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

silentpush.com/blog/from-russia-with-a-71

September 7, 2023

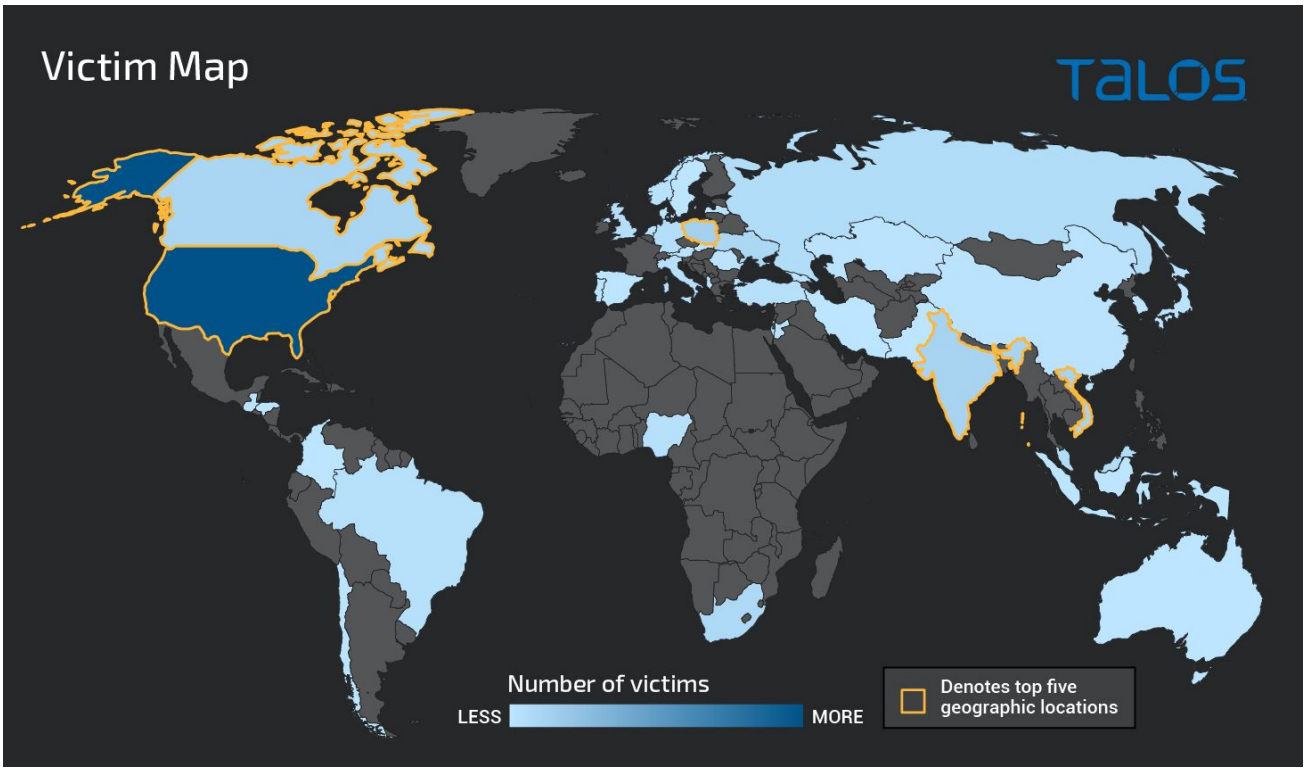
Sep 7
Written By Silent Push Labs Team

Key points

- Silent Push explores the extent of the Gamaredon Group's fast flux operation.
- 300+ new apex domain IOCs discovered from a single Gamaredon domain.
- Proprietary fingerprinting techniques used to expose the deployment of new attacker infrastructure using wildcard A records

Background

Gamaredon - also known as Primitive Bear, Actinium or Shuckworm - are a Russian Advanced Persistent Threat (APT) group that has been active since at least 2013, historically across the US and the Indian Subcontinent, and more recently in Ukraine, including reported attacks on Western government entities:



Source: Talos, 2021

Gamaredon are a highly-belligerent threat group who deviate 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

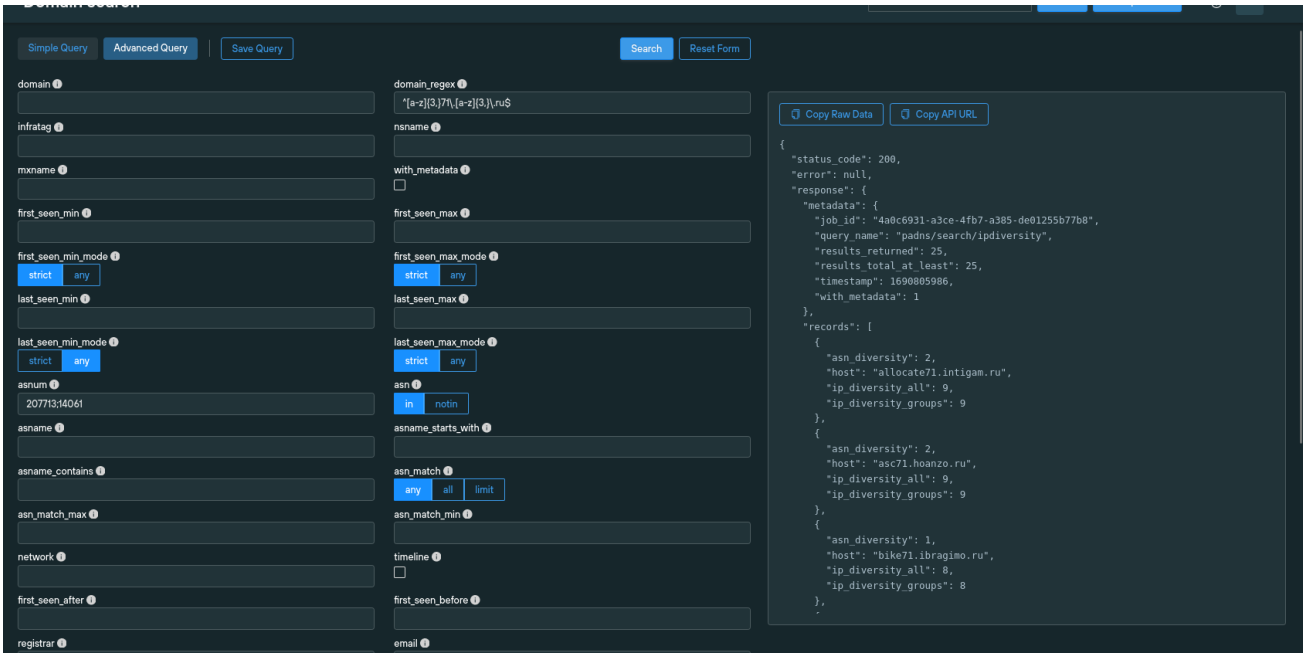
The group uses spear phishing and social engineering to deliver malware hidden within MS Word documents:

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	af7442f42ada549db5b18...	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 and system specification - prior to delivery.

A large amount of Gamaredon subdomains used in spear phishing attacks are linked to the TLD .ru, registered via REGRU-RU and contain the number 71.



Gamaredon subdomains using the number 71

Use of fast fluxing

Gamaredon operates with an innumerable amount 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 are 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.

Fast fluxing is used by APT groups to circumvent traditional methods of threat detection that rely on threat feeds containing full domain names, including subdomains.

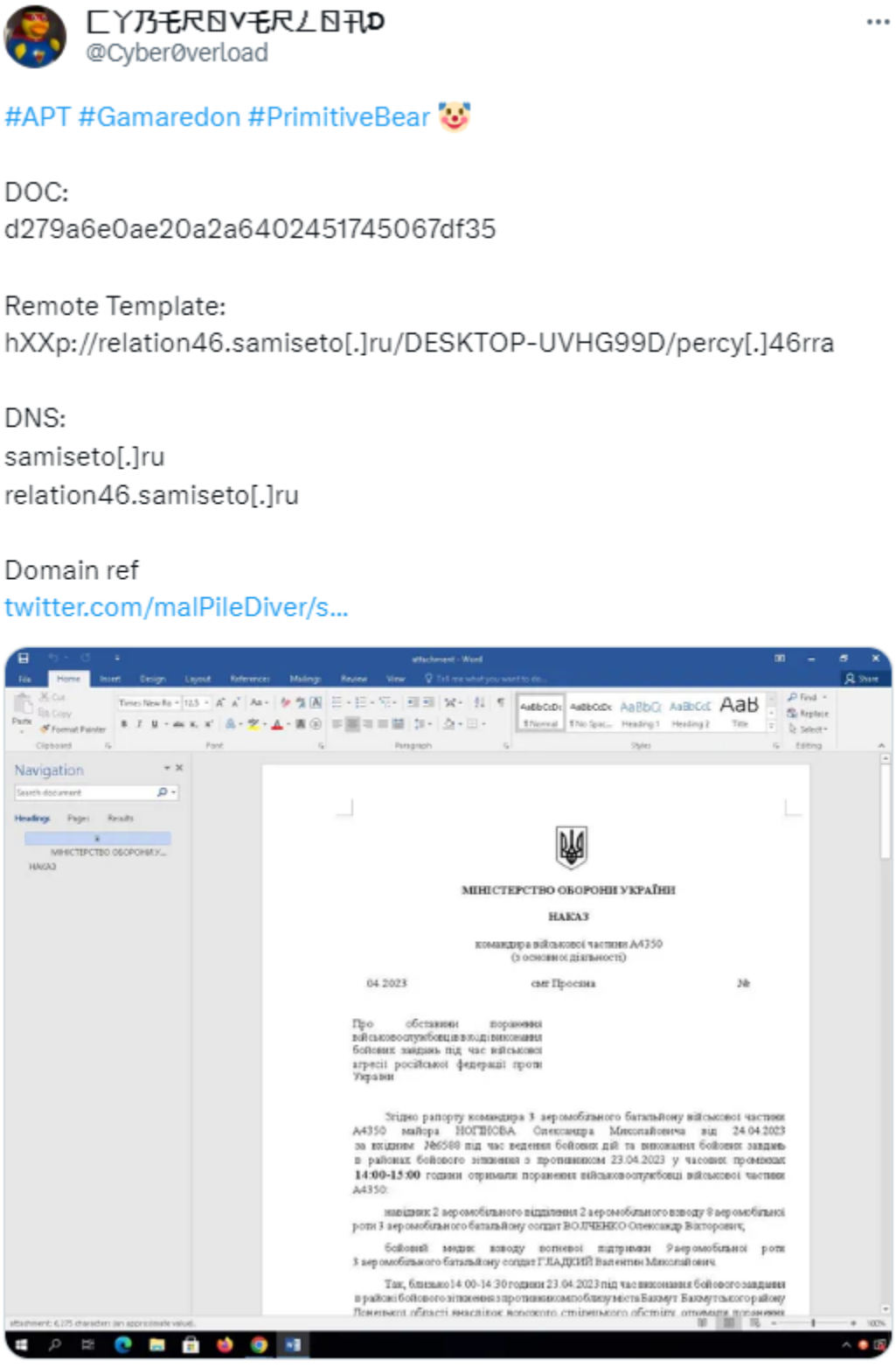
Rather than relying on lists of isolated IOCs, organizations need to deploy countermeasures that track the underlying **infrastructure** that accommodates an attack - apex domains, ASNs, registrars, authoritative nameservers etc. - and extrapolate correlative datasets that allow security teams to identify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

In order to defend themselves against fast flux TTPs, organizations need to 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 have 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://relation46.**samiseto[.]ru**/DESKTOP-UVHG99D/percy[.]46rra

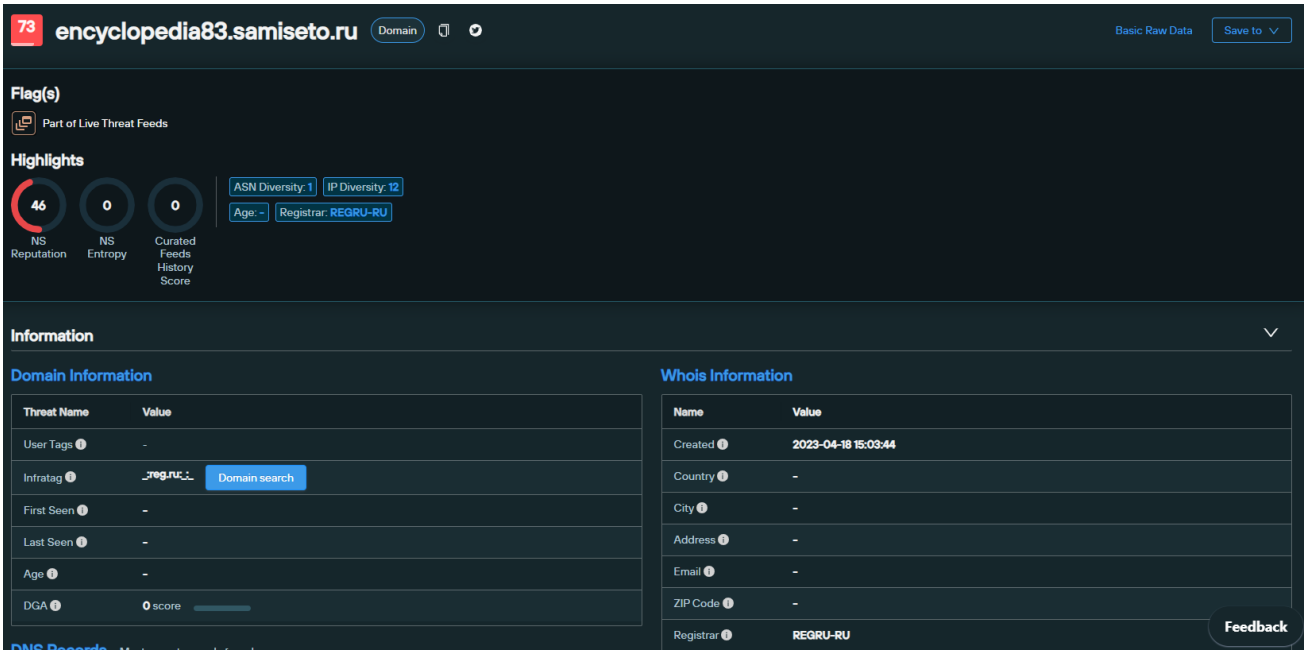


Twitter post announcing malware hosted on samiseto[.]ru

Checking Virus Total confirms that the domains have been flagged as malicious, largely due to the domains being reported on Twitter as post-breach intelligence:

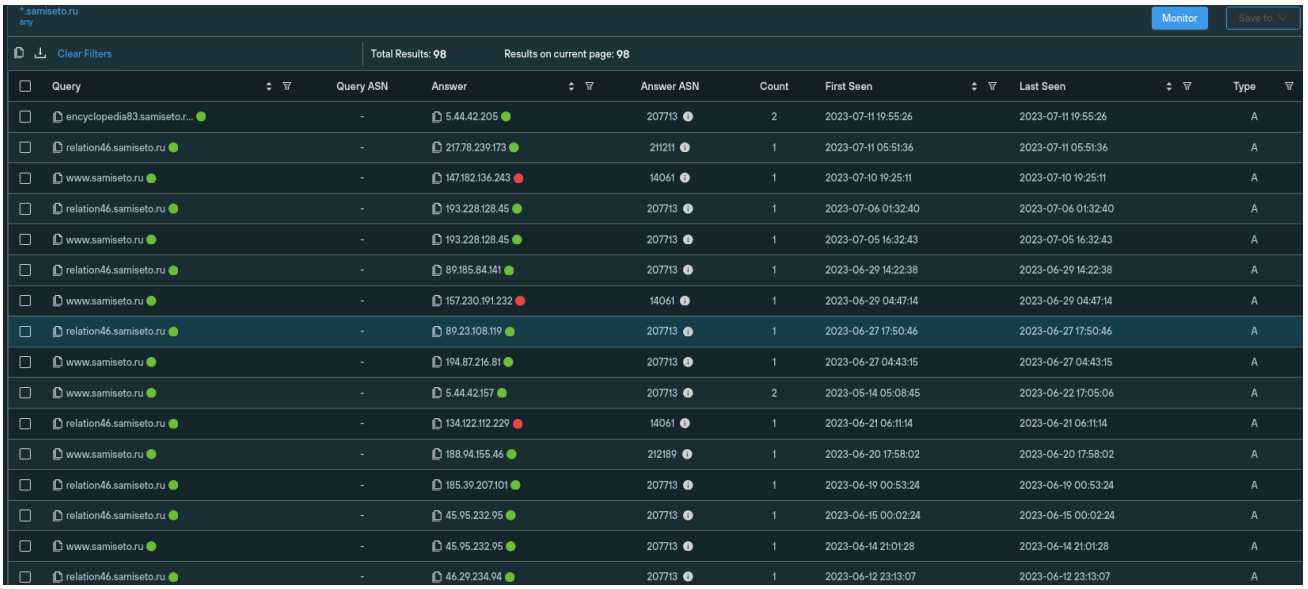
Traversing Gamaredon's infrastructure

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



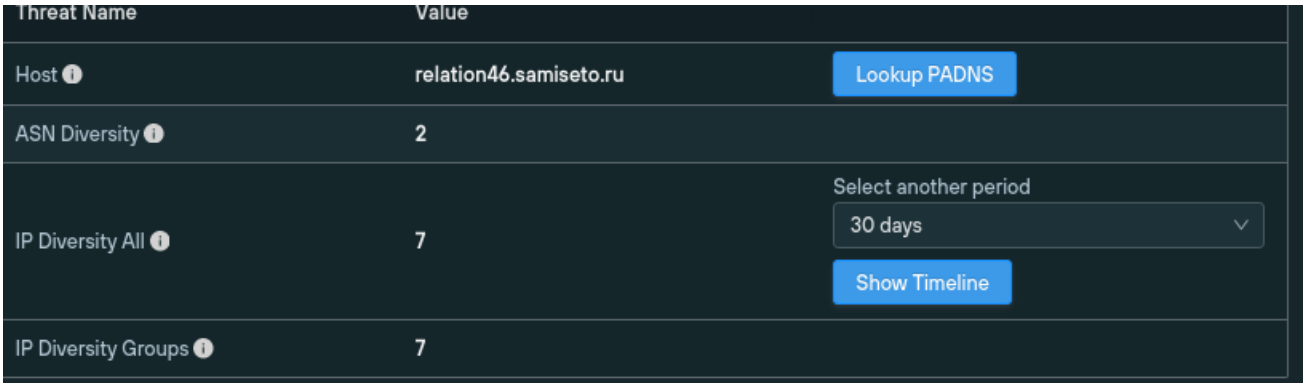
Enriching encyclopedia83.samiseto[.]ru

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



A record lookup for samiseto[.]ru

Further analysis revealed that IP addresses are used for no more than 4 days before being substituted by a fresh IP (along with new subdomains), helping the threat actors to evade detection and rendering most isolated IOCs obsolete upon discovery:



High IP diversity score

To extract actionable IOCs, we then created a list of all the IP addresses that a subdomain of samiseto[.]ru has ever pointed to and applied a reverse lookup to uncover all domains associated with those IPs, 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 wilcard 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 are using a wildcard A record to point to the aforementioned domain:

```
; <<>> 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
```

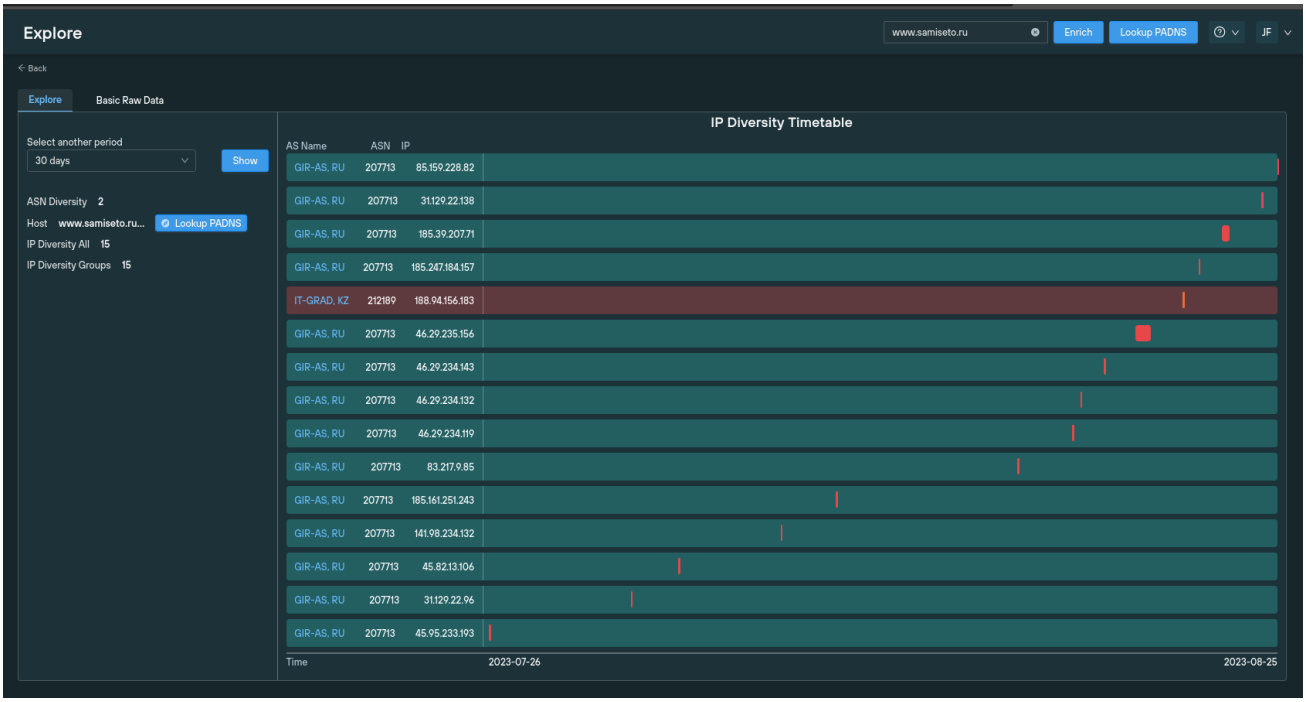
Dig command showing use of wildcard A record

```
; <<>> 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 use of wildcard A record

IP diversity and ASN analysis

Using IP diversity data, we established that samiseto[.]ru has pointed to 15 IP addresses within a 30-day period, all of them bar one being hosted on the 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

Whilst 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:

Historical ASN data for samiseto[.]ru

Using Silent Push to combat Gamaredon's fast flux techniques

Our Threat Analysts used 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 are able to ingest curated threat feeds containing IOCs related to the Gamaredon group's fast flux infrastructure using the tags #russo, #gamaredon and #apt.

The Silent Push Community Edition also contains many of the lookups that we used in our research. Sign up here for free.

Email for further guidance on any of the countermeasures we've talked about in this article.

Explore our Knowledge Base for in-depth articles on how to use Silent Push to defend against attacks.

IOCs

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

Silent Push Labs Team

https://www.silentpush.com/