8f18315a2ee781de48565dc8a087a1564557c42c66067f65c267120c894</td></tr>
</table>

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 CVE</th></tr>
<tr><td rowspan="3">SnipBot</td><td rowspan="7">SnipBot, a newly identified variant of the RomCom malware family, employs advanced infection and evasion techniques. Typically delivered via phishing emails disguised as PDF attachments, it downloads additional malicious payloads from remote command-and-control servers. This malware demonstrates capabilities for remote command execution and data exfiltration, while using anti-sandbox methods to evade detection.</td><td>Exploiting Vulnerability</td><td>CVE-2025-8088</td></tr>
<tr><th>IMPACT</th><th>AFFECTED PRODUCT</th></tr>
<tr><td rowspan="5">Remote Command Execution, Payload Delivery, System Resource Utilization</td><td rowspan="3">RARLAB WinRAR</td></tr>
<tr><th>TYPE</th></tr>
<tr><td>RAT</td></tr>
<tr><th>ASSOCIATED ACTOR</th><th>PATCH LINK</th></tr>
<tr><td>RomCom</td><td>https://www.win-rar.com/download.html?&L=0</td></tr>
<tr><th>IOC TYPE</th><th colspan="3">VALUE</th></tr>
<tr><td>SHA256</td><td colspan="3">8082956ace8b016ae8ce16e4a777fe347c7f80f8a576a6f935f9d636a30204e7</td></tr>
</table>

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVE</th></tr>
<tr><td rowspan="3">RustyClaw</td><td rowspan="7">RustyClaw is a malware downloader built in Rust, incorporating advanced anti-analysis measures. Before initiating its malicious actions, the malware verifies the system's keyboard layout against specific language codes. Additionally, it generates a hash of its file name and compares it to a hardcoded value to prevent execution in sandbox environments with randomized file names. Once these checks are successful, RustyClaw can optionally display a decoy PDF to the infected user while downloading the next-stage implant to proceed with the attack.</td><td>Exploiting Vulnerability</td><td>CVE-2025-8088</td></tr>
<tr><th>IMPACT</th><th>AFFECTED PRODUCT</th></tr>
<tr><td rowspan="5">Bypassing Sandboxing and Detection, Persistence</td><td rowspan="3">RARLAB WinRAR</td></tr>
<tr><th>TYPE</th></tr>
<tr><td>Downloader</td></tr>
<tr><th>ASSOCIATED ACTOR</th><th>PATCH LINK</th></tr>
<tr><td>RomCom</td><td>https://www.win-rar.com/download.html?&L=0</td></tr>
<tr><th>IOC TYPE</th><th colspan="3">VALUE</th></tr>
<tr><td>SHA256</td><td colspan="3">0517d413beb3e124e773d7ccc1983b226d6593d1f46a81ba7e79a8b48d6242fa</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-2025-8088	✗	WinRAR versions before 7.13	RomCom, Paper Werewolf
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:rarlab:winrar:*:*:*:*:*:*:*:*	Mythic agents, SnipBot variants, and RustyClaw downloaders
RARLAB WinRAR Path Traversal Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-35	T1204: User Execution, T1204.002: Malicious File, T1059: Command and Scripting Interpreter	https://www.win-rar.com/download.html?&L=0

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTOR
CVE-2025-6218	✗	WinRAR Version Prior to 7.12	Paper Werewolf
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:rarlab:winrar:*:*:*:*	-
RARLAB WinRAR Directory Traversal Remote Code Execution Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-22	T1204: User Execution, T1204.002: Malicious File, T1059: Command and Scripting Interpreter	https://www.win-rar.com/download.html?&L=0

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-25256	⊗	FortiSIEM Versions 7.3.0 through 7.3.1, 7.2.0 through 7.2.5, 7.1.0 through 7.1.7, 7.0.0 through 7.0.3, 6.7.0 through 6.7.9, FortiSIEM 6.6, 6.5, 6.4, 6.3, 6.2, 6.1, and 5.4 All Versions	-
	ZERO-DAY		
	⊗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:fortinet:fortisiem:*:*:*:*:*:*:*:*	-
Fortinet FortiSIEM OS Command Injection Vulnerability	⊗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1588.005: Exploits, T1059: Command and Scripting Interpreter, T1068: Exploitation for Privilege Escalation	https://fortiguard.fortinet.com/psirt/FG-IR-25-152

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTOR
CVE-2025-53779	BadSuccessor	Windows Server 2025	-
	ZERO-DAY		
	⊗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows_server:-:*:*:*:*:*:*:*	-
BadSuccessor (Windows Kerberos Elevation of Privilege Vulnerability)	⊗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-23	T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-53779

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-32433	✗	All Erlang/OTP SSH servers running versions: OTP-27.3.2 and earlier OTP-26.2.5.10 and earlier OTP-25.3.2.19 and earlier	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:erlang:otp:*:*:*:*:*:*:*:*	-
Erlang Erlang/OTP SSH Server Missing Authentication for Critical Function Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-306	T1210: Exploitation of Remote Services, T1078: Valid Accounts	https://github.com/erlang/otp/releases, https://github.com/erlang/otp/security/advisories/GHSA-37cp-fgq5-7wc2

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
RomCom (aka Tropical Scorpius, Void Rabisu, DEV-0978, Storm-0978, UNC2596, CIGAR, UAC-0180)	Russia	Financial, Manufacturing, Defense, Logistics	Europe, Canada
	MOTIVE		
	Information theft and espionage, Financial gain		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCT**
	CVE-2025-8088	Mythic agents, SnipBot variants, and RustyClaw downloaders	RARLAB WinRAR
TTPs			
TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; TA0040: Impact; T1583: Acquire Infrastructure; T1587.001: Malware; T1587.004: Exploits; T1588.005: Exploits; T1588.006: Vulnerabilities; T1608: Stage Capabilities; T1566.001: Spearphishing Attachment; T1204.002: Malicious File; T1547.001: Registry Run Keys / Startup Folder; T1546.015: Component Object Model Hijacking; T1497: Virtualization/Sandbox Evasion; T1480: Execution Guardrails; T1036.001: Invalid Code Signature; T1027.007: Dynamic API Resolution; T1027.013: Encrypted/Encoded File; T1555.003: Credentials from Web Browsers; T1552.001: Credentials In Files; T1087: Account Discovery; T1518: Software Discovery; T1021: Remote Services; T1560: Archive Collected Data; T1185: Man in the Browser; T1005: Data from Local System; T1114.001: Local Email Collection; T1113: Screen Capture; T1071.001: Web Protocols; T1573.002: Asymmetric Cryptography; T1041: Exfiltration Over C2 Channel; T1657: Financial Theft			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGION
Paper Werewolf (aka GOFFEE)	-	All	Russia
	MOTIVE		
	Espionage and Destruction		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCT
	CVE-2025-8088, CVE-2025-6218	-	RARLAB WinRAR

TTPs
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0011: Command and Control; T1566.001: Spearphishing Attachment; T1566: Phishing; T1598: Phishing for Information; T1598.003: Spearphishing Link; T1059.003: Windows Command Shell; T1059: Command and Scripting Interpreter; T1203: Exploitation for Client Execution; T1204: User Execution; T1204.002: Malicious File; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys / Startup Folder; T1564: Hide Artifacts; T1564.003: Hidden Window; T1027: Obfuscated Files or Information; T1027.007: Dynamic API Resolution; T1027.009: Embedded Payloads; T1082: System Information Discovery; T1033: System Owner/User Discovery; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1105: Ingress Tool Transfer; T1095: Non-Application Layer Protocol

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **five exploited vulnerabilities** and block the indicators related to the threat actors **RomCom, Paper Werewolf,** and malware **CastleBot, DarkCloud, Efimer, Charon, SWORDLDR, Mythic, SnipBot, RustyClaw.**

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 **five exploited vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actors **RomCom, Paper Werewolf,** and malware **CastleBot, DarkCloud, Efimer, Snipbot, and Charon** in Breach and Attack Simulation(BAS).

Threat Advisories

CastleBot Rising: The Evolving Malware-as-a-Service Threat

DarkCloud Uses Fileless Techniques Turning into a Nightmare for Windows

Zero-Day in WinRAR Actively Weaponized by Multiple Threat Groups

Efimer Trojan: From Fake Lawsuits to Crypto Heists

CVE-2025-25256: Fortinet Rushes to Patch High-Risk FortiSIEM Vulnerability

Charon Ransomware Encrypts Files Belonging to Middle East Industries

Microsoft’s August 2025 Patch Tuesday Roundup

Erlang/OTP SSH Flaw Lets Hackers Bypass Login and Run Code

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
CastleBot	URL	hxxp[:]//173[.]44[.]141[.]89/service/download/data_4x[.]bin, hxxp[:]//173[.]44[.]141[.]89/service/download/data_3x[.]bin, hxxp[:]//173[.]44[.]141[.]89/service/, hxxp[:]//mhousecreative [.]com/service/, hxxp[:]//80[.]77[.]23[.]48/service/, hxxp[:]//62[.]60[.]226[.]73/service/, hxxp[:]//107[.]158[.]128[.]45/service/, hxxp[:]//62[.]60[.]226[.]73/service/
	SHA256	202f6b6631ade2c41e4762e5877ce0063a3beabce0c3f8564b6499a1164c1e04, d6eea6cf20a744f3394fb0c1a30431f1ef79d6992b552622ad17d86490b7aa7b, cbaf513e7fd4322b14adcc34b34d793d79076ad310925981548e8d3cff886527, e6aab1b6a150ee3cbc721ac2575c57309f307f69cd1b478d494c25cde0baaf85, b45cce4ede6ffb7b6f28f75a0cbb60e65592840d98dcb63155b9fa0324a88be2, 8bf93cef46fda2bdb9d2a426fbcd35ffedea9ed9bd97bf78cc51282bd1fb2095, 53dddae886017fbfbb43ef236996b9a4d9fb670833dfa0c3eac982815dc8d2a5
DarkCloud	SHA256	bd8c0b0503741c17d75ce560a10eeeaa0cdd21dff323d9f1644c62b7b8eb43d9, 9588c9a754574246d179c9fb05fea9dc5762c855a3a2a4823b402217f82a71c1,

Attack Name	TYPE	VALUE
DarkCloud	SHA256	6b8a4c3d4a4a0a3aea50037744c5fec26a38d3fb6a596d006457f1c51bbc75c7, f6d9198bd707c49454b83687af926ccb8d13c7e43514f59eac1507467e8fb140, 24552408d849799b2cac983d499b1f32c88c10f88319339d0eec00fb01bb19b4, ce3a3e46ca65d779d687c7e58fb4a2eb784e5b1b4cebe33dbb2bf37cccb6f194, 381aa445e173341f39e464e4f79b89c9ed058631bcbbb2792d9ecbdf9ffe027d, 82ba4340be2e07bb74347ade0b7b43f12cf8503a8fa535f154d2e228efbef69c
Efimer	MD5	39fa36b9bfcf6fd4388eb586e2798d1a, 16057e720be5f29e5b02061520068101, 100620a913f0e0a538b115dbace78589
	SHA256	6199960f2ec96d4851e4f36d5a5095922e422e3b4265bdb537ccdbb8d44ac8dc, 3e9e666b06d3708ab9591454ac119e276bcaea7f7e6c4b8e5c349c9baa3c0faa, 006c397ec5b65e0c646598ee6014813ff601802d927fb90571e5ad1204d7f70f
Charon	SHA256	80711e37f226ef1dc86dc80a8cbc0b2ec895b361e9ade85da793d94b1d876be8, 739e2cac9e2a15631c770236b34ba569aad1d1de87c6243f285bf1995af2cdc2
	SHA1	92750eb5990cdcda768c7cb7b654ab54651c058a, a1c6090674f3778ea207b14b1b55be487ce1a2ab
SWORDLDR	SHA256	e0a23c0d99c45d40f6ef99c901bacf04bb12e9a3a15823b663b392abadd2444e
	SHA1	21b233c0100948d3829740bd2d2d05dc35159ccb
Mythic	SHA256	e0cbe8f18315a2ee781de48565dc8a087a1564557c42c66067f65c267120c894
	SHA1	ae687bef963cb30a3788e34cc18046f54c41ffba
	IPv4	194[.]36[.]209[.]127
	Domain	srlaptop[.]com
SnipBot	SHA256	8082956ace8b016ae8ce16e4a777fe347c7f80f8a576a6f935f9d636a30204e7
	SHA1	1aea26a2e2a7711f89d06165e676e11769e2fd68

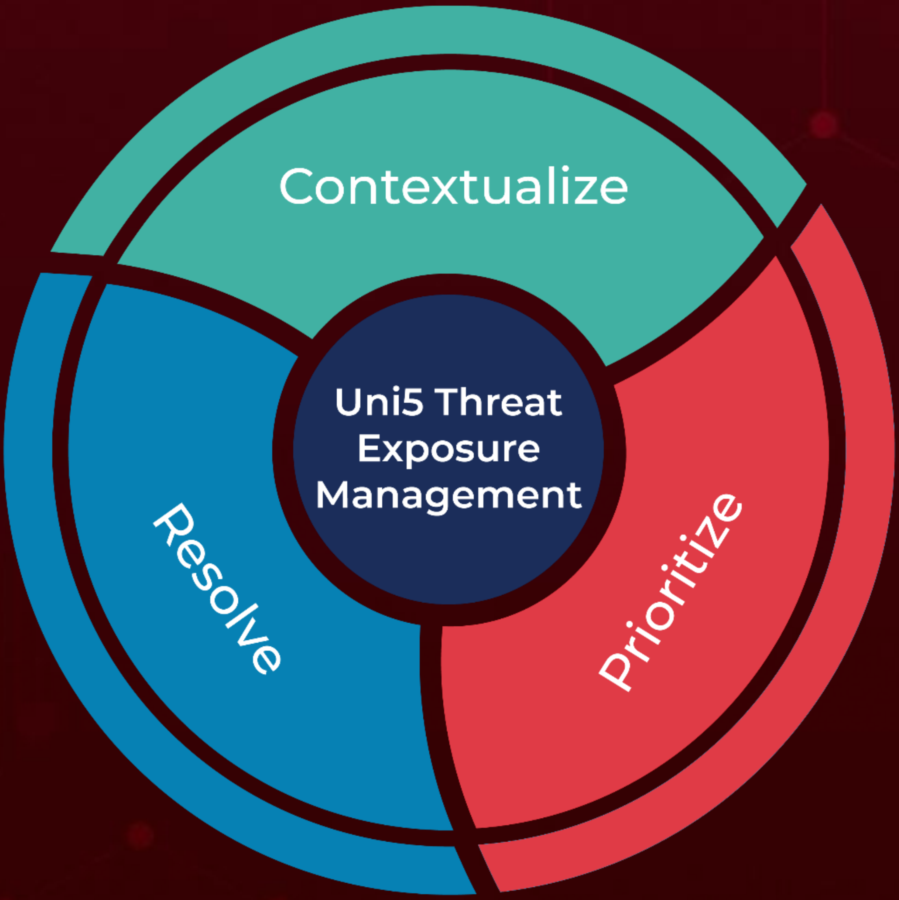
Attack Name	TYPE	VALUE
SnipBot	IPv4	185[.]173[.]235[.]134
	Domain	campanole[.]com
RustyClaw	SHA256	0517d413beb3e124e773d7ccc1983b226d6593d1f46a81ba7e79a8b48d6242fa
	SHA1	ab79081d0e26ea278d3d45da247335a545d0512e
	IPv4	85[.]158[.]108[.]62
	Domain	melamorri[.]com

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

August 18, 2025 • 9:30 PM

More at www.hivepro.com