

From Russia with a 71: Uncovering Gamaredon's fast flux infrastructure. New Apex domains and ASN/IP diversity patterns discovered

By Silent Push Threat Team

Published: 2023-09-07 · Archived: 2026-04-05 19:47:30 UTC

Update May 1, 2025:

A recent Joint Cybersecurity [Advisory](#) from the NSA, FBI, CISA, along with law enforcement in Australia, Canada, and New Zealand, warns that many enterprise organizations have defensive gaps when it comes to detecting and mitigating Fast Flux techniques, such as those utilized by the Gamaredon Group. These gaps expose vulnerabilities that cybercriminals and nation-state actors can exploit to maintain stealthy, persistent access to systems.

Gamaredon's Fast Flux evasion techniques involve rapidly rotating IP addresses associated with domain names, making it difficult for law enforcement and security systems to block or trace the group's malicious activity and ultimately avoid detection. Silent Push's proprietary infrastructure variance metrics are the perfect counter-measure, being purpose-built for tracking, mapping, and blocking Fast Flux networks as they are spun up.

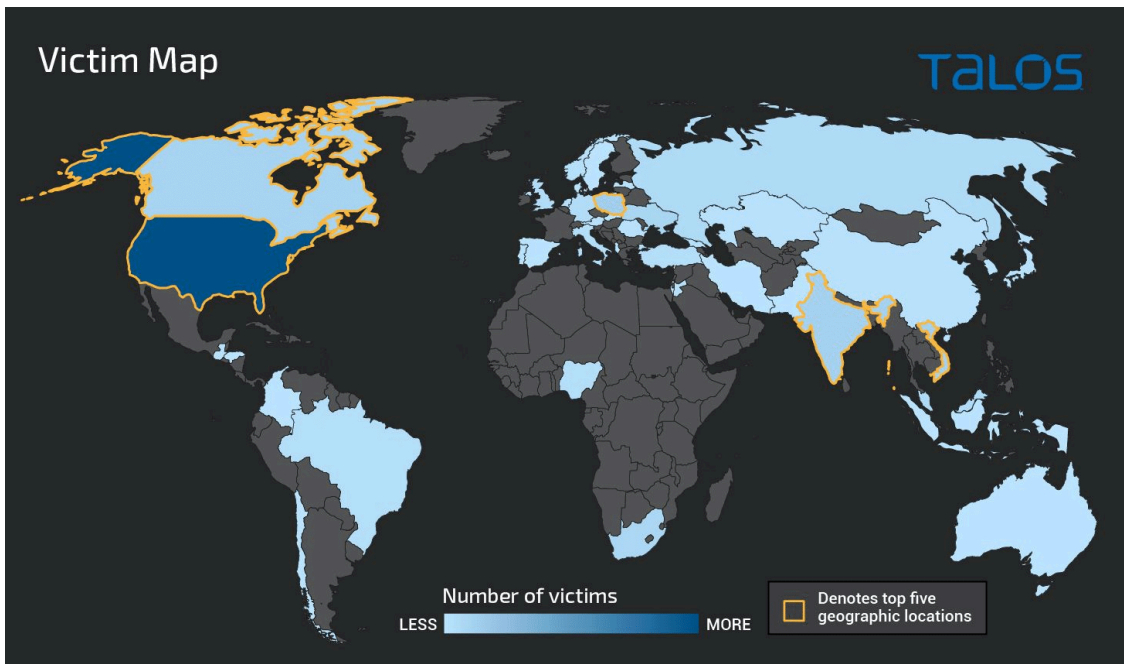
[Interested to learn more?](#) Our team has recently published a new technical report on Gamaredon, available exclusively to our enterprise subscribers, which provides live examples of how to utilize our platform's advanced capabilities to track and proactively block Gamaredon's malicious infrastructure.

Key Findings

- Silent Push explored the extent of the Gamaredon Group's fast flux operation.
- We discovered 300+ new Apex domain indicators of compromise (IOCs) from a single Gamaredon domain.
- Our proprietary fingerprinting techniques exposed the deployment of new attacker infrastructure using wildcard A records.

Background

Gamaredon—also known as Primitive Bear, Actinium, or Shuckworm—is a Russian Advanced Persistent Threat (APT) group that has been active since at least 2013 and [more recently in Ukraine](#), including [reported attacks on Western government entities](#):



Source: Talos, 2021

Gamaredon is a highly belligerent threat group that deviates from the standard hit-and-run tactics used by other APT groups by propagating sustained attacks that are both heavily obfuscated and uniquely aggressive.

Gamaredon TTPs

The group uses [spear phishing and social engineering](#) to deliver malware hidden within MS Word documents, as referenced below:

Date (UTC)	SHA256 hash	Type	Signature	Tags	Reporter	DL
2023-08-29 20:57	e4de676ddb2ef92816a5...	doc	Gamaredon	apt doc gamaredon UKR	smica83	📄
2023-07-27 08:10	80bcacd8eb08caa7533f5...	doc	Gamaredon	apt doc gamaredon	smica83	📄
2022-11-04 18:26	dcaa7fe64dd5016aac13b...	exe	Gamaredon	exe gamaredon	vxunderground	📄
2022-11-04 18:25	bfd66412e80e3044d432...	exe	Gamaredon	exe gamaredon	vxunderground	📄
2022-08-31 06:22	3e84ce7b8a3c8bab4cdc6...	exe		exe gamaredon Ukraine	JAMESWT_MHT	📄
2022-02-24 09:53	496213612d873633a803...	doc		doc gamaredon maldoc	Arkbird_SOLG	📄
2021-08-02 09:10	032fbc5e0f7d65d7cc104...	doc		apt doc gamaredon	JAMESWT_MHT	📄
2021-08-02 09:10	1375d8021159ba2f4e6cd...	doc		apt cve-2017-0199 doc gamaredon	JAMESWT_MHT	📄
2021-08-02 09:05	c34f7ec5bbdc3a40d709d...	doc		apt doc gamaredon	JAMESWT_MHT	📄
2021-08-02 09:05	ba6582d2225f498e6cad5...	doc		apt doc gamaredon	JAMESWT_MHT	📄
2021-08-02 09:04	44847cbd0514de214cda...	doc		apt doc gamaredon	JAMESWT_MHT	📄
2021-08-02 09:04	21542f9b9f633b6ef399c...	doc		apt cve-2017-0199 doc gamaredon	JAMESWT_MHT	📄
2021-08-02 08:53	df05037974636c59d9e7...	doc		apt doc gamaredon	JAMESWT_MHT	📄
2021-08-02 08:53	f14192bc76e4a37585b29...	doc		apt doc gamaredon	JAMESWT_MHT	📄
2021-08-02 08:52	199b413b421644c1f3854...	doc		apt doc gamaredon	JAMESWT_MHT	📄
2021-08-02 08:52	78d9a3b832ade4695f16...	doc		apt doc gamaredon	JAMESWT_MHT	📄
2021-08-02 08:52	8b1fc13434c8c66cecb0b...	doc		apt doc gamaredon	JAMESWT_MHT	📄
2021-08-02 08:52	c3396b2b06dc9c3c0c199...	doc		apt doc gamaredon	JAMESWT_MHT	📄
2021-08-02 08:51	e0db2c1bfca863d60b005...	doc		apt doc gamaredon	JAMESWT_MHT	📄
2021-08-02 08:51	809d03810fcb2f04958f3...	doc		apt doc gamaredon	JAMESWT_MHT	📄
2021-08-02 08:51	af7442f2ada549db5b18...	rar		apt gamaredon rar	JAMESWT_MHT	📄
2021-05-18 19:16	5c20d1f0c60a10e7d656c...	doc		cve-2017-0199 gamaredon rtf	JAMESWT_MHT	📄
2021-04-06 13:36	7c3c090959feaaa4ce79a...	doc		apt gamaredon	JAMESWT_MHT	📄
2021-04-06 13:34	9ebcbf1e57596020b73a9...	zip		apt gamaredon	JAMESWT_MHT	📄
2020-06-10 07:21	8e598335d0de4438b80d...	doc		apt gamaredon	JAMESWT_MHT	📄

MalwareBazaar directory of Gamaredon MS Word malware

Using MS Word combats static analysis by hosting the payload on a template that is downloaded from an attacker-controlled server; once the document is opened and the user has met one or more conditions, such as geographic location, device type, or system specification, before delivery.

A large number of Gamaredon subdomains used in spear phishing attacks were linked to the top-level domain (TLD) “.ru,” registered via REGRU-RU, and contained the number “71.”

The screenshot shows a domain search tool with various filters on the left and a JSON response on the right. The filters include domain, infratag, maxname, first_seen_min, first_seen_min_mode, last_seen_min, last_seen_min_mode, asnum, asname, asname_contains, asn_match_max, network, first_seen_after, and register. The JSON response on the right contains metadata and records for IP diversity, listing hostnames like allocate71.intigan.ru, asc71.boanzo.ru, and bike71.ibragino.ru.

Gamaredon subdomains using the number 71

Use of fast fluxing

Gamaredon operates with an innumerable number of IP addresses and uses wildcard A records in place of definable subdomains to evade detection in a technique known as [fast fluxing](#).

A large group of IPs was associated with a single Fully Qualified Domain Name (FQDN) and rotated through an attack at an extremely high frequency via automated DNS resource record (RR) amendments in the zone file.

APT groups employ fast fluxing to circumvent traditional threat detection methods that rely on threat feeds containing full domain names, including subdomains.

Rather than relying on lists of isolated IOCs, organizations need to deploy countermeasures that track the underlying **infrastructure** that accommodates an attack—Apex domains, ASNs, registrars, and authoritative nameservers—and extrapolate correlative datasets that allow security teams to identify **patterns** in attacker behavior—such as ASN and IP diversity data or naming conventions.

To defend against fast-flux TTPs, organizations must identify and block Apex domains, regardless of the subdomain. Let's take a look at how we used Silent Push to do just that...

Deep Dive: samiseto[.]ru

Every investigation begins with a series of observables. [Several online sources](#) reported recent attempts by Gamaredon to inject [malware](#), using an MS Word template, from the following domains:

- [http://encyclopedia83.samiseto\[.\]ru/HOME-PC/registry/amiable/prick/sorry\[.\]83glf](http://encyclopedia83.samiseto[.]ru/HOME-PC/registry/amiable/prick/sorry[.]83glf)
- [http://relation46.samiseto\[.\]ru/DESKTOP-UVHG99D/percy\[.\]46rra](http://relation46.samiseto[.]ru/DESKTOP-UVHG99D/percy[.]46rra)



С Y 乃 毛 尺 0 V 毛 尺 人 0 卅 0
@CyberOverload



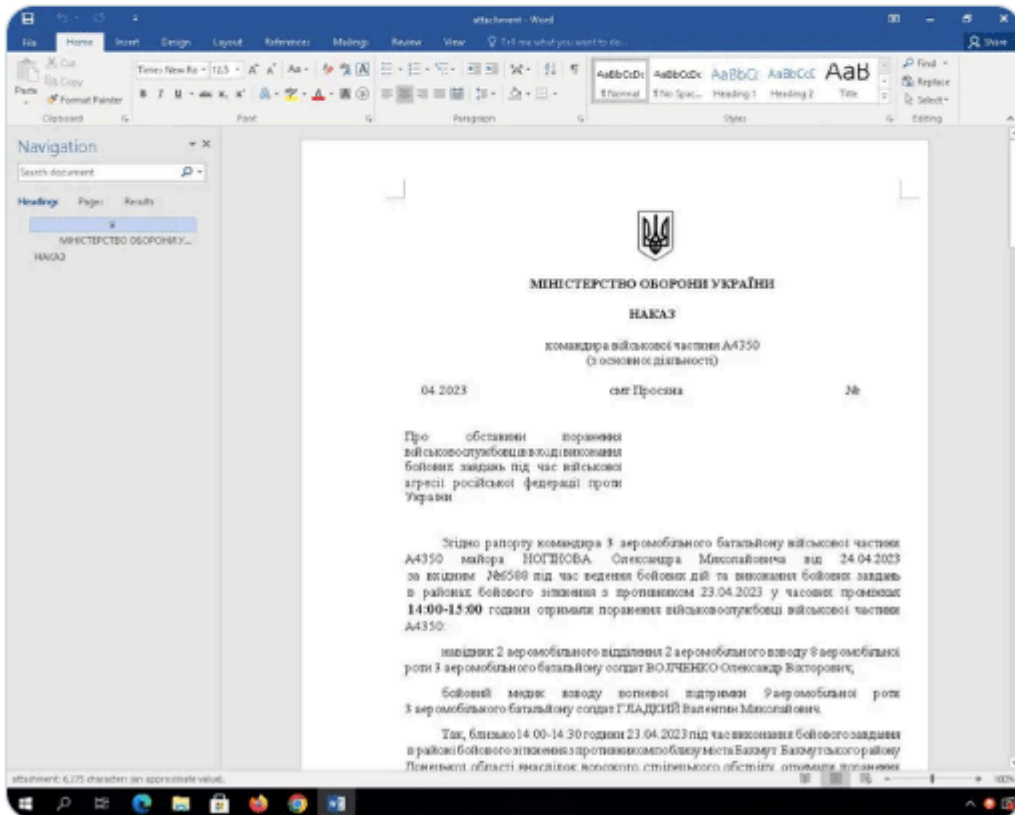
#APT #Gamaredon #PrimitiveBear 🐻

DOC:
d279a6e0ae20a2a6402451745067df35

Remote Template:
hXXp://relation46.samisetto[.]ru/DESKTOP-UVHG99D/percy[.]46rra

DNS:
samisetto[.]ru
relation46.samisetto[.]ru

Domain ref
twitter.com/malPileDiver/s...



Twitter post announcing malware hosted on samisetto[.]ru

Checking VirusTotal confirmed that the domains had been flagged as malicious. This was mainly due to the domains being reported on Twitter as post-breach intelligence:

We took one of the above domains, encyclopedia83.samisetto[.]ru (hosted on REGRU-RU), and analyzed it by cross-referencing WHOIS information, IP diversity data, and reverse lookups that laid bare a fresh list of domain

IOCs:

encyclopedia83.samisetto.ru Domain

Flag(s)
Part of Live Threat Feeds

Highlights
 ASN Diversity: 1 | IP Diversity: 12
 Age: - | Registrar: REGRU-RU

Information

Domain Information

Threat Name	Value
User Tags	-
Infratag	REGRU-RU
First Seen	-
Last Seen	-
Age	-
DGA	0 score

Whois Information

Name	Value
Created	2023-04-18 15:03:44
Country	-
City	-
Address	-
Email	-
ZIP Code	-
Registrar	REGRU-RU

Enriching encyclopedia83.samisetto[.]ru

We discovered 98 A records associated with *samisetto[.]ru, that were used in constant rotation:

Query	Query ASN	Answer	Answer ASN	Count	First Seen	Last Seen	Type
encyclopedia83.samisetto.ru	-	5.44.42.205	207713	2	2023-07-11 19:55:26	2023-07-11 19:55:26	A
relation46.samisetto.ru	-	217.78.239.173	211211	1	2023-07-11 05:51:36	2023-07-11 05:51:36	A
www.samisetto.ru	-	147.182.134.243	14061	1	2023-07-10 19:25:11	2023-07-10 19:25:11	A
relation46.samisetto.ru	-	193.228.128.45	207713	1	2023-07-06 01:32:40	2023-07-06 01:32:40	A
www.samisetto.ru	-	193.228.128.45	207713	1	2023-07-05 16:32:43	2023-07-05 16:32:43	A
relation46.samisetto.ru	-	89.185.84.141	207713	1	2023-06-29 14:22:38	2023-06-29 14:22:38	A
www.samisetto.ru	-	157.230.191.232	14061	1	2023-06-29 04:47:14	2023-06-29 04:47:14	A
relation46.samisetto.ru	-	89.23.108.119	207713	1	2023-06-27 17:50:46	2023-06-27 17:50:46	A
www.samisetto.ru	-	194.87.216.81	207713	1	2023-06-27 04:43:15	2023-06-27 04:43:15	A
www.samisetto.ru	-	5.44.42.157	207713	2	2023-05-14 05:08:45	2023-04-22 17:05:06	A
relation46.samisetto.ru	-	134.122.112.229	14061	1	2023-06-21 04:11:14	2023-06-21 04:11:14	A
www.samisetto.ru	-	188.94.155.46	21289	1	2023-06-20 17:58:02	2023-06-20 17:58:02	A
relation46.samisetto.ru	-	185.39.207.101	207713	1	2023-06-19 00:53:24	2023-06-19 00:53:24	A
relation46.samisetto.ru	-	45.95.232.95	207713	1	2023-06-15 00:02:24	2023-06-15 00:02:24	A
www.samisetto.ru	-	45.95.232.95	207713	1	2023-06-14 21:01:28	2023-06-14 21:01:28	A
relation46.samisetto.ru	-	46.29.234.04	207713	1	2023-06-12 23:13:07	2023-06-12 23:13:07	A

An A record lookup for samisetto[.]ru

Further analysis revealed that IP addresses were used for no more than four days before being replaced with a fresh IP (along with new subdomains). This helped the threat actors evade detection and rendered most isolated IOCs obsolete upon discovery.

Threat Name	Value
Host	relation46.samisetto.ru
ASN Diversity	2
IP Diversity All	7
IP Diversity Groups	7

Select another period
30 days

Show Timeline

High IP diversity score

To extract actionable IOCs, we created a list of all IP addresses that a subdomain of samiseto[.]ru had ever pointed to. We then applied a reverse lookup to identify all domains associated with those IP addresses, before matching the domains to threat activity using a series of key indicators.

The results returned a list of 375 Apex domains, which we used to populate our Gamaredon early detection feed (available to Silent Push Enterprise customers).

Use of wildcard records

We noticed that any string combination added before .samiseto[.]ru pointed to 5.44.42[.]154. After running a dig command, we were able to ascertain that attackers were using a wildcard A record to point to the domain 5.44.42[.]154:

```
; <<>> DiG 9.18.12-0ubuntu0.22.04.2-Ubuntu <<>> *.samiseto.ru
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 5382
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

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

;; ANSWER SECTION:
*.samiseto.ru.          21600  IN      A      5.44.42.154

;; Query time: 247 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Wed Aug 30 13:35:34 WEST 2023
;; MSG SIZE rcvd: 58
```

We ran a dig command

```
; <<>> DiG 9.18.12-0ubuntu0.22.04.2-Ubuntu <<>> thisprobablydoesnotexistorsomething.samiseto.ru
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 40428
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

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

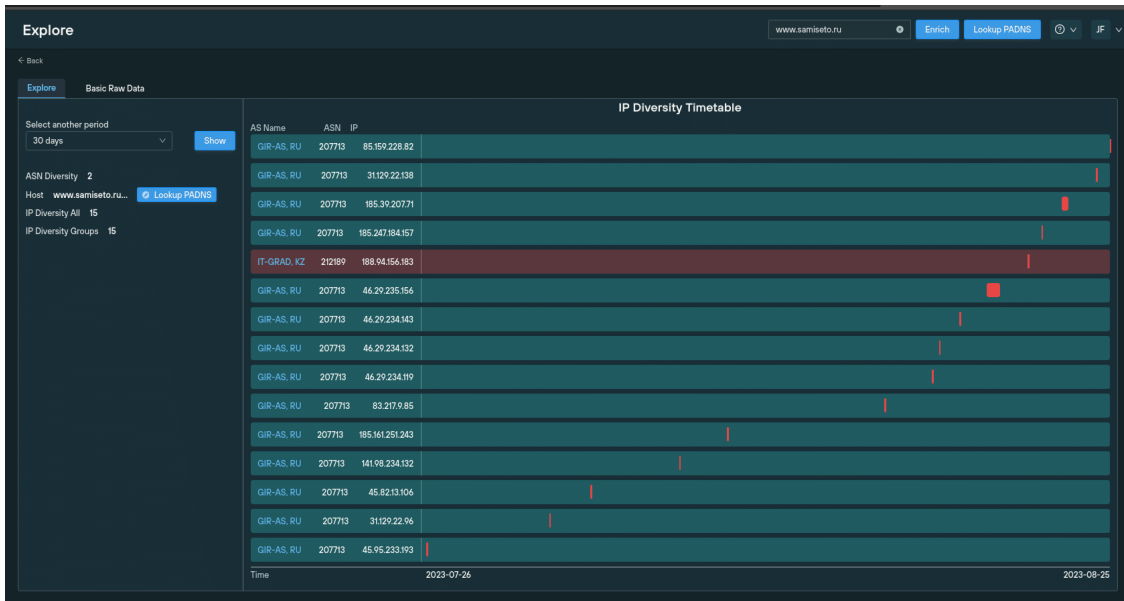
;; ANSWER SECTION:
thisprobablydoesnotexistorsomething.samiseto.ru. 21600 IN A 5.44.42.154

;; Query time: 503 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Wed Aug 30 13:46:18 WEST 2023
;; MSG SIZE rcvd: 92
```

Dig command proving the use of wildcard A record

IP diversity and ASN analysis

Using IP diversity data, we established that samiseto[.]ru had pointed to 15 IP addresses within a 30-day period, all of them bar one being hosted on the Russian ASN GIR-AS, RU (207713), with the remainder hosted via Kazakhstan on IT-GRAD, KZ (212819):



IP/ASN diversity data for samiseto[.]ru

While the majority of IPs over a 90-day period were traced back to GIR-AS RU, we discovered that DIGITALOCEAN US, the New York-based cloud services organization, was also used:

GIR-AS, RU	207713	46.29.238.88
GIR-AS, RU	207713	45.82.13.106
GIR-AS, RU	207713	31.129.22.96
GIR-AS, RU	207713	46.29.235.58
GIR-AS, RU	207713	194.87.45.120
GIR-AS, RU	207713	194.87.45.101
GIR-AS, RU	207713	46.29.238.62
GIR-AS, RU	207713	46.29.238.5
GIR-AS, RU	207713	194.87.216.112
GIR-AS, RU	207713	185.39.204.185
GIR-AS, RU	207713	141.98.234.135
ITDEVELOP-AS,...	211211	217.78.239.173
GIR-AS, RU	207713	193.228.128.45
GIR-AS, RU	207713	89.185.84.141
GIR-AS, RU	207713	89.23.108.119
DIGITALOCEAN...	14061	134.122.112.229
GIR-AS, RU	207713	185.39.207.101
GIR-AS, RU	207713	45.95.232.95
GIR-AS, RU	207713	46.29.234.94
IT-GRAD, KZ	212189	188.94.156.131
DIGITALOCEAN...	14061	192.241.141.176
GIR-AS, RU	207713	185.39.204.119
DIGITALOCEAN...	14061	164.92.104.215

Historical ASN data for samiseto[.]ru

Using Silent Push to Combat Gamaredon's Fast Flux Techniques

Our threat analysts utilized IP/ANS diversity data and advanced DNS fingerprinting techniques to reveal the extent of Gamaredon's fast flux infrastructure and populate an early detection feed with hundreds of unique malicious Apex domains, using a single reported subdomain as the target IOC.

Silent Push Enterprise users can ingest curated threat feeds containing IOCs related to the Gamaredon group's fast flux infrastructure using the tags #russo, #gamaredon, and #apt.

The free Silent Push Community Edition also includes many of the lookups used in our research. Sign up [here](#) for your complimentary account.

Email info@silentpush.com for further guidance on any of the countermeasures we've talked about in this blog article.

Explore our [Knowledge Base](#) for in-depth articles on how to use Silent Push to defend against attacks.

Sample Indicators of Compromise List

A sample list of IOCs associated with this threat for a public-facing blog. *(A full list of IOCs is available with a Silent Push Enterprise subscription).*

- quyenzo[.]ru
- ulitron[.]ru
- bromumo[.]ru
- erinaceuso[.]ru
- ayrympo[.]ru
- caccabius[.]ru
- madzhidgo[.]ru
- amalsa[.]ru
- dedspac[.]ru

- 141.98.233.109
- 46.29.234.119
- 141.98.233.103

Source: <https://www.silentpush.com/blog/from-russia-with-a-71/>