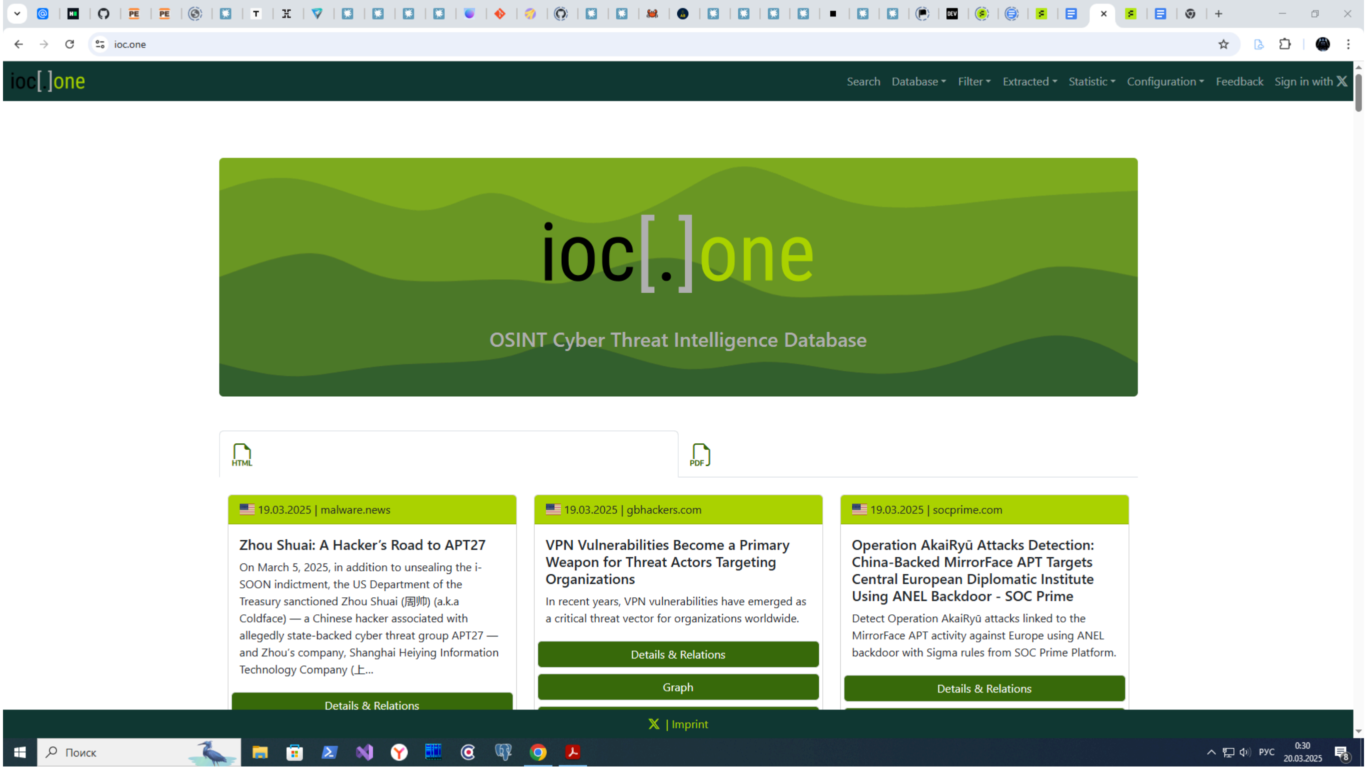
Для поиска дополнительной информации по открытым источникам будем использовать ресурс https://ioc.one/ (OSINT Cyber Threat Intelligence Database):



19.03.2025 | malware.news

Zhou Shuai: A Hacker's Road to APT27

On March 5, 2025, in addition to unsealing the i-SOON indictment, the US Department of the Treasury sanctioned Zhou Shuai (周帅) (a.k.a Coldface) — a Chinese hacker associated with allegedly state-backed cyber threat group APT27 — and Zhou's company, Shanghai Heiying Information Technology Company (上...

Details & Relations

19.03.2025 | gbhackers.com

VPN Vulnerabilities Become a Primary Weapon for Threat Actors Targeting Organizations

In recent years, VPN vulnerabilities have emerged as a critical threat vector for organizations worldwide.

Details & Relations

Graph

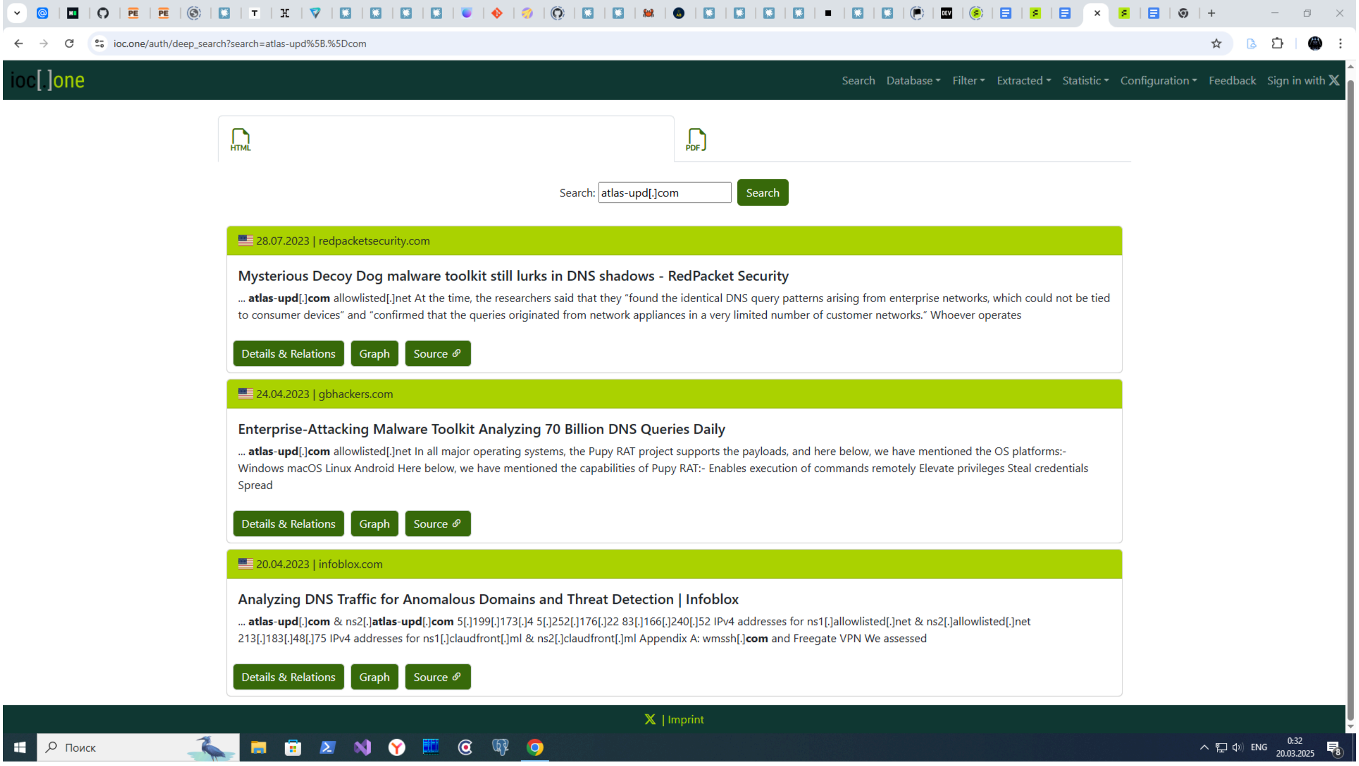
19.03.2025 | socprime.com

Operation AkaiRyū Attacks Detection: China-Backed MirrorFace APT Targets Central European Diplomatic Institute Using ANEL Backdoor - SOC Prime

Detect Operation AkaiRyū attacks linked to the MirrorFace APT activity against Europe using ANEL backdoor with Sigma rules from SOC Prime Platform.

Details & Relations

Поиск по вредоносному домену atlas-upd[.]com дает нам следующий результат:



Search: atlas-upd[.]com Search

28.07.2023 | redpacketsecurity.com

Mysterious Decoy Dog malware toolkit still lurks in DNS shadows - RedPacket Security

... **atlas-upd**[.]**com** allowlisted[.]net At the time, the researchers said that they "found the identical DNS query patterns arising from enterprise networks, which could not be tied to consumer devices" and "confirmed that the queries originated from network appliances in a very limited number of customer networks." Whoever operates

Details & Relations | Graph | Source

24.04.2023 | gbhackers.com

Enterprise-Attacking Malware Toolkit Analyzing 70 Billion DNS Queries Daily

... **atlas-upd**[.]**com** allowlisted[.]net In all major operating systems, the Pupy RAT project supports the payloads, and here below, we have mentioned the OS platforms:- Windows macOS Linux Android Here below, we have mentioned the capabilities of Pupy RAT:- Enables execution of commands remotely Elevate privileges Steal credentials Spread

Details & Relations | Graph | Source

20.04.2023 | infoblox.com

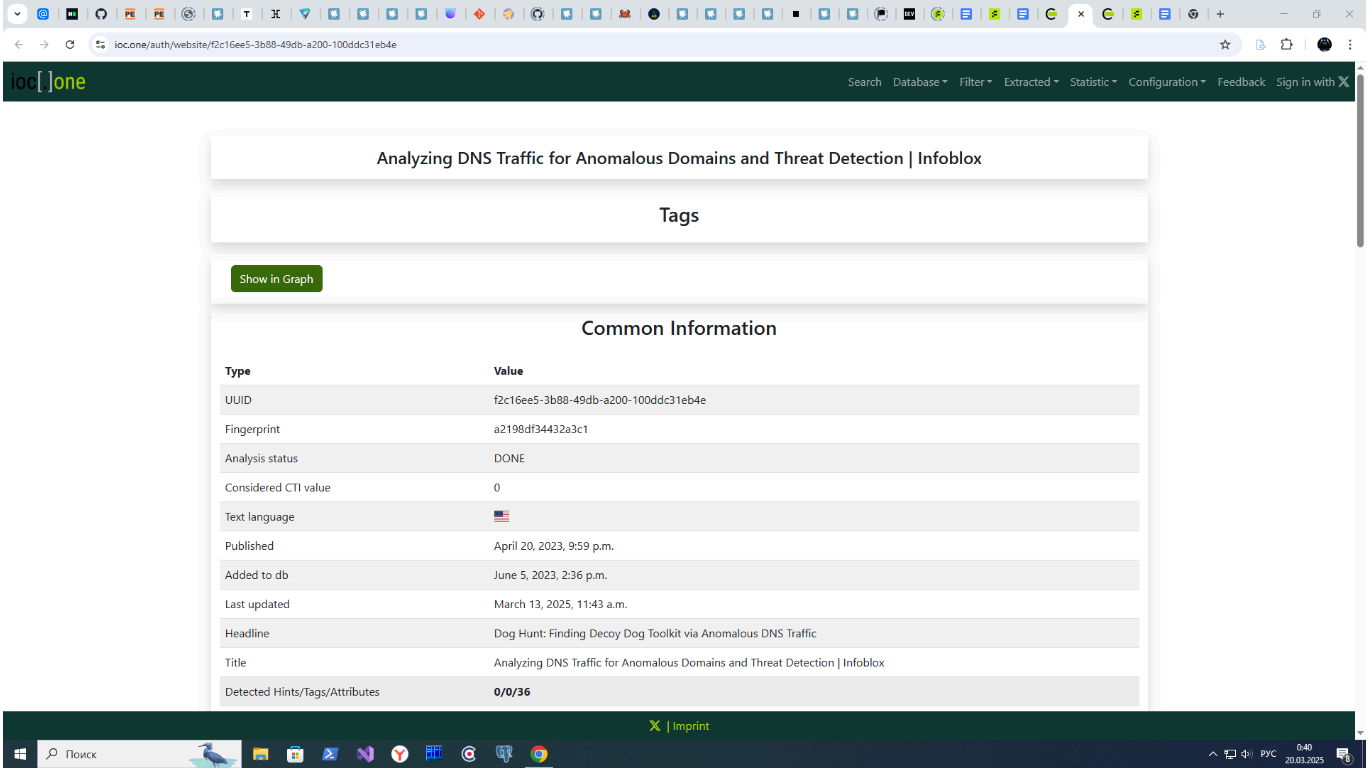
Analyzing DNS Traffic for Anomalous Domains and Threat Detection | Infoblox

... **atlas-upd**[.]**com** & ns2[.]**atlas-upd**[.]**com** 5[.]199[.]173[.]4 5[.]252[.]176[.]22 83[.]166[.]240[.]52 IPv4 addresses for ns1[.]allowlisted[.]net & ns2[.]allowlisted[.]net 213[.]183[.]48[.]75 IPv4 addresses for ns1[.]claudfront[.]ml & ns2[.]claudfront[.]ml Appendix A: wmssh[.]**com** and Freegate VPN We assessed

Details & Relations | Graph | Source

Видно, что есть еще 3 IOC, связанных с активностью вредоносного домена atlas-upd[.]com:

1) IOC от 20.04.2023



Analyzing DNS Traffic for Anomalous Domains and Threat Detection | Infoblox

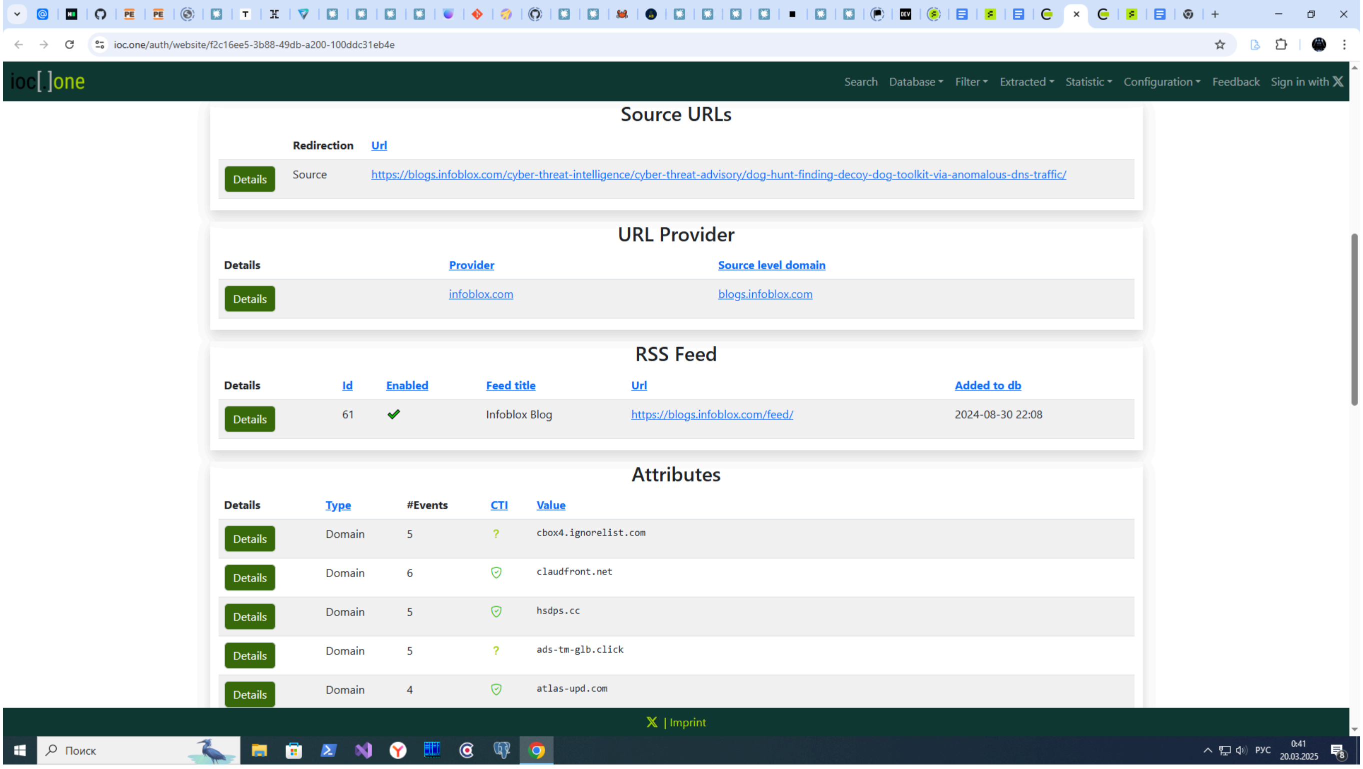
Tags

Show in Graph

Common Information

Type	Value
UUID	f2c16ee5-3b88-49db-a200-100ddc31eb4e
Fingerprint	a2198df34432a3c1
Analysis status	DONE
Considered CTI value	0
Text language	🇺🇸
Published	April 20, 2023, 9:59 p.m.
Added to db	June 5, 2023, 2:36 p.m.
Last updated	March 13, 2025, 11:43 a.m.
Headline	Dog Hunt: Finding Decoy Dog Toolkit via Anomalous DNS Traffic
Title	Analyzing DNS Traffic for Anomalous Domains and Threat Detection | Infoblox
Detected Hints/Tags/Attributes	**0/0/36**

X | Imprint



Source URLs

	Redirection	Url
Details	Source	https://blogs.infoblox.com/cyber-threat-intelligence/cyber-threat-advisory/dog-hunt-finding-decoy-dog-toolkit-via-anomalous-dns-traffic/

URL Provider

Details	Provider	Source level domain
Details	infoblox.com	blogs.infoblox.com

RSS Feed

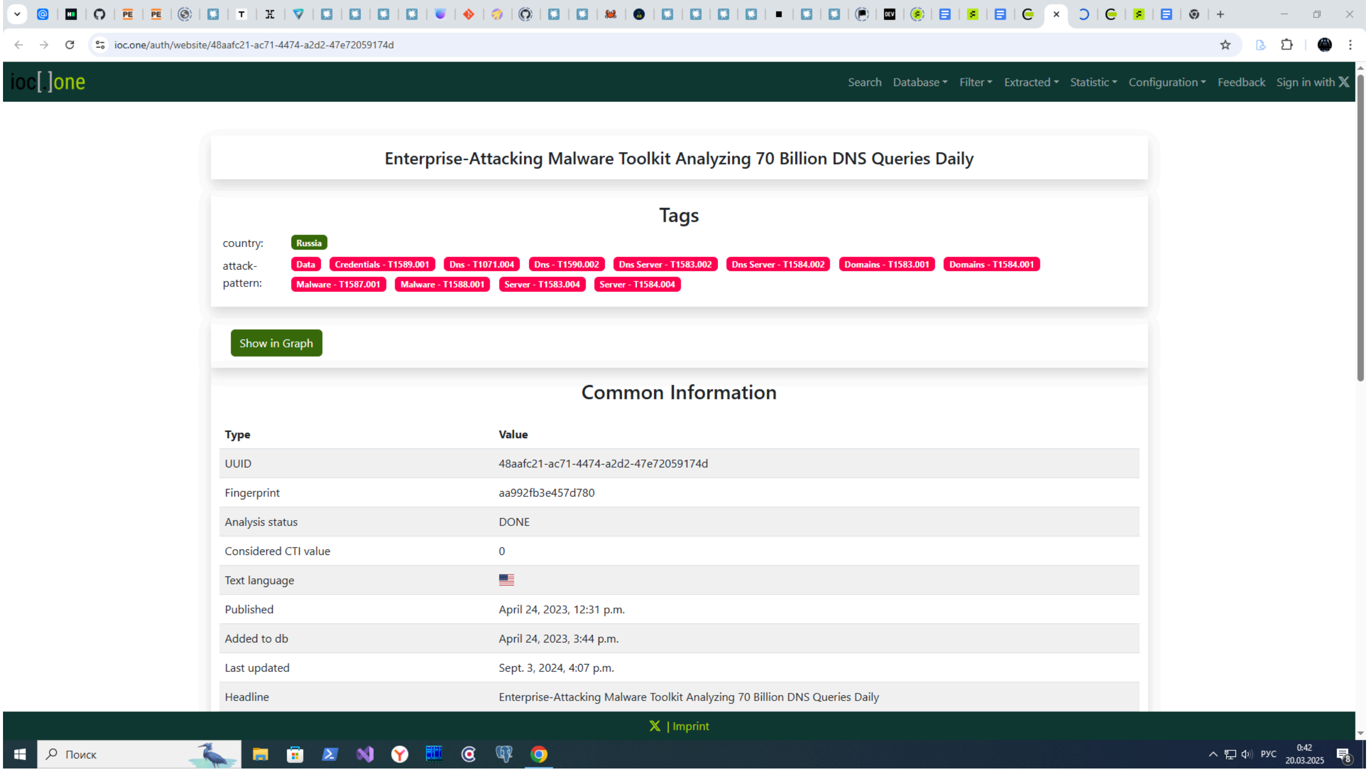
Details	Id	Enabled	Feed title	Url	Added to db
Details	61	✓	Infoblox Blog	https://blogs.infoblox.com/feed/	2024-08-30 22:08

Attributes

Details	Type	#Events	CTI	Value
Details	Domain	5	?	cbox4.ignorelist.com
Details	Domain	6	🛡	claudfront.net
Details	Domain	5	🛡	hsdps.cc
Details	Domain	5	?	ads-tm-glb.click
Details	Domain	4	🛡	atlas-upd.com

X | Imprint

2) IOC от 24.04.2023



Enterprise-Attacking Malware Toolkit Analyzing 70 Billion DNS Queries Daily

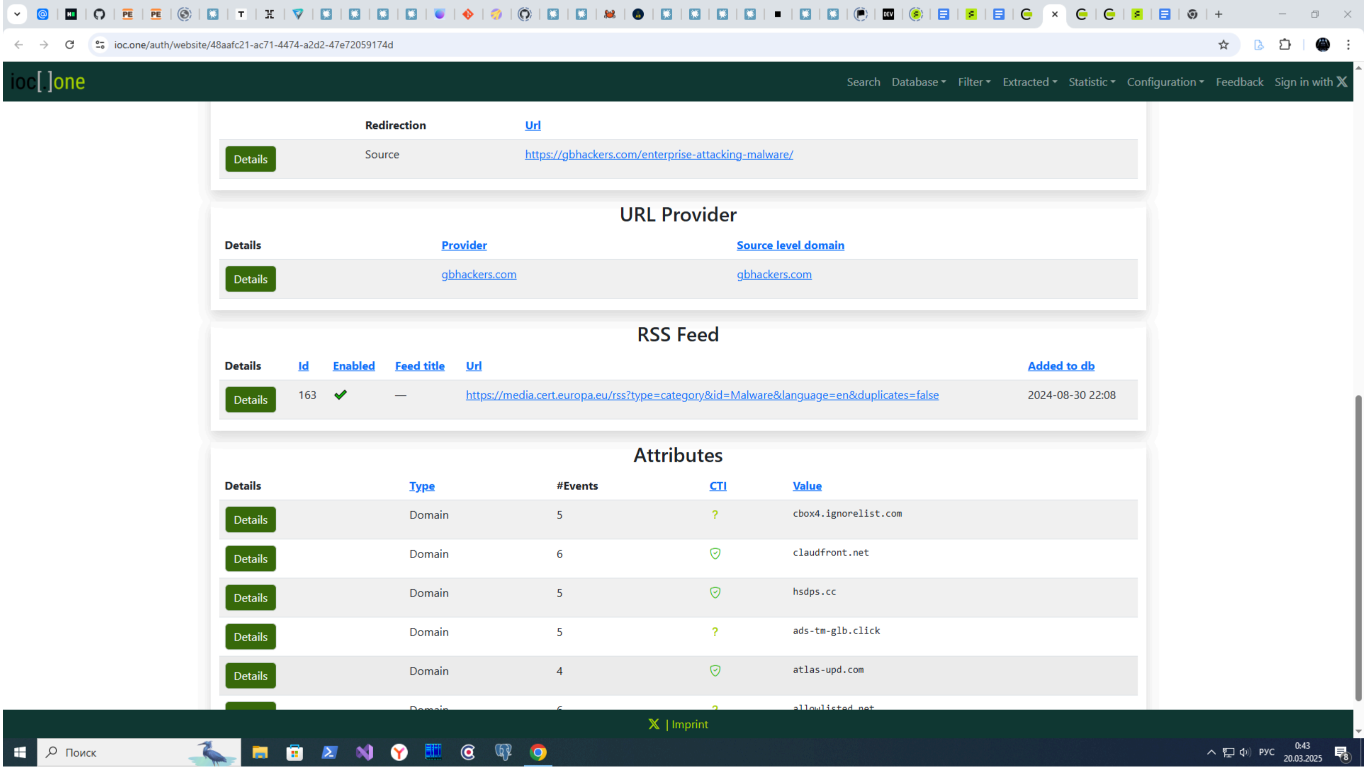
Tags

country: Russia

attack-pattern: Data | Credentials - T1589.001 | Dns - T1071.004 | Dns - T1590.002 | Dns Server - T1583.002 | Dns Server - T1584.002 | Domains - T1583.001 | Domains - T1584.001 | Malware - T1587.001 | Malware - T1588.001 | Server - T1583.004 | Server - T1584.004

Common Information

Type	Value
UUID	48aafc21-ac71-4474-a2d2-47e72059174d
Fingerprint	aa992fb3e457d780
Analysis status	DONE
Considered CTI value	0
Text language	🇺🇸
Published	April 24, 2023, 12:31 p.m.
Added to db	April 24, 2023, 3:44 p.m.
Last updated	Sept. 3, 2024, 4:07 p.m.
Headline	Enterprise-Attacking Malware Toolkit Analyzing 70 Billion DNS Queries Daily



	Redirection	Url
Details	Source	https://gbhackers.com/enterprise-attacking-malware/

URL Provider

Details	Provider	Source level domain
Details	gbhackers.com	gbhackers.com

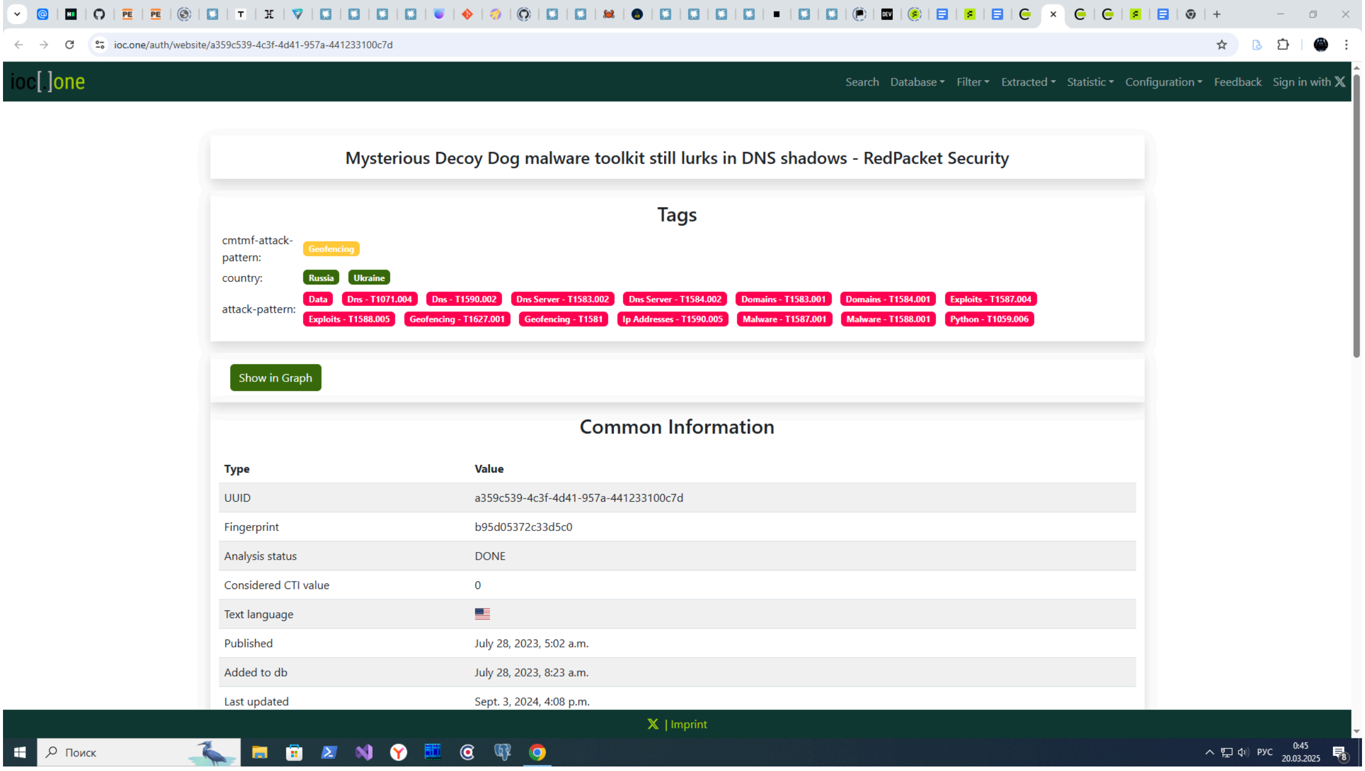
RSS Feed

Details	Id	Enabled	Feed title	Url	Added to db
Details	163	✓	—	https://media.cert.europa.eu/rss?type=category&id=Malware&language=en&duplicates=false	2024-08-30 22:08

Attributes

Details	Type	#Events	CTI	Value
Details	Domain	5	?	cbox4.ignorelist.com
Details	Domain	6	✓	claudfront.net
Details	Domain	5	✓	hsdps.cc
Details	Domain	5	?	ads-tm-glb.click
Details	Domain	4	✓	atlas-upd.com
	Domain	6	?	allowlisted.net

3) IOC от 28.07.2023



Mysterious Decoy Dog malware toolkit still lurks in DNS shadows - RedPacket Security

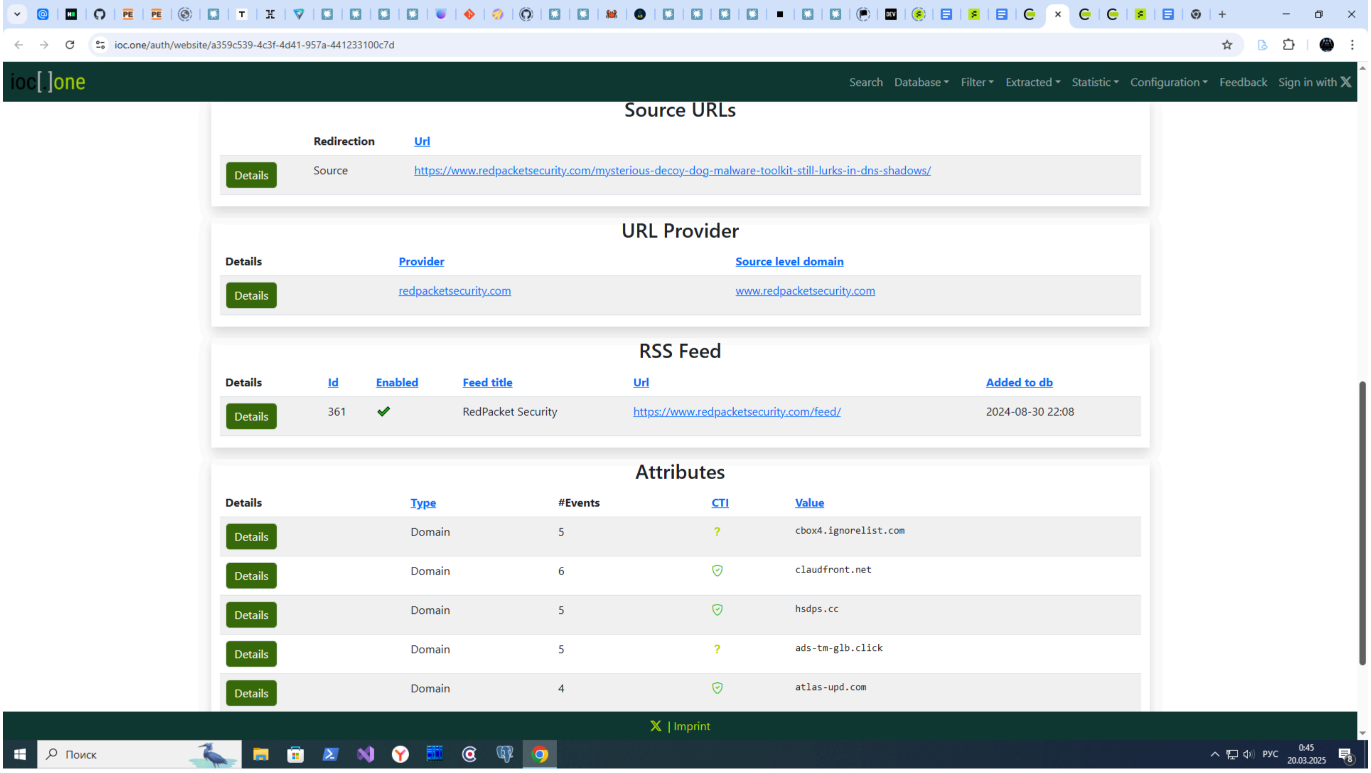
Tags

cmtmf-attack-pattern:	Geofencing
country:	Russia, Ukraine
attack-pattern:	Data, Dns - T1071.004, Dns - T1590.002, Dns Server - T1583.002, Dns Server - T1584.002, Domains - T1583.001, Domains - T1584.001, Exploits - T1587.004, Exploits - T1588.005, Geofencing - T1627.001, Geofencing - T1581, Ip Addresses - T1590.005, Malware - T1587.001, Malware - T1588.001, Python - T1059.006

Show in Graph

Common Information

Type	Value
UUID	a359c539-4c3f-4d41-957a-441233100c7d
Fingerprint	b95d05372c33d5c0
Analysis status	DONE
Considered CTI value	0
Text language	🇺🇸
Published	July 28, 2023, 5:02 a.m.
Added to db	July 28, 2023, 8:23 a.m.
Last updated	Sept. 3, 2024, 4:08 p.m.



Source URLs

	Redirection	Url
Details	Source	https://www.redpacketsecurity.com/mysterious-decoy-dog-malware-toolkit-still-lurks-in-dns-shadows/

URL Provider

Details	Provider	Source level domain
Details	redpacketsecurity.com	www.redpacketsecurity.com

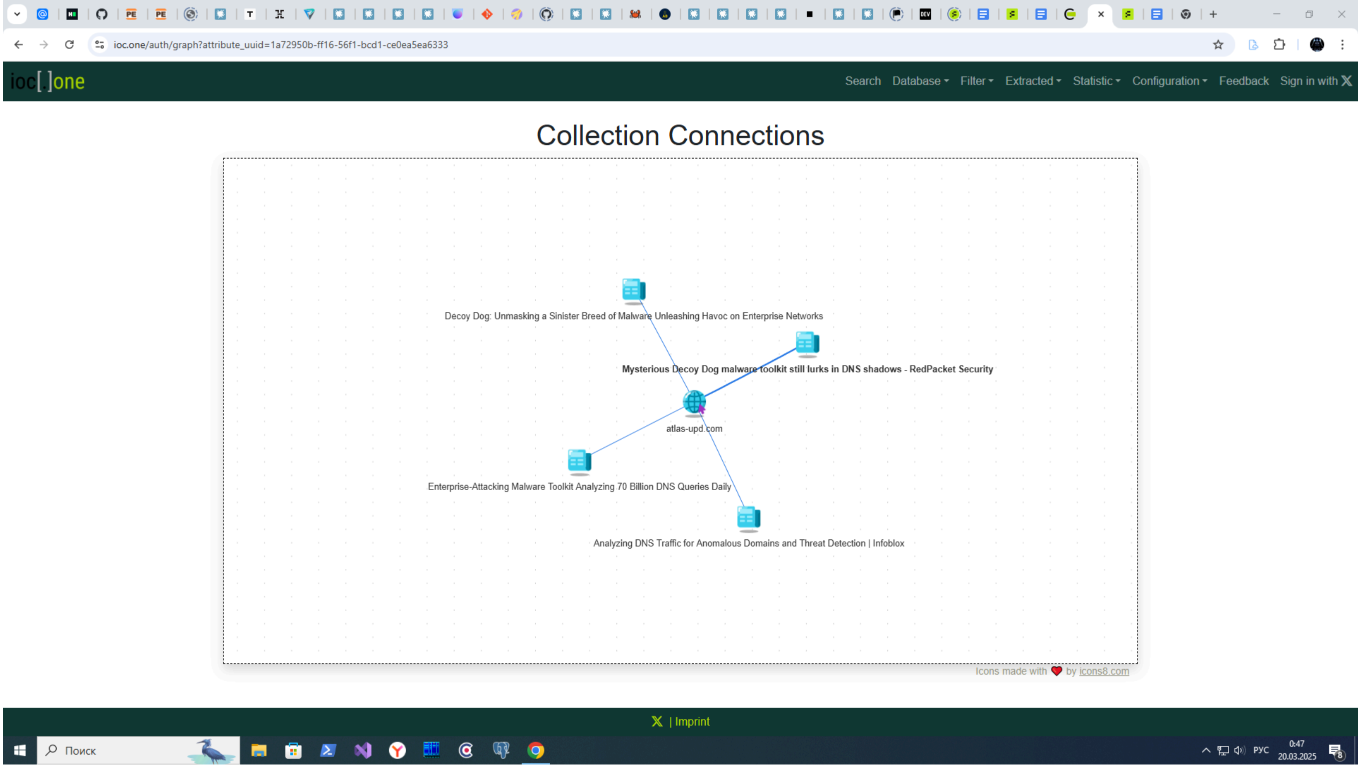
RSS Feed

Details	Id	Enabled	Feed title	Url	Added to db
Details	361	✓	RedPacket Security	https://www.redpacketsecurity.com/feed/	2024-08-30 22:08

Attributes

Details	Type	#Events	CTI	Value
Details	Domain	5	?	cbox4.ignorelist.com
Details	Domain	6	🛡	claudfront.net
Details	Domain	5	🛡	hsdps.cc
Details	Domain	5	?	ads-tm-glb.click
Details	Domain	4	🛡	atlas-upd.com

Можно привести еще граф событий, который можно получить с этого же ресурса, связанных с этим вредоносным доменом atlas-upd[.]com (что интересно: событий 4, а зарегистрированных IOC - 3):

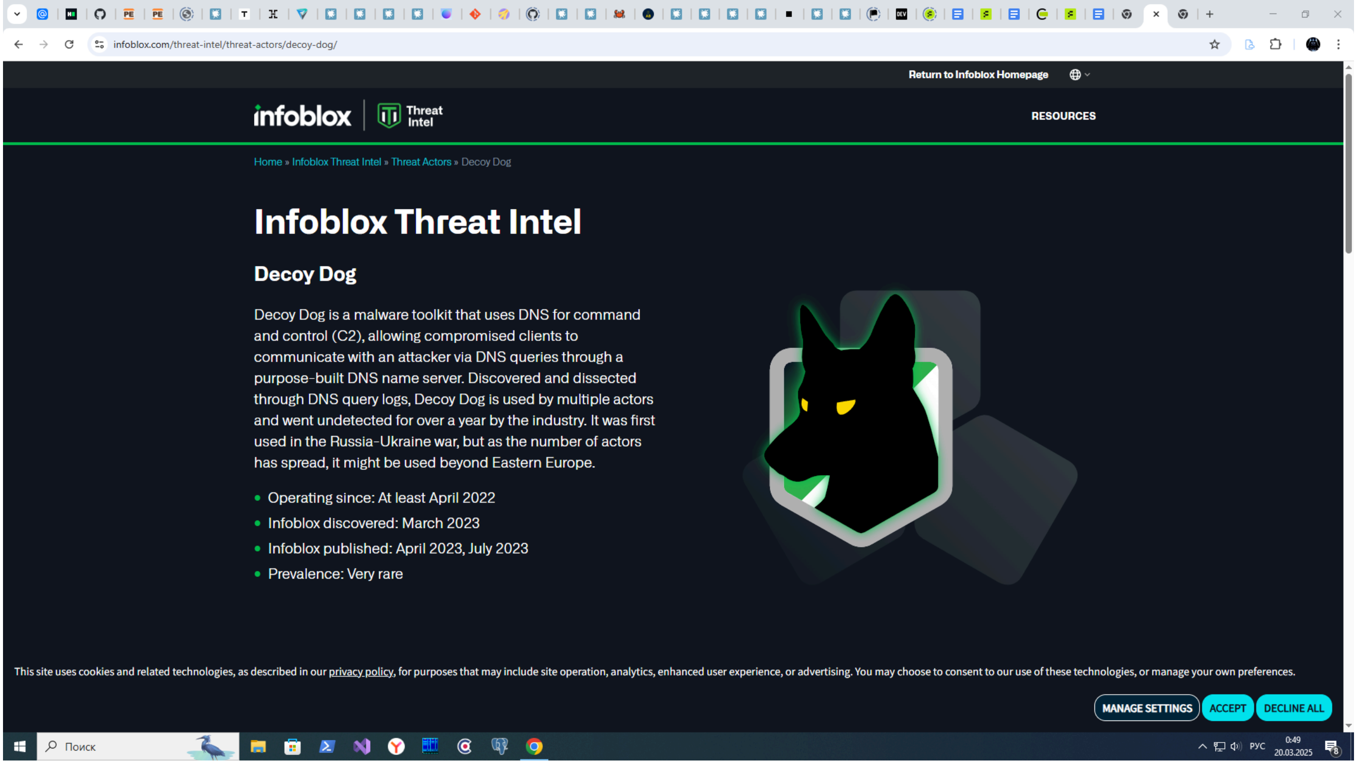


ioc.one/auth/graph?attribute_uuid=1a72950b-ff16-56f1-bcd1-ce0ea5ea6333
ioc[.]one
Search
Database
Filter
Extracted
Statistic
Configuration
Feedback
Sign in with X

Collection Connections

Decoy Dog: Unmasking a Sinister Breed of Malware Unleashing Havoc on Enterprise Networks
Mysterious Decoy Dog malware toolkit still lurks in DNS shadows - RedPacket Security
atlas-upd.com
Enterprise-Attacking Malware Toolkit Analyzing 70 Billion DNS Queries Daily
Analyzing DNS Traffic for Anomalous Domains and Threat Detection | Infoblox
Icons made with ❤ by icons8.com
X | Imprint
Поиск
РУС
0:47
20.03.2025

В 2 из 3 IOC упоминается Decoy Dog malware toolkit. Вот информация о нем, например с ресурса https://www.infoblox.com:



infoblox.com/threat-intel/threat-actors/decoy-dog/
Return to Infoblox Homepage
infoblox
Threat Intel
RESOURCES
Home » Infoblox Threat Intel » Threat Actors » Decoy Dog

Infoblox Threat Intel

Decoy Dog

Decoy Dog is a malware toolkit that uses DNS for command and control (C2), allowing compromised clients to communicate with an attacker via DNS queries through a purpose-built DNS name server. Discovered and dissected through DNS query logs, Decoy Dog is used by multiple actors and went undetected for over a year by the industry. It was first used in the Russia-Ukraine war, but as the number of actors has spread, it might be used beyond Eastern Europe.

- Operating since: At least April 2022
- Infoblox discovered: March 2023
- Infoblox published: April 2023, July 2023
- Prevalence: Very rare

This site uses cookies and related technologies, as described in our privacy policy, for purposes that may include site operation, analytics, enhanced user experience, or advertising. You may choose to consent to our use of these technologies, or manage your own preferences.

По итогу можно сделать следующие выводы:

1) Заражение системы действительно произошло

2) Потенциально, система заражена Decoy Dog ВПО.