RomCom Exploitation of CVE-2025-8088 (WinRAR Zero-Day) Reproduction & Forensic Analysis

Technical Threat Report & Lab Reproduction – October 2025

Written by: Kevin Pigney | Cybersecurity Major | Focus: DFIR

Table of Contents

CVE-2025-8088 (WinRAR Zero-Day Exploited by RomCom)

1.0 Executive Summary:

I am a senior cybersecurity student specializing in incident response, digital forensics, and threat intelligence, with a strong interest in researching threat actors and documenting their tradecraft in a way that defenders can apply directly. This report focuses on RomCom (aka Storm-0978/DEV-0978), a Russia-linked group active since 2022 that blends espionage with financially motivated operations. RomCom has targeted government, defense, and energy sectors in Ukraine, pharmaceutical and insurance firms in the U.S., and legal and critical infrastructure organizations across Europe and the U.K. Their campaigns pair convincing social engineering with technical stealth, using phishing lures, stolen code-signing certificates, and deceptive infrastructure to gain initial access and maintain persistence.

One of RomCom's current techniques involves exploiting CVE-2025-8088, a high-severity path-traversal vulnerability in WinRAR. By embedding decoy documents and crafted archive headers, RomCom can cause payloads to be written directly into persistence locations such as the Windows Startup folder whenever a user extracts the archive. This write-up highlights why the vulnerability is dangerous, demonstrates it in a controlled lab setting, and presents forensic evidence, indicators of compromise, and defensive recommendations. The goal is to provide actionable insights that security teams can use to detect similar activity and to showcase how targeted research and documentation contribute to effective threat hunting and SOC operations.

2.0 Who is RomCom?

RomCom is a Russia-linked cybercriminal group active since 2022. They operate at the intersection of espionage and financial crime, blending traditional APT-style targeting with opportunistic monetization. Security vendors and government agencies track them under multiple aliases, and they've steadily expanded their operations across critical industries in the U.S. and Europe.

2.1 Aliases (depending on reporting organization):

- Storm-0978 (Microsoft)
- DEV-0978
- RomCom
- Tropical Scorpius

- UNC2596 (Mandiant)
- Void Rabisu
- UAC-0180

2.2 Known Motives:

- Espionage in support of Russian geopolitical interests (Ukraine defense, European governments)
- Financially motivated operations (targeting insurance, pharmaceutical, and legal sectors for data theft, extortion, or resale)

2.3 Operational characteristics:

- Active since 2022, steadily increasing in sophistication and scope
- Combines custom malware with widely available vulnerabilities and tools
- Emphasizes social engineering and masquerading (complaints, resumes, invoices)
- Uses deceptive infrastructure (shorteners, fake cloud domains, VPS-hosted redirectors) to evade detection.

3.0 Targeting History:

RomCom's campaigns have been global in scope, but they consistently focus on sectors where disruption or intelligence gathering supports both espionage and financial gain. Their targeting reflects a dual mission: advancing Russian strategic interests while profiting from opportunistic data theft and monetization.

3.1 By geography and sector:

- Ukraine:
    - Government ministries, defense contractors, and energy providers
    - Espionage operations linked to ongoing conflict and intelligence collection.
- United States:
    - Pharmaceutical companies (intellectual property theft)
    - Insurance providers (financially motivated, data for resale or extortion)
- United Kingdom:
    - Retail, hospitality and critical national infrastructure (CNI)
    - Notably through Operation Deceptive Prospect (2024), which abused customer feedback portals with malicious complaint submissions
- Germany & broader Europe:

- Legal firms and government organizations
- Likely focused on intelligence collection and disruption of policy/decision-making

3.2 Trends:

- Consistent pivot from high-value espionage (Ukraine, Europe) to opportunistic financial crime (U.S. commercial sectors)
- Preference for entry via trusted communications channels (feedback portals, resumes, CVs, legal documents)
- Gradual increase in scope since 2022, suggesting sustained resources and operational support.

4.0 Tactics, Techniques, and Procedures (TTPs):

4.1 Delivery & Initial Access:

- Spear-phishing – Emails or feedback portal submissions disguised as customer complaints or resumes (T1566.002)
- Masquerading – Payloads disguised as benign PDFs or documents (T1036 / T1036.008)
- Exploitation of Trust – Using formats that mimic trusted services (Google Drive, OneDrive) (T1199)
- Use of AI-generated content – Polished, templated phishing emails suggest AI assistance (T1588.007)

4.2 Execution & Persistence:

- Impersonation – Fake personas, customer complaints, or legal correspondence to build credibility (T1656)
- Code signing with stolen certificates – Malicious binaries appear legitimately signed (T1553.002 / T1587.002)
- Payload placement in autorun folders – Via CVE-2025-8088 exploitation of WinRAR

4.3 Defense Evasion:

- Sandbox evasion – Malware checks registry values (e.g., RecentDocs) to detect VMs before execution (T1497)
- Masquerading / decoys – Use of professional-looking documents to distract analysts (T1036)

4.4 Command & Control / Infrastructure:

- Domain and infrastructure acquisition – Registering deceptive domains through services like Rebrandly (T1583)
- Compromised hosting / VPS use – Payload hosting on third-party VPS or redirector

---

5.0 CVE-2025-8088 – Vulnerability Details

CVE-2025-8088 is a high-severity path traversal vulnerability in the Windows version of WinRAR and the associated UnRAR library. The flaw enables attackers to craft malicious RAR archives that, when extracted, cause files to be written outside the intended directory. RomCom has actively exploited this weakness in phishing campaigns to drop payloads into persistence locations such as the Windows Startup folder, ensuring execution at the next logon.

5.1 Key facts about CVE-2025-8088:

- Vulnerability type: Path traversal (CWE-22)
- Root cause: WinRAR failed to properly validate and canonicalize file paths from archive headers, allowing sequences like `..\..\` to escape the extraction directory.
- Exploit method: Attackers embed decoy documents alongside malicious entries. Crafted headers with traversal sequences redirect extraction into sensitive folders (e.g., `Startup`, `ProgramData`). Some proofs-of-concept also use NTFS Alternate Data Streams (ADS) to hide payloads within seemingly benign files.
- Exploitation outcome: Arbitrary code execution and persistence – for example, a `.bat` or `.exe` file executing the next reboot.

5.2 Affected Versions of WinRAR (and Related Software):

- WinRAR versions prior to 7.13 (confirmed vulnerable).
- Other applications bundling UnRAR`.dll` (e.g., dtSearch for Windows ≤ 2022.02) are also vulnerable if not updated.

5.3 CVSS Score and Impact:

Metric	CVSS v3.1	CVSS v4.0	Explanation
Attack Vector	**AV:N** – Network	**AV:L** – Local	v3.1 scores "Network" since the RAR can be delivered remotely. v4.0 emphasizes that exploitation actually occurs *locally* when the victim extracts the archive.
Attack Complexity	**AC:L** – Low	**AC:L** – Low	Straightforward exploit - no special conditions needed.
Privileges Required	**PR:N** – None	**PR:N** – None	Attacker doesn't need any prior access.
User Interaction	**UI:R** – Required	**UI:A** – Active	User must interact: open and extract the malicious RAR. v4.0 makes this "Active" interaction explicit.
Scope	**S:U** – Unchanged	N/A (handled via system vs vulnerability impact split)	v3.1 includes a scope field; v4.0 separates component vs system impacts.
Confidentiality Impact	**C:H** – High	**VC:H** – High	Both models: attacker can gain sensitive data access.
Integrity Impact	**I:H** – High	**VI:H** – High	Attacker can alter files, inject malware, modify system state.
Availability Impact	**A:H** – High	**VA:H** – High	Attacker can cause crashes or enable ransomware for denial of service.
System Impact Metrics	N/A	**SC:N / SI:N / SA:N** – None	v4.0 explicitly adds "system impact" metrics, clarifying that the bug itself doesn't directly cross into broader OS scope without payload.
Base Score	**8.8 – High**	**8.4 – High**	Both rate as High severity. v4.0 drops slightly due to "Local" vector.

5.4 Why it matters:

- The vulnerability turns a single user action (extracting an archive) into a reliable persistence mechanism.
- It is easy to weaponize (low complexity, no privileges required).

- The exploit fits RomCom's delivery style (phishing/feedback portals with convincing decoy documents).
- Organizations often underestimate archive vulnerabilities – making this an attractive zero-day for threat actors.

6.0 Exploit Chain Explained – decoy doc, ADS, RAR headers, path traversal, persistence

Short overview:

- RomCom crafts malicious RAR archives that combine a believable decoy document with hidden payload entries and carefully manipulated header filenames so that, when extracted by a vulnerable WinRAR, one or more payloads are written into persistence locations (e.g., the user Startup folder), achieving execution at next logon.

6.1 The components – what each piece does

- Decoy document (social engineering + carrier):
    - A polished, legitimate-looking file (CV, invoice, complaint) sits as the visible artifact in the archive.
    - Purpose: Encourages manual extraction/opening and provides a plausible host for alternate data streams; reduces immediate suspicion during casual inspection.
- NTFS Alternate Data Streams (ADS):
    - ADS allow additional data to be attached to a file without creating a separate visible file (e.g., `document.pdf:stream`).
    - Attackers may include payload bytes as streams on the decoy so that even after extraction the malicious content is not visible in directory listings unless specifically enumerated.
    - ADS use increases stealth and complicates cursory triage.
- RAR header manipulation (filename fields):
    - Each archive entry contains header fields including the filename the extractor will write to disk. Attackers set those fields to attacker-controlled strings that include relative path traversal markers (e.g., `..\` sequences) or ADS-like notation.

        - The vulnerability arises when the extractor trusts/uses that header value without correctly canonicalizing or validating the resulting target path.
    - Path traversal / canonicalization bug:
        - Secure extraction should join the destination directory and the entry filename, canonicalize the path (normalize .. segments), and verify the result remains inside the intended extraction root.
        - The bug in the vulnerable library occurs when this validation is missing, incomplete, or performed incorrectly – allowing an entry like `..\..\AppData\Roaming\...\Startup\payload.bat` to escape the extraction root and be written to the Startup folder.
    - Persistence & execution:
        - The end goal is a write to a persistence location (Startup, Run keys, ProgramData, scheduled task). Once present in Startup, the payload executes at the next user login, a reliable persistence primitive for threat actors.

6.2 A realistic scenario (realistic story to illustrate the chain)

Scenario – Malicious resume delivered to HR:

A RomCom operator targets a human-resources inbox at a mid-size organization by submitting or emailing a job application. The lure is a professional-looking resume named `Alicia_Sheree_CV_2025.pdf` bundled inside a compressed archive with a plausible filename (for example, `Alicia_Sheree_Application.zip` or `Alice_Sheree_CV.rar`). The archive is delivered via email or a feedback/portal upload where HR staff routinely download and open attachments.

When the recipient extracts or opens the visible resume from the archive using a vulnerable WinRAR build, the crafted archive headers cause hidden entries to be written into a persistence location. The result is a dropped payload.bat (or similar artifact) placed in the user's startup, which executes at next logon and provides the attacker with a reliable foothold.

6.3 Forensic Artifacts & Investigation Checklist

This section summarizes all key forensic artifacts and recommended investigation steps for identifying exploitation of CVE-2025-8088 (WinRAR Path Traversal). Each

artifact type includes both what to look for and how to validate it in a real-world analysis.

1. Process Evidence
    - What to look for: `WinRAR.exe` performing a `WriteFile` operation targeting the Windows Startup folder.
    - How to validate: Confirm in Procmon (or Sysmon) that WinRAR wrote a new file in `C:\Users\<user>\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup`.
    - Follow-up: Check subsequent process creation events (Sysmon or DeviceProcessEvents tables in EDRs) for the dropped files being executed at logon via `cmd.exe` or `powershell.exe`.
2. File System Artifacts (Persistence Confirmation):
    - What to look for: The dropped payload in the user's startup folder (this confirms persistence).
    - How to validate:
        - Verify the payload's presence in the Startup path.
        - Check creation and modification timestamps, they should closely align with the time the malicious RAR archive was extracted or opened.
    - Real-world IOCs:
        - `ApbxHelper.exe` – linked to the SnipBot backdoor used by RomCom.
        - `msedge.dll` - associated with the Mythic agent payload
          Note: These filenames have been observed in real RomCom incidents and should be prioritized during investigation.
    - Follow-up: Hash and analyze any `.exe`, `.dll`, or `.bat` discovered; compare against current threat intelligence databases and internal baselines.
3. Network Indicators (if applicable):
    - What to look for: Outbound HTTP(S) or DNS traffic initiated post-logon by the dropped payload.
    - How to validate: Review EDR or firewall telemetry for network connections occurring within seconds of the payload's execution, particularly to uncommon or recently registered domains.
4. Evidence Documentation:
    - What to capture:
        - Procmon trace showing `WinRAR.exe` writing to Startup.
        - Autoruns output highlighting the new entry.
        - File Explorer view confirming payload presence in Startup.

    - Screenshot of the payload executing after rebooting.
- Why it matters: This visual provides end-to-end confirmation for exploitation, persistence, and execution. They also create a clear chain of evidence for later reporting or sharing with security or legal teams.

Analyst Note

The presence of a user-dropped payload within the Windows Startup folder, especially one created by `WinRAR.exe`, is a strong indicator of this exploit. These filenames `ApbxHelper.exe` and `msedge.dll` have been linked to RomCom follow-on payloads in the wild and should be treated as priority indicators in enterprise threat hunting and forensic review.

7.0 Recent RomCom Activity Exploiting CVE-2025-8088

Since mid-2025 RomCom has actively weaponized CVE-2025-8088 (a WinRAR path-traversal zero-day) in targeted social-engineering campaigns that delivered RAR archives containing decoy documents and hidden payloads to place files into persistence locations.

7.1 What researchers observed:

- ESET and multiple industry teams reported active exploitation of a WinRAR directory-traversal zero-day by a Russia-linked group attributed to RomCom (aka Storm-0978 / DEV-0978). The PoC/weaponized archives commonly used job applications, CVs, complaint documents, or other believable business files as decoys to induce extraction.
- Public reporting connects the exploitation of CVE-2025-8088 to campaigns that target help-desk and frontline teams (e.g., customer feedback portals) as well as HR/job-application workflows, an operational choice that increases the chance an archive will be extracted manually. This pattern is described in vendor writeups and CTI analysis of “Operation Deceptive Prospect.”
- Multiple security vendors and blogs note that the exploit’s outcome is a direct file write to persistence locations (Startup, ProgramData), enabling immediate persistence and reliable execution at next logon; vendors publicly advised urgent patching to WinRAR 7.13.

7.2 Scope & targets:

- Reported target sets align with RomCom's prior activity: government and defense in Ukraine, pharmaceutical and insurance companies in the U.S., legal firms in Germany/Europe, and UK retail/hospitality and CNI via the feedback-portal vector. These sectoral focuses are visible across multiple CTI writeups.
- Public reporting also highlights campaigns that used job-application themed lures (e.g., fake CVs), a delivery method that was observed in several ESET analyses and follow-on vendor writeups. This is the scenario that I will be recreating later in this report, a deceptive resume .pdf file on an HR employee's endpoint.

7.3 Malware and post-exploit behavior (what RomCom has been observed doing after initial foothold):

- Reports indicate operators often deploy small stagers or downloaders as the first payload (allowing staged delivery of more capable backdoors). Some public vendor writeups mention follow-on tooling families observed in associated campaigns (vendor coverage varies by reporting organization).

Operational notes (why this is attractive to RomCom)

- *The attack requires comparatively little sophistication from the victim, the primary action required is extraction of the archive, yet yields reliable persistence, making it highly efficient for an actor that favors socially plausible lures and broad reach. Public advisories emphasize this low-complexity, high-impact profile.*

7.4 Defensive posture & vendor guidance

- Multiple vendors and advisories (ESET, GHSA/CVE entries, vendor blogs) recommended immediate upgrade to WinRAR 7.13 (or removal of vulnerable UnRAR components where updates are not possible). They also advised treating archive attachments from external/untrusted sources as high-risk and sandboxing/examining them prior to user delivery.

8.0 Lab Reproduction & Forensic Observations:

8.1 Objective:

My goal of this exercise was twofold: (1) reproduce CVE-2025-8088 exploit in an isolated environment to validate the attack chain observed in public reports, and (2) perform a pragmatic forensic examination using free, readily available tools so defenders and entry-level DFIR analysts can reproduce the analysis, beyond simply proving the exploit works, I wanted to show "what happens in the background" when a user, for example, opens what appears to be an innocent resume PDF, without knowing that the archive they extracted is performing hidden actions.

8.2 Test Environment:

- Virtualization Platform: Oracle VirtualBox
- Operating System: Windows 10 Pro (64-bit) – Build 19045 (10.0.19045)
- Base Memory: 4 GB (4096 MB)
- Processors: 2 vCPUs
- Virtual Disk: 40 GB (Win10.vdi)
- Python: 3.13.7 (Installed for PoC execution)
- WinRAR: 6.24 (File version 6.24.0.0, Copyright © Alexander Roshal 1993-2023)
- Additional Tools: Procmon and Autoruns

Note: Wireshark is recommended when the payload may perform network activity; this lab used a benign local payload, so network capture was not required.

8.3 Methodology – brief explanation as to how the lab was performed

1. Restore an isolated pre-test VM snapshot to guarantee a known clean state.
2. Launch Procmon with narrow inclusion filters focusing on WinRAR and file writes operations to persistence paths (to reduce noise and highlight relevant events).
3. Collect a baseline Autoruns export (`autoruns_before.txt`) as an administrator to capture the pre-exploit persistence state.
4. Download the public PoC (`CVE-2025-8088.py`) from GitHub into the VM and execute it to generate the malicious test archive. The PoC produces `exploit.rar`, which includes a visible decoy document (`Alicia_Sheree_CV_2025.pdf`) and the crafted entries designed to trigger the vulnerability upon extraction.

5. Place `exploit.rar` on the VM desktop to simulate a real victim, then open `Alicia_Sheree_CV_2025.pdf` directly from the archive, doing so triggers the exploit.
6. Stop the Procmon capture immediately after extraction and export the capture file (PML) and a filtered CSV of relevant rows for reporting and review.
7. Export post-exploit Autoruns (`autoruns_after.txt`) to capture any newly created persistence artifacts (Startup entries or registry run keys).
8. Reboot the VM to confirm the payload's execution on the next logon and capture a screenshot of the benign payload running to demonstrate persistence.
9. Calculate the SHA256 of the dropped payload and record it in `hashes.txt` within your evidence folder; check the hash on VirusTotal (zero detections for the benign lab payload)
10. Preserve the investigation artifacts – `procmon_run1.pml`, `procmon_run1.csv`, `autoruns_before.txt`, `autoruns_after.txt`, screenshots, and `hashes.txt`, in an evidence folder for further review.

8.4 Findings – what the evidence shows

1. RAR generation and contents
   - Observation: The PoC created exploit.rar containing the decoy PDF and multiple hidden entries. WinRAR displays the visible PDF in the archive content's view.
   - Why it matters: Demonstrates the payload and decoy co-exist in the archive.

```
PS C:\CVE-2025-8088-Exploit-main> py -3 .\CVE-2025-8088.py
Notes: Using your own file will work with .txt,.sh,.py,.sql but not PDF, jpeg, png etc
Choose input mode:
1. Create fake document
2. Use existing file from this folder
Enter choice (1 or 2): 1

Choose document type:
1. PDF CV document (.pdf)
2. PDF PENTEST document (.pdf)
Enter choice: 1
Creating CV document...
Created professional CV: Alicia_Sheree_CV_2025.pdf
Attaching 10 ADS streams to Alicia_Sheree_CV_2025.pdf...
Successfully patched 10 streams

Exploit created: exploit.rar
Payload will attempt to drop to startup folder using 10 different depths
Note: At least one should succeed in common extraction locations
To test, extract 'exploit.rar' to a folder (e.g., Desktop) and check:
  - %APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\payload.bat
  - Run 'dir /R' on the extracted PDF to verify ADS streams
PS C:\CVE-2025-8088-Exploit-main>
```

Figure 1 & 2 – The Python proof-of-concept (`CVE-2025-8088.py`) was executed to generate a malicious archive named `exploit.rar`. During execution, the script created a decoy document (`Alicia_Sheree_CV_2025.pdf`) and attached multiple Alternate Data Streams (ADS) to it, then crafted the RAR headers to embed traversal paths. The resulting archive was designed so that when files within are extracted or opened, `payload.bat` would be written into the Windows Startup directory.

2. Decoy PDF present and visually legitimate
    - Observation: The archive contained a decoy resume named `Alicia_Sheree_CV_2025.pdf` that was visible to the user. In this lab run, either extracting the archive or opening the decoy PDF from the archive was sufficient to trigger the vulnerability, resulting in `payload.bat` being written to `C:\Users\<user>\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup`.
    - Why it matters: This behavior lowers the bar for successful compromise: a user does not need to knowingly execute an EXE or run a script, a normal action (open or extract) is enough. That makes the attack highly effective against help-desk, HR, and other staff who regularly handle document attachments.

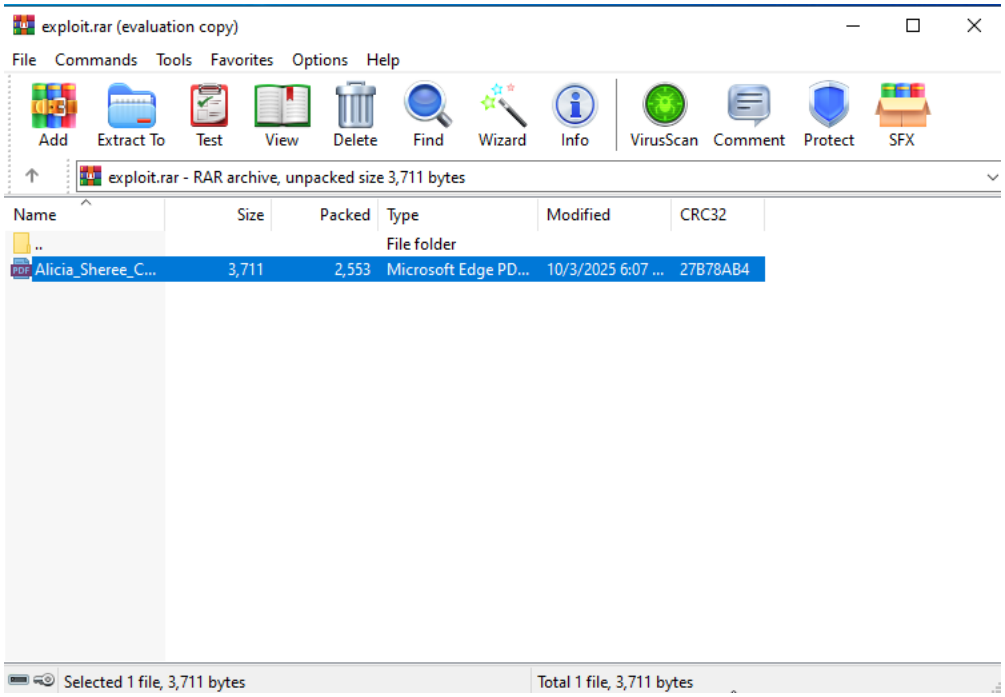


Figure 3 – Decoy PDF present in the exploit archive. The file `Alicia_Sheree_CV_2025.pdf` appears harmless but extracting or opening it triggers the vulnerability and writes `payload.bat` into the Startup folder.

3. WinRAR writes files to Startup (process-level evidence)
    - Observation: Procmon captured a `WriteFile` operation by `WinRAR.exe` to `C:\Users\<user>\AppData\Roaming\Microsoft\Windows\Start`

`Menu\Programs\Startup\payload.bat`. The Procmon line contains the operation name, process, path, and success status. Procmon PML saved.

- Why it matters: This is definitive proof that extraction caused a write to a persistence location outside the intended extraction directory.

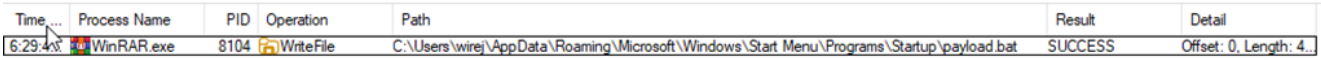


Figure 4 – Procmon capture showing `WinRAR.exe` writing to Startup.

4. Persistence confirmed via Autoruns
    - Observation: Procmon captured a `WriteFile` operation from `WinRAR.exe` targeting `C:\Users\<user>\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\payload.bat`. Subsequent analysis in Autoruns confirmed a new Startup entry pointing to the same `payload.bat` path. Cross-referencing both tools verifies that the extraction process established OS-level persistence.
    - Why it matters: This demonstrates how this vulnerability can be weaponized to achieve persistence without elevated privileges or direct registry modification, the attacker gains a guaranteed code execution point every logon.

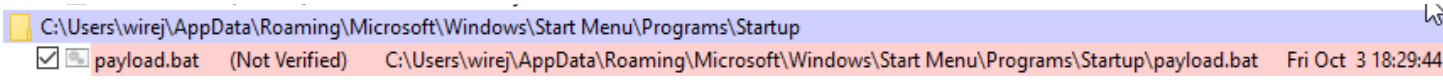


Figure 5 – Autoruns output confirming a new Startup entry.

5. Dropped file in Explorer & payload execution
    - Observation: The Startup folder contains the payload. After a reboot, the payload executed. Creation timestamps and file hash recorded. VirusTotal returned no detections for this lab's benign payload.
    - Why it matters: Completes the end-to-end chain: extraction → write to Startup → execution at logon.

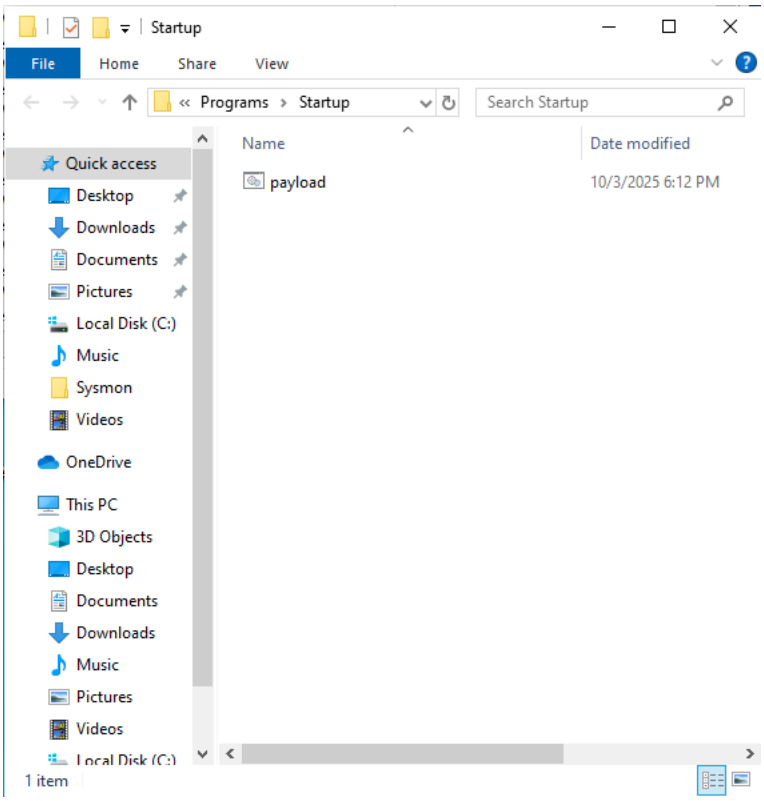


Figure 6 – File explorer view of the Startup folder containing the dropped payload.

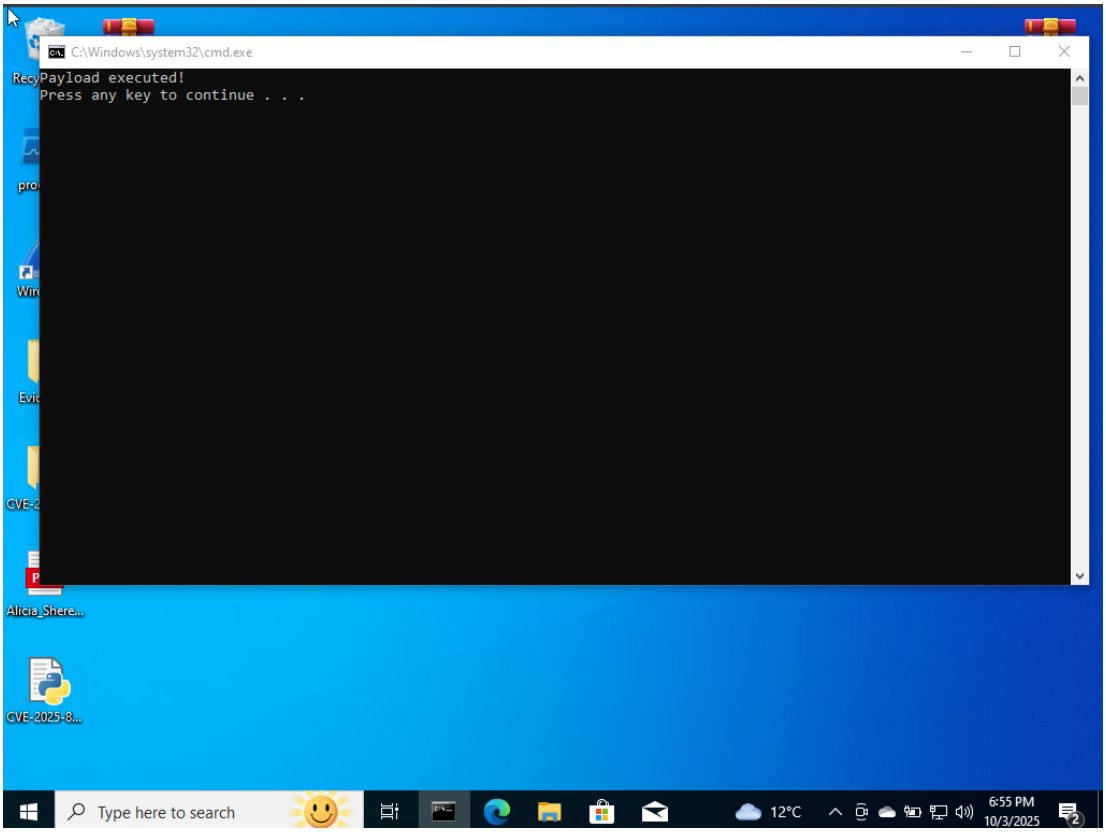
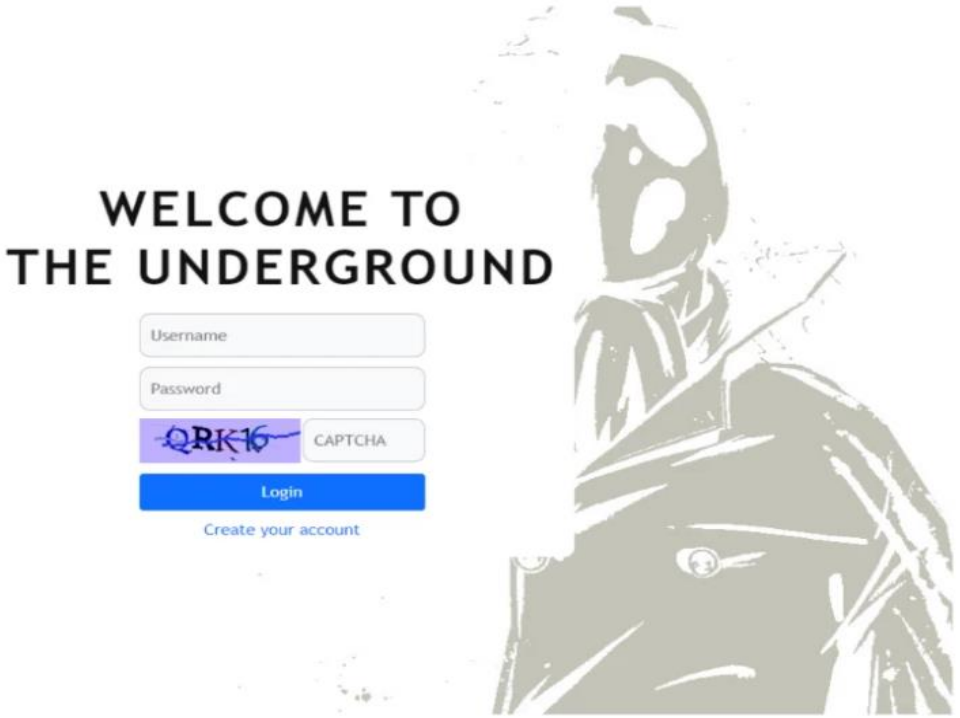


Figure 7 – Benign payload execution (post-reboot)

```
Note:

The Underground team welcomes you!


We would like to inform that your network has been tested by us for vulnerabilities.


Poor network security could cause your data to be lost forever.


Your files are currently encrypted, they can be restored to their original state with a decryptor key that only we have.

The key is in a single copy on our server.


Attempting to recover data by your own efforts may result in data loss.

It is important not to change their current state. Each file additionally has a unique cipher, which you can restore only with our help.


We also examined your infrastructure and downloaded the most sensitive data.

The list of hosts from which the information was downloaded:
```



Figures 8 & 9 – These are real-world post-infection artifacts, victims of a real-world cyber-attack would likely see something like this note on their screens. This was a RomCom ransomware-note sample I found in other write-ups involving RomCom's ransomware attacks. Along with this login screen that read "Welcome To The Underground".

8.5 Limitations & what I did not capture

- Sysmon logging was configured but Sysmon exports were not available for this run due to log visibility issues; Procmon and Autoruns provided sufficient evidence for the exploit chain. If desired, a re-run with validated Sysmon logging would produce Event ID 11 (file create) and Event ID 1 (process create) entries for more structured telemetry.
- Network activity was minimal in the lab because the payload was a harmless test stub; in live incidents, network captures and EDR logs are invaluable for identifying C2 infrastructure and subsequent stages.

Conclusion & short recommendation tie-in

- My lab reproduction shows a compact, reliable chain: user extracts/opens file within RAR archive → WinRAR writes payload into Startup → persistence and execution at logon. The artifacts captured (Procmon + Autoruns + file metadata + screenshots) form a defensible triage package suitable for a technical report or a SOC handoff.
- Immediate recommendations from these observations: patch vulnerable WinRAR instances, monitor archive extractors for writes to persistence folders, and instruct intake teams (help-desk/customer-portal handlers) to treat incoming archive attachments as high risk.

9.0 Detection & Hunting Guidance

The following detection queries focus on observable behaviors associated with the exploitation of CVE-2025-8088. These were developed using Kusto Query Language (KQL) for Microsoft Defender for Endpoint but can be easily adapted for any modern EDR or SIEM platform.

1. WinRAR writing into Startup

```
DeviceFileEvents
| where Timestamp > ago (14d)
| where FolderPath has @"\Microsoft\Windows\Start Menu\Programs\Startup"
| where FileName matches regex @"(?i)\.(bat|cmd|exe|vbs|js|dll)$"
| where InitiatingProcessFileName =~ "WinRAR.exe"
      or FileName in~ ("ApbxHelper.exe","msedge.dll")
| project Timestamp, DeviceName, AccountName, FileName, FolderPath,
      InitiatingProcessFileName, InitiatingProcessCommandLine, SHA256
```

Why? Directly spots the exploit outcome: WinRAR.exe creating a payload in Startup.

2. Any archive extractor writing into Startup

```
let archivers =
dynamic(["WinRAR.exe","UnRAR.exe","7z.exe","7za.exe","7zG.exe","tar.exe"]);
DeviceFileEvents
| where Timestamp > ago (30d)
| where FolderPath has @"\Microsoft\Windows\Start Menu\Programs\Startup"
| where FileName matches regex @"(?i)\.(bat|cmd|exe|lnk|vbs|js|ps1|dll)$"
| where InitiatingProcessFileName in~ (archivers)
      or FileName in~ ("ApbxHelper.exe","msedge.dll")
| project Timestamp, DeviceName, InitiatingProcessFileName,
      InitiatingProcessCommandLine, FileName, FolderPath, SHA256
```

Tip: Triage any .lnk or script dropped here by an archiver.

3. Post-reboot execution from Startup

```
DeviceProcessEvents
| where Timestamp > ago (14d)
| where InitiatingProcessFolderPath has
       @"\Microsoft\Windows\Start Menu\Programs\Startup"
| where FileName in~ ("cmd.exe","powershell.exe","wscript.exe","cscript.exe")
      or ProcessCommandLine has_any ("ApbxHelper.exe","msedge.dll")
| project Timestamp, DeviceName, FileName, ProcessCommandLine,
      InitiatingProcessFileName, InitiatingProcessFolderPath
```

Brief Tuning Suggestions:

- Scope by user groups (help-desk/HR) to reduce noise; they'll handle archives often.
- Suppress known-good software updaters that legitimately write to Startup (rare).
- Verify if any devices with vulnerable WinRAR and prioritize those machines, get them patched as soon as possible.
- Response playbook: isolate device, collect Startup contents, device timeline, hash + VirusTotal check.

10.0 Mitigation Recommendations

The following recommendations are designed to reduce organizational exposure to CVE-2025-8088 (WinRAR Path Traversal) and similar archive exploitation techniques.

10.1 Patch Management

- Update WinRAR immediately to version 7.13 or later, which remediates the directory traversal vulnerability.
- Audit for vulnerable builds:
  - Run `wmic product get name, version | find "WinRAR"` or check EDR software inventory for WinRAR versions less than or equal to 7.12.
- Remove or disable legacy archivers (e.g., outdated WinRAR, unRAR DLLs) found in third-party applications such as dtSearch.

10.2 User Awareness & Email Controls

- Educate employees, especially HR, Help Desk, and recruiting teams, about the risks of extracting unsolicited archives (e.g., "resume" or "invoice" .RARs).
- Enable Attachment Sandboxing or Detonation Analysis in email gateways for compressed file attachments.
- Block or quarantine .RAR attachments from untrusted senders until verified by security staff.

10.3 Application Control & Policy Enforcement

- Implement Software Restriction Policies (SRP) or AppLocker to prevent execution from:
  - `%AppData%\Microsoft\Windows\Start Menu\Programs\Startup`
  - `%Temp%`, `%Downloads%`, and user-writable directories
- Use Controlled Folder Access or Windows Defender Application Control (WDAC) to restrict which processes can write to persistence paths.
- Consider using Attack Surface Reduction (ASR) rules such as:
  - `Block executable content from email and webmail clients`

10.4 Network and Endpoint Monitoring

- Monitor for WinRAR.exe WriteFile events targeting the Startup folder (DeviceFileEvents).
- Track new autorun entries via the Registry (DeviceRegistryEvents).

- Deploy custom EDR detections based on the queries provided in the previous section.

10.5 Incident Response Preparedness

- Maintain snapshots or images of clean Windows builds to rapidly compare and revert systems.
- Periodically test the organization's ability to detect path traversal and archive-based exploitation techniques in red-team exercises.
- Ensure analysts can quickly retrieve telemetry from endpoints for rapid triage.

Summary

Mitigating CVE-2025-8088 relies on layered defense strategy:

- Prevent exploitation via patching and application controls.
- Detect suspicious writes or autorun persistence.
- Respond quickly with verified forensic data.

Organizations that keep WinRAR and related components current and enforce least-privilege execution policies will be effectively protected against this vulnerability and future archive exploitation techniques.

11.0 Conclusion

My research and lab exercise successfully demonstrates how CVE-2025-8088, a path traversal vulnerability in WinRAR, can be exploited to achieve OS-level persistence simply by convincing a user to extract or open a seemingly harmless archive. By reproducing this attack in a controlled virtual environment, I was able to confirm that the exploit allows arbitrary file writes into the Windows Startup directory, enabling execution on reboot without elevated privileges.

My simulated scenario, featuring a convincing decoy resume and a benign startup payload, illustrates just how minimal the user interaction required for compromise can be. Through forensic observation using Procmon and Autoruns, my report identified the exact sequence of events that occur under the hood: WinRAR's file-write operation, persistence establishment, and payload execution at logon.

From a defensive standpoint, this exercise reinforces the importance of basic hygiene, keeping software updated, monitoring for unusual file writes, and validating new

persistence entries. It also highlights the value of cross-tool correlation during triage: using multiple data sources (file events, autoruns, and process creation) to confirm compromise rather than relying on a single artifact.

While my lab used a safe, controlled payload, real-world threat actors such as RomCom (Storm-0978) have used this exact vulnerability to deploy malware and ransomware in the wild. Organizations that fail to patch promptly or lack behavioral monitoring remain susceptible to similar low-interaction attacks.

On a personal note, conducting this reproduction deepened my understanding of both attacker and the defender's visibility window. It bridged the gap between theory and hands-on forensics, showing how even small misconfigurations or user actions can cascade into persistence.

In summary, CVE-2025-8088 serves as a reminder that even mature, trusted software can become a foothold for threat actors when overlooked. Through continued vulnerability awareness, patch discipline, and behavioral detection, defenders can stay one step ahead of the next "simple" exploit that turns into a breach headline.

---

12. Sources

CVE – CVE-2025-8088 – WinRAR Path Traversal.

URL: https://www.cve.org/CVERecord?id=CVE-2025-8088

dtSearch – RAR library advisory.

URL: https://support.dtsearch.com/faq/dts0245.htm

Vicarius (VSociety) – Detect WinRAR Zero-day.

URL: https://www.vicarius.io/vsociety/posts/cve-2025-8088-detect-winrar-zero-day

Vicarius (VSociety) – Mitigations for WinRAR Zero-day.

URL: https://www.vicarius.io/vsociety/posts/cve-2025-8088-mitigate-winrar-zero-day-using-srp-and-ifeo

URL: https://www.vicarius.io/vsociety/vulnerabilities/cve-2025-8088

Microsoft Threat Intelligence – Storm-0978 / RomCom reporting.

URL: https://www.microsoft.com/en-us/security/blog/2023/07/11/storm-0978-attacks-reveal-financial-and-espionage-motives/

Bridewell – Operation Deceptive Prospect (RomCom).

URL: https://www.bridewell.com/insights/blogs/detail/operation-deceptive-prospect-romcom-targeting-uk-organisations-through-customer-feedback-portals

ESET Research – WinRAR exploitation analysis.

URL: https://www.eset.com/us/about/newsroom/research/eset-research-russian-romcom-group-exploits-new-vulnerability-targets-companies-in-europe-and-canada/?srsltid=AfmBOopKK1MuhlV41jhv50Qmah9nufxbQO_6dX70_V9LBucftHBT-Nku

PoC repository (used for lab reproduction) – CVE-2025-8088 Exploit TechCorp

URL: https://github.com/techcorp/CVE-2025-8088-Exploit

Tom's Hardware – WinRAR exploit linked to Russian hacking group.

URL: https://www.tomshardware.com/tech-industry/cyber-security/newly-discovered-winrar-exploit-linked-to-russian-hacking-group-can-plant-backdoor-malware-zero-day-hack-requires-manual-update-to-fix

Qualys. Community – Zero-Day to Zero-Risk

URL: https://blog.qualys.com/product-tech/2025/09/05/cve-2025-8088-winrar-exploit-from-zero-day-to-zero-risk-with-trurisk-eliminate

Picus – RomCom Threat Actor Evolution (2023-2025)

URL: https://www.picussecurity.com/resource/blog/romcom-threat-actor-evolution