

Diverse Threat Actors Exploiting Critical WinRAR Vulnerability CVE-2025-8088

 cloud.google.com/blog/topics/threat-intelligence/exploiting-critical-winrar-vulnerability

Google Threat Intelligence Group

January 27, 2026



Google Cloud

Threat Intelligence

Google Threat Intelligence

Visibility and context on the threats that matter most.

[Contact Us & Get a Demo](#)

Introduction

The Google Threat Intelligence Group (GTIG) has identified widespread, active exploitation of the critical vulnerability [CVE-2025-8088](#) in WinRAR, a popular file archiver tool for Windows, to establish initial access and deliver diverse payloads. Discovered and patched in July 2025, government-backed threat actors linked to Russia and China as well as financially motivated threat actors continue to exploit this n-day across disparate operations. The consistent exploitation method, a path traversal flaw allowing files to be dropped into the Windows Startup folder for persistence, underscores a defensive gap in fundamental application security and user awareness.

In this blog post, we provide details on CVE-2025-8088 and the typical exploit chain, highlight exploitation by financially motivated and state-sponsored espionage actors, and provide IOCs to help defenders detect and hunt for the activity described in this post.

To protect against this threat, we urge organizations and users to keep software fully up-to-date and to install security updates as soon as they become available. After a vulnerability has been patched, malicious actors will continue to rely on n-days and use slow patching rates to their advantage. We also recommend the use of [Google Safe Browsing](#) and Gmail, which actively identifies and blocks files containing the exploit.

Vulnerability and Exploit Mechanism

CVE-2025-8088 is a high-severity path traversal vulnerability in WinRAR that attackers exploit by leveraging Alternate Data Streams (ADS). Adversaries can craft malicious RAR archives which, when opened by a vulnerable version of WinRAR, can write files to arbitrary locations on the system. Exploitation of this vulnerability in the wild [began as early](#) as July 18, 2025, and the vulnerability was addressed by RARLAB with the release of [WinRAR version 7.13](#) shortly after, on July 30, 2025.

The exploit chain often involves concealing the malicious file within the ADS of a decoy file inside the archive. While the user typically views a decoy document (such as a PDF) within the archive, there are also malicious ADS entries, some containing a hidden payload while others are dummy data.

The payload is written with a specially crafted path designed to traverse to a critical directory, frequently targeting the Windows Startup folder for persistence. The key to the path traversal is the use of the ADS feature combined with directory traversal characters.

For example, a file within the RAR archive might have a composite name like `innocuous.pdf:malicious.lnk` combined with a malicious path: `../../../../../../../../Users/<user>/AppData/Roaming/Microsoft/Windows/Start Menu/Programs/Startup/malicious.lnk`.

When the archive is opened, the ADS content (`malicious.lnk`) is extracted to the destination specified by the traversal path, automatically executing the payload the next time the user logs in.

State-Sponsored Espionage Activity

Multiple government-backed actors have adopted the CVE-2025-8088 exploit, predominantly focusing on military, government, and technology targets. This is similar to the [widespread exploitation of a known WinRAR bug in 2023, CVE-2023-38831](#), highlighting that exploits for known vulnerabilities can be highly effective, despite a patch being available.

Figure 1: Timeline of notable observed exploitation

Russia-Nexus Actors Targeting Ukraine

Suspected Russia-nexus threat groups are consistently exploiting CVE-2025-8088 in campaigns targeting Ukrainian military and government entities, using highly tailored geopolitical lures.

UNC4895 (CIGAR): UNC4895 (also publicly reported as RomCom) is a dual financial and espionage-motivated threat group whose [campaigns](#) often involve spearphishing emails with lures tailored to the recipient. We observed subjects indicating targeting of Ukrainian military units. The final payload belongs to the NESTPACKER malware family (externally known as Snipbot).

Figure 2: Ukrainian language decoy document from UNC4895 campaign

- **APT44 (FROZENBARENTS):** This Russian APT group exploits CVE-2025-8088 to drop a decoy file with a Ukrainian filename, as well as a malicious LNK file that attempts further downloads.
- **TEMP.Armageddon (CARPATHIAN):** This actor, also targeting Ukrainian government entities, uses RAR archives to drop HTA files into the Startup folder. The HTA file acts as a downloader for a second stage. The initial downloader is typically contained within an archive packed inside an HTML file. This activity has continued through January 2026.
- **Turla (SUMMIT):** This actor adopted CVE-2025-8088 to deliver the STOCKSTAY malware suite. Observed lures are themed around Ukrainian military activities and drone operations.

China-Nexus Actors

A PRC-based actor is exploiting the vulnerability to deliver POISONIVY malware via a BAT file dropped into the Startup folder, which then downloads a dropper.

Financially Motivated Activity

Financially motivated threat actors also quickly adopted the vulnerability to deploy commodity RATs and information stealers against commercial targets.

- A group that has targeted entities in Indonesia using lure documents used this vulnerability to drop a .cmd file into the Startup folder. This script then downloads a password-protected RAR archive from Dropbox, which contains a backdoor that communicates with a Telegram bot command and control.
- A group known for targeting the hospitality and travel sectors, particularly in LATAM, is using phishing emails themed around hotel bookings to eventually deliver commodity RATs such as XWorm and AsyncRAT.
- A group targeting Brazilian users via banking websites delivered a malicious Chrome extension that injects JavaScript into the pages of two Brazilian banking sites to display phishing content and steal credentials.
- In December and January 2026, we have continued to observe malware being distributed by cyber crime exploiting CVE-2025-8088, including commodity RATS and stealers.

The Underground Exploit Ecosystem: Suppliers Like "zeroplayer"

The widespread use of CVE-2025-8088 by diverse actors highlights the demand for effective exploits. This demand is met by the underground economy where individuals and groups specialize in developing and selling exploits to a range of customers. A notable example of such an upstream supplier is the actor known as "zeroplayer," who advertised a WinRAR exploit in July 2025.

The WinRAR vulnerability is not the only exploit in zeroplayer's arsenal. Historically, and in recent months, zeroplayer has continued to offer other high-priced exploits that could potentially allow threat actors to bypass security measures. The actor's advertised portfolio includes the following among others:

- In November 2025, zeroplayer claimed to have a sandbox escape RCE zero-day exploit for Microsoft Office advertising it for \$300,000.
- In late September 2025, zeroplayer advertised a RCE zero-day exploit for a popular, unnamed corporate VPN provider; the price for the exploit was not specified.
- Starting in mid-October 2025, zeroplayer advertised a zero-day Local Privilege Escalation (LPE) exploit for Windows listing its price as \$100,000.
- In early September 2025, zeroplayer advertised a zero-day exploit for a vulnerability that exists in an unspecified drive that would allow an attacker to disable antivirus (AV) and endpoint detection and response (EDR) software; this exploit was advertised for \$80,000.

zeroplayer's continued activity as an upstream supplier of exploits highlights the continued commoditization of the attack lifecycle. By providing ready-to-use capabilities, actors such as zeroplayer reduce the technical complexity and resource demands for threat actors, allowing groups with diverse motivations—from ransomware deployment to state-sponsored intelligence gathering—to leverage a diverse set of capabilities.

Conclusion

The widespread and opportunistic exploitation of CVE-2025-8088 by a wide range of threat actors underscores its proven reliability as a commodity initial access vector. It also serves as a stark reminder of the enduring danger posed by n-day vulnerabilities. When a reliable proof of concept for a critical flaw enters the cyber criminal and espionage marketplace, adoption is instantaneous, blurring the line between sophisticated government-backed operations and financially motivated campaigns. This vulnerability's rapid commoditization reinforces that a successful defense against these threats requires immediate application patching, coupled with a fundamental shift toward detecting the consistent, predictable post-exploitation TTPs.

Indicators of Compromise (IOCs)

To assist the wider community in hunting and identifying activity outlined in this blog post, we have included indicators of compromise (IOCs) in a [GTI Collection for registered users](#).

File Indicators

Filename	SHA-256
1_14_5_1472_29.12.2025.rar	272c86c6db95f1ef8b83f672b65e64df16494cae261e1aba1aeb1e59dcb68524
2_16_9_1087_16.01.2026.rar	33580073680016f23bf474e6e62c61bf6a776e561385bfb06788a4713114ba9d
5_18_6_1405_25.12.2025.rar	498961237cf1c48f1e7764829818c5ba0af24a234c2f29c4420fb80276aec676
2_13_3_1593_26.12.2025.rar	4f4567abe9ff520797b04b04255bbbe07ecdddb594559d436ac53314ec62c1b3
5_18_6_1028_25.12.2025.rar	53f1b841d323c211c715b8f80d0efb9529440caae921a60340de027052946dd9
2_12_7_1662_26.12.2025.rar	55b3dc57929d8eacfdadc71d92483eabe4874bf3d0189f861b145705a0f0a8fe
1_11_4_1742_29.12.2025.rar	68d9020aa9b509a6d018d6d9f4c77e7604a588b2848e05da6a4d9f82d725f91b
2_18_3_1468_16.01.2026.rar	6d3586aa6603f1c1c79d7bd7e0b5c5f0cc8e8a84577c35d21b0f462656c2e1f9
1_16_2_1428_29.12.2025.rar	ae93d9327a91e90bf7744c6ce0eb4afbf3acb62a5d1b2dafd645cba9af28d795
1_12_7_1721_29.12.2025.rar	b90ef1d21523eeffbca17181ccccf269bca3840786fcbf5c73218c6e1d6a51a9
N/A	c7726c166e1947fdbf808a50b75ca7400d56fa6fef2a76cefe314848db22c76c
1_15_7_1850_29.12.2025.rar	e836873479ff558cfb885097e8783356aad1f2d30b69d825b3a71cb7a57cf930
2_16_2_1526_26.12.2025.rar	ffc6c3805bbaef2c4003763fd5fac0ebcccf99a1656f10cf7677f6c2a5d16dbd
N/A	958921ea0995482fb04ea4a50bbdb654f272ab991046a43c1fdbd22da302d544
підтверджуючі документи.pdf	defe25e400d4925d8a2bb4b1181044d06a8bf61688fd9c9ea59f1e0bb7bc21d8
Desktop_Internet.lnk	edc1f7528ca93ec432daca820f47e08d218b79cceca1ee764966f8f90d6a58bd
N/A	29f89486bb820d40c9bee8bf70ee8664ea270b16e486af4a53ab703996943256
N/A	2c40e7cf613bf2806ff6e9bc396058fe4f85926493979189dbdbc7d615b7cb14
N/A	3b85d0261ab2531aba9e2992eb85273be0e26fe61e4592862d8f45d6807ceee4
N/A	54305c7b95d8105601461bb18de87f1f679d833f15e38a9ee7895a0c8605c0d0
N/A	5dee69127d501142413fb93fd2af8c8a378682c140c52b48990a5c41f2ce3616

N/A	867a05d67dd184d544d5513f4f07959a7c2b558197c99cb8139ea797ad9fbece
N/A	91e61fd77460393a89a8af657d09df6a815465f6ce22f1db8277d58342b32249
N/A	b2b62703a1ef7d9d3376c6b3609cd901cbcccca80fba940ce8ed3f4e54cdbe6
N/A	cf35ce47b35f1405969f40633fcf35132ca3ccb3fdfded8cc270fc2223049b80
N/A	d981a16b9da1615514a02f5ebb38416a009f5621c0b718214d5b105c9f552389
N/A	ddd67dda5d58c7480152c9f6e8043c3ea7de2e593beedf86b867b83f005bf0cc
N/A	ea0869fa9d5e23bdd16cddfefbbf9c67744598f379be306ff652f910db1ba162
N/A	ef0e1bb2d389ab8b5f15d2f83cf978662e18e31dbe875f39db563e8a019af577
N/A	f3e5667d02f95c001c717dfc5a0e100d2b701be4ec35a3e6875dc276431a7497
N/A	f6761b5341a33188a7a1ca7a904d5866e07b8ddbde9adebdbce4306923cfc60a
N/A	fc2a6138786fae4e33dc343aea2b1a7cd6411187307ea2c82cd96b45f6d1f2a0
N/A	a97f460bfa612f1d406823620d0d25e381f9b980a0497e2775269917a7150f04
N/A	d418f878fa02729b38b5384bcb3216872a968f5d0c9c77609d8c5aacedb07546
3-965_26.09.2025.HTA	ba86b6e0199b8907427364246f049efd67dc4eda0b5078f4bc7607253634cf24
Заява про скоєння злочину 3-965_26.09.2025.rar	cf8ebfd98da3025dc09d0b3bbeef874d8f9c4d4ba4937719f0a9a3aa04c81beb
Proposal_for_Cooperation_3415.05092025.rar	5b64786ed92545eeac013be9456e1ff03d95073910742e45ff6b88a86e91901b
N/A	8a7ee2a8e6b3476319a3a0d5846805fd25fa388c7f2215668bc134202ea093fa
N/A	3b47df790abb4eb3ac570b50bf96bb1943d4b46851430ebf3fc36f645061491b
document.rar	bb4856a66bf7e0de18522e35798c0a8734179c1aab21ed2ad6821aaa99e1cb4c
update.bat	aea13e5871b683a19a05015ff0369b412b985d47eb67a3af93f44400a026b4b0
ocean.rar	ed5b920dad5dcd3f9e55828f82a27211a212839c8942531c288535b92df7f453
expl.rar	a54bcafd9d4ece87fa314d508a68f47b0ec3351c0a270aa2ed3a0e275b9db03c
BrowserUpdate.Ink	b53069a380a9dd3dc1c75888d0e50dd43935f16df0f7124c77569375a9f44f5

Posted in [Threat Intelligence](#)