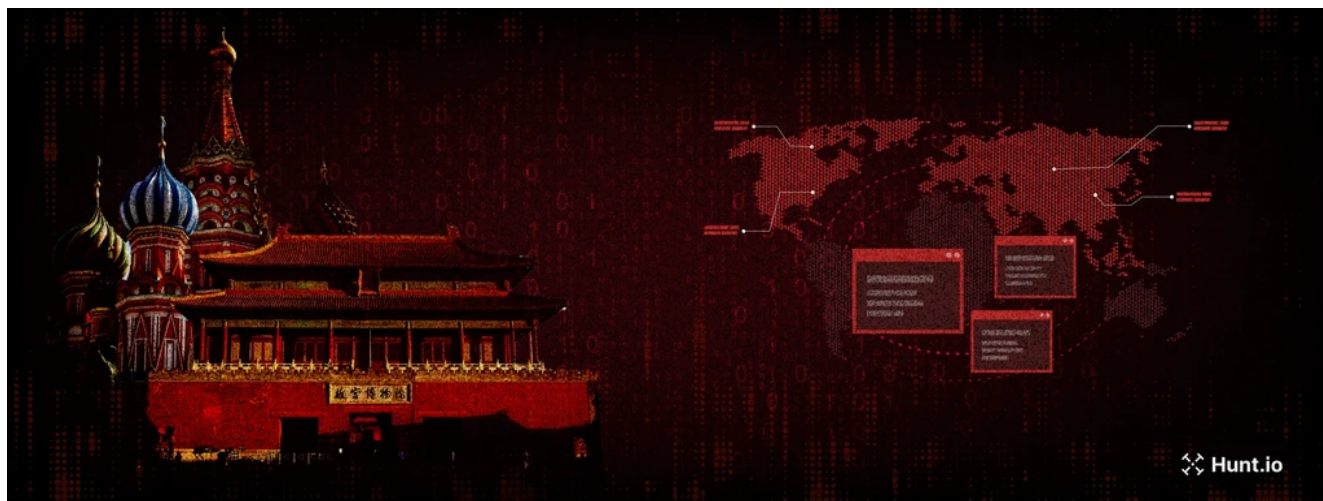


Gamaredon's Flux-Like Infrastructure and a Look at Recent ShadowPad Activity

 hunt.io/blog/state-sponsored-activity-gamaredon-shadowpad



As part of our ongoing research into internet-facing infrastructure, Hunt.io regularly surfaces indicators tied to known malware families, legitimate security testing tools, and state-linked threat activity. This visibility allows us to identify patterns in how attacker-controlled infrastructure is configured, rotated, and positioned in preparation for-or in parallel with-operational use.

In this post, we share recent observations from two distinct infrastructure clusters linked to state-sponsored groups suspected of operating out of Russia and China:

- A large number of domains using the .ru TLD registered through REGRU-RU associated with **Gamaredon**, where flux-like DNS behavior has been seen over time.
- A group of servers linked through a shared TLS certificate, including one that was recently identified communicating with the **ShadowPad** backdoor. The infrastructure has several characteristics that overlap with RedFoxtrot/Nomad Panda.

Understanding how adversaries administer their [malicious networks](#) can be just as important as analyzing the malware it supports. The following sections highlight what we've surfaced through internet-wide scanning.

Gamaredon: Flux-Like Infrastructure and Operational Patterns

Gamaredon, also tracked as Primitive Bear, is a Russian state-linked threat actor active since at least 2013. The group has primarily set its sights on the Ukrainian government and civil society organizations but has also attacked Western government entities, Africa, and NATO member states through phishing campaigns. Gamaredon has also been reported using fast flux-style DNS behavior to obscure and maintain its infrastructure.

Understanding Fast Flux

Fast flux is a DNS technique used to obscure the infrastructure behind a domain by rapidly rotating the associated IP addresses. [Domain Generation Algorithms](#) (DGAs) are often used alongside it, generating large numbers of disposable domains to further complicate attribution and takedown.

One of the earliest examples of fast flux used in a malicious manner was by the [Storm Worm](#) botnet in 2007.

Two core implementations include:

- **Single Flux:** a domain resolves to a changing set of IP addresses, while the nameservers remain static. This provides operational control while allowing the backend infrastructure to shift rapidly.
- **Double Flux:** both the domain's A records and its authoritative nameservers rotate frequently. This adds a second layer of indirection, making infrastructure takedown significantly harder.

While similar DNS behaviors exist in legitimate technologies like CDNs and load balancing, their use in attacker infrastructure often reflects different priorities-stealth, redundancy, and evasion.

For defenders, identifying these patterns through DNS anomaly detection, infrastructure clustering, and threat intelligence correlation can provide early visibility into domains likely to support phishing, malware staging, or [command-and-control server](#) activity.

Observed Trends: Domain Usage, Hosting Trends, and DNS Behavior

Gamaredon continues to operate a wide infrastructure footprint, relying heavily on .ru domains registered through REGRU-RU. Between March 31 and April 7, Hunt.io scanners identified over 30 servers linked to the group.

The majority were hosted by DigitalOcean, with BL Networks making up a number of the IPs with resolving domains. This reinforces previous reporting that the actors rely on VPS providers.

Filters

×

Mar 31 - Apr 07

Selected

Malware

1 Selected

Country

▼

Hosting Company

▼

Port

▼

32 Results



























IP	Port	Country	Malware	First Seen ↕	Last Seen ▼
 159.223.227.41	443	 NL	APT Gamaredon	04/07/2025	an hour ago
 139.59.189.155	443	 GB	APT Gamaredon	03/30/2025	an hour ago
 167.99.89.45	443	 GB	APT Gamaredon	04/06/2025	a day ago
 159.203.2.177	443	 CA	APT Gamaredon	04/05/2025	a day ago
 64.225.55.201	443	 US	APT Gamaredon	04/06/2025	a day ago
 167.172.33.160	443	 NL	APT Gamaredon	04/06/2025	a day ago
 206.189.29.231	443	 GB	APT Gamaredon	03/23/2025	a day ago
 104.131.168.255	443	 US	APT Gamaredon	04/06/2025	a day ago
 159.203.127.226	443	 US	APT Gamaredon	04/05/2025	2 days ago
 138.197.148.172	443	 CA	APT Gamaredon	04/05/2025	2 days ago
 157.230.152.7	443	 US	APT Gamaredon	04/05/2025	2 days ago
 139.59.153.79	443	 DE	APT Gamaredon	04/04/2025	3 days ago
 206.189.135.34	443	 IN	APT Gamaredon	04/04/2025	3 days ago

Figure 1: Snapshot of IP addresses detected as being associated with Gamaredon in [Hunt](#). In addition to tracking domain and IP relationships-including registrar and nameserver data-Hunt also [monitors a TLS certificate consistently](#) reused across Gamaredon infrastructure.

Many of the associated IPs briefly resolve to .ru domains, often for just a day, making the certificate an effective pivot for identifying changes before new infrastructure becomes fully operational.

As an example of the anomalous DNS behavior we've observed, both **innocentmillions[.]ru** and **langra[.]ru** initially resolved to **64.94.84[.]166**. A dig query on the first domain returned two interesting details:

- The TTL (time to live) was set to five seconds, indicating DNS records were designed to rapidly change.
- A new IP-**64.7.199[.]19**-began appearing in subsequent queries.

Further lookups to arbitrary subdomains that are not likely to exist (e.g., **thisisonlyatest[.]innocentmillions[.]ru**) returned the same IP addresses, indicating the presence of wildcard A records.

This tactic allows operators to route traffic across subdomains without managing individual DNS entries, adding another layer of evasion.

```
; <<>> DiG 9.18.30-0ubuntu0.24.04.2-Ubuntu <<>> innocentmillions.ru
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60989
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;innocentmillions.ru.          IN      A

;; ANSWER SECTION:
innocentmillions.ru.  5      IN      A      64.7.199.19

;; Query time: 786 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Sat Apr 05 15:37:36 KST 2025
;; MSG SIZE rcvd: 64
```

Figure 2: Results of dig being run against the domain `innocentmillions[.]ru`.

While the domains continued to point to `ns1.reg[.]ru` and `ns2.reg[.]ru`, the IP address gradually shifted. Over a span of two days, we observed the below:

- `64.94.85[.]18`
- to `168.100.9[.]156` (as of April 7)

```
; <<>> DiG 9.18.30-0ubuntu0.24.04.2-Ubuntu <<>> ichibanshouldnotwork.innocentmillions.ru
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 18471
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;ichibanshouldnotwork.innocentmillions.ru. IN A

;; ANSWER SECTION:
ichibanshouldnotwork.innocentmillions.ru. 5 IN A 168.100.9.156

;; Query time: 568 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Mon Apr 07 17:10:49 KST 2025
;; MSG SIZE rcvd: 85
```

Figure 3: Most recent results of dig as of `Apr 7, 2025`.

This setup mirrors a low-frequency variant of single flux DNS. Unlike fast flux used in botnets, which cycles through large pools of IPs within minutes, Gamaredon appears to maintain a slower, more controlled cadence--either managed manually or via automation.

The U.S. Cybersecurity and Infrastructure Security Agency (CISA), released a joint [report](#) discussing the threat fast flux DNS poses, as well as its malicious uses by cybercriminals and state-linked actors alike.

Although the behavior above doesn't exhibit the high-volume churn of bot-driven flux networks, the short TTLs, static nameservers and reused infrastructure tactics form a consistent pattern, one that defenders can use to track domains and servers in near real-time.

Server Cluster Tied to ShadowPad Sample With RedFoxtrot Overlaps

It all started with a certificate.

While [searching for anomalous TLS certificates](#) using [HuntSQL™](#), our SQL-powered engine for threat infrastructure discovery, we uncovered a group of servers sharing traits consistent with infrastructure previously attributed to the suspected Chinese APT group RedFoxtrot, as named by Recorded Future's Iniskt Group.

The certificate--which spoofs Microsoft--was first seen in late 2024 according to our scan data. Using a combination of certificate details and [JA4X fingerprinting](#), we uncovered a set of servers hosted across known VPS providers like The Constant Company, XNNET, Akamai, and Digital Ocean.

Results

HTTPMalwareCertificatesHoneypotOpen DirectoriesPhishingCrawlerProtocolURLxSSHFilenamesJARM

Custom Timeframe.

5 Results

Download

ip

172.236.187.135

172.235.10.252

45.77.33.174

139.84.142.99

64.227.185.216

Rows per page100

Page 1 of 1

<<<>>>

Figure 4: Results of our HuntSQL query for the suspicious TLS certificate.

As we are still tracking this set of servers, we will be withholding detailing specific queries. As we gain additional insight into this activity, the data will be added to the Hunt app and available to users.

Domain Characteristics

The domains make use of dynamic DNS services, including [giize\[.\]com](#) and [kozow\[.\]com](#), which have a long history of being abused by both cybercriminal and state-linked actors for malicious operations.

Current servers include domains that spoof Cloudflare and what appears to be a mail server for 'OPW'-a name that may reference the Office of Public Works in Ireland, OPW Fueling Components, or an unrelated internal service.

Separately, earlier domains impersonated entities such as Broadcom, an American semiconductor manufacturer, as well as Indian telecom and government organizations.

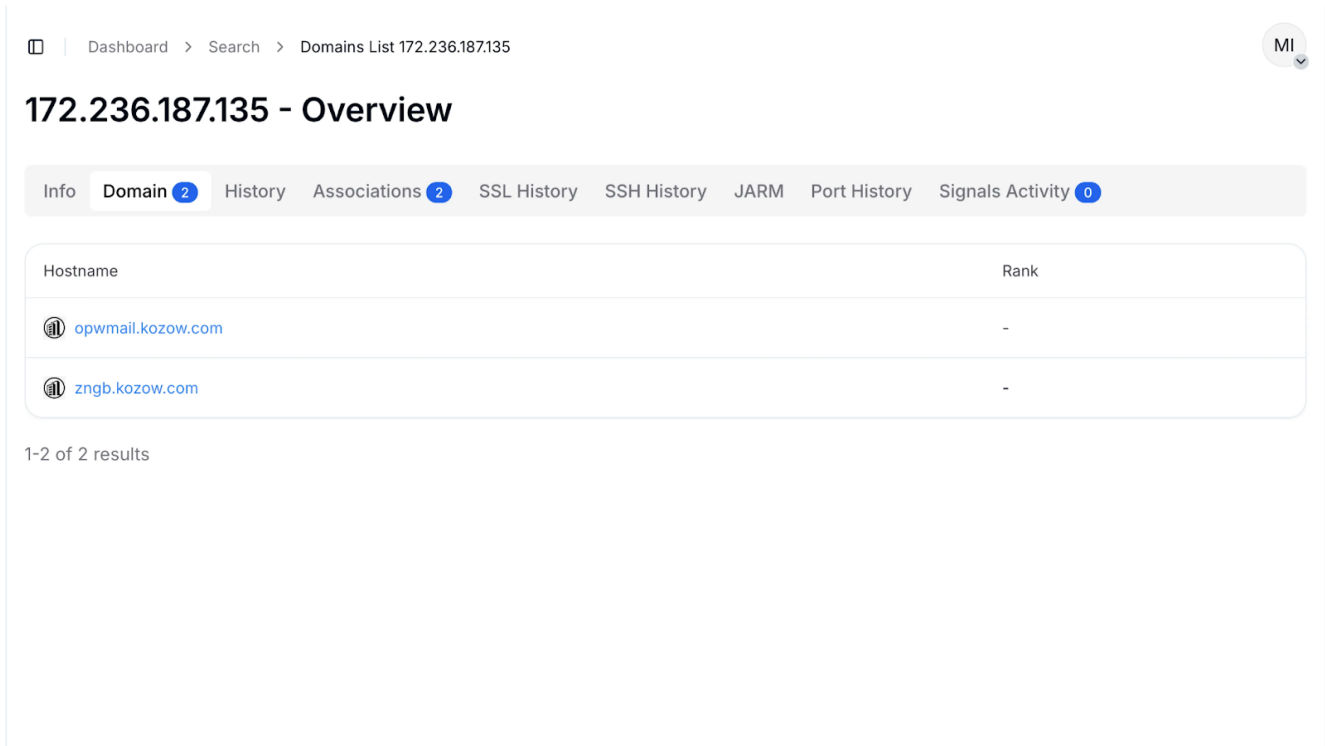


Figure 5: DDNS domains resolving to one of the IPs within the identified cluster.
A complete list of domains and IP addresses can be found in the IOC section at the end of this post.

ShadowPad Link

ShadowPad is a modular backdoor selectively used in targeted espionage operations by Chinese state-linked threat groups. Its appearance in an environment is often considered a high-confidence indicator of advanced persistent threat activity.

One server in the group- 45.77.33[.]174-resolves to a ShadowPad command-and-control domain, update.updatemic[.]com, which is contacted by a ZIP archive named Dvx.zip. The sample, detected by 25 vendors on VirusTotal, includes several files, including a legitimate signed Windows executable vulnerable to DLL side-loading.

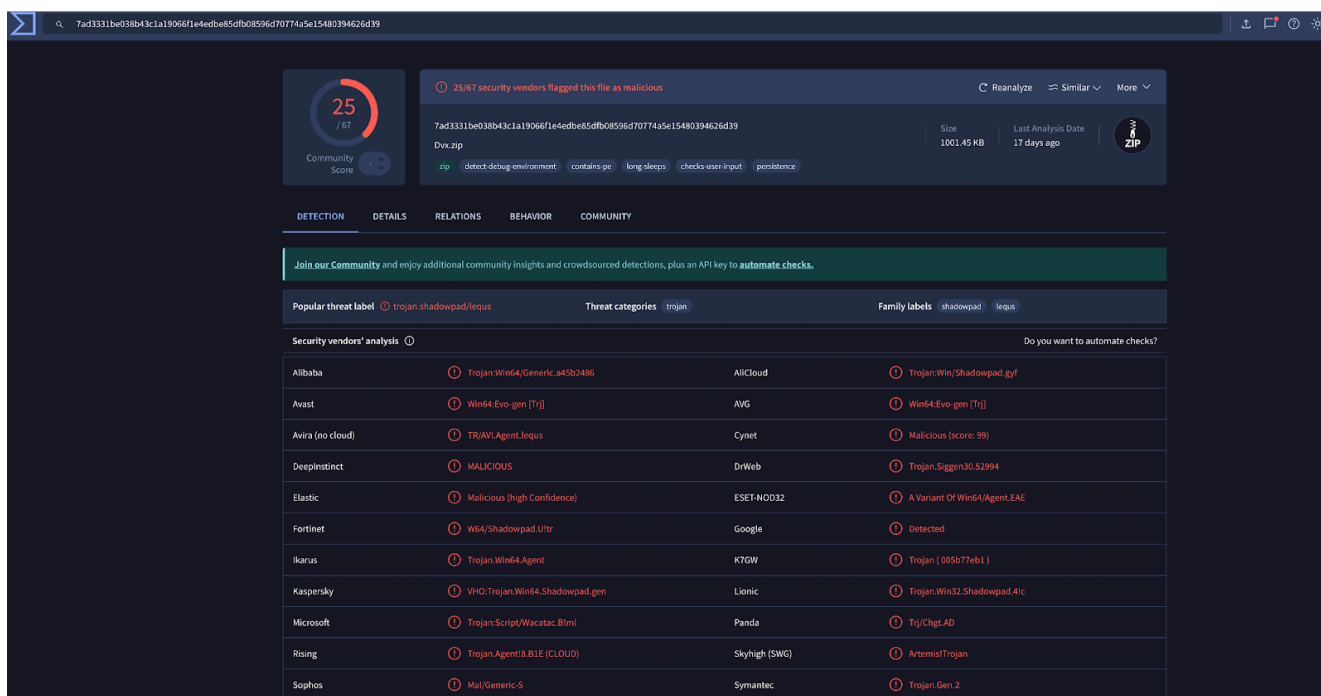


Figure 6: [VirusTotal](#) results for the zip archive containing the ShadowPad backdoor.

Within the archive are the following files:

- msimg32.dll -- The ShadowPad backdoor
- h.exe -- A legitimate NETGATE Amity Antivirus binary, renamed and used for sideloading
- Ak.bat -- A batch script that launches h.exe
- Package.ps1 -- A PowerShell script used for delivery

Dvx.zip is downloaded from a second IP, **149.28.137[.]179**, at the path `/a/Dvx.zip`, using the same Package.ps1 script. A single domain spoofing Cloudflare- **static.developers-cloudflare[.]us**- resolves to the server. The script appearing across multiple delivery points suggests a modular approach, allowing the operator to rotate infrastructure while maintaining a consistent delivery mechanism.

The reuse of a spoofed TLS certificate, consistent naming patterns, and the presence of ShadowPad suggest an actor maintaining controlled access points across a small but deliberate infrastructure set. While the broader purpose remains unclear, the setup reflects a level of preparation aligned with targeted access operations.

Final thoughts

The infrastructure outlined in this post reflects how persistent, state-linked threat actors continue to administer and evolve their operational footprint. From Gamaredon's flux-like DNS activity to the reuse of ShadowPad-linked certificates and staging scripts, each cluster provides a window into how adversaries prepare access points long before payloads are delivered.

Understanding how threat actors shape and maintain their infrastructure offers defenders an opportunity to detect activity earlier in the intrusion lifecycle. While payloads may change, the operational habits behind staging, delivery, and control often remain consistent-and that's where long-term visibility matters most.

Gamaredon Network Observables and Indicators of Compromise (IOCs)

*This list was compiled: Apr 7, 2025

159.203.2[.]177	N/A	DigitalOcean	DigitalOcean
157.230.152[.]7	N/A	DigitalOcean	DigitalOcean
139.59.153[.]79	N/A	DigitalOcean	DigitalOcean
206.189.135[.]34	N/A	DigitalOcean	DigitalOcean
159.65.192[.]30	N/A	DigitalOcean	DigitalOcean
64.94.84[.]66	studomed[.]ru vinnichich[.]ru www[.]langra[.]ru meuviresse[.]ru lafren[.]ru www[.]neonation[.]ru baklchug[.]ru rudanka[.]ru prostali[.]ru innocentmillions[.]ru antitrots[.]ru	BL Networks	BL Networks
64.227.72[.]253	N/A	DigitalOcean	DigitalOcean
159.65.205[.]28	N/A	DigitalOcean	DigitalOcean
139.68.15[.]131	N/A	DigitalOcean	DigitalOcean
149.248.77[.]157	N/A	BL Networks	BL Networks
139.59.13[.]239	N/A	DigitalOcean	DigitalOcean
45.55.235[.]87	N/A	DigitalOcean	DigitalOcean
142.93.145[.]206	N/A	DigitalOcean	DigitalOcean
168.100.11[.]43	N/A	BL Networks	BL Networks
159.203.17[.]42	N/A	DigitalOcean	DigitalOcean
209.38.196[.]253	N/A	DigitalOcean	DigitalOcean
216.245.184[.]160	N/A	BL Networks	BL Networks
104.131.190[.]132	N/A	DigitalOcean	DigitalOcean
134.209.244[.]43	N/A	DigitalOcean	DigitalOcean

139.59.189[.]155	N/A	DigitalOcean	DigitalOcean
168.100.11[.]116	N/A	BL Networks	BL Networks
165.227.39[.]7	N/A	DigitalOcean	DigitalOcean
139.59.95[.]111	N/A	DigitalOcean	DigitalOcean
178.62.238[.]209	N/A	DigitalOcean	DigitalOcean
64.94.85[.]230	N/A	BL Networks	BL Networks
45.55.42[.]145	N/A	DigitalOcean	DigitalOcean
167.99.90[.]162	N/A	DigitalOcean	DigitalOcean
142.93.232[.]225	N/A	DigitalOcean	DigitalOcean
68.183.201[.]96	N/A	DigitalOcean	DigitalOcean
162.33.179[.]216	N/A	BL Networks	BL Networks
46.101.240[.]172	N/A	DigitalOcean	DigitalOcean
143.110.218[.]175	N/A	DigitalOcean	DigitalOcean
45.61.139[.]116	N/A	BL Networks	BL Networks
46.101.91[.]224	N/A	DigitalOcean	DigitalOcean
206.189.29[.]231	N/A	DigitalOcean	DigitalOcean
64.7.199[.]19	home1and[.]ru	BL Networks	BL Networks
149.248.77[.]157	www[.]phlove[.]ru chinosadame[.]ru toretsky[.]ru jedemdasseine[.]ru spanishsky[.]ru endless-bridge[.]ru www[.]bakalchug[.]ru rookida[.]ru	BL Networks	BL Networks

RedFoxtrot-Linked Network Observables and Indicators of Compromise (IOCs)

45.77.33[.]174	update.updatemic[.]com	The Constant Company	The Constant Company
64.227.185[.]216	N/A	DigitalOcean	DigitalOcean
139.84.142[.]99	N/A	The Constant Company	The Constant Company

172.236.187[.]135	opwmail.kozow[.]com zngb.kozow[.]com	Akamai Connected Cloud	Akamai Connected Cloud
172.235.10[.]252	gsslxqxqzyo.giize[.]com	Akamai Connected Cloud	Akamai Connected Cloud
149.28.137[.]179	static.developers- cloudfare[.]us	The Constant Company	The Constant Company

RedFoxtrot-Linked Host Observables and Indicators of Compromise (IOCs)

Dvx.zip	7ad3331be038b43c1a19066f1e4edbe85dfb08596d70774a5e15480394626d39
AK.bat	cf0403934749f9d6cbcc80e38d0fca87f7d9e519d9a9031b1797b5568a8e3534
AmitiAntivirusSkin.exe (Legitimate file)	200db5f89d58ce0060da0fac909162f66d9fa27dfe590e929ce9b42fd8d55ae3
msimg32.dll	8b557df773156a87f2fe6bf7bb1b10a690e650c08abb924181165ce82d3fc4af
Package.ps1	a596d4a1ede0d022d77f0b03c723c7071ffec0e89b35f0d30fb9ff15feeb4969