Update WinRAR tools now: RomCom and others exploiting zero-day vulnerability

By Anton CherepanovPeter StrýčekDamien Schaeffer

Archived: 2026-04-05 19:54:29 UTC

ESET researchers have discovered a previously unknown vulnerability in WinRAR, being exploited in the wild by Russia-aligned group RomCom. This is at least the third time that RomCom has been caught exploiting a significant zero-day vulnerability in the wild. Previous examples include the abuse of CVE-2023-36884 via Microsoft Word in June 2023, and the combined vulnerabilities assigned CVE-2024-9680 chained with another previously unknown vulnerability in Windows, CVE-2024-49039, targeting vulnerable versions of Firefox, Thunderbird, and the Tor Browser, leading to arbitrary code execution in the context of the logged-in user in October 2024.

> **Key points of this blogpost:**
>
> - If you use WinRAR or other affected components such as the Windows versions of its command line utilities, UnRAR.dll, or the portable UnRAR source code, upgrade immediately to the latest version.
> - On July 18th, 2025, ESET researchers discovered a previously unknown zero-day vulnerability in WinRAR being exploited in the wild.
> - Analysis of the exploit led to the discovery of the vulnerability, now assigned CVE-2025-8088: a path traversal vulnerability, made possible with the use of alternate data streams. After immediate notification, WinRAR released a patched version on July 30th, 2025.
> - The vulnerability allows hiding malicious files in an archive, which are silently deployed when extracting.
> - Successful exploitation attempts delivered various backdoors used by the RomCom group, specifically a SnipBot variant, RustyClaw, and Mythic agent.
> - This campaign targeted financial, manufacturing, defense, and logistics companies in Europe and Canada.

RomCom (also known as Storm-0978, Tropical Scorpius, or UNC2596) is a Russia-aligned group that conducts both opportunistic campaigns against selected business verticals and targeted espionage operations. The group's focus has shifted to include espionage operations collecting intelligence, in parallel with its more conventional cybercrime operations. The backdoor commonly used by the group is capable of executing commands and downloading additional modules to the victim's machine.

The discovery of CVE-2025-8088

On July 18th, 2025, we observed a malicious DLL named msedge.dll in a RAR archive containing unusual paths that caught our attention. Upon further analysis, we found that the attackers were exploiting a previously unknown

vulnerability affecting WinRAR, including the then-current version, 7.12. On July 24th, 2025, we contacted the developer of WinRAR, and on the same day, the vulnerability was fixed and WinRAR 7.13 beta 1 published. WinRAR 7.13 was published on July 30th, 2025. Users of WinRAR are advised to install the latest version as soon as possible to mitigate the risk. Note that software solutions relying on publicly available Windows versions of UnRAR.dll or its corresponding source code are affected as well, especially those that have not updated their dependencies.

The vulnerability, tracked as CVE-2025-8088, uses alternate data streams (ADSes) for path traversal. Note that a similar path traversal vulnerability (CVE-2025-6218) affecting WinRAR was disclosed on June 19th, 2025, approximately a month earlier.

The attackers specially crafted the archive to apparently contain only one benign file (see Figure 1), while it contains many malicious ADSes (there's no indication of them from the user's point of view).

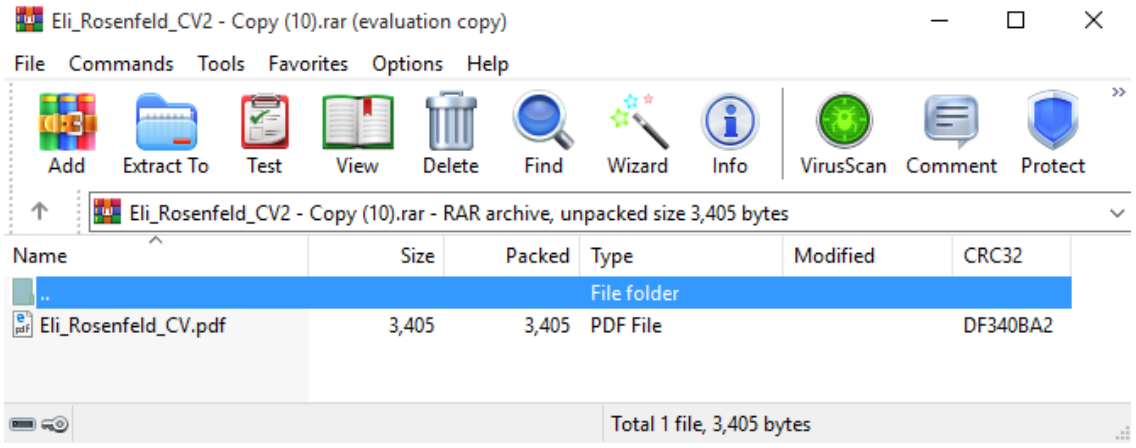

Figure 1. Eli_Rosenfeld_CV2 - Copy (10).rar *opened in WinRAR*

Once a victim opens this seemingly benign file, WinRAR unpacks it along with all its ADSes. For example, for Eli_Rosenfeld_CV2 - Copy (10).rar, a malicious DLL is deployed into %TEMP%. Likewise, a malicious LNK file is deployed into the Windows startup directory, thereby achieving persistence via execution on user login.

To ensure higher success, the attackers provided multiple ADSes with increasing depths of parent directory relative path elements (..\\). However, this introduces nonexistent paths that WinRAR visibly warns about. Interestingly, the attackers added ADSes that contain dummy data and are expected to have invalid paths. We suspect that the attackers introduced them so that the victim does not notice the suspicious DLL and LNK paths (see Figure 2). Only when scrolling down in the WinRAR user interface are the suspicious paths revealed, as seen in Figure 3.

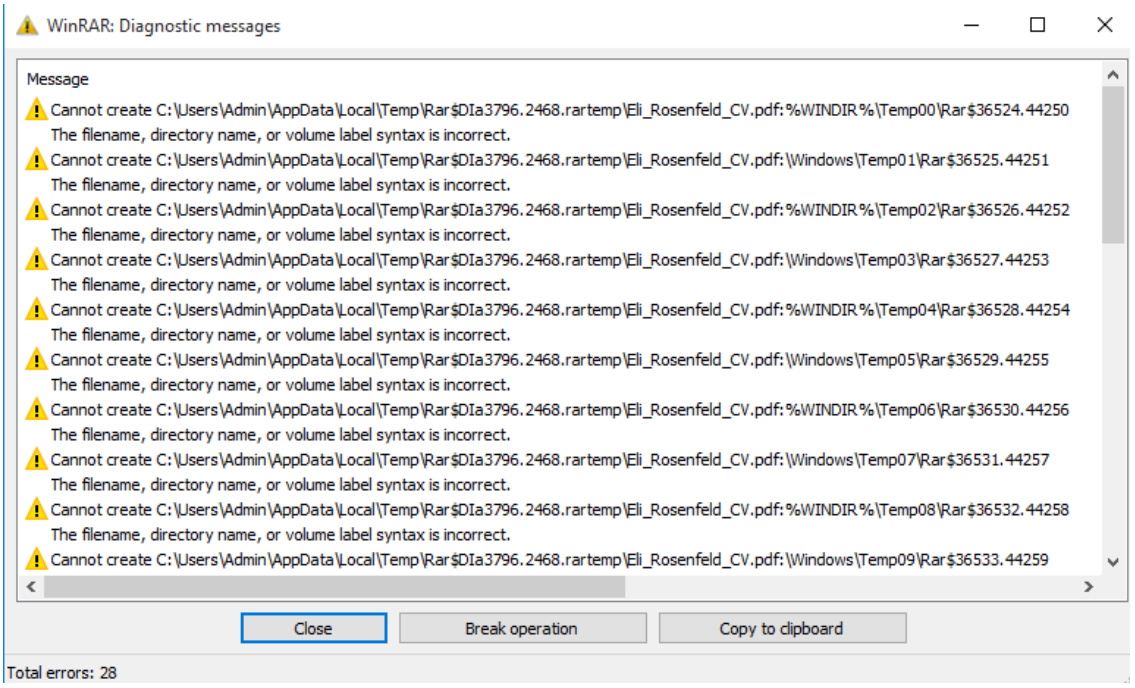

Figure 2. Displayed WinRAR errors when unpacking Eli_Rosenfeld_CV2 - Copy (10).*rar*

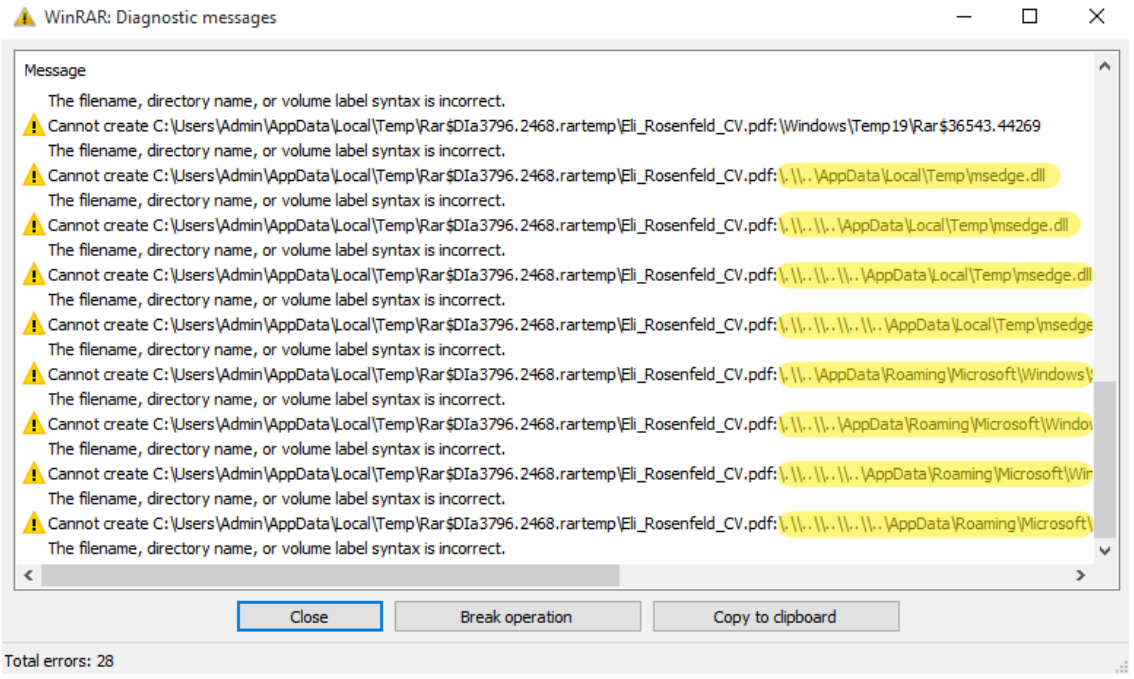

Figure 3. Displayed WinRAR errors when unpacking Eli_Rosenfeld_CV2 - Copy (10).rar*; scrolled down and highlighted*

Compromise chain

According to ESET telemetry, such archives were used in spearphishing campaigns from the 18th to 21st July, 2025, targeting financial, manufacturing, defense, and logistics companies in Europe and Canada. Table 1 contains the spearphishing emails – sender, subject, and filename of the attachment – used in the campaigns, and Figure 4 shows the message we observed in an email. In all cases, the attackers sent a CV hoping that a curious target would open it. According to ESET telemetry, none of the targets were compromised.

Table 1. Spearphishing emails observed in ESET telemetry

Sender	Subject	Attachment
Simona <2constheatcomshirl@seznam[.]cz>	Experienced Web3 Developer вЂ“ CV Attached for Consideration	Eli_Rosenfeld_CV2 - Copy (100) - Copy - Copy - Copy - Copy - Copy - Copy.rar
		Eli_Rosenfeld_CV2 - Copy (100) - Copy - Copy - Copy - Copy - Copy.rar
		Eli_Rosenfeld_CV2 - Copy (100) - Copy - Copy - Copy - Copy.rar
		Eli_Rosenfeld_CV2 - Copy (10).rar
Marshall Rico <geoshilovyf@gmx[.]com>	Motivated Applicant - Resume Enclosed	cv_submission.rar
Simona <93leocarperpiyd@seznam[.]cz>		
Simona <93geoprobmenfuuu@seznam[.]cz>		
Simona <2constheatcomshirl@seznam[.]cz>		
Simona <3tiafratferpate@seznam[.]cz>		
Russell Martin <sampnestpihydbi@gmx[.]com>	Job Application	Datos adjuntos sin título 00170.dat
Pepita Cordero <stefanmuribi@gmx[.]net>	Application for Job Openings - Pepita Cordero	JobDocs_July2025.rar
Sacchetti Jami <patricklofiri@gmx[.]net>	Application for Job Openings - Sacchetti Jami	Recruitment_Dossier_July_2025.rar
Jennifer Hunt <emponafinpu@gmx[.]com>	Applying for the Role	cv_submission.rar

Hello,

I hope this message finds you well.

My name is Eli Rosenfeld, and I'm a seasoned Web3 and software developer with over 8 years of experience building decentralized applications, smart contracts, and user-facing crypto platforms. I've contributed to several leading blockchain ventures and am passionate about creating secure, scalable, and user-focused solutions in the Web3 space.

I'm currently exploring new opportunities where I can bring both my technical expertise and creative mindset to an ambitious, mission-driven team. I've attached my resume for your review.

I'm also fully open to relocating to any country if the role requires—it's important to me to be where I can contribute most effectively and grow alongside the right team.

Thank you for your time, and I would welcome the opportunity to connect.

Best regards,

Eli Rosenfeld

Brooklyn, NY

Figure 4. Observed email message

These RAR files always contain two malicious files: a LNK file, unpacked to the Windows startup directory, and a DLL or EXE, unpacked to either %TEMP% or %LOCALAPPDATA%. Some of the archives share the same malware. We have identified three execution chains.

Mythic agent execution chain

In the first execution chain, depicted in Figure 5, the malicious LNK file Updater.lnk adds the registry value HKCU\SOFTWARE\Classes\CLSID\{1299CF18-C4F5-4B6A-BB0F-2299F0398E27}\InprocServer32 and sets it to %TEMP%\msedge.dll. This is used to trigger execution of that DLL via COM hijacking. Specifically, the CLSID corresponds to the PSFactoryBuffer object present in npmproxy.dll. As a result, any executable trying to load it (e.g., Microsoft Edge) will trigger code execution of the malicious DLL. This DLL is responsible for decrypting embedded shellcode via AES and subsequently executing it. Interestingly, it retrieves the domain name for the current machine, which typically contains the company name, and compares it with a hardcoded value,

exiting if the two values do not match. This means that the attackers had conducted reconnaissance beforehand, confirming that this email was highly targeted.

The loaded shellcode appears to be a dynamichttp C2 profile for the Mythic agent having the following C&C server: https://srlaptop[.]com/s/0.7.8/clarity.js.

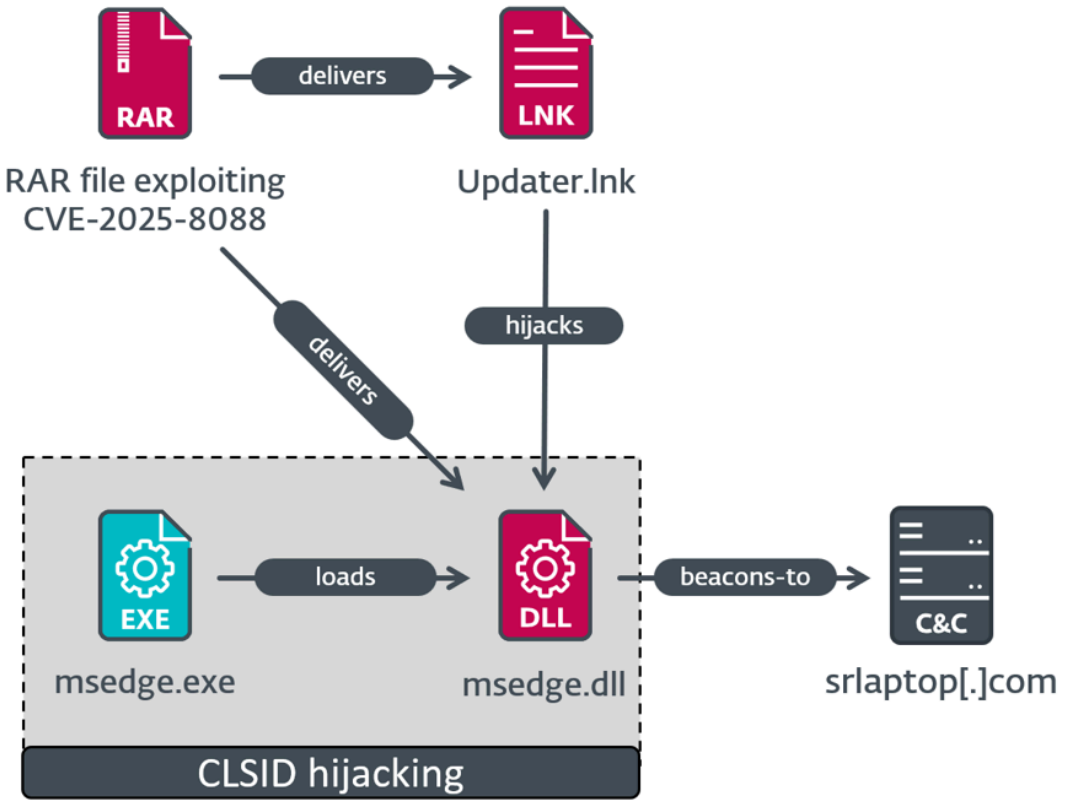

Figure 5. Mythic agent execution chain

It comes with a standard configuration for the dynamichttp C2 profile and a custom one, which is displayed in Figure 6. Just like in the previous stage, this configuration contains a hardcoded domain name of the target.

```
{'disable_etw': '2', 'block_non_ms_dlls': '3', 'child_process': 'wmic.exe', 'use_winhttp': 1, 'inject_method':
```

Figure 6. Custom configuration in the Mythic execution chain

SnipBot variant execution chain

In the second execution chain, which is depicted in Figure 7, the malicious LNK file Display Settings.lnk runs %LOCALAPPDATA%\ApbxHelper.exe. It is a modified version of PuTTY CAC, which is a fork of PuTTY, and is signed with an invalid code-signing certificate. The extra code uses the filename as a key for decrypting strings and the next stage, which is shellcode. The shellcode appears to be a variant of SnipBot, malware attributed to RomCom by UNIT 42. Execution of the shellcode only proceeds if a specific registry value (68 for this sample) is present in the HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\ registry key (in other words, if at least 69 documents were recently opened); this is an anti-analysis technique to prevent execution in an empty virtual machine or sandbox. If at least 69 documents were recently opened, next-stage shellcode is

decrypted using the registry key name (e.g., 68, but converted from string to integer), and executed, downloading yet another stage from https://campanole[.]com/TOfrPOseJKZ.

We also found an identical ApbxHelper.exe within Adverse_Effect_Medical_Records_2025.rar, uploaded to VirusTotal from Germany. This archive also exploits the CVE-2025-8088 vulnerability.

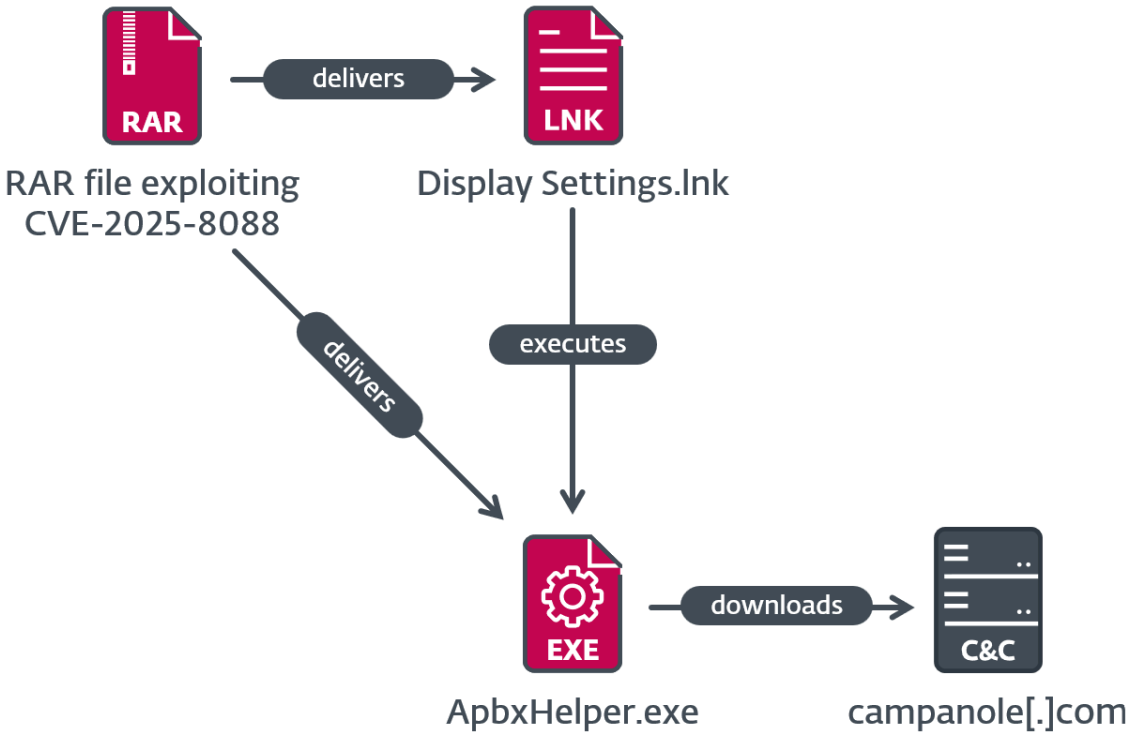

Figure 7. SnipBot variant execution chain

MeltingClaw execution chain

In the third execution case, which is depicted in Figure 8, the malicious LNK file Settings.lnk runs %LOCALAPPDATA%\Complaint.exe, which is RustyClaw – a downloader written in Rust previously analyzed by Talos. This sample is signed with an invalid code-signing certificate, which is different from the code-signing certificate used in the SnipBot variant. RustyClaw downloads and executes another payload, from https://melamorri[.]com/iEZGPctehTZ. This payload (SHA-1: 01D32FE88ECDEA2B934A00805E138034BF85BF83), with internal name install_module_x64.dll, partially matches the analysis of MeltingClaw by Proofpoint, a different downloader attributed to RomCom. The C&C server of the MeltingClaw sample that we observed is https://gohazeldale[.]com.

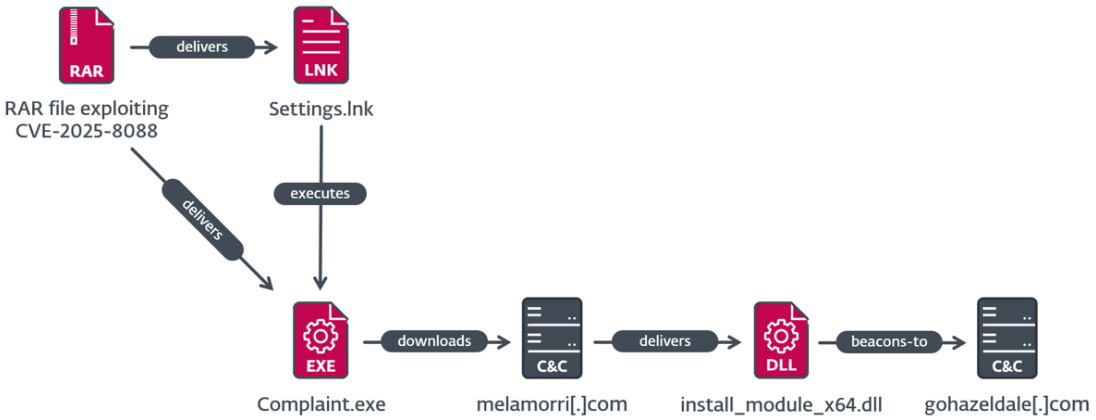

Figure 8. MeltingClaw execution chain

Attribution

We attribute the observed activities to RomCom with high confidence based on the targeted region, TTPs, and malware used.

This is not the first time that RomCom has used exploits to compromise its victims. In June 2023, the group performed a spearphishing campaign targeting defense and governmental entities in Europe, with lures related to the Ukrainian World Congress. The Microsoft Word document attached to the email attempted to exploit the CVE-2023-36884 vulnerability, as documented by the BlackBerry Threat Research and Intelligence team.

On October 8th, 2024, the group exploited a then-unknown vulnerability in the Firefox browser. The exploit targeted a use-after-free vulnerability in Firefox Animation timelines, allowing an attacker to achieve code execution in a content process, with the objective of delivering the RomCom backdoor. The vulnerability identifier CVE-2024-9680 was assigned, as documented in our WeLiveSecurity blogpost.

Other activities

We are aware that this vulnerability has also been exploited by another threat actor, and was independently discovered by the Russian cybersecurity company BI.ZONE. Notably, this second threat actor began exploiting CVE-2025-8088 a few days after RomCom started doing so.

Conclusion

By exploiting a previously unknown zero-day vulnerability in WinRAR, the RomCom group has shown that it is willing to invest serious effort and resources into its cyberoperations. This is at least the third time RomCom has used a zero-day vulnerability in the wild, highlighting its ongoing focus on acquiring and using exploits for targeted attacks. The discovered campaign targeted sectors that align with the typical interests of Russian-aligned APT groups, suggesting a geopolitical motivation behind the operation.

We would like to thank the WinRAR team for its cooperation and quick response, and recognize its effort in releasing a patch within just one day.

Thanks to Peter Košinár for his assistance in the analysis.

> *For any inquiries about our research published on WeLiveSecurity, please contact us at threatintel@eset.com.*
>
> *ESET Research offers private APT intelligence reports and data feeds. For any inquiries about this service, visit the ESET Threat Intelligence page.*

IoCs

A comprehensive list of indicators of compromise (IoCs) and samples can be found in our GitHub repository.

Files

SHA-1	Filename	Detection	Description
371A5B8BA86FBCAB80D4E0087D2AA0D8FFDDC70B	Adverse_Effect_Medical_Records_2025.rar	LNK/Agent.AJN Win64/Agent.GPM	Archive exploiting CVE-2025-8088; found on VirusTotal.
D43F49E6A586658B5422EDC647075FFD405D6741	cv_submission.rar	LNK/Agent.AJN July Win64/Agent.GPM	Archive exploiting CVE-2025-8088.
F77DBA76010A9988C9CEB8E420C96AEBC071B889	Eli_Rosenfeld_CV2 - Copy (10).rar	Win64/Agent.GMQ	Archive exploiting CVE-2025-8088.
676086860055F6591FED303B4799C725F8466CF4	Datos adjuntos sin título 00170.dat	LNK/Agent.AJN Win64/Agent.GPM	Archive exploiting CVE-2025-8088.
1F25E062E8E9A4F1792C3EAC6462694410F0F1CA	JobDocs_July2025.rar	LNK/Agent.AJN Win64/TrojanDownloader.Agent.BZV	Archive exploiting CVE-2025-8088.
C340625C779911165E3983C77FD60855A2575275	cv_submission.rar	LNK/Agent.AJN Win64/Agent.GPM	Archive exploiting CVE-2025-8088.
C94A6BD6EC88385E4E831B208FED2FA6FAED6666	Recruitment_Dossier_July_2025.rar	LNK/Agent.AJN	Archive exploiting CVE-2025-8088.

SHA-1	Filename	Detection	Description
		Win64/TrojanDownloader.Agent.BZV	
01D32FE88ECDEA2B934A00805E138034BF85BF83	install_module_x64.dll	Win64/Agent.GNV	MeltingClaw
AE687BEF963CB30A3788E34CC18046F54C41FFBA	msedge.dll	Win64/Agent.GMQ	Mythic agent used by RomCom
AB79081D0E26EA278D3D45DA247335A545D0512E	Complaint.exe	Win64/TrojanDownloader.Agent.BZV	RustyClaw
1AEA26A2E2A7711F89D06165E676E11769E2FD68	ApbxHelper.exe	Win64/Agent.GPM	SnipBot variant

Network

IP	Domain	Hosting provider	First seen	Details
162.19.175[.]44	gohazeldale[.]com	OVH SAS	2025-06-05	MeltingClaw C&C server.
194.36.209[.]127	srlaptop[.]com	CGI GLOBAL LIMITED	2025-07-09	C&C server of the Mythic agent used by RomCom.
85.158.108[.]62	melamorri[.]com	HZ-HOSTING-LTD	2025-07-07	RustyClaw C&C server.
185.173.235[.]134	campanole[.]com	FiberXpress BV	2025-07-18	C&C server of the SnipBot variant.

MITRE ATT&CK techniques

This table was built using version 17 of the MITRE ATT&CK framework.

Tactic	ID	Name	Description
Resource Development	T1583	Acquire Infrastructure	RomCom sets up VPSes and buys domain names.
	T1587.001	Develop Capabilities: Malware	RomCom develops malware in multiple programming languages.

Tactic	ID	Name	Description
	T1587.004	Develop Capabilities: Exploits	RomCom may develop exploits used for initial compromise.
	T1588.005	Obtain Capabilities: Exploits	RomCom may acquire exploits used for initial compromise.
	T1588.006	Obtain Capabilities: Vulnerabilities	RomCom may obtain information about vulnerabilities that it uses for targeting victims.
	T1608	Stage Capabilities	RomCom stages malware on multiple delivery servers.
Initial Access	T1566.001	Phishing: Spearphishing Attachment	RomCom compromises victims with a malicious RAR attachment sent via spearphishing.
Execution	T1204.002	User Execution: Malicious File	RomCom lures victims into opening a weaponized RAR archive containing an exploit.
Persistence	T1547.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	For persistence, RomCom stores a LNK file in the Startup folder.
	T1546.015	Event Triggered Execution: Component Object Model Hijacking	RomCom hijacks CLSIDs for persistence.
Defense Evasion	T1497	Virtualization/Sandbox Evasion	RomCom detects virtual environments by checking for enough RecentDocs.
	T1480	Execution Guardrails	RomCom stops execution if running in a virtual environment. It also checks for a hardcoded domain name before executing.
	T1036.001	Masquerading: Invalid Code Signature	RomCom tries to appear more legitimate to users and security tools that improperly handle digital signatures.
	T1027.007	Obfuscated Files or Information: Dynamic API Resolution	RomCom decrypts and resolves API dynamically.

Tactic	ID	Name	Description
	T1027.013	Obfuscated Files or Information: Encrypted/Encoded File	RomCom decrypts shellcode based on filename and machine artifacts.
Credential Access	T1555.003	Credentials from Password Stores: Credentials from Web Browsers	The RomCom backdoor collects passwords, cookies, and sessions using a browser stealer module.
	T1552.001	Unsecured Credentials: Credentials In Files	The RomCom backdoor collects passwords using a file reconnaissance module.
Discovery	T1087	Account Discovery	The RomCom backdoor collects username, computer, and domain data.
	T1518	Software Discovery	The RomCom backdoor collects information about installed software and versions.
Lateral Movement	T1021	Remote Services	The RomCom backdoor creates SSH tunnels to move laterally within compromised networks.
Collection	T1560	Archive Collected Data	The RomCom backdoor stores data in a ZIP archive for exfiltration.
	T1185	Man in the Browser	The RomCom backdoor steals browser cookies, history, and saved passwords.
	T1005	Data from Local System	The RomCom backdoor collects specific file types based on file extensions.
	T1114.001	Email Collection: Local Email Collection	The RomCom backdoor collects files with .msg, .eml, and .email extensions.
	T1113	Screen Capture	The RomCom backdoor takes screenshots of the victim’s computer.
Command and Control	T1071.001	Application Layer Protocol: Web Protocols	The RomCom backdoor uses HTTP or HTTPS as a C&C protocol.
	T1573.002	Encrypted Channel: Asymmetric Cryptography	The RomCom backdoor encrypts communication using SSL certificates.

Tactic	ID	Name	Description
Exfiltration	T1041	Exfiltration Over C2 Channel	The RomCom backdoor exfiltrates data using the HTTPS C&C channel.
Impact	T1657	Financial Theft	RomCom compromises companies for financial interest.

Source: https://www.welivesecurity.com/en/eset-research/update-winrar-tools-now-romcom-and-others-exploiting-zero-day-vulnerability/