

Old WinRAR Flaw Fuels Attacks on Ukraine: How Unmanaged Software Keeps the Door Open

 trendmicro.com/en_us/research/26/f/old-winrar-flaw-fuels-attacks-on-ukraine.html

June 8, 2026

Судова повістка про виклик до суду
в справі цивільній, адміністративній, про адміністративне правопорушення, іншій
(потрібне підкреслити)

Дата документа 03.02.2026 Справа № [REDACTED]

Дніпропетровський окружний адміністративний суд <i>(найменування суду)</i> викликає Вас як: особа, яка притягається до адмін. відповідальності на 11:30 год. 24.03.2026 р. у справі про поширення неправдивих чуток Місцезнаходження суду: м. Дніпро, вул. Академіка Янгеля, 4, Зала судового засідання Зал судових засідань №3 Суддя: П. Д. Тимчик <i>(підпис, ініціали, прізвище)</i>	Кому : [REDACTED] Місцезнаходження/ місце проживання: [REDACTED] Додатково просимо подати такі документи: Паспорт
Наслідки неприбуття за викликом суду Наслідки неприбуття на судові засідання осіб, які беруть участь у справі, передбачені статтями 223, 372 ЦПК України, статтями 205, 313 КАС України та статтями 268, 185-3 про адміністративні правопорушення. Для вручення в суді Розписка Повістку про виклик до суду на ім'я [REDACTED] про з'явлення до Дніпропетровського окружного адміністративного суду <i>(найменування суду)</i> на 11:30 хв. 24.03.2026 року , як особа, яка притягається до адмін. відповідальності одержав "___" _____ 20__ року: 1. Особисто _____ <i>(підпис одержувача)</i> 2. Для передання Секретар _____ <i>(підпис)</i> <i>(підпис одержувача із зазначенням посади або відношення до адресата, а також даних документа, що посвідчують особу)</i>	

Figure 1. Example decoy document: A spoofed Ukrainian court summons accusing the target of "spreading false rumors" to create a sense of urgency and compel interaction
[download](#)

Key Findings

- CVE-2025-8088, a path traversal vulnerability in WinRAR patched in July 2025, is still being exploited by multiple intrusion sets targeting Ukraine, including an intrusion set we temporarily designated as **SHADOW-EARTH-066** and Russia-aligned groups such as **Earth Dahu** (Gamaredon). At least until April 2026, both groups continued producing new exploit samples. Earth Dahu remains active at the time of writing.
- SHADOW-EARTH-066, tracked by CERT-UA as [UAC-0226](#) since 2025, has deployed an updated version of its **GIFTEDCROOK** information stealer designed for rapid credential and document theft. The stealer harvests browser passwords, session cookies, and files matching 35 extensions.
- The threat actor shifted from basic Excel macros with plaintext Telegram exfiltration to WinRAR exploit chains, in-memory DLL loading via direct NT system calls, and encrypted command-and-control (C&C) infrastructure in under a year.
- WinRAR is not covered by Group Policy or centralized update mechanisms. Software with these characteristics tends to remain exploitable long after patches are released, creating a persistent blind spot in organizational vulnerability management.

Introduction

When Russia annexed Crimea in 2014, the Russia-aligned cyber threat landscape was defined by a handful of known actors: [Pawn Storm](#) (also known as APT28), Sandworm, Earth Koshchei (also known as APT29), Turla, and Earth Dahu (also known as Gamaredon). A decade later, those groups remain active, but they have been joined by a much larger number of distinct activity clusters targeting Ukraine. One pattern cuts across these clusters: the rapid adoption of vulnerabilities in widely used software. [CVE-2025-8088](#), the WinRAR vulnerability at the center of this report, was first reported in July 2025 as a zero-day used by [Void Rabisu](#) (ROMCOM) and has since been exploited by other groups, including [Sandworm and Turla](#). SHADOW-EARTH-066 (known as UAC-0226) and Earth Dahu also exploited this vulnerability.

WinRAR is deeply embedded in daily operations across Ukrainian organizations, making it an attractive target for exploitation. CVE-2025-8088 is a path traversal flaw (CVSS 8.4), patched in WinRAR 7.13 in July 2025, that allows an attacker to silently write files outside the extraction directory via NTFS Alternate Data Streams. Once the victim opens the archive, no further interaction is needed; they see only a decoy document. All the samples we analyzed exploit this vulnerability.

In this report, we examine two separate campaigns that exploit CVE-2025-8088 against Ukrainian targets. The first is attributed to SHADOW-EARTH-066 and delivers an updated version of the GIFTEDCROOK information stealer that rapidly harvests credentials and

documents before deleting itself. The second is attributed to Earth Dahu (Gamaredon) and delivers espionage tools through an HTA-based chain. The two groups use different tooling and infrastructure, but share the same entry point.

The vulnerability: CVE-2025-8088

Victims receive a RAR archive, typically through email. When they open the archive with an older version of WinRAR, a PDF appears. That PDF can look like a court summons (see Figure 1), an administrative notice, or a defense ministry document. Nothing else is visible to the victim, but in the background, WinRAR has silently written additional files to locations outside the extraction directory, such as the Windows Startup folder. No dialog or warning appears. The next time the user logs in, the files execute.

Both campaigns examined in this post used CVE-2025-8088, which is related to an earlier directory traversal vulnerability (CVE-2025-6218, patched in WinRAR 7.12) but exploits a different code path through NTFS **Alternate Data Streams (ADS)**.

ADS is a feature of the NTFS file system that allows additional named data streams to be attached to a file. Legitimate uses include metadata storage such as zone identifiers added by browsers, but ADS can also carry arbitrary data. RAR5 archives can include **SERVICE headers** (header type 0x03) with the STMz marker to represent ADS metadata. WinRAR before version 7.13 did not sanitize directory traversal sequences in these ADS names, allowing an attacker to embed `..\..\` sequences in the STMz entries and write files to arbitrary locations. *Figure 2* illustrates this mechanism.

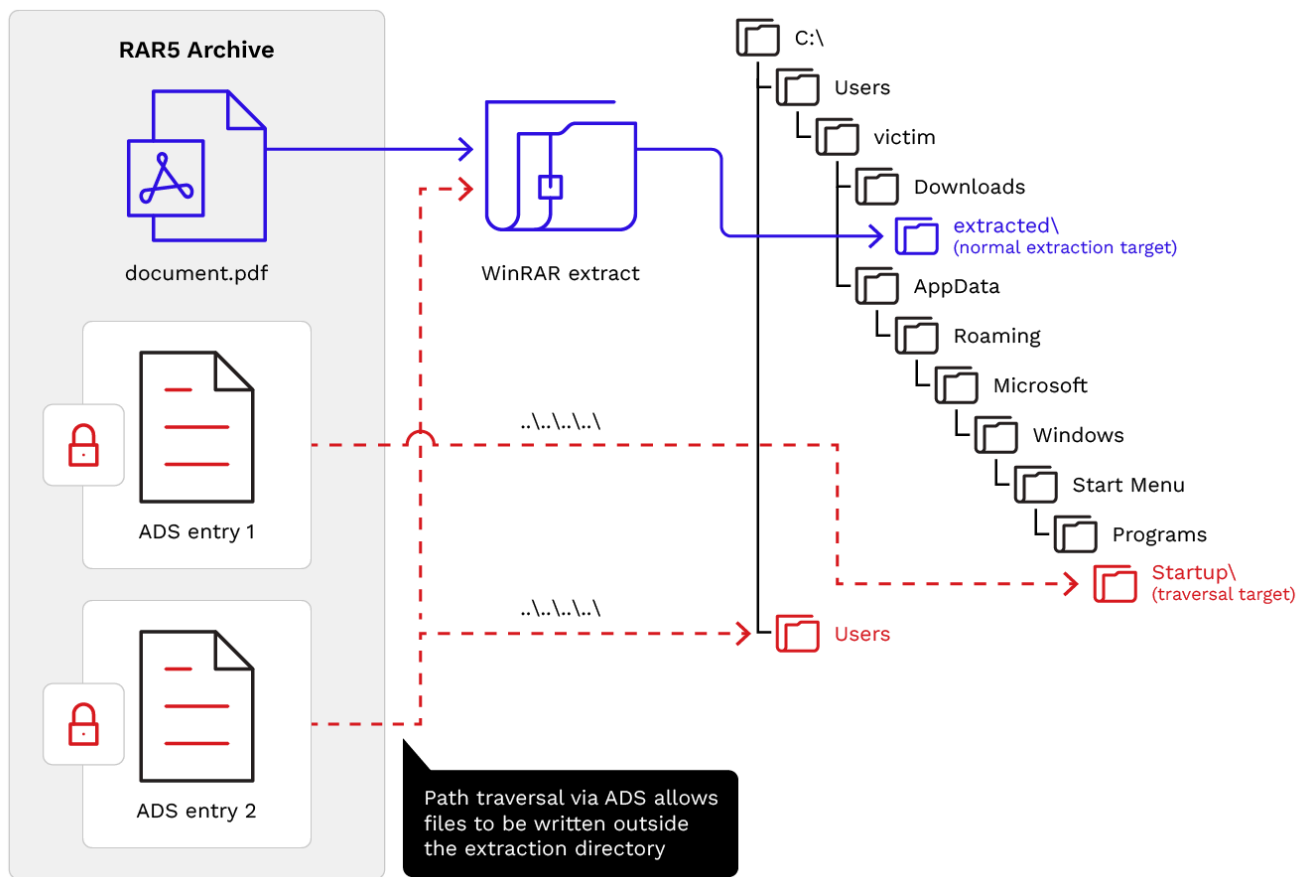


Figure 2. How CVE-2025-8088 works: a RAR5 archive contains a visible decoy file and hidden ADS entries with path traversal sequences.

SHADOW-EARTH-066: from GIFTEDCROOK campaign to a WinRAR exploit chain

Background

SHADOW-EARTH-066 is our temporary designation for the threat actor cluster tracked by CERT-UA as [UAC-0226](#), whose activities were first documented in [CERT-UA advisory #14303](#) in April 2025. The campaign has targeted Ukrainian military innovation centers, military formations, law enforcement agencies, and local self-government bodies near Ukraine's eastern border since at least February 2025.

The original campaign used spear phishing emails with macro-enabled Excel files (.xlsm) that referenced demining, administrative fines, UAV production, and compensation for destroyed property. The payloads, stored as base64-encoded strings in Excel cells, included a .NET reverse shell and a C/C++ credential stealer that CERT-UA named **GIFTEDCROOK**. The first version was a standalone executable that stole browser credentials from Chrome, Edge, and

Firefox, archived them with PowerShell's Compress-Archive, and exfiltrated the archive to a Telegram channel. The bot tokens and chat IDs were hardcoded in plaintext.

By February 2026, SHADOW-EARTH-066 had shifted from Excel macro droppers to CVE-2025-8088 as its initial access vector, and from embedded .NET payloads with Telegram exfiltration to an in-memory DLL loading chain with dedicated C&C servers.

Inside the CVE-2025-8088 attack chain

The most recent build artifact, dated April 9, 2026, indicates the campaign remained active through at least early April (the full attack chain is shown in Figure 3). The crafted RAR archives contain a visible decoy PDF alongside three hidden ADS payloads that use path traversal to write files outside the extraction directory:

- **5 levels up:** An LNK shortcut file targeting %APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\
- **12 levels up:** A PowerShell loader script dropped to C:\ProgramData\
- **12 levels up:** An encoded DLL payload dropped to C:\ProgramData\

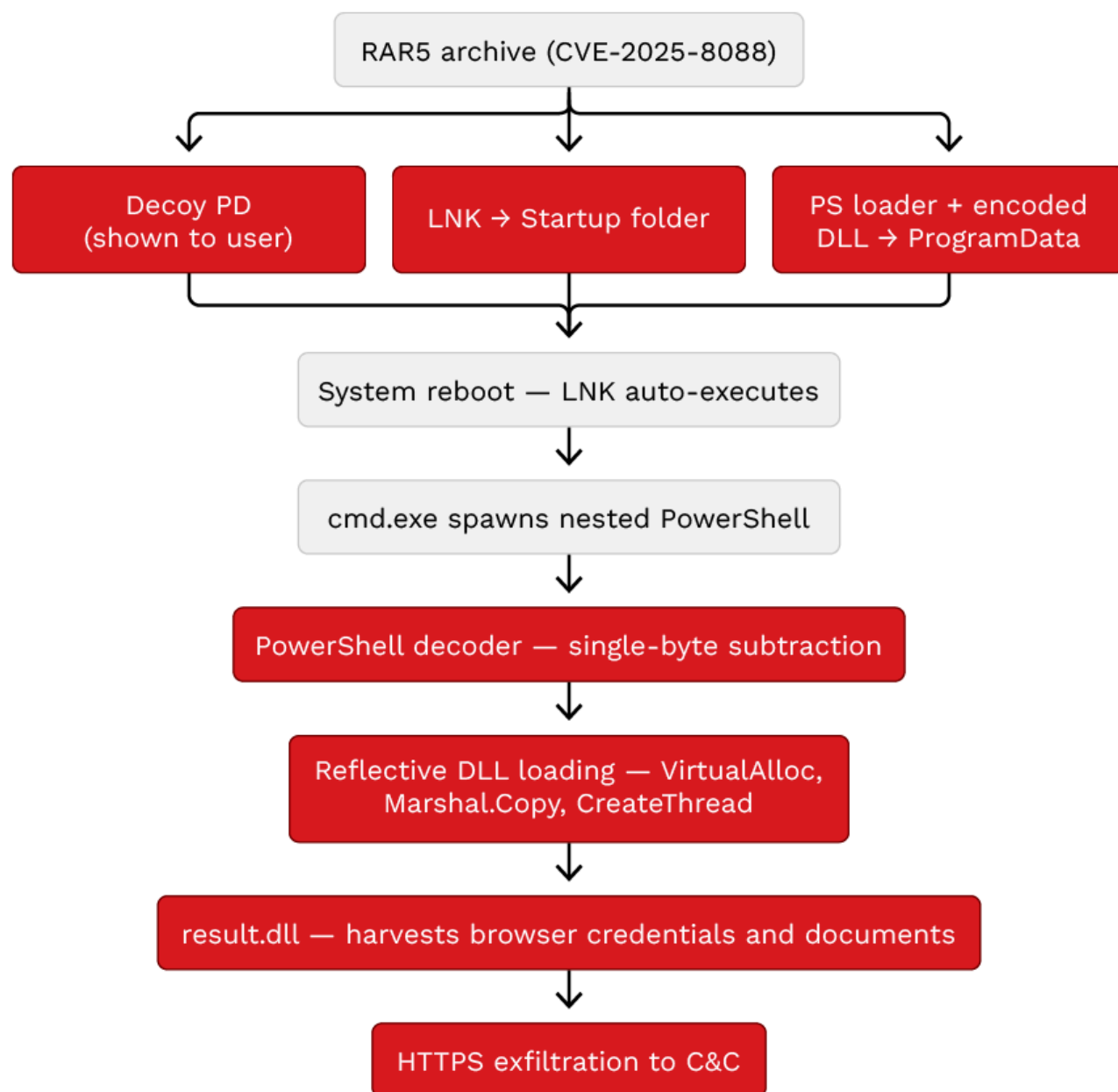


Figure 3. SHADOW-EARTH-066 attack chain from CVE-2025-8088 exploitation to HTTPS exfiltration.

These traversal depths are calculated to reach the user's AppData directory tree from a typical email client with a temporary extraction path. The LNK is placed in the Startup folder so that it executes on the next login, triggering the payload chain. Twelve levels overshoot to the drive root, reaching C:\ProgramData\. From the victim's perspective, they extract the archive and see a PDF document. No warning is displayed, as the additional files are written silently in the background.

We analyzed multiple RAR samples across several distinct build groups. While file names, encoding keys, and C&C addresses differ between builds, all share structural fingerprints: the DLL export name result.dll with a single Func export, the non-standard PE offset e_lfanew =

0x110, statically linked libcurl 8.14.0-DEV, identical RC4 exfiltration keys, and the same builder machine SID embedded in all LNK files. One sample (SHA256: 3d371ef71e40c34a75c168d4647db096c2f386499d99a88d4e16b63cd4acda25) is examined below.

This RAR archive drops a court summons PDF from the Dnipropetrovsk Regional Administrative Court as a decoy (as seen in Figure 2). The three hidden ADS payloads are:

- an LNK file (bfF3BxteabXqg.lnk) to the Startup folder
- a PowerShell loader (KKN) to C:\ProgramData\
- a SUB-encoded DLL (ND8, key 0x38) to C:\ProgramData\.

Other samples use different decoy themes, including a Ministry of Defense registry of military obliges and military equipment manifests for KrAZ truck fleets.

How the chain is executed

When the victim next logs in, Windows executes the LNK file from the Startup folder. The LNK target is *cmd.exe* with arguments that launch a double-nested PowerShell session:

```
| cmd.exe /c start /min "" powershell -NoPr -Win Hidd -Ex Bypass  
-Com "powershell -NoPr -Ex Bypass -Com ""iex (gc 'C:\ProgramData\KKN' -raw)"""
```

The outer *powershell.exe* spawns an inner *powershell.exe*. Both use *-ExecutionPolicy Bypass* to circumvent script execution restrictions and *-WindowStyle Hidden* to suppress visible windows. The inner session reads the loader script from C:\ProgramData\ and executes it via *Invoke-Expression*. Each build uses a different alias for *Get-Content* (*gc*, *cat*, or *type*), varying the command-line signature without changing functionality.

The PowerShell loaders are heavily obfuscated scripts (65 to 74 KB). Functions are named with random English words joined by underscores (e.g., *flexibility_denominator_wiretap()*, *polliwog_scenery_reward_plane_preset()*). Hundreds of junk comment lines and *Sleep* calls with fractional values (e.g., *Sleep 1.453*) inflate the script and extend execution time to evade sandbox analysis (Figure 4).

```

Write-Host (province_dragonfruit_permafrost_courtroom 7);$cocktail_hilarious_endurable_intent = ([Type]::(fax_squalid
coat_streetcar_carol 32 "vJews003wXHgZlVaVb2");$juicy_insolence_gauntlet_momentous_connotation = $cocktail_hilarious_e
$fortress_ebook_dollar = $cocktail_hilarious_endurable_intent.(fax_squalid_retirement $bouquet_wisteria_exaggeration_

function polyp_wolf_stepdaughter_diam($contract_rudiment_paperback, $say_defense_quantity_shallow_recondite){
    return $juicy_insolence_gauntlet_momentous_connotation.Invoke($null, @([System.Runtime.InteropServices.HandleRef]
    $bronchitis_inconvenience_write_fiery_hallowed = [Type]::(fax_squalid_retirement $listening_thaw_mark_shortwave_s
    $shark_syndrome_evolution_external = $cost_tadpole_pants_winter.(fax_squalid_retirement $snowsuit_mole_wildernes
#difficult candle hockey checking various
Write-Host (pipeline_tachometer_tomatillo "UJ3i6zygr9x_p3Jyey");Sleep 0.743;Write-Host (snarl_seek_empire 71 38 118)
#lowly cassava hormone counter accountability mailer member dogsled gratitude
    $shark_syndrome_evolution_external.(fax_squalid_retirement $driveway_name_collaboration_wallet_triangle $executiv
$candidate_chairlift_belfry_manipulation = flexibility_denominator_wiretap @(30,45,78,56,71,27,56,75,57,41,84,79,77,3
Write-Host (snarl_seek_empire 140 28 183);    return $shark_syndrome_evolution_external.(fax_squalid_retirement $work
#grandpa umbrella creator cage solidity placode symbolize
Write-Host (province_dragonfruit_permafrost_courtroom 7)
Sleep 0.785;coat_streetcar_carol 30 "Ry8aJk4TkWNRcgAbwun"
;function satire_hake_communist_halloween($contract_rudiment_paperback, $say_defense_quantity_shallow_recondite, [typ
#criticism motorcycle acoustic grade
Sleep 1.049
#inhabitant proctor oxygen entirety semantics timeout makeshift memo
$adoption_havoc_message_hornet_speechsogloss_grouper_context_payee = removal_lookout_seeker_inversion_snobbish "tZvcc
Write-Host $adoption_havoc_message_hornet_speechsogloss_grouper_context_payee
}
#pocketbook coordination gazelle blossom tornado outline galoshes endpoint taco
Write-Host (province_dragonfruit_permafrost_courtroom 7)
;$zoologist_linguist_homely_dishwasher = @();function developing_color_competence([UInt32] $lava_woebegone_promote_or
Write-Host (snarl_seek_empire 183 16 105);Sleep 0.857
#homeland eaglet bureau meddle complain association smite scrub lobster
Write-Host (province_dragonfruit_permafrost_courtroom 5)
    $exhusband_support_printing_cousin_zoo = [Type]::(fax_squalid_retirement $brooch_professional_bather $pimp_parsle
    if ($lava_woebegone_promote_organizing_nibble -eq 4) {;        [Type]::(fax_squalid_retirement $schizophrenic_bud
#club disagreeable cowboy rust
    } elseif ($lava_woebegone_promote_organizing_nibble -eq 8) {
#commodity ballistic pirate component retention

```

Figure 4. Excerpt from the obfuscated PowerShell loader (KKN): random-word function names, junk comments, and Sleep-based anti-sandbox calls.

[download](#)

Beneath the obfuscation, the loader performs in-memory DLL loading using direct NT system calls (NtAllocateVirtualMemory, NtProtectVirtualMemory, NtCreateThreadEx) to avoid user-mode API hooks:

1. Reads the SUB-encoded binary from C:\ProgramData\
2. Decodes each byte by subtracting a fixed key value: $\text{decoded}[i] = (\text{encoded}[i] - \text{key}) \& 0xFF$
3. Allocates memory with NtAllocateVirtualMemory, copies the decoded DLL via Marshal.Copy, then changes the memory protection to executable
4. Creates a thread at the DLL entry point via NtCreateThreadEx and waits for completion

The encoded payload does exist on disk under C:\ProgramData\, but the decoded DLL is never written as a file. The decoding and loading process runs in memory within the *powershell.exe* process, making file-based detection of the final payload difficult.

GIFTEDCROOK evolved: result.dll

The final payload is a DLL internally named *result.dll* that exports a single function *Func*. The file is a custom information stealer compiled for x86-64 with libcurl 8.14.0-DEV statically linked. It targets Chromium-based browsers (Chrome, Edge, Opera) and Firefox, and also collects documents and files from the victim’s filesystem.

Browser targets

Browser	User Data Path
Google Chrome	%LOCALAPPDATA%\Google\Chrome\User Data
Microsoft Edge	%LOCALAPPDATA%\Microsoft\Edge\User Data
Opera	%APPDATA%\Opera Software\Opera Stable
Mozilla Firefox	%APPDATA%\Mozilla\Firefox\Profiles

Table 1. Browser targets

For each Chromium-based browser (Chrome, Edge, Opera), the stealer reads the Local State JSON file and extracts the DPAPI-protected master key via *CryptUnprotectData*. It then collects Login Data (passwords) and cookies per profile, along with the decrypted master key. For Firefox, the stealer reads the NSS key databases *key3.db* and *key4.db*, along with *cookies.sqlite* from each profile directory.

The stealer also extracts *app_bound_encrypted_key* from Chrome’s Local State file. Chrome version 127 and later uses this field to implement **App-Bound Encryption (ABE)**, a protection that binds credential decryption to the Chrome application context. Google introduced ABE specifically to make infostealer malware less effective, but ABE bypass has been adopted in many infostealers since late 2024, and its presence in *result.dll* indicates the developer is tracking browser security changes and may have borrowed ideas from the broader infostealer ecosystem.

Document and file theft

Beyond browser data, *result.dll* scans the victim’s Documents, Downloads, and TEMP directories for files matching 35 extensions:

Category	Extensions
Documents	.txt, .doc, .docx, .docm, .rtf, .dot, .dotx, .dotm, .odt, .pdf, .md, .log
Spreadsheets	.xls, .xlsx, .xlsm, .xlt, .xltx, .xltm, .csv
Presentations	.ppt, .pptx, .pptm, .pps, .ppsx, .pot
Email	.eml
Archives	.rar, .zip, .7z, .cab, .gzip, .tar
Sensitive	.kdbx (KeePass), .ovpn (OpenVPN), .conf

Table 2. File extensions targeted for theft, by category

This file theft capability aligns with the evolution documented by [Arctic Wolf](#), who reported that intermediate GIFTEDCROOK versions already added file collection before the shift to *result.dll*.

Self-deletion

After exfiltration, *result.dll* removes all three staging artifacts from disk. The following delete operations then execute in sequence:

1. CreateProcessW with CREATE_NO_WINDOW launches cmd.exe /c "timeout /t 5 & del " to delete one staging file after a 5-second delay
2. Two DeleteFileW calls remove the remaining files, including the PowerShell loader from C:\ProgramData\

After cleanup, no startup mechanism and no staging files remain on the endpoint; the stealer operates as a one-shot execution.

Anti-analysis measures

To resist static and sandbox analysis, *result.dll* layers several techniques:

- **PEB walk with FNV-1a hashing** (seed: 0x811c9dc5, prime: 0x01000193): this technique resolves API addresses at runtime by walking the Process Environment Block and hashing module and function names.

- **Dual-layer RC4-encrypted string tables:** 100+ strings (browser paths, file extensions, directory names, C&C URLs) are individually RC4-encrypted in the .rdata section with per-string keys; C&C URLs use ASCII RC4 encoding. All strings are decrypted only at runtime.
- **Identity function anti-analysis padding:** thousands of calls to a trivial function (mov eax, ecx; ret) are interspersed throughout the code. Each call appears to pass a meaningful constant, but the function returns it unchanged. This inflates code size and analysis time without affecting functionality. Separately, LCG PRNG delay loops (multiplier 0x41C64E6D) introduce variable execution delays to exceed sandbox analysis windows.

C&C communication

Before exfiltrating data, the DLL sends an HTTP GET to `hxxp://1[.]1[.]1[.]1` as a connectivity check. The request uses Cloudflare's public DNS IP on a non-standard port to verify internet access without depending on domain resolution.

Stolen credentials are encrypted with dual-layer RC4 , then sent via HTTPS POST as multipart/form-data to the `/rcv/` path on dedicated C&C servers. The primary RC4 key also serves as the multipart boundary string.

C&C IP address	Port
166[.]0[.]132[.]237	7044
136[.]0[.]141[.]41	9580
136[.]0[.]141[.]138	8406
38[.]225[.]209[.]229	9623
136[.]0[.]141[.]112	9200*
38[.]225[.]209[.]122	8009*
23[.]26[.]237[.]80	8941*

Table 3. C&C server IP addresses and ports

*Note that we have not observed any samples communicating directly with these IP addresses. They are hosts pivoted via a self-signed TLS certificate with CN "john" that overlaps with the top four IPs listed in the table.

All seven servers are hosted on Evoxt Sdn. Bhd. (AS149440), a Malaysian VPS provider with points of presence across Europe. These servers are distributed across France, the Netherlands (two servers), and Switzerland. All use non-standard high ports and the same URI path (/rcv/), indicating shared server-side tooling.

From GIFTEDCROOK to result.dll: Key changes

Our analysis confirms that *result.dll* belongs to the same malware family as GIFTEDCROOK. The two share the same compiler toolchain (MSVC C++, x64), the same cryptographic API set (CryptUnprotectData, CryptImportKey, BCryptGenRandom), the same anti-analysis checks (IsDebuggerPresent, wine_get_version), and the same multipart/form-data exfiltration format.

The C++ runtime patterns indicate the same C++20 standard., while the libcurl version was upgraded from 8.12.1-DEV to 8.14.0-DEV. Intermediate versions (v1.2 and v1.3, [documented by Arctic Wolf](#)) had already added file theft capabilities while still using Telegram for exfiltration; *result.dll* continues and extends this trajectory.

The changes represent a substantial upgrade:

Aspect	GIFTEDCROOK (original, 2025)	result.dll (evolved, 2026)
PE format	Standalone EXE	DLL with in-memory loading via direct NT syscalls
Delivery	Excel macro dropper (.xlsm)	CVE-2025-8088 RAR5 exploit chain
Exfiltration	Telegram Bot API (plaintext tokens)	Dedicated C&C servers, dual-layer RC4 + HTTPS
browser targets	Chrome, Edge, Firefox	Chrome, Edge, Opera, Firefox
File theft	No (added in intermediate versions)	35 extensions from Documents, Downloads, TEMP
Chrome ABE bypass	No	Yes

Aspect	GIFTEDCROOK (original, 2025)	result.dll (evolved, 2026)
String protection	Minimal (plaintext paths and tokens)	Dual RC4 (ASCII + UTF-16LE) per-string keys
API resolution	Static imports	PEB walk + FNV-1a hashing
Anti-analysis padding	Sleep-based sandbox evasion	Identity function junk calls + LCG PRNG delays
Self-delete	Batch script loop	cmd.exe /c timeout & del + DeleteFileW (removes all staging artifacts and Startup LNK)
Disk footprint	EXE file on disk	SUB-encoded on disk, decoded DLL loaded only in memory

Table 4. GIFTEDCROOK vs. result.dll: feature-by-feature comparison

The shift from Telegram to dedicated C&C servers is notable for operational security, and it also possibly tracks with a broader change in the operating environment: in February 2026, Russia began severely restricting access to Telegram, throttling the service before moving toward a full block. The original GIFTEDCROOK samples contained plaintext Telegram bot tokens that could be trivially extracted and used for monitoring or takedown. In the new version, C&C URLs are RC4-encrypted in the binary's *.rdata* section. They can still be recovered statically by RC4-decrypting the adjacent key-blob pairs, but they are no longer visible through basic string analysis.

Earth Dahu: Espionage attack via HTA chain

Background

Earth Dahu is our designation for the threat actor commonly known as [Gamaredon](#) (also tracked as Primitive Bear, Shuckworm, Aqua Blizzard, UAC-0010, BlueAlpha, and ACTINIUM). The group is one of the most prolific Russia-aligned groups targeting Ukraine, with documented operations since at least 2013. Earth Dahu, which has historically favored script-based tooling, adopts new delivery techniques as older ones are detected and blocked, which includes Office macros, self-extracting archives (SFX), BAT scripts, and vulnerability exploitation such as CVE-2025-8088.

Since at least September 2025, Earth Dahu has also incorporated CVE-2025-8088 into its operations. We first reported on this adoption in a private intelligence report distributed through TrendAI Vision One™ in December 2025, when Earth Dahu used the vulnerability with an HTA-to-VBScript infection chain that delivered espionage modules. Based on RAR internal file timestamps and file naming conventions, the chain remained active through at least April 10, 2026.

The HTA-based attack chain

This section focuses on Earth Dahu's exploitation of CVE-2025-8088 as an initial access vector. Post-exploitation TTPs, including the delivery of GammaSteel and other espionage modules, are documented by [ClearSky](#) and [HarfangLab](#); we refer readers to those reports for detailed coverage.

Unlike SHADOW-EARTH-066's three-file approach, Earth Dahu's CVE-2025-8088 exploitation drops a single file via ADS path traversal: a malicious **HTA (HTML Application)**, or a **VBS or VBE** file written to the Startup folder. Some samples drop HTA files directly, while others drop obfuscated VBS or VBE downloader scripts that fetch and execute an HTA payload from a Cloudflare Tunnel (trycloudflare[.]com), adding an extra download stage before reaching the same HTA-to-VBScript execution flow. Each RAR archive contains one visible PDF and one hidden ADS entry traversing six directory levels.

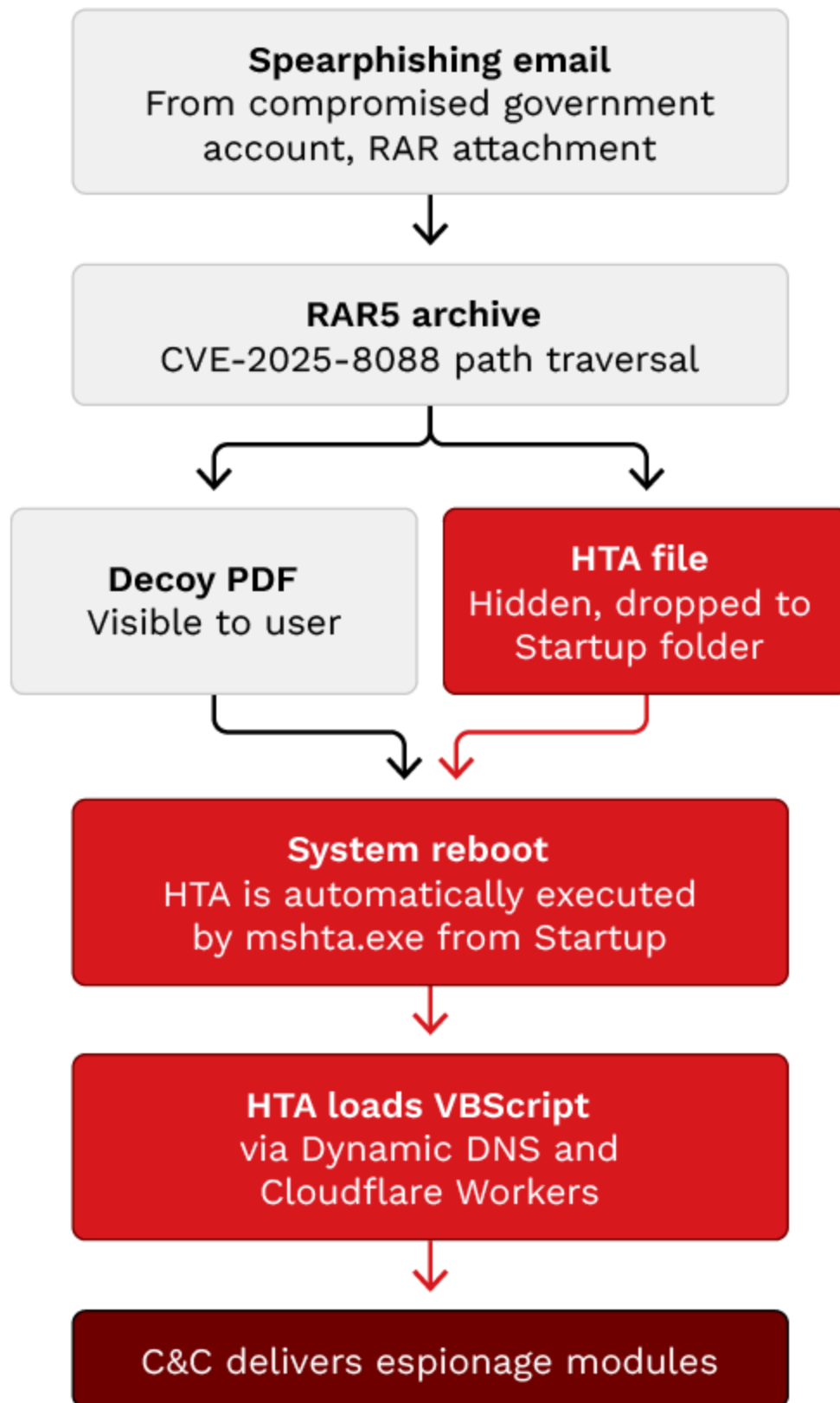


Figure 5. Earth Dahu's HTA chain: CVE-2025-8088 drops an HTA file to the Startup folder. On the next login, mshta.exe executes the HTA, which loads VBScript from external resources via Dynamic DNS and Cloudflare Workers.

[download](#)

At the next login, mshta.exe automatically executes the HTA file. The HTA loads and runs VBScript from external resources hosted through **Dynamic DNS** and **Cloudflare Workers** infrastructure. This use of Cloudflare Workers as a C&C proxy is a characteristic pattern of recent Earth Dahu operations. The C&C delivers various espionage modules depending on the target. [ClearSky Cyber Security](#) has also reported a Wiper component delivered through this chain.

The C&C URLs embedded in these HTA files frequently use HTTP basic-auth @-notation to spoof trusted domains in the URL bar. For example, a URL structured as `hxxps://ssu[.]gov[.]ua@malicious[.]workers[.]dev/path` displays `ssu.gov.ua` to the left of the @ symbol, making the URL appear to originate from the Security Service of Ukraine, while the actual request is directed to the attacker-controlled `workers[.]dev` subdomain. Spoofed brands observed in the campaign include:

- Ukrainian government domains (`ssu[.]gov[.]ua`, `president[.]gov[.]ua`, `rnbo[.]gov[.]ua`, `mil[.]gov[.]ua`)
- Ukrainian news outlets (`nv[.]ua`, `tsn[.]ua`, `www[.]unian[.]net`, `sensor[.]net`)
- International media (`www[.]bbc[.]com`, `www[.]dw[.]com`, `www[.]rbc[.]ru`)

We observed a minor TTP evolution in newer samples: approximately half of the HTA-chain archives append an additional `Startup\.\Startup\` sequence to the ADS traversal path. The final destination is the same, but the variation may be intended to evade detection rules matching the original traversal pattern. Both patterns coexisted in the latest campaign, suggesting the operator runs multiple build templates in parallel.

Spear-phishing delivery

We obtained multiple spear-phishing emails associated with Earth Dahu's HTA campaign, spanning December 2025 to April 2026. The majority were sent from compromised accounts within Ukrainian government organizations and free email services. In one cluster, four separate accounts on a single regional government Exchange server shared the same internal originating IP, suggesting a compromised workstation distributing emails through multiple mailboxes. Additional compromised accounts were identified on justice and criminal-executive service systems.

One email was sent via `astrocaf[.]com`, an attacker-controlled domain registered through `reg.ru` on December 18, 2025, resolving to 194[.]58[.]66[.]82 (Baxet Group Inc., AS26383). The From header spoofed a Ukrainian law enforcement agency; DMARC validation failed and no DKIM signature was present. Two additional emails used

vodafoneu33@joymobile[.]com[.]ua as the Return-Path, routed through mail[.]c1[.]com[.]ua (5[.]9[.]241[.]27, Hetzner, Germany).

Most emails exhibit a self-addressed BCC pattern in which the From and To fields are identical, hiding the actual recipient list. Email subjects consistently impersonate Ukrainian judicial correspondence: court summons, writs of execution, and property seizure resolutions. All attachments follow the naming pattern {DocType}_{N}_{N}_{N}_{N}_{dd.mm.yyyy}.rar.

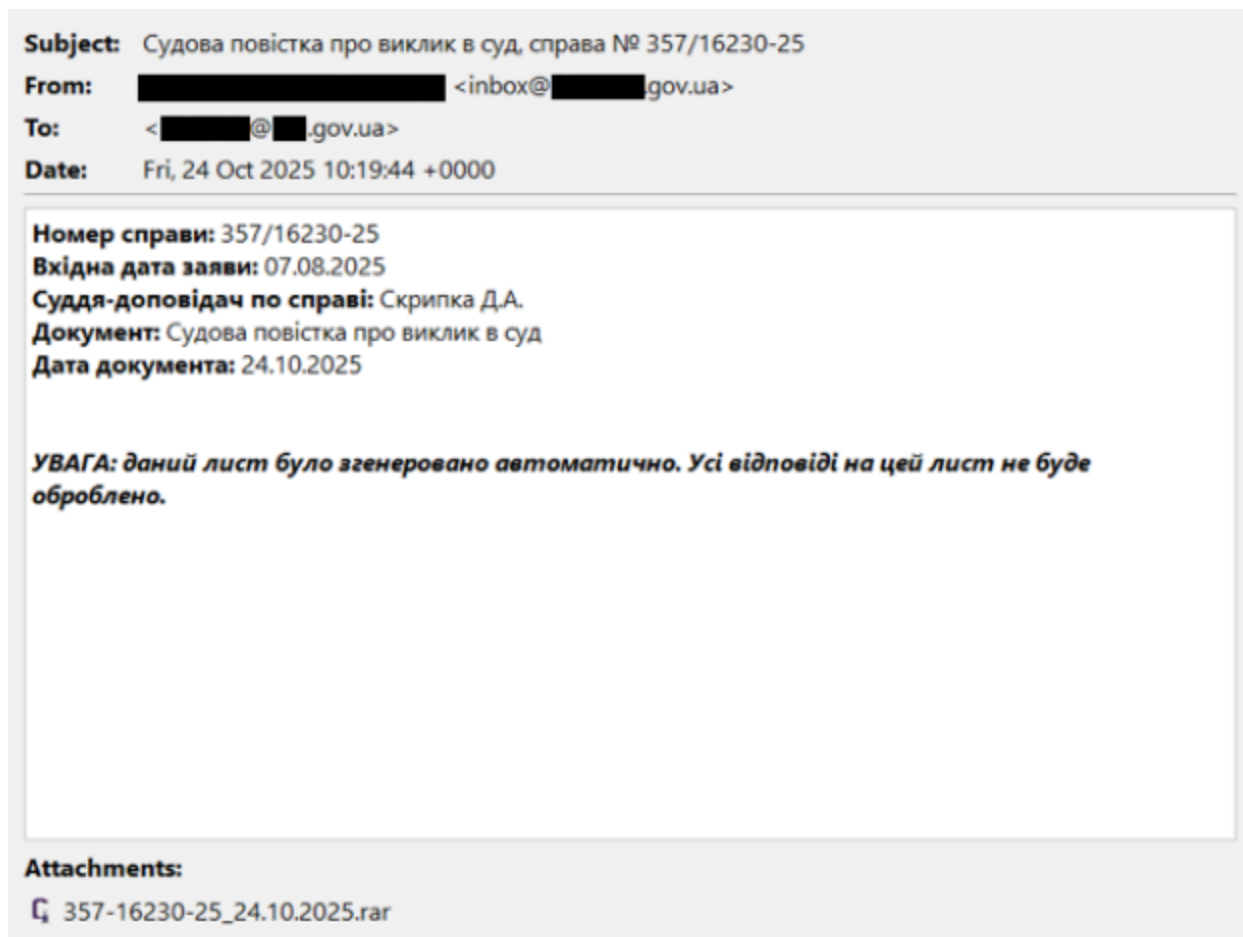


Figure 6. Example spear-phishing email from a compromised regional government account.

Attribution

SHADOW-EARTH-066 (binary chain)

We track the binary payload chain (CVE-2025-8088 to LNK to PowerShell to *result.dll*) under **SHADOW-EARTH-066**, our temporary designation for the intrusion set that CERT-UA tracks as [UAC-0226](#).

The attribution to UAC-0226 is based on the malware lineage. Our analysis confirms that *result.dll* is a direct evolution of GIFTEDCROOK, the stealer that CERT-UA attributed to UAC-

0226 in April 2025. The two share the same compiler toolchain, cryptographic framework, anti-analysis checks, and exfiltration protocol, as detailed in the evolution comparison above.

Timestamp analysis provides an additional attribution data point. All LNK files share the same creation timestamp and builder machine identifier (desktop-hagd25b), confirming a single build environment. The PE compile timestamps of four distinct DLL builds (February 3, February 17, March 16, and April 9, 2026) cluster between 06:33 and 11:32 UTC. RAR archive timestamps for the packaged decoy PDFs independently corroborate these build sessions, aligning within seconds of the corresponding PE compile times.

Mapped to UTC+3 (Moscow time), these correspond to 09:33–14:32 local time. All six build events fall on weekdays. While these timestamps can be manipulated, the consistent weekday pattern across multiple sources and the alignment with UTC+3 working hours suggest an operator based near that time zone.

Earth Dahu (HTA chain)

We attribute the HTA-based infection chain to **Earth Dahu** (Gamaredon) with **high confidence**. This assessment is based on:

- **Direct continuity:** The HTA chain is a continuation of the campaign we reported in the APT Research Report (which is available to subscribers of the Trend Vision One™ Threat Intelligence Hub). The exploitation method, post-exploitation chain (HTA to VBScript to espionage modules), and C&C infrastructure pattern (Dynamic DNS with Cloudflare Workers) are identical.
- **TTP consistency:** The spear-phishing delivery TTPs match established Earth Dahu patterns, including compromising government email accounts, BCC self-addressed distribution, and C&C proxying through Cloudflare Workers.
- **Victimology:** Exclusive targeting of Ukrainian government and military entities is consistent with Earth Dahu's documented operational mandate.

Distinguishing the two campaigns: same flaw, different actors

The two campaigns examined in this report share the same initial exploit (CVE-2025-8088) and overlapping victimology, but the post-exploitation chains are fundamentally different:

- SHADOW-EARTH-066 communicates with **direct IP-based C&C servers** and delivers a **compiled x86-64 DLL** with PEB-walk API resolution and RC4-encrypted strings. Earth Dahu uses **Cloudflare Workers** as a C&C proxy and relies on **script-based tooling** (HTA, VBScript, PowerShell).
- **No shared infrastructure** has been identified between the two campaigns.

The tooling reflects different development traditions: the GIFTEDCROOK family is a compiled C++ codebase with statically linked libcurl. Earth Dahu has historically favored script-based approaches.

Conclusion

Despite CVE-2025-8088 was patched in WinRAR 7.13 in July 2025, yet at the time of writing, multiple threat actor groups continued to build new exploit samples with fresh lure documents and use this vulnerability as a reliable initial access vector against Ukrainian organizations.

SHADOW-EARTH-066 uses it to deploy an evolved information stealer, while Earth Dahu uses it to deliver espionage tools. Russia-aligned threat actors, including Sandworm, Turla, and Void Rabisu, have also been [reported](#) exploiting the same vulnerability.

The convergence of both established state-backed groups and independently tracked clusters on a single vulnerability reflects the scale of the cyber threats that Ukraine faces. Since the full-scale invasion in 2022, the number of intrusion sets conducting operations against Ukrainian government and military networks has grown steadily, and credentials and documents stolen in these campaigns will not stay contained. Compromised accounts in military and government organizations may create downstream risks for allied nations and partners in their contact networks.

The vulnerability works because WinRAR remains unpatched on enough endpoints to make the investment worthwhile. WinRAR does not auto-update, does not support Group Policy, and falls outside enterprise patch channels like WSUS, SCCM, or Intune. Verifying patch status across hundreds of endpoints requires third-party tools or manual auditing.

SHADOW-EARTH-066 and Earth Dahu use different tooling and infrastructure, a compiled C++ stealer chain on one side, a script-based espionage framework on the other; but both relied on the same unpatched entry point.

This problem is not unique to WinRAR, to Ukraine, or to these threat actors. Many utility applications, archiving tools, and file viewers share the same traits: widely installed, infrequently updated, and difficult to manage at enterprise scale. They accumulate known vulnerabilities over time, and threat actors deliberately look for them. CVE-2018-20250, a WinRAR vulnerability from 2018, was still being exploited in targeted attacks years after its disclosure. CVE-2025-8088 appears to be following the same pattern — and when threat actors find a vulnerability that works, they will keep using it until it stops working.

Tracking and patching these applications is not optional. It is a basic requirement for reducing the attack surface that threat actors rely on.

Risk management guidance

Prioritizing immediate actions

1. **Patch WinRAR.** IT teams should verify installed versions on all endpoints and deploy the latest version of WinRAR. Because WinRAR has no auto-update, use software distribution tools (SCCM, Intune, PDQ Deploy, etc.) to push the update. Prioritize endpoints in government, military, and defense-adjacent organizations.
 2. **Hunt for indicators.** Security teams should search endpoints for:
 - LNK or HTA files in %APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\ with randomized names
 - Files in C:\ProgramData\ with short alphanumeric names: KKN, ND8, U0U, YDV, NdV, QB5k, uaP, WnX, wq_, Arj, 05fE
 - Network connections to 23[.]26[.]237[.]80, 38[.]225[.]209[.]122, 38[.]225[.]209[.]229, 136[.]0[.]141[.]41, 136[.]0[.]141[.]112, 136[.]0[.]141[.]138, 166[.]0[.]132[.]237
- Note:** GIFTEDCROOK's self-delete mechanism removes the Startup LNK and both C:\ProgramData\ staging files after exfiltration. These file-based indicators are only present between initial infection and the next user's login. On systems where the stealer has already executed, hunting should focus on network indicators, cmd.exe spawning PowerShell from Startup context, and residual Prefetch or ShimCache entries.
3. **Rotate credentials.** For confirmed or suspected compromises, affected businesses should force password resets on all accounts with saved browser credentials, invalidate active web sessions, and rotate stored tokens and API keys, and enable MFA on all critical accounts if not already in place.
 4. **Block C&C infrastructure.** Security teams should block the SHADOW-EARTH-066 C&C addresses at the network perimeter (all ports).

Applying ongoing measures

- **Email gateway controls:** Security teams should block or quarantine RAR archives at the email gateway where feasible. Organizations that require RAR file delivery should consider inspecting ADS entries (RAR5 SERVICE headers with STMz markers).

- **Security teams should configure endpoint monitoring to:**
 - Alert on `cmd.exe` launching PowerShell with `-ExecutionPolicy Bypass` and `-WindowStyle Hidden`, especially when reading from `C:\ProgramData\`.
 - Monitor for PowerShell processes allocating executable memory. The loader uses direct NT system calls (`NtAllocateVirtualMemory`, `NtProtectVirtualMemory`) to bypass user-mode API hooks, so detection should rely on kernel-level telemetry (e.g., ETW Threat Intelligence provider or EDR kernel callbacks) rather than user-mode hooking of `VirtualAlloc`. This pattern is a strong indicator of in-memory DLL loading.
 - Monitor for `mshta.exe` execution from the Startup folder.
- **Security teams should configure network monitoring to:**
 - Alert on HTTP/HTTPS traffic with User-Agent `libcurl/8.14.0-DEV`.
- **Third-party application management:** IT teams should inventory applications that do not receive patches through standard update channels, integrate them into the patch management workflow, and track their version status across the fleet.

TrendAI Vision One™ Threat Intelligence Hub

[TrendAI Vision One™ Threat Intelligence Hub](#) provides the latest insights on emerging threats and threat actors, exclusive strategic reports from TrendAI™ Research, and TrendAI Vision One™ Threat Intelligence Feed in the TrendAI Vision One™ platform. This research was first reported to Threat Intelligence Hub subscribers in February 2026.

Emerging threats: [Persistent Exploitation of WinRAR Vulnerability CVE-2025-8088 by SHADOW-EARTH-066 and Earth Dahu Against Ukraine](#)

Threat actors: [Earth Dahu](#), [SHADOW-EARTH-066](#)

TrendAI Vision One™ Intelligence Reports (IOC Sweeping)

[Persistent Exploitation of WinRAR Vulnerability CVE-2025-8088 by SHADOW-EARTH-066 and Earth Dahu Against Ukraine](#)

Indicators of Compromise

The indicators of compromise for this entry can be found .

Appendix: MITRE ATT&CK Mapping

Tactic	Technique	ID	Campaign
Initial Access	Spearphishing Attachment	T1566.001	Earth Dahu
Execution	User Execution: Malicious File	T1204.002	Both
Execution	PowerShell	T1059.001	SHADOW-EARTH-066
Persistence	Startup Folder	T1547.001	Earth Dahu
Defense Evasion	NTFS File Attributes	T1564.004	Both
Defense Evasion	Obfuscated Files or Information	T1027	SHADOW-EARTH-066
Defense Evasion	Reflective Code Loading	T1620	SHADOW-EARTH-066
Defense Evasion	Masquerading	T1036	Both
Defense Evasion	Sandbox Evasion	T1497	SHADOW-EARTH-066
Defense Evasion	Indicator Removal: File Deletion	T1070.004	SHADOW-EARTH-066
Credential Access	Web Browser Credentials	T1555.003	SHADOW-EARTH-066
Credential Access	Steal Web Session Cookie	T1539	SHADOW-EARTH-066
Collection	Data from Local System	T1005	SHADOW-EARTH-066
Exfiltration	Exfiltration Over C&C Channel	T1041	SHADOW-EARTH-066

Appendix: MITRE ATT&CK Mapping

C&C	Web Protocols	T1071.001	Both
C&C	Encrypted Channel	T1573.001	SHADOW-EARTH-066
Impact	Data Destruction	T1485	Earth Dahu (reported by ClearSky)