Predicting IOCs with Historical Analysis

From Behavior Patterns to Proactive Threat Hunting

Josh Pyorre, DeepSec, November 21, 2025

Predicting IOCs with Historical Analysis

TALOS

zscaler

CISCO Umbrella

OpenDNS

MANDIANT

NASA

This is my 7th time presenting at DeepSec, starting in 2015!!

Predicting IOCs with Historical Analysis

Outline

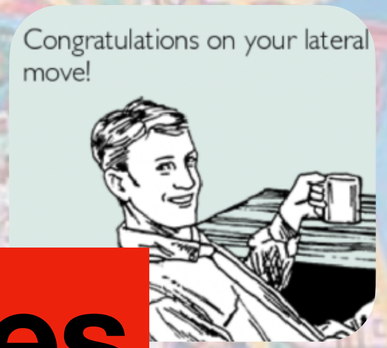
- The Problems of Chasing IOCs
- Threat Actor Behaviors
- Building a Framework for Prediction
- Behavioral Patterns Transcend Individual Campaigns - Findings
- Operationalize with the PREDICT framework

The Fundamental Problem

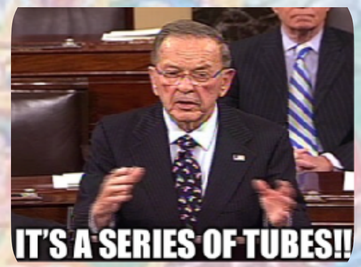
Putting out Fires

- Reactive approach

Incident Response Circle of Frustration



This continues FOREVER



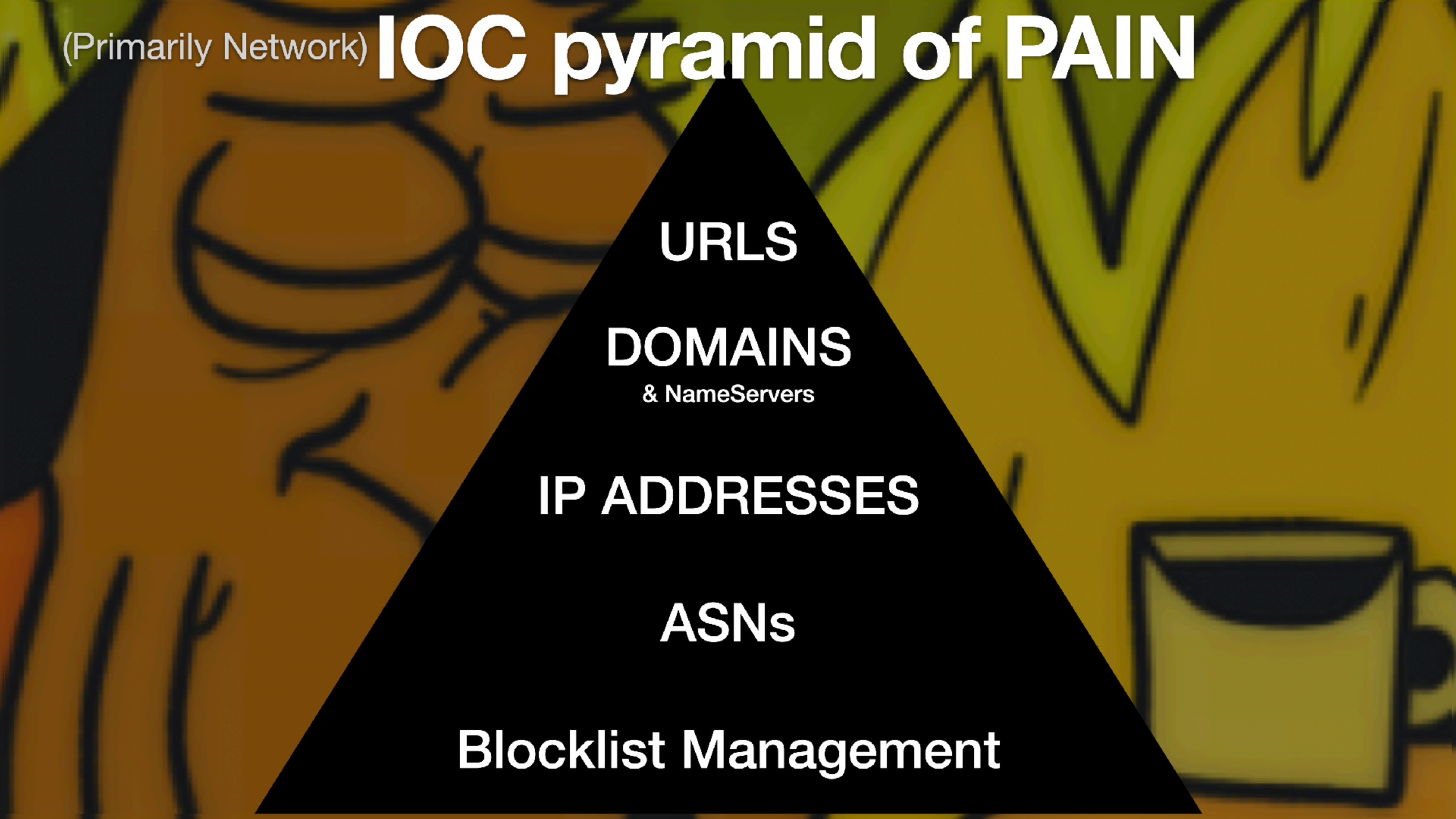
SIEM Dashboard

SYSTEM STATUS	SENSORS	UPTIME
ONLINE	47/47	99.56%

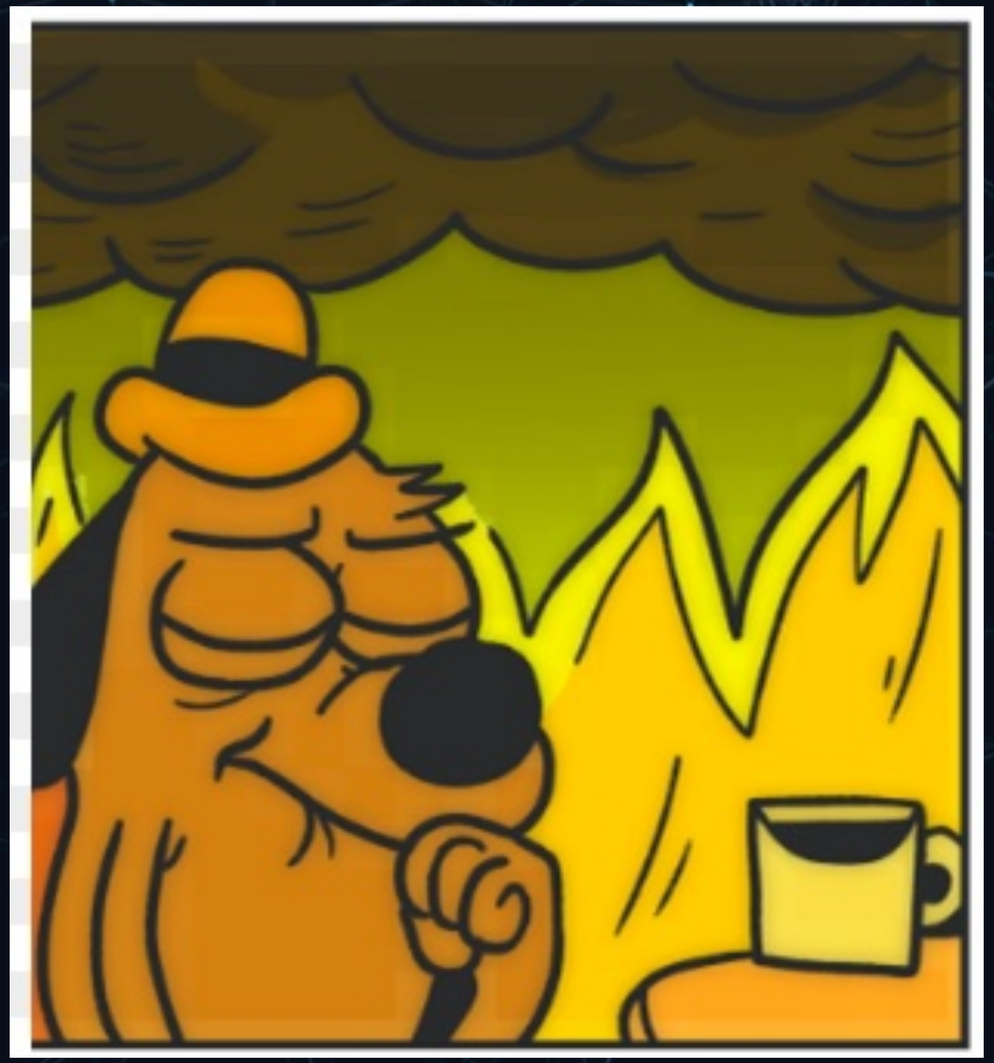
10:45:33 PM	CRITICAL	Malware Download	Malicious file download prevented (180.105.122.214)	YARA
10:45:31 PM	CRITICAL	C2 Beaconing	Command and control communication identified (86.50.93.147)	Sigma
10:45:28 PM	MEDIUM	Brute Force	Dictionary attack on user accounts (155.69.109.219)	Wazuh
10:45:25 PM	HIGH	DDoS Attack	SYN flood attack in progress (18.28.104.80)	Windows Defender
10:45:22 PM	HIGH	Data Exfiltration	Large data transfer to external destination (23.137.40.218)	ClamAV
10:45:19 PM	HIGH	SQL Injection	Database query manipulation detected (46.77.10.191)	Fail2Ban
10:45:17 PM	HIGH	SQL Injection	Database query manipulation detected (165.118.184.40)	OSSEC
10:45:16 PM	MEDIUM	Port Scan	Stealth scan detected on critical services (16.2.2.146)	YARA
10:45:16 PM	HIGH	C2 Beaconing	Suspicious outbound connection to known C2 server (181.20.64.58)	Zeek
10:45:15 PM	MEDIUM	XSS Attack	XSS payload in form submission (10.54.195.34)	Wazuh
10:45:15 PM	MEDIUM	Port Scan	Multiple port probe attempts (194.111.123.208)	Sigma
10:45:14 PM	HIGH	C2 Beaconing	Suspicious outbound connection to known C2 server (17.14.180.211)	OSSEC

And you spend all your time chasing alerts

2	6	4	0	12
CRITICAL	HIGH	MEDIUM	LOW	TOTAL


(Primarily Network) IOC pyramid of PAIN
URLS
DOMAINS
& NameServers
IP ADDRESSES
ASNs
Blocklist Management

IOCs change



Domains and URLs:

- Change fast
- So fast, it can be difficult to discover

NameServers:

- Great for pivoting
- Legit NS used frequently

IP Addresses:

- Change less often
- Can host legitimate domains

Blocklists

- stop *known* attacks
- Get Stale


Behavior is Hard to Change
Malware authors are human (sometimes)

From Ramnit to Bumblebee (via NeverQuest): similarities and code overlap shed light on relationships between malware developers.

MASTER SEMINAR

CHAIR FOR SYSTEMS SECURITY

RUHR-UNIVERSITY BOCHUM

Attributing Malware Binaries to Threat Actors based on Authorship Style

3.1. Source Code Authorship Attribution

Source Code Authorship Attribution (SCAA) is the process of assigning program code to developers. Over time, each programmer develops a personal programming style which can be visible at different levels. [CIHL+15] divides the stylistic characteristics of program code into layout, lexical and syntactic features.

Coding Styles can match behavior

DCRat

A distinctive feature of the campaign is the appearance of certain words in the second-level domains of the malicious infrastructure, such as “nyashka”, “nyashkoon”, “nyashtyan”, etc. Users interested in Japanese pop culture will surely recognize these slang terms. Among anime and manga fans, “nyasha” has come to mean “cute” or “hon”, and it’s this word that’s most often seen in the second-level domains.

https://securelist.com/new-wave-of-attacks-with-dcrat-backdoor-distributed-by-maas/115850/

```
http://003659cm.nyash.es/avascriptJsRequestHttpprocessormultitempdownloadsTemporary.php
http://020854cm.nyashvibe.ru/toJavascriptmultiLocalprivatetempcentral.php
http://027894cm.nyash.es/mageTojavascriptlocalpublic.php
http://055871cm.nyash.es/mpipePhpHttpUpdateAuthGameserver.php
http://075229cm.nyash.es/hpJsServerDefaultbasetrackdownloads.php
http://075641cm.nyashvibe.ru/LineJspacketprocessAuthGamedefaulttraffic.php
http://120907cm.nyash.es/ternalimagepythonLongpollapiDefaultgeneratoruploads.php
http://132961cm.nyash.es/lowerdatalife.php
http://144403cm.nyash.es/xternalJavascriptmultiWp.php
http://162838cm.nyashvibe.ru/imagelowUpdateprocessprocessorLongpollProtecttestCdn.php
http://167472cm.nyashru.ru/nyashsupport.php
http://201906cm.nyash.es/ipejavascriptHttpProcessprocessorflowerasyncWordpresscentraltemporary.php
http://223451cm.nyashvibe.ru/WindowslocalTemporary.php
http://239024cm.nyash.es/slow.php
http://247471cm.nyash.es/hpgeoProtect.php
http://304542cm.nyashware.ru/videoMultilinuxpublic.php
http://346720cm.nyashvibe.ru/PhpRequesttrafficDleTemp.php
http://357129cm.nyash.es/ythonPollLowbasePrivate.php
http://387780cm.nyashvibe.ru/providerTrackWppublic.php
http://391316cm.nyashvibe.ru/phpSqlbasePublicDownloads.php
http://402317cm.nyashvibe.ru/EternalLongpollAsynctest.php
http://404830cm.nyashvibe.ru/External_SecureProcessProcessorDle.php
http://407440cm.nyash.es/ollBigloadprotect.php
http://413426cm.nyash.es/rotectFlowerdownloads.php
http://431188cm.nyashvibe.ru/LowDatalife.php
http://453971cm.nyash.es/ternalimageVideoPipeGameflowerLocalprivateCentral.php
http://463957cm.nyash.es/ternalJavascript_RequestpollhttpLongpollLinux.php
```

```
http://476301cm.nyashk.ru/ineToJavascript_HttpBigloaddbLinuxDownloads.php
http://512920cm.nyash.es/xternalTogeoUpdateDefaultSqlwindowstestTrackUploads.php
http://516063cm.nyash.es/mageGeobaselinuxGeneratortestuniversalWp.php
http://530182cm.nyashvibe.ru/Externalimagepipe_geoCpuServerbasewpcentral.php
http://539068cm.nyashvibe.ru/linePipePythonprocessorAsynctestuploads.php
http://542733cm.nyash.es/gameserverdefaultbaseWpPublictempCdncentralUploads.php
http://543672cm.nyashvibe.ru/UpdatebigloadmultiWordpressDownloads.php
http://590178cm.nyashvibe.ru/SecurewindowsTestwpcdn.php
http://603646cm.nyashvibe.ru/LinehttpcpuprocessorgameServerWindowswordpress.php
http://706858cm.nyashvibe.ru/PacketUpdatewindowsdatalife.php
http://715239cm.nyashvibe.ru/UpdateGenerator.php
http://716244cm.nyashvibe.ru/securecpuGamemultiDownloadsTemporary.php
http://724499cm.renyash.to/ProvidereternalPythonRequestGeoprocessorFlowerdlelocalcdn.php
http://726346cm.nyash.es/ultiwordpress.php
http://730294cm.nyashvibe.ru/eternalgeogamesqlPubliccdnDownloads.php
http://737347cm.nyash.es/oPhpLinuxtemp.php
http://776162cm.shnyash.ru/providerline_Securedefaultsqllocal.php
http://841333cm.nyash.es/imagevideo_PacketProtectBaseLinuxuniversal.php
http://843801cm.nyashvibe.ru/external_.php
http://881035cm.nyashvibe.ru/JsprocessorBaseLocalcentraldownloadstemporary.php
http://892408cm.nyash.es/ServerDatalifeTemporary.php
http://901730cm.nyash.es/_processprocessorBigload.php
http://982361cm.nyash.es/imagelineLongpollDefaultdbuploads.php
http://nyashtecmshop.online/42bc5333.php
http://nyashtecmshop.ru/c15672f5.php
```

URL Patterns sometimes match behavior

AS 14061

Current information

Period	Creation date	Registry	Network Owner Description
11/17/2024 - 10/17/2025	09/25/2012	ARIN	DIGITALOCEAN-ASN, US 86400
11/16/2024 - 11/17/2024	09/25/2012	ARIN	DIGITALOCEAN-ASN, US 86400
11/11/2024 - 11/16/2024	09/25/2012	ARIN	DIGITALOCEAN-ASN, US 86400
10/25/2024 - 11/11/2024	09/25/2012	ARIN	DIGITALOCEAN-ASN, US 86400
08/03/2024 - 10/25/2024	09/25/2012	ARIN	DIGITALOCEAN-ASN, US 86400
07/24/2023 - 08/03/2024	09/25/2012	ARIN	DIGITALOCEAN-ASN, US 86400
01/18/2020 - 07/24/2023	09/25/2012	ARIN	DIGITALOCEAN-ASN, US 86400
05/24/2019 - 01/19/2020	09/25/2012	ARIN	DIGITALOCEAN-ASN - DigitalOcean, LLC, US 86400
03/04/2018 - 05/20/2019	09/25/2012	ARIN	DIGITALOCEAN-ASN - DigitalOcean, LLC, US 86400
02/28/2018 - 03/02/2018	09/25/2012	ARIN	DIGITALOCEAN-ASN - DigitalOcean, LLC, US 86400

Showing 10

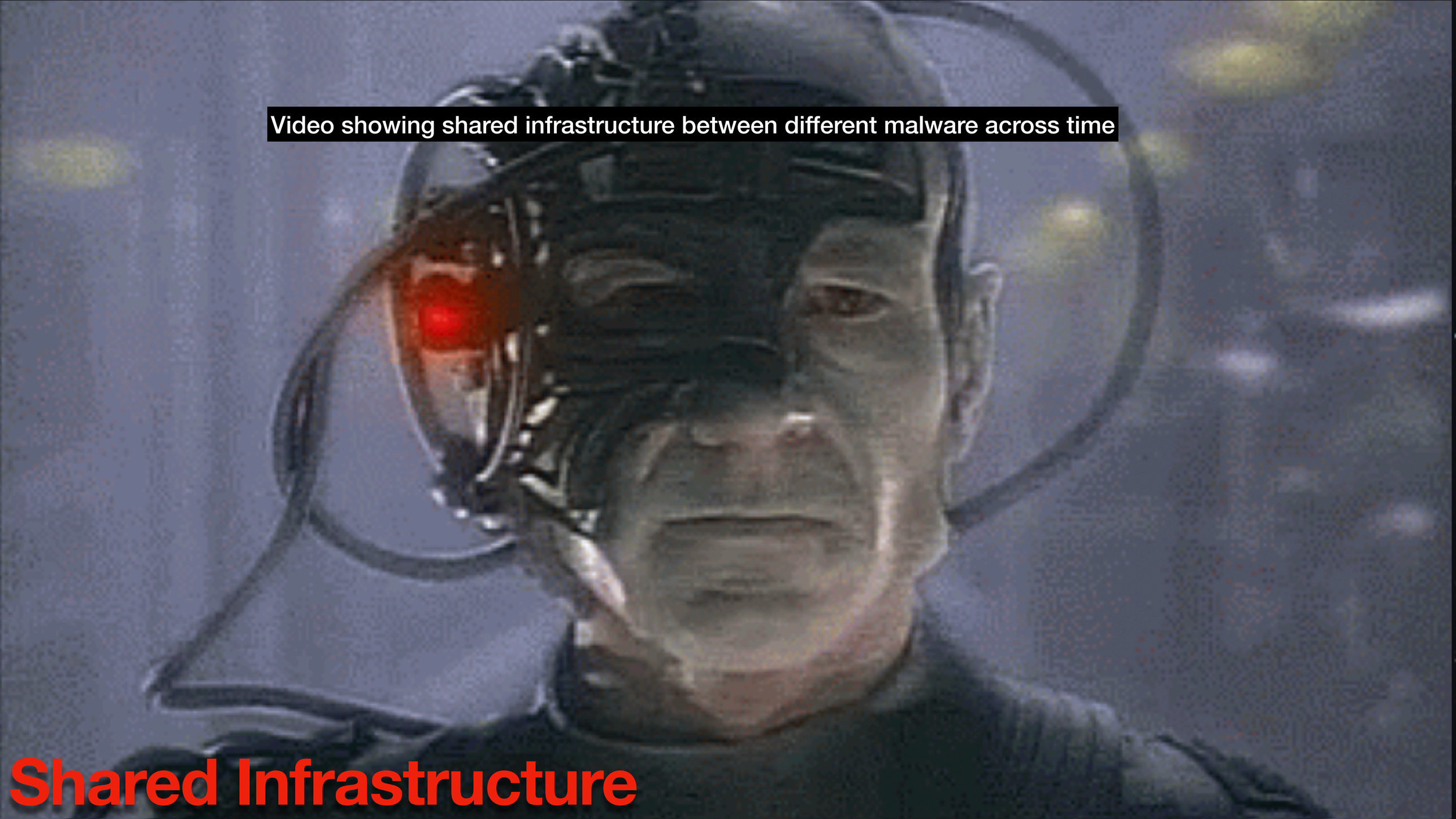
Bulletproof Hosting - threat actors reuse suspicious hosting providers

https://dashboard.umbrella.com/o/1755319/#/investigate/as-view/14061

14061 INVESTIGATE BACK TO TOP

Prefix	Country/Region	Suspicious activity in the past week
5.101.96.0/21	Netherlands	
5.101.104.0/22	Netherlands	
5.101.108.0/24	United States of America	
5.101.109.0/24	Germany	fgksgpsdgolgjogjopedbksdk-sdkgsdkgmsdkgsdkmg-dgksmdgksdmkdgfnsd.fra1.digitaloceanspaces.com digital116.fra1.digitaloceanspaces.com digital69.fra1.digitaloceanspaces.com
5.101.110.0/24	Netherlands	
5.101.111.0/24	United States of America	
24.144.64.0/22	United States of America	drive-shares-dm-noreply.com classictileimports.digitaltilecatalog.com
24.144.68.0/22	United States of America	
24.144.76.0/22	Netherlands	authenticaonline.com hlekkr.com greanfootball.com hamidsolutions.com d1115.secretvps1.top pitangobikes.com radioclaretamerica.org swindonfestivalofliterature.com skillyschool.com mersinlemoncity.com mpmcreativos.com pv40.biz 1800ortho.com asiacitylife.com billybeezuk.com karthiksureshiyer.com peperoutine.com pv39.biz sportstalentasia.com bathroomstore.online sekolahmaumere.org iambookshop.com aventurineresources.com naturyum.com upjvoid.bluedotsafety.com watermarkedgroup.com 293onkomba.com belowcomp.skrrrk.com derryaccommodation.com aurovine.com dicedmball.casedare.com wpautomate.net bas grade.casedare.com cellflu.arenastack.com vowskumquat.apptinken.com endorsementbolt.apptinken.com betsequences.com club21idsofficial.com storageauctionclub.com

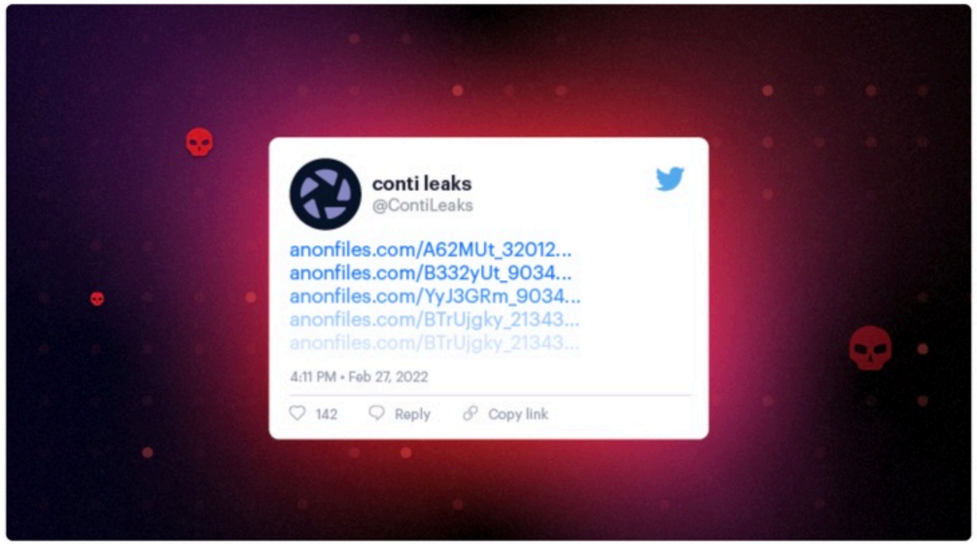
Shared IPs - its easy to remain in the same network


Video showing shared infrastructure between different malware across time
Shared Infrastructure

ContiLeaks: Ransomware Gang Suffers Data Breach

Conti, a prolific ransomware group, has suffered a leak of both internal chat transcripts and source code being shared by a reported Ukrainian member

Jason Hill | 6 min read | Last updated April 3, 2025



Human/Threat Actor Drama

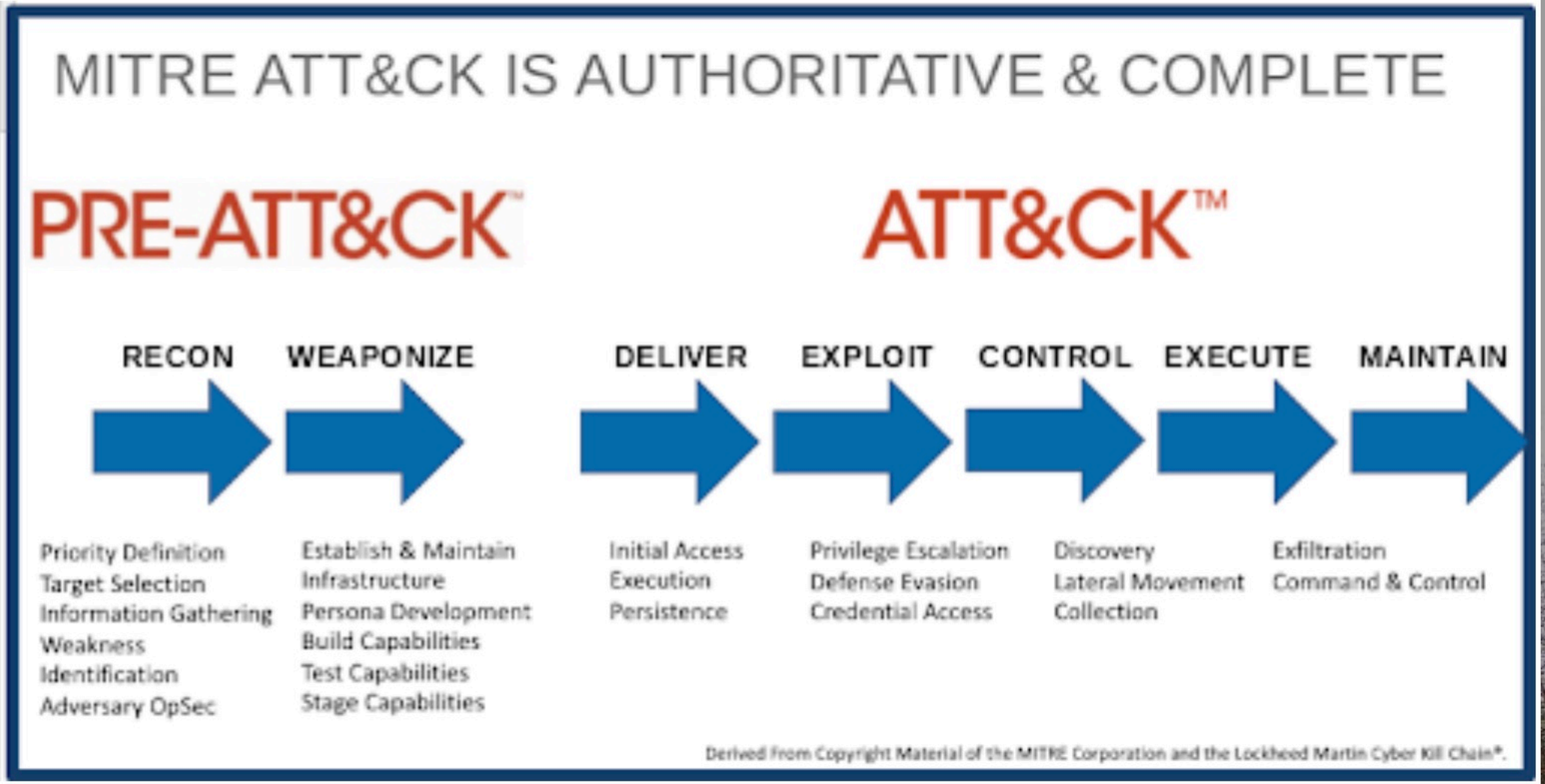
IOC Prediction with Historical Data

Inspired by

MITRE ATT&CK

Using Past Behavior to Identify Current Actions

MITRE ATT&CK IS AUTHORITATIVE & COMPLETE




Video showing timeline of an attack mapped to MITRE ATT&CK
Reconnaissance
Resource Development
Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Command and Control
Exfiltration
Impact
T1595 Active Scanning
T1583 Acquire Infrastructure
T1200 Hardware Additions
T1059
T1098
T1548
T1548
T1557
T1087
T1210
T1557
T1071 Application Layer Protocol
T1020 Automated Exfiltration
T1531 Account Access Removal
T1592 Gather Victim Host Information
T1586 Compromise Accounts
T1566.001 Phishing: Spearphishing Attachment
T1609 Container Administration Command
T1197 BITS Jobs
T1134 Access Token Manipulation
T1134 Access Token Manipulation
T1110 Brute Force
T1010 Application Window Discovery
T1534 Internal Spearphishing
T1560 Archive Collected Data
T1092 Communication Through Removable Media
T1030 Data Transfer Size Limits
T1485 Data Destruction
T1589 Gather Victim Identity Information
T1584 Compromise Infrastructure
T1566.002 Phishing: Spearphishing Link
T1610 Deploy Container
T1547 Boot or Logon Autostart Execution
T1547 Boot or Logon Autostart Execution
T1197 BITS Jobs
T1555 Credentials from Password Stores
T1217 Browser Bookmark Discovery
T1570 Lateral Tool Transfer
T1123 Audio Capture
T1132 Data Encoding
T1048 Exfiltration Over Alternative Protocol
T1486 Data Encrypted for Impact
T1590 Gather Victim Network Information
T1587 Develop Capabilities
T1566.003 Phishing: Spearphishing via Service
T1203 Exploitation for Client Execution
T1037 Boot or Logon Initialization Scripts
T1037 Boot or Logon Initialization Scripts
T1140 Deobfuscate/Decode Files or Information
T1212 Exploitation for Credential Access
T1580 Cloud Infrastructure Discovery
T1021.001 Remote Services: Remote Desktop Protocol
T1119 Automated Collection
T1001 Data Obfuscation
T1041 Exfiltration Over C2 Channel
T1565 Data Manipulation
T1591 Gather Victim Org Information
T1585 Establish Accounts
T1091 Replication Through Removable Media
T1559 Inter-Process Communication
T1136 Create Account
T1543 Create or Modify System Process
T1610 Deploy Container
T1187 Forced Authentication
T1538 Cloud Service Dashboard
T1021.002 Remote Services: SMB/Windows Admin Shares
T1185 Browser Session Hijacking
T1568 Dynamic Resolution
T1011 Exfiltration Over Other Network Medium
T1491.001 Defacement: Internal Defacement
T1598 Phishing for Information
T1588 Obtain Capabilities
T1195 Supply Chain Compromise
T1106 Native API
T1543 Create or Modify System Process
T1484 Domain Policy Modification
T1006 Direct Volume Access
T1606 Forge Web Credentials
T1526 Cloud Service Discovery
T1021.003 Remote Services: Distributed Component Object Model
T1115 Clipboard Data
T1573 Encrypted Channel
T1052 Exfiltration Over Physical Medium
T1491.002 Defacement: External Defacement
T1597 Search Closed Sources
T1608 Stage Capabilities
T1199 Trusted Relationship
T1053 Scheduled Task/Job
T1546 Event Triggered Execution
T1611 Escape to Host
T1484 Domain Policy Modification
T1056 Input Capture
T1613 Container and Resource Discovery
T1021.004 Remote Services: SSH
T1530 Data from Cloud Storage Object
T1008 Fallback Channels
T1567 Exfiltration Over Web Service
T1561 Disk Wipe
T1596 Search Open Technical Databases
T1078 Valid Accounts
T1129 Shared Modules
T1133 External Remote Services
T1546 Event Triggered Execution
T1480 Execution Guardrails
T1556 Modify Authentication Process
T1482 Domain Trust Discovery
T1021.005 Remote Services: VNC
T1602 Data from Configuration Repository
T1105 Ingress Tool Transfer
T1029 Scheduled Transfer
T1499 Endpoint Denial of Service
T1593 Search Open Websites/Domains
T1072 Software Deployment Tools
T1574 Hijack Execution Flow
T1068 Exploitation for Privilege Escalation
T1211 Exploitation for Defense Evasion
T1111 Multi-Factor Authentication Interception
T1083 File and Directory Discovery
T1021.006 Remote Services: Windows Remote Management
T1213 Data from Information Repositories
T1104 Multi-Stage Channels
T1537 Transfer Data to Cloud Account
T1495 Firmware Corruption
T1594 Search Victim-Owned Websites
T1569 System Services
T1525 Implant Internal Image
T1574 Hijack Execution Flow
T1222 File and Directory Permissions Modification
T1621 Multi-Factor Authentication Request Generation
T1615 Group Policy Discovery
T1021 Remote Services
T1005 Data from Local System
T1095 Non-Application Layer Protocol
T1490 Inhibit System Recovery
T1204.001 User Execution: Malicious Link
T1556 Modify Authentication Process
T1055 Process Injection
T1564 Hide Artifacts
T1040 Network Sniffing
T1046 Network Service Scanning
T1091 Replication Through Removable Media
T1039 Data from Network Shared Drive
T1571 Non-Standard Port
T1498 Network Denial of Service
T1204.002 User Execution: Malicious File
T1137 Office Application Startup
T1053 Scheduled Task/Job
T1574 Hijack Execution Flow
T1003.001 OS Credential Dumping: LSASS Memory
T1135 Network Share Discovery
T1072 Software Deployment Tools
T1025 Data from Removable Media
T1572 Protocol Tunneling
T1496 Resource Hijacking
T1047 Windows Management Instrumentation
T1542 Pre-OS Boot
T1078 Valid Accounts
T1562 Impair Defenses
T1003 OS Credential Dumping
T1040 Network Sniffing
T1080 Taint Shared Content
T1074 Data Staged
T1090 Proxy
T1489 Service Stop

The

PREDICT

Framework

Predictive Relationship / Evolution Detection of Infrastructure in Cyber Threats

A framework for analyzing and predicting malware infrastructure reuse patterns

This is where I talk about the tool I built to visualize the relationships I've been analyzing

PREDICT

The

Automatically find connections between malware Infrastructure

Framework

- How Social Networks Connect People
- How Maps show routes between locations

A Structured framework for Analyzing and predicting malware infrastructure reuse patterns

Predictive Defense

Following the easy path

- Build profiles of infrastructure over time
- Map malware families through shared infrastructure
- Predict likely next attack infrastructure
- Enable soft blocklists → flag related suspicious activity early

PREDICT

The Framework

A Structured framework for Analyzing and predicting malware infrastructure reuse patterns

Before PREDICT:

You: "This IP address (1.2.3.4) is malicious."
Team: "Okay, we blocked it. Now what?"

After PREDICT:

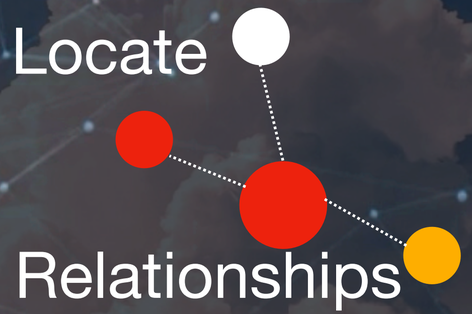
You: "This IP connects to 47 other servers in the same network,
used by 3 different hacking groups, spanning 8 countries."
Team: "We now have 47 more targets to block and patterns to watch!"

Implementation

1. Collect IOCs
2. Locate relationships between them
3. Graph clusters of relationships for searching and analysis

Collect IOCs

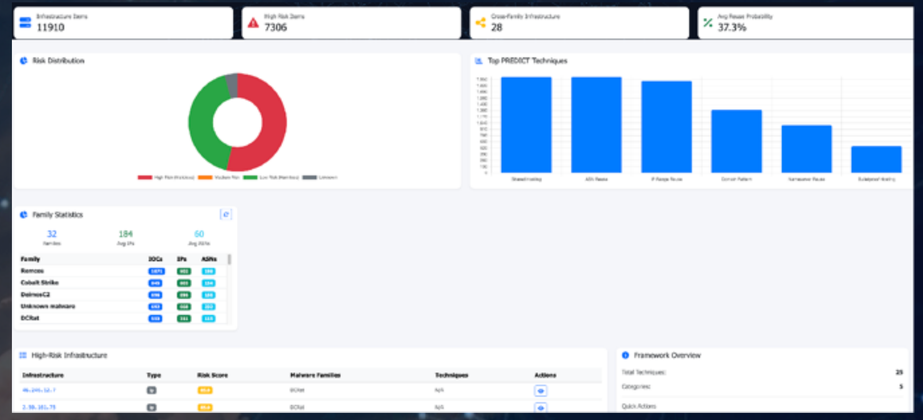
620714.5h4553.ru
http://101.35.95.220:18062/Sem8
25e9fc6010b89648f02e8da1121c4b29
196.251.72.72:5444
157.20.182.9:4443
sit.ngiz5.ru



1. Clients can then query these graphs using the API or website

Clients

Website/API

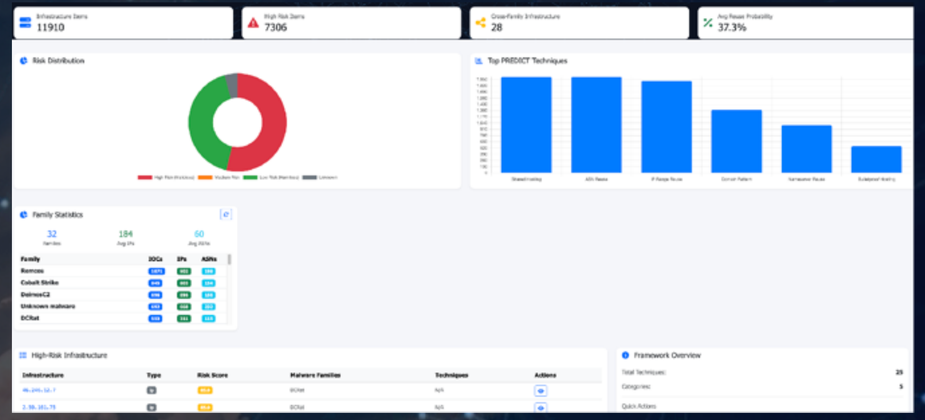


Looking up an IP

Clients

142.250.73.78?

Website/API



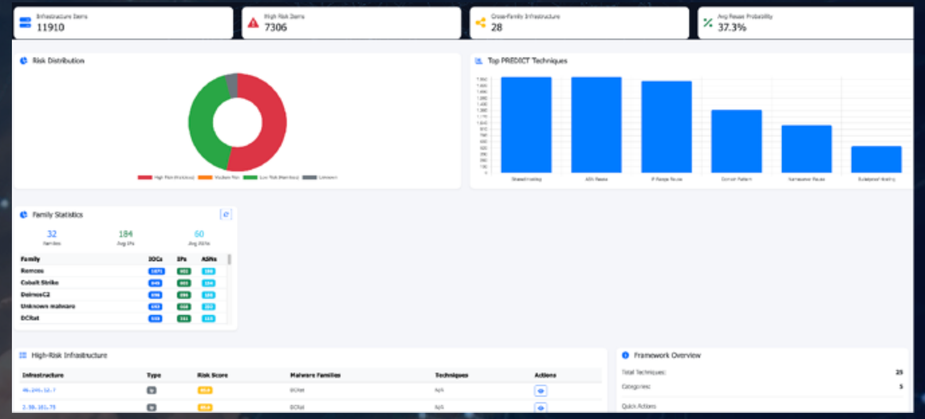
Looking up an IP: It’s a literal match for a known-good IP

Clients

142.250.73.78?

It’s good!

Website/API

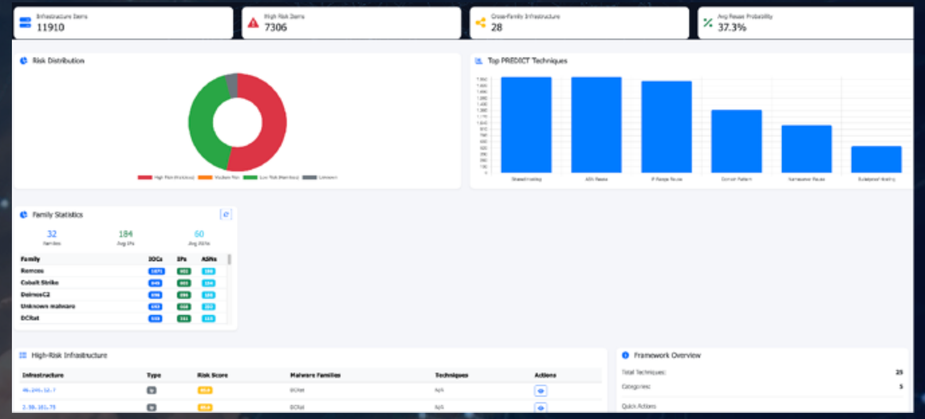


Looking up another IP

Clients

104.21.36.123?

Website/API



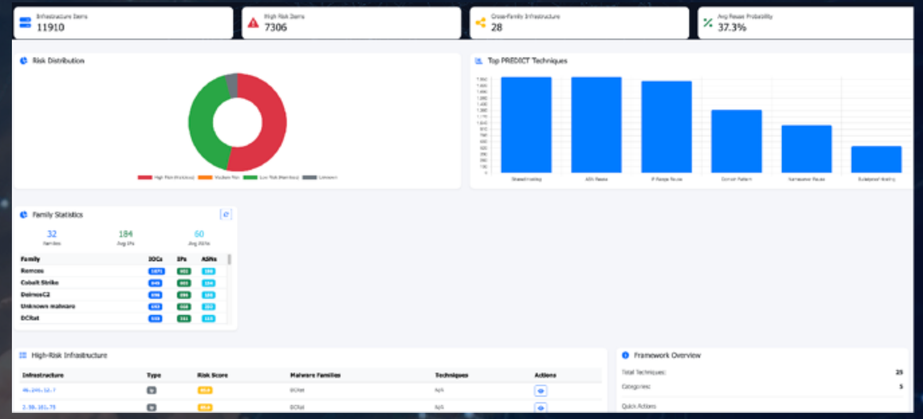
Looking up an IP: It’s a literal match for a known-bad IP

Clients

104.21.36.123?

It’s BAD!!!!!

Website/API



Looking up another IP

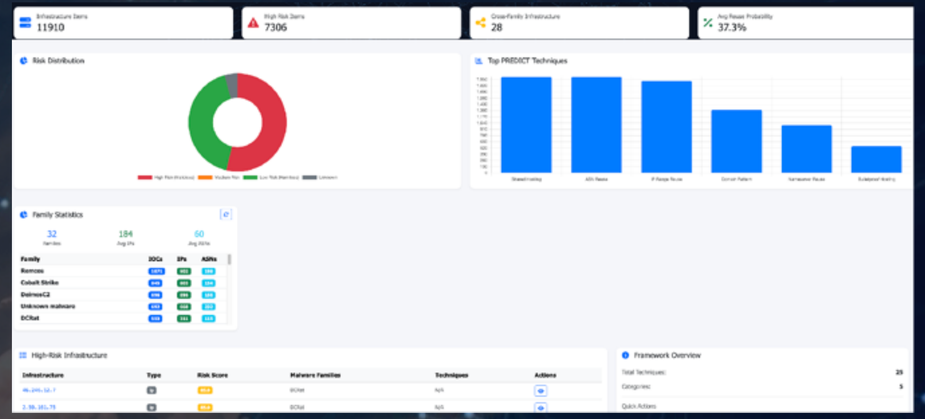
Same network as: 104.21.36.123

The bad IP from before

Clients

104.21.36.110?

Website/API



Looking up an IP: It’s a CIDR and fuzzy match for a known-bad IP

Same network as: 104.21.36.123

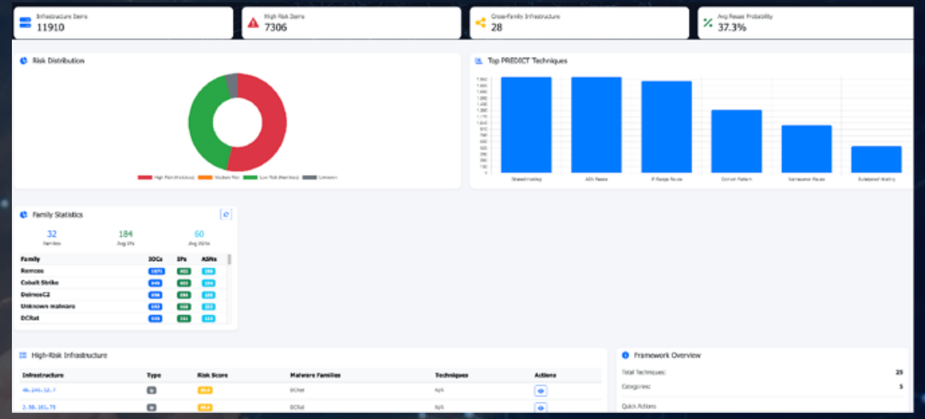
The bad IP from before

Clients

104.21.36.110?

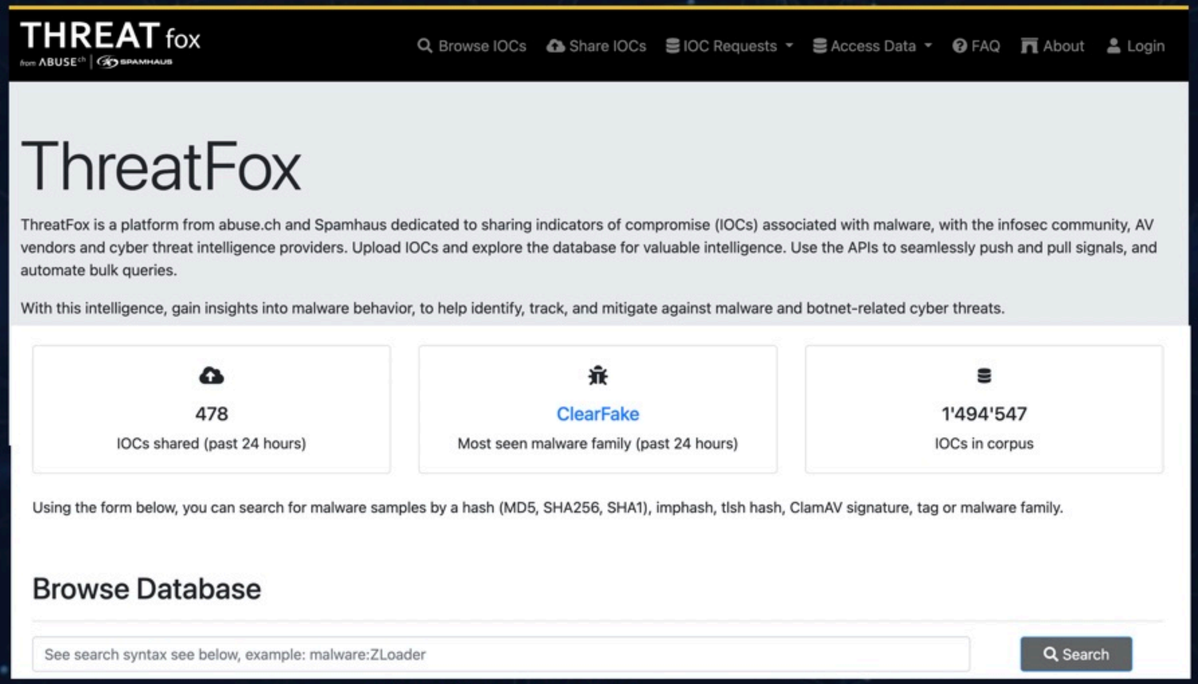
It’s POSSIBLY BAD!!!!!

Website/API



Where I get my IOCs and how I enrich them

Data Sources



threatfox.abuse.ch

virustotal.com

Tracking 30 malware families from 2012 to 2025

2012

Xtreme RAT

Remote Access Trojan used in attacks targeting Israeli and Syrian governments in 2012.

2014

Bashlite

Linux Malware used to launch DDoS attacks

2016

Cobalt Strike

Commercial penetration testing product, released in 2012. Cracked versions used in malware activity after 2016

2016

Formbook

Infostealer that steals form data from web browsers and applications

2016

Quasar RAT

Open source malware written in .NET, often packed to make analysis difficult

2016

Remcos

Commercial Remote Access Tool used in real-world attacks

2016

magecart

Malware and group that deploys web-based card skimmers

2017

LokiBot

Malware designed to steal private data from infected machines, and submit that info to a command and control host via HTTP POST

2017

Revenge RAT

Remote Access Trojan that automatically gathers system information before allowing threat actors to remotely access system components

2018

PoshC2

Proxy aware C2 framework for penetration testers

2018

Vidar

Forked stealer malware based on Arkei. Looks for information from 2FA Software and Tor Browser

2019

AsyncRAT

Open Source Remote Access Trojan used in real-world attacks

2019

DCRat

Backdoor malware provided as a service

2019

REvil Ransomware

Also known as Sodinokibi. RaaS run by affiates. Related to BlackMatter, LockBit, and BlackCat Ransomware

2019

Sodinokibi Ransomware

Also known as REvil. RaaS run by affiates. Related to BlackMatter, LockBit, and BlackCat Ransomware

2020

DarkSide Ransomware

RaaS run by affiates. Related to BlackMatter, REvil/Sodinokibi, LockBit, and BlackCat Ransomware

2020

MooBot

Mirai-based botnet

2020

RedLine Stealer

Standalone or subscription-based malware sold on underground forums. Harvests information from web browsers

2020

Venom RAT

Remote Access Trojan that includes tools for password theft and stealthy access

2021

BlackCat Ransomware

RaaS run by affiates. Potential rebranding of DarkSide Ransomware

2021

BlackMatter Ransomware

RaaS run by affiates. Related to DarkSide, REvil/Sodinokibi, LockBit, and BlackCat Ransomware

2021

FatalRat

Remote access tool distributed through forums and Telegram channels

2022

Brute Ratel C4

Commercial framework for attack simulation. First seen in 2020. Cracked version appeared in 2022 and used in real-world attacks

2022

DeimosC2

open-source C&C framework released in 2020

2022

Lumma Stealer

Malware-as-a-Service (MaaS) infostealer

2022

PureLogs Stealer

Infostealer malware

2022

Rhadamanthys

Stealer-type malware designed to extract data from infected machines

2022

XWorm

Malware with wide range of capabilities ranging from RAT to ransomware

2023

ClearFake

Malicious JavaScript framework deployed on compromised websites to deliver malware

2025

AdaptixC2

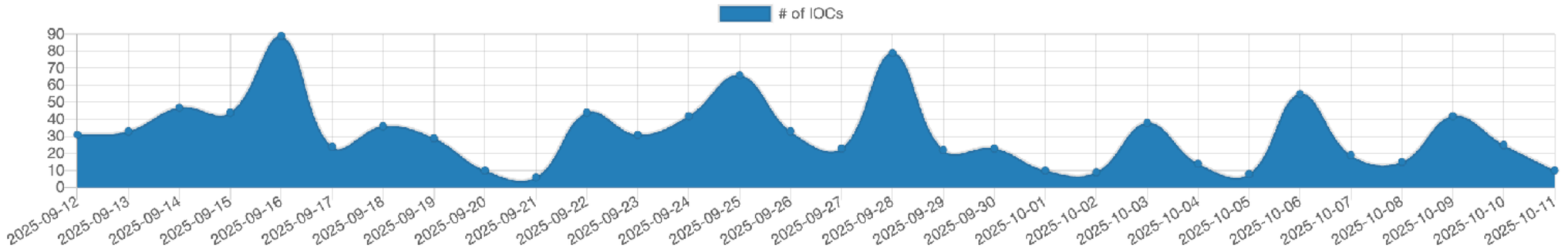
Open Source post-exploitation framework used in real-world attacks

Source IOC Collection

Database Entry

Malware:	Cobalt Strike
Malware alias:	Agenter
First seen:	2020-12-16 15:19:53 UTC
Last seen:	2025-10-11 20:51:21 UTC
Number of IOCs:	116'664
Malpedia:	https://malpedia.caad.fkie.fraunhofer.de/details/win.cobalt_strike

From threatfox.abuse.ch: They have stats



Indicators Of Compromise

The table below shows all indicators of compromise (IOCs) that are associated with this particulare malware family (**max 1000**).

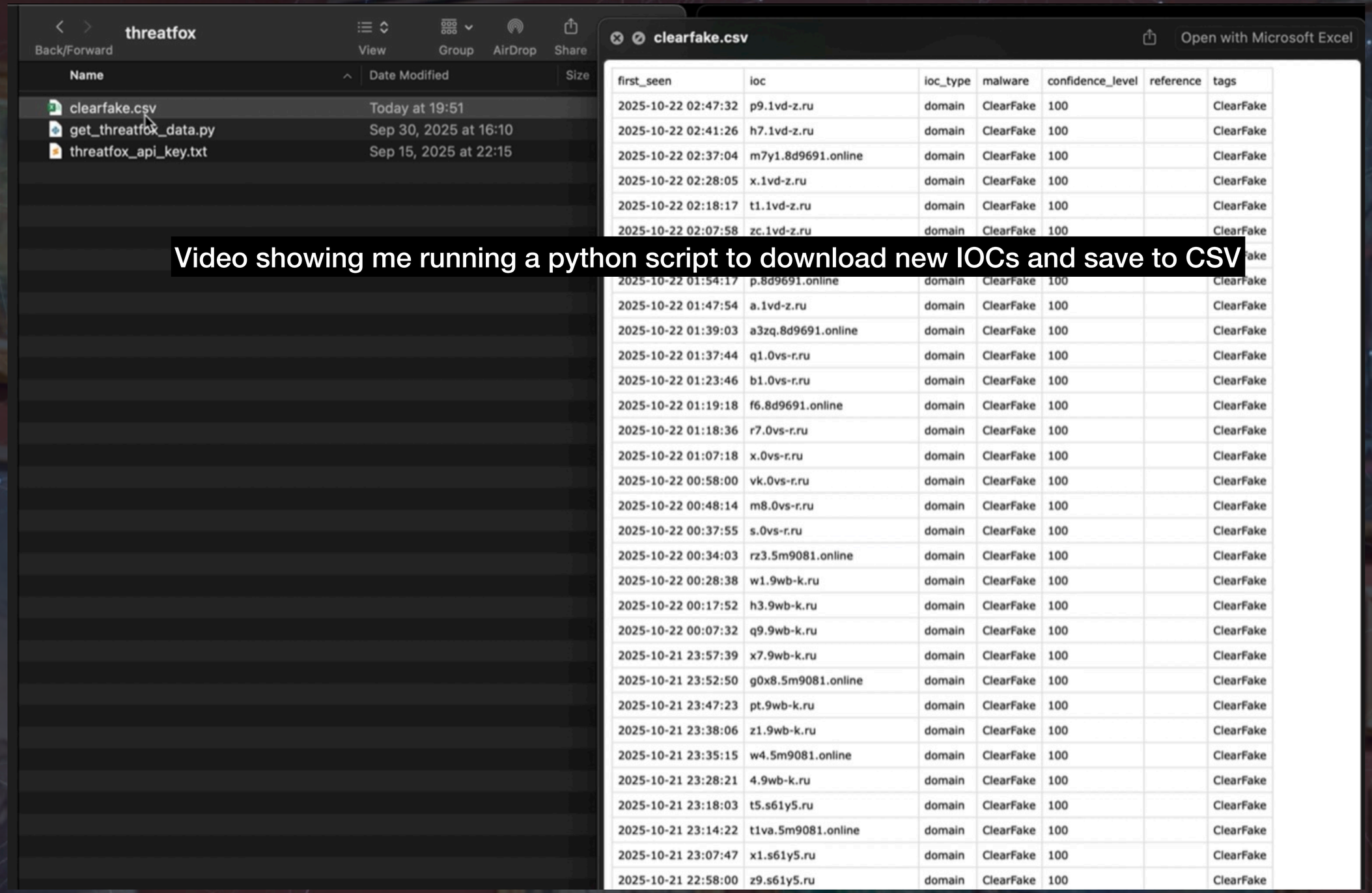
Show 50 entries

Search:

Date (UTC)	IOC	Malware	Tags	Reporter
2025-10-11 20:51:21	8.137.100.162:7002	Cobalt Strike	CobaltStrike drb-ra	abuse_ch
2025-10-11 16:00:59	103.236.55.233:8080	Cobalt Strike	AS4816 c2 censys CHINANET-IDC-GD CobaltStrike cs-watermark-987654321	DonPasci

From threatfox.abuse.ch: They have IOCs

Date (UTC)	IOC	Malware	Tags	Reporter
2025-10-11 20:51	8.137.100.162:7002	Cobalt Strike	CobaltStrike drb-ra	abuse_ch
2025-10-11 20:50	jlk.db-3-a-4.ru			Anonymous
2025-10-11 20:49	tq1.5u-zk.ru	ClearFake	ClearFake	Anonymous
2025-10-11 20:47	x.b10ou.ru	ClearFake	ClearFake	threatcat_ch
2025-10-11 20:39	x5c.db-3-a-4.ru	ClearFake	ClearFake	Anonymous
2025-10-11 20:37	h9m.b10ou.ru	ClearFake	ClearFake	threatcat_ch
2025-10-11 20:29	qns.db-3-a-4.ru	ClearFake	ClearFake	Anonymous
2025-10-11 20:27	tq.b10ou.ru	ClearFake	ClearFake	threatcat_ch
2025-10-11 20:25	196.251.80.62:4651	Remcos	RAT RemcosRAT	abuse_ch
2025-10-11 20:23	b2.5u-zk.ru	ClearFake	ClearFake	Anonymous
2025-10-11 20:18	z1.b10ou.ru	ClearFake	ClearFake	threatcat_ch
2025-10-11 20:14	ai.db-3-a-4.ru	ClearFake	ClearFake	Anonymous
2025-10-11 20:09	x.5u-zk.ru	ClearFake	ClearFake	Anonymous
2025-10-11 20:08	bd.b10ou.ru	ClearFake	ClearFake	threatcat_ch
2025-10-11	193.242.184.136:443	Empire Downloader	AS215381 c2 censys PowershellEmpire ROCKHOSTER	DonPasci

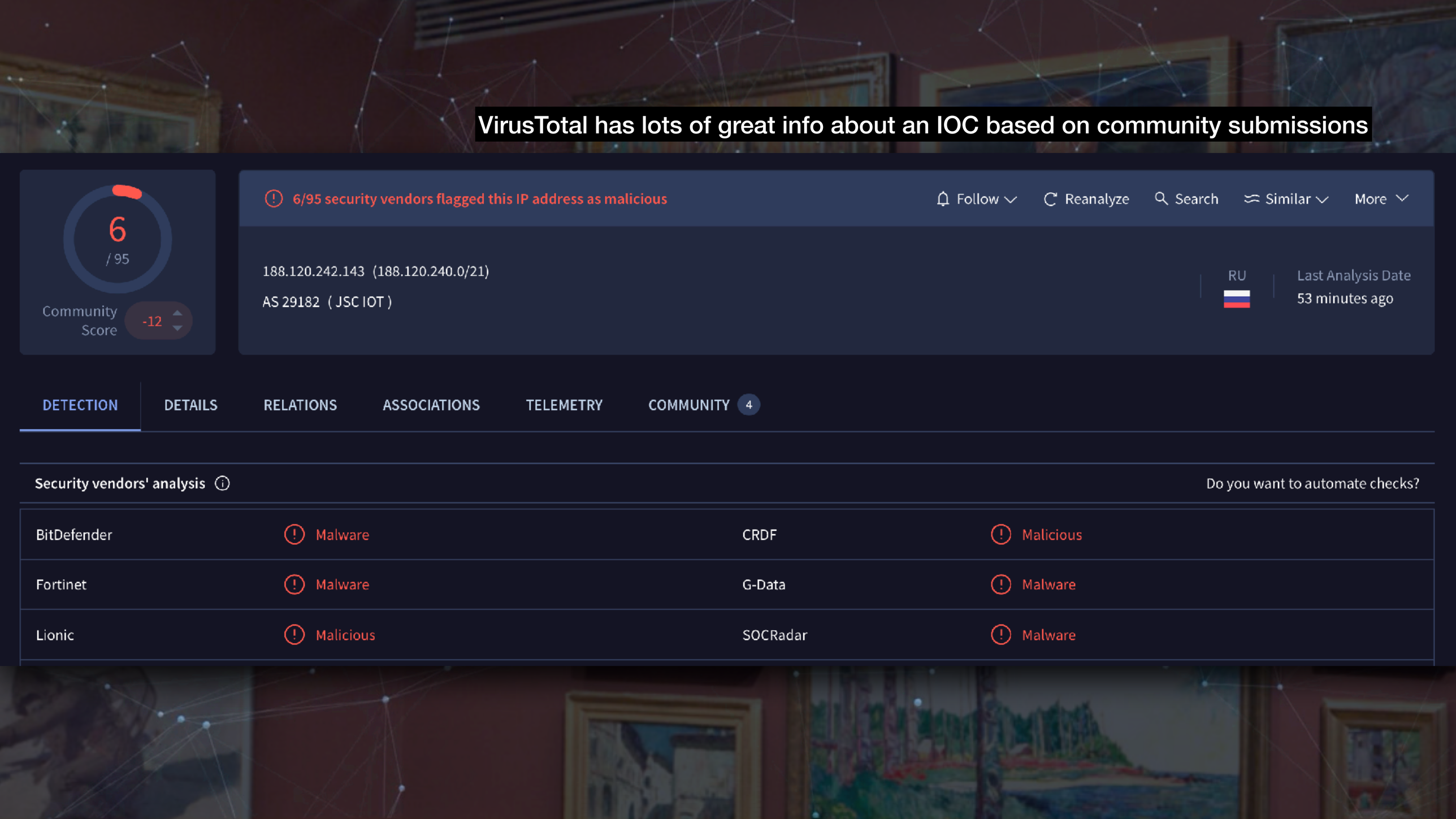


first_seen	ioc	ioc_type	malware	confidence_level	reference	tags
2025-10-22 02:47:32	p9.1vd-z.ru	domain	ClearFake	100		ClearFake
2025-10-22 02:41:26	h7.1vd-z.ru	domain	ClearFake	100		ClearFake
2025-10-22 02:37:04	m7y1.8d9691.online	domain	ClearFake	100		ClearFake
2025-10-22 02:28:05	x.1vd-z.ru	domain	ClearFake	100		ClearFake
2025-10-22 02:18:17	t1.1vd-z.ru	domain	ClearFake	100		ClearFake
2025-10-22 02:07:58	zc.1vd-z.ru	domain	ClearFake	100		ClearFake
2025-10-22 01:54:17	p.8d9691.online	domain	ClearFake	100		ClearFake
2025-10-22 01:47:54	a.1vd-z.ru	domain	ClearFake	100		ClearFake
2025-10-22 01:39:03	a3zq.8d9691.online	domain	ClearFake	100		ClearFake
2025-10-22 01:37:44	q1.0vs-r.ru	domain	ClearFake	100		ClearFake
2025-10-22 01:23:46	b1.0vs-r.ru	domain	ClearFake	100		ClearFake
2025-10-22 01:19:18	f6.8d9691.online	domain	ClearFake	100		ClearFake
2025-10-22 01:18:36	r7.0vs-r.ru	domain	ClearFake	100		ClearFake
2025-10-22 01:07:18	x.0vs-r.ru	domain	ClearFake	100		ClearFake
2025-10-22 00:58:00	vk.0vs-r.ru	domain	ClearFake	100		ClearFake
2025-10-22 00:48:14	m8.0vs-r.ru	domain	ClearFake	100		ClearFake
2025-10-22 00:37:55	s.0vs-r.ru	domain	ClearFake	100		ClearFake
2025-10-22 00:34:03	rz3.5m9081.online	domain	ClearFake	100		ClearFake
2025-10-22 00:28:38	w1.9wb-k.ru	domain	ClearFake	100		ClearFake
2025-10-22 00:17:52	h3.9wb-k.ru	domain	ClearFake	100		ClearFake
2025-10-22 00:07:32	q9.9wb-k.ru	domain	ClearFake	100		ClearFake
2025-10-21 23:57:39	x7.9wb-k.ru	domain	ClearFake	100		ClearFake
2025-10-21 23:52:50	g0x8.5m9081.online	domain	ClearFake	100		ClearFake
2025-10-21 23:47:23	pt.9wb-k.ru	domain	ClearFake	100		ClearFake
2025-10-21 23:38:06	z1.9wb-k.ru	domain	ClearFake	100		ClearFake
2025-10-21 23:35:15	w4.5m9081.online	domain	ClearFake	100		ClearFake
2025-10-21 23:28:21	4.9wb-k.ru	domain	ClearFake	100		ClearFake
2025-10-21 23:18:03	t5.s61y5.ru	domain	ClearFake	100		ClearFake
2025-10-21 23:14:22	t1va.5m9081.online	domain	ClearFake	100		ClearFake
2025-10-21 23:07:47	x1.s61y5.ru	domain	ClearFake	100		ClearFake
2025-10-21 22:58:00	z9.s61y5.ru	domain	ClearFake	100		ClearFake

Enriching IOCs with relationships

IOC Enrichment

VirusTotal has lots of great info about an IOC based on community submissions



DETECTION | DETAILS | RELATIONS | ASSOCIATIONS | TELEMETRY | COMMUNITY 4

They also have information on related domains, hashes, IPs, etc

Passive DNS Replication (9)

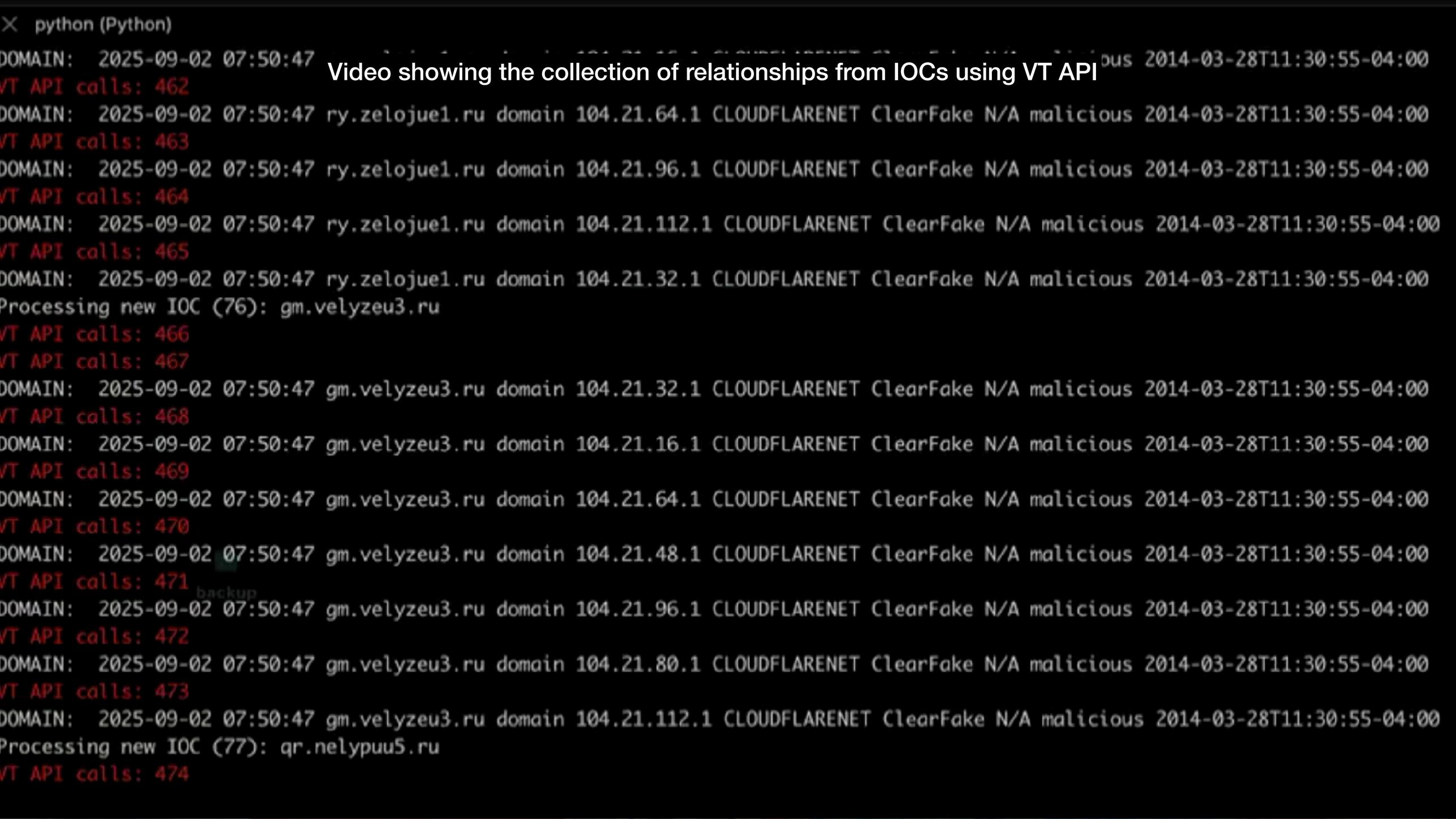
Date resolved	Detections	Resolver	Domain
2022-02-23	0 / 95	VirusTotal	www.volonterq.xyz
2022-02-23	0 / 95	VirusTotal	volonterq.xyz
2022-02-07	0 / 95	VirusTotal	lcb97416.justinstalledpanel.com
2021-10-05	0 / 95	VirusTotal	klovderinvestin.com
2019-09-30	0 / 95	VirusTotal	www.checkroom.ru
2019-09-28	0 / 95	VirusTotal	checkroom.ru
2019-09-28	0 / 95	VirusTotal	test.checkroom.ru
2015-09-06	0 / 95	VirusTotal	intellectik.com
2013-11-11	0 / 95	VirusTotal	fotoramkiforyou.ru

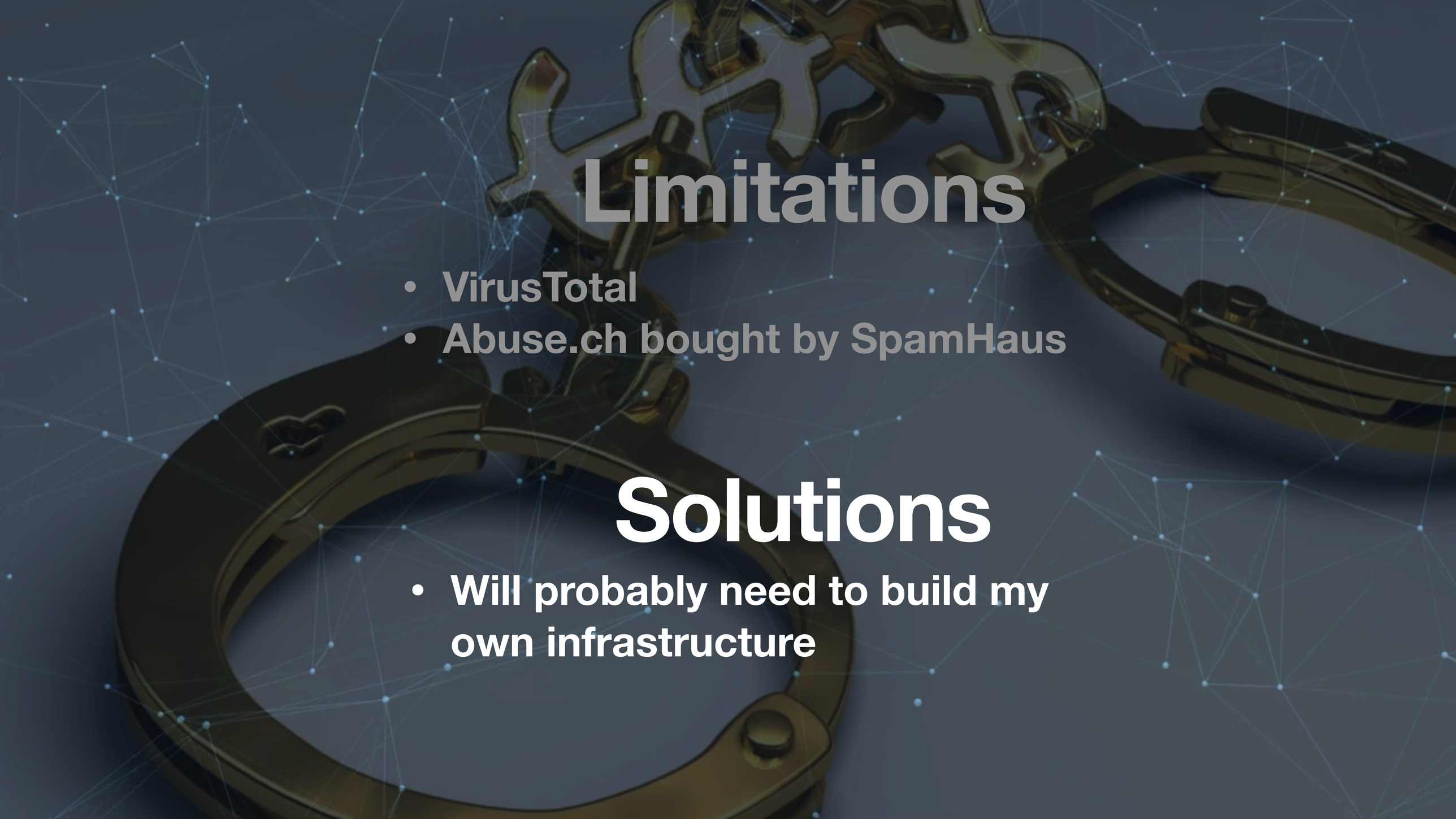
URLs (21)

Scanned	Detections	Status	URL
2025-10-20	5 / 98	200	http://188.120.242.143/
2018-07-09	1 / 67	-	http://188.120.242.143/tags/%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD+%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD+%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD+%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD
2018-07-09	0 / 67	-	http://188.120.242.143/tags/%EF%BF%BD
2014-12-14	1 / 61	-	http://188.120.242.143/tags/%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD %EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD %EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD %EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD
2018-07-12	0 / 67	-	http://188.120.242.143/tags/%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD+%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD+%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD+%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD
2019-05-13	0 / 66	-	http://fotoramkiforyou.ru/

Video showing the collection of relationships from IOCs using VT API

```
================================================================================
Related URLs f
================

Found 10 related URL(s)

URL #1:
--------------------------------------------------------------------------------
  URL:        http://188.120.242.143/
  Title:      IIS7
  Detections: Malicious: 5 | Suspicious: 0 | Harmless: 61 | Undetected: 32
  First seen: 2014-05-01 12:24:27
  Last scan:  2025-10-20 15:10:06
  Flagged by: Lionic, BitDefender, CRDF, Fortinet, G-Data

URL #2:
--------------------------------------------------------------------------------
  URL:
http://188.120.242.143/tags/%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF
%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD+%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF
%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD+%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD
%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD+%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF
%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD
  Title:      N/A
  Detections: Malicious: 1 | Suspicious: 0 | Harmless: 57 | Undetected: 9
  First seen: 2016-12-25 11:27:45
  Last scan:  2018-07-08 19:50:32
  Flagged by: Fortinet

URL #3:
--------------------------------------------------------------------------------
  URL:
http://188.120.242.143/tags/%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF
%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD
  Title:      N/A
  Detections: Malicious: 0 | Suspicious: 0 | Harmless: 58 | Undetected: 9
  First seen: 2014-11-24 15:05:12
  Last scan:  2018-07-09 15:18:58
```


python (Python)
Video showing the collection of relationships from IOCs using VT API
DOMAIN: 2025-09-02 07:50:47 ry.zelojue1.ru domain 104.21.64.1 CLOUDFLARENET ClearFake N/A malicious 2014-03-28T11:30:55-04:00
VT API calls: 463
DOMAIN: 2025-09-02 07:50:47 ry.zelojue1.ru domain 104.21.96.1 CLOUDFLARENET ClearFake N/A malicious 2014-03-28T11:30:55-04:00
VT API calls: 464
DOMAIN: 2025-09-02 07:50:47 ry.zelojue1.ru domain 104.21.112.1 CLOUDFLARENET ClearFake N/A malicious 2014-03-28T11:30:55-04:00
VT API calls: 465
DOMAIN: 2025-09-02 07:50:47 ry.zelojue1.ru domain 104.21.32.1 CLOUDFLARENET ClearFake N/A malicious 2014-03-28T11:30:55-04:00
Processing new IOC (76): gm.velyzeu3.ru
VT API calls: 466
VT API calls: 467
DOMAIN: 2025-09-02 07:50:47 gm.velyzeu3.ru domain 104.21.32.1 CLOUDFLARENET ClearFake N/A malicious 2014-03-28T11:30:55-04:00
VT API calls: 468
DOMAIN: 2025-09-02 07:50:47 gm.velyzeu3.ru domain 104.21.16.1 CLOUDFLARENET ClearFake N/A malicious 2014-03-28T11:30:55-04:00
VT API calls: 469
DOMAIN: 2025-09-02 07:50:47 gm.velyzeu3.ru domain 104.21.64.1 CLOUDFLARENET ClearFake N/A malicious 2014-03-28T11:30:55-04:00
VT API calls: 470
DOMAIN: 2025-09-02 07:50:47 gm.velyzeu3.ru domain 104.21.48.1 CLOUDFLARENET ClearFake N/A malicious 2014-03-28T11:30:55-04:00
VT API calls: 471
DOMAIN: 2025-09-02 07:50:47 gm.velyzeu3.ru domain 104.21.96.1 CLOUDFLARENET ClearFake N/A malicious 2014-03-28T11:30:55-04:00
VT API calls: 472
DOMAIN: 2025-09-02 07:50:47 gm.velyzeu3.ru domain 104.21.80.1 CLOUDFLARENET ClearFake N/A malicious 2014-03-28T11:30:55-04:00
VT API calls: 473
DOMAIN: 2025-09-02 07:50:47 gm.velyzeu3.ru domain 104.21.112.1 CLOUDFLARENET ClearFake N/A malicious 2014-03-28T11:30:55-04:00
Processing new IOC (77): qr.nelypuu5.ru
VT API calls: 474

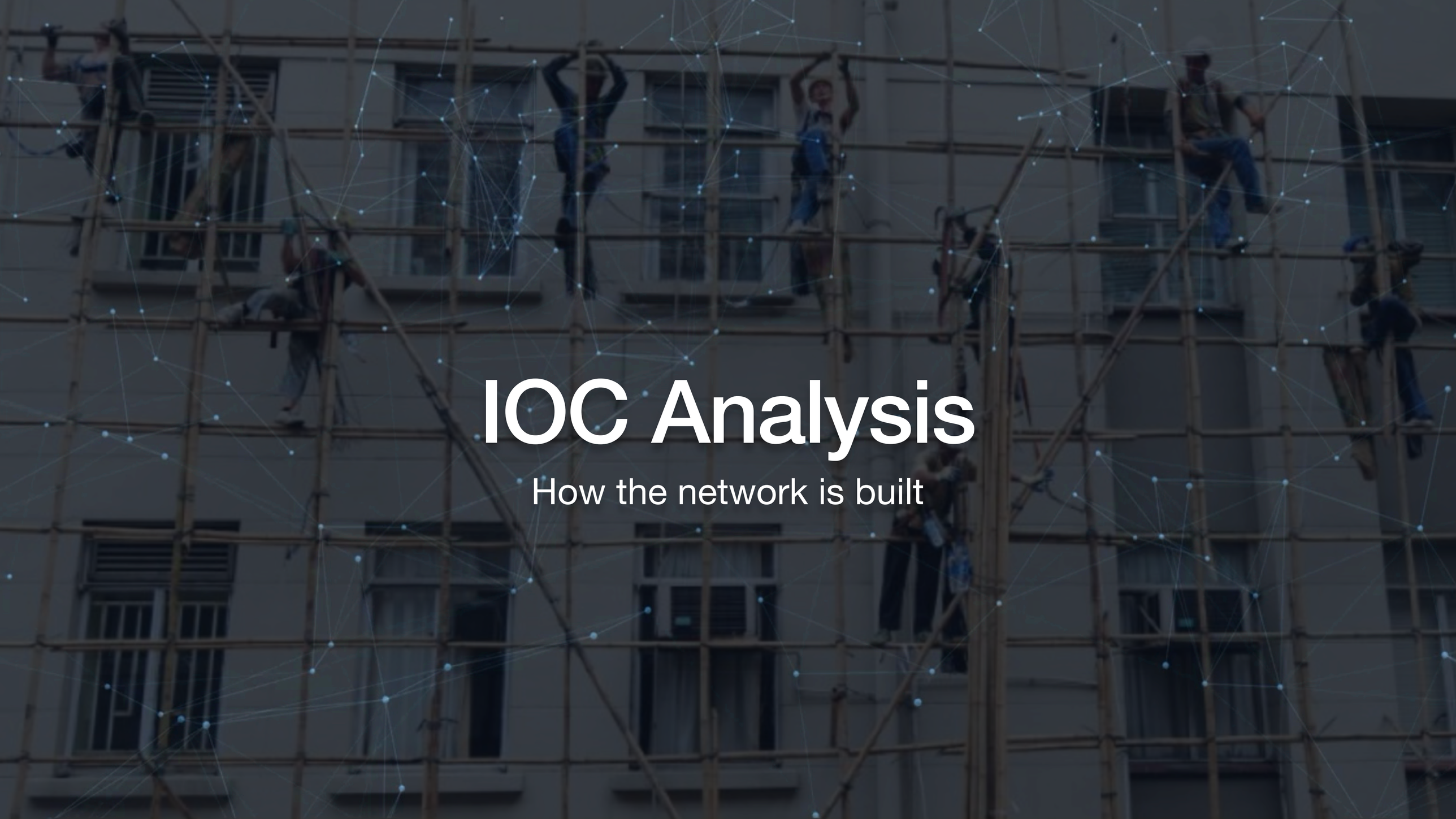


Limitations

- VirusTotal
- Abuse.ch bought by SpamHaus

Solutions

- Will probably need to build my own infrastructure



IOC Analysis

How the network is built

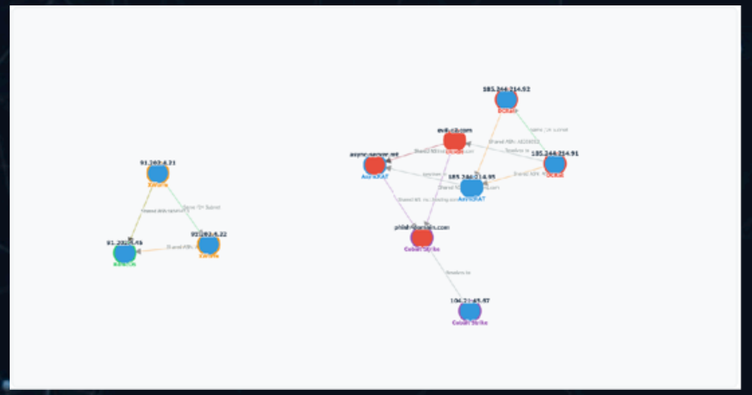
Data Ingestion

adaptixc2_api_parsed.csv	Oct 16, 2025 at 12:21	44 KB	comma...values
asyncrat_api_parsed.csv	Oct 16, 2025 at 12:21	287 KB	comma...values
bashlite_api_parsed.csv	Oct 16, 2025 at 12:21	82 KB	comma...values
blackcat_api_parsed.csv	Oct 16, 2025 at 12:21	45 KB	comma...values
blackmatter_api_parsed.csv	Oct 16, 2025 at 12:21	284 KB	comma...values
brute_ratel_c4_api_parsed.csv	Oct 16, 2025 at 22:37	31 KB	comma...values
clearfake_api_parsed.csv	Oct 16, 2025 at 22:47	704 KB	comma...values
cobalt_strike_api_parsed.csv	Oct 16, 2025 at 12:21	208 KB	comma...values
darkside_api_parsed.csv	Oct 16, 2025 at 12:21	109 KB	comma...values
dcrat_api_parsed.csv	Oct 16, 2025 at 12:21	465 KB	comma...values
deimosc2_api_parsed.csv	Oct 16, 2025 at 12:21	100 KB	comma...values
fatalrat_api_parsed.csv	Oct 16, 2025 at 12:21	20 KB	comma...values
formbook_api_parsed.csv	Oct 16, 2025 at 12:21	304 KB	comma...values
lokibot_api_parsed.csv	Oct 16, 2025 at 12:21	133 KB	comma...values
lumma_stealer_api_parsed.csv	Oct 16, 2025 at 12:21	225 KB	comma...values
magecart_api_parsed.csv	Oct 16, 2025 at 12:21	15 KB	comma...values
moobot_api_parsed.csv	Oct 16, 2025 at 12:21	13 KB	comma...values
poshc2_api_parsed.csv	Oct 16, 2025 at 12:21	3 KB	comma...values
purelogs_stealer_api_parsed.csv	Oct 16, 2025 at 22:33	25 KB	comma...values
quasar_api_parsed.csv	Oct 16, 2025 at 12:21	49 KB	comma...values
redline_api_parsed.csv	Oct 16, 2025 at 12:21	80 KB	comma...values
reevil_api_parsed.csv	Oct 16, 2025 at 12:21	39 KB	comma...values
remcos_api_parsed.csv	Oct 16, 2025 at 12:21	485 KB	comma...values
revenge_rat_api_parsed.csv	Oct 16, 2025 at 12:21	937 KB	comma...values
rhadamanthys_api_parsed.csv	Oct 16, 2025 at 12:21	472 KB	comma...values
sodinokibi_api_parsed.csv	Oct 16, 2025 at 12:21	205 KB	comma...values
unknown_malw..._api_parsed.csv	Oct 16, 2025 at 12:21	254 KB	comma...values
unknown_rat_api_parsed.csv	Oct 16, 2025 at 12:21	378 KB	comma...values

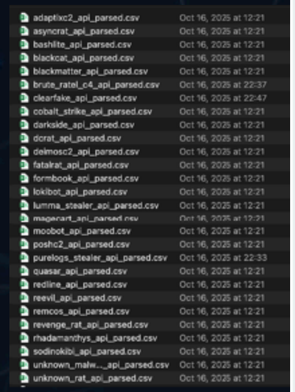
Data Ingestion

adaptixc2_api_parsed.csv	Oct 16, 2025 at 12:21	44 KB	comma...values
asyncrat_api_parsed.csv	Oct 16, 2025 at 12:21	287 KB	comma...values
bashlite_api_parsed.csv	Oct 16, 2025 at 12:21	82 KB	comma...values
blackcat_api_parsed.csv	Oct 16, 2025 at 12:21	45 KB	comma...values
blackmatter_api_parsed.csv	Oct 16, 2025 at 12:21	284 KB	comma...values
brute_ratel_c4_api_parsed.csv	Oct 16, 2025 at 22:37	31 KB	comma...values
clearfake_api_parsed.csv	Oct 16, 2025 at 22:47	704 KB	comma...values
cobalt_strike_api_parsed.csv	Oct 16, 2025 at 12:21	208 KB	comma...values
darkside_api_parsed.csv	Oct 16, 2025 at 12:21	109 KB	comma...values
dcrat_api_parsed.csv	Oct 16, 2025 at 12:21	465 KB	comma...values
deimosc2_api_parsed.csv	Oct 16, 2025 at 12:21	100 KB	comma...values
fatalrat_api_parsed.csv	Oct 16, 2025 at 12:21	20 KB	comma...values
formbook_api_parsed.csv	Oct 16, 2025 at 12:21	304 KB	comma...values
lokibot_api_parsed.csv	Oct 16, 2025 at 12:21	133 KB	comma...values
lumma_stealer_api_parsed.csv	Oct 16, 2025 at 12:21	225 KB	comma...values
mageccart_api_parsed.csv	Oct 16, 2025 at 12:21	15 KB	comma...values
moobot_api_parsed.csv	Oct 16, 2025 at 12:21	13 KB	comma...values
poshc2_api_parsed.csv	Oct 16, 2025 at 12:21	3 KB	comma...values
purelogs_stealer_api_parsed.csv	Oct 16, 2025 at 22:33	25 KB	comma...values
quasar_api_parsed.csv	Oct 16, 2025 at 12:21	49 KB	comma...values
redline_api_parsed.csv	Oct 16, 2025 at 12:21	80 KB	comma...values
reevil_api_parsed.csv	Oct 16, 2025 at 12:21	39 KB	comma...values
remcos_api_parsed.csv	Oct 16, 2025 at 12:21	485 KB	comma...values
revenge_rat_api_parsed.csv	Oct 16, 2025 at 12:21	937 KB	comma...values
rhadamanthys_api_parsed.csv	Oct 16, 2025 at 12:21	472 KB	comma...values
sodinokibi_api_parsed.csv	Oct 16, 2025 at 12:21	205 KB	comma...values
unknown_malw..._api_parsed.csv	Oct 16, 2025 at 12:21	254 KB	comma...values
unknown_rat_api_parsed.csv	Oct 16, 2025 at 12:21	378 KB	comma...values

Calculate Relationships



Data Ingest



Infrastructure Files

dcrat_api_parsed.csv	2,879 rows
asyncrat_api_parsed.csv	1,822 rows
cobalt_strike_api_parsed.csv	1,262 rows
xworm_api_parsed.csv	3,907 rows
remcos_api_parsed.csv	3,177 rows

Processing Pipeline

- Reading CSV files ✓
- Parsing IOC data ✓
- Deduplicating entries ✓
- Building relationships ✓
- Inserting into database ✓

43,634

PostgreSQL Database

iocs

Unique records: **17,285**
Columns: ip, malware, result, country, asn...

relationships

Total: **8.8M**
Types: same_ip, same_asn, same_subnet...

geo_url_results

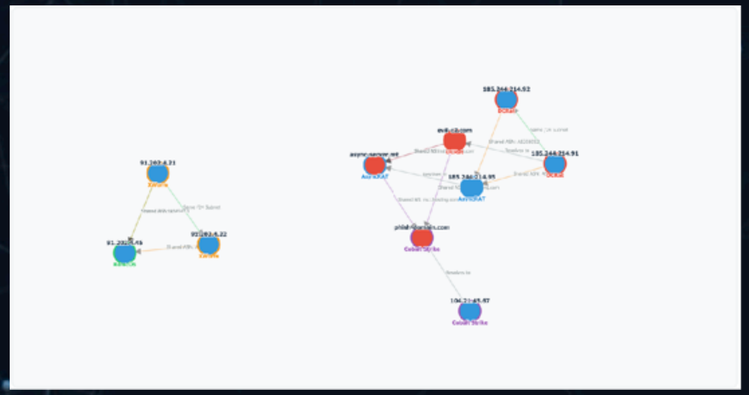
Geolocated IPs: **11235**
Columns: domain, lat, lon, city, country

TOTAL CSV ROWS	UNIQUE IOCS	RELATIONSHIPS	PROCESSING TIME
43,634	17,285	8,835,279	2.5 min

Data Ingestion

adaptixc2_api_parsed.csv	Oct 16, 2025 at 12:21	44 KB	comma...values
asyncrat_api_parsed.csv	Oct 16, 2025 at 12:21	287 KB	comma...values
bashlite_api_parsed.csv	Oct 16, 2025 at 12:21	82 KB	comma...values
blackcat_api_parsed.csv	Oct 16, 2025 at 12:21	45 KB	comma...values
blackmatter_api_parsed.csv	Oct 16, 2025 at 12:21	284 KB	comma...values
brute_ratel_c4_api_parsed.csv	Oct 16, 2025 at 22:37	31 KB	comma...values
clearfake_api_parsed.csv	Oct 16, 2025 at 22:47	704 KB	comma...values
cobalt_strike_api_parsed.csv	Oct 16, 2025 at 12:21	208 KB	comma...values
darkside_api_parsed.csv	Oct 16, 2025 at 12:21	109 KB	comma...values
dcrat_api_parsed.csv	Oct 16, 2025 at 12:21	465 KB	comma...values
deimosc2_api_parsed.csv	Oct 16, 2025 at 12:21	100 KB	comma...values
fatalrat_api_parsed.csv	Oct 16, 2025 at 12:21	20 KB	comma...values
formbook_api_parsed.csv	Oct 16, 2025 at 12:21	304 KB	comma...values
lokibot_api_parsed.csv	Oct 16, 2025 at 12:21	133 KB	comma...values
lumma_stealer_api_parsed.csv	Oct 16, 2025 at 12:21	225 KB	comma...values
magecart_api_parsed.csv	Oct 16, 2025 at 12:21	15 KB	comma...values
moobot_api_parsed.csv	Oct 16, 2025 at 12:21	13 KB	comma...values
poshc2_api_parsed.csv	Oct 16, 2025 at 12:21	3 KB	comma...values
purelogs_stealer_api_parsed.csv	Oct 16, 2025 at 22:33	25 KB	comma...values
quasar_api_parsed.csv	Oct 16, 2025 at 12:21	49 KB	comma...values
redline_api_parsed.csv	Oct 16, 2025 at 12:21	80 KB	comma...values
reevil_api_parsed.csv	Oct 16, 2025 at 12:21	39 KB	comma...values
remcos_api_parsed.csv	Oct 16, 2025 at 12:21	485 KB	comma...values
revenge_rat_api_parsed.csv	Oct 16, 2025 at 12:21	937 KB	comma...values
rhadamanthys_api_parsed.csv	Oct 16, 2025 at 12:21	472 KB	comma...values
sodinokibi_api_parsed.csv	Oct 16, 2025 at 12:21	205 KB	comma...values
unknown_malw..._api_parsed.csv	Oct 16, 2025 at 12:21	254 KB	comma...values
unknown_rat_api_parsed.csv	Oct 16, 2025 at 12:21	378 KB	comma...values

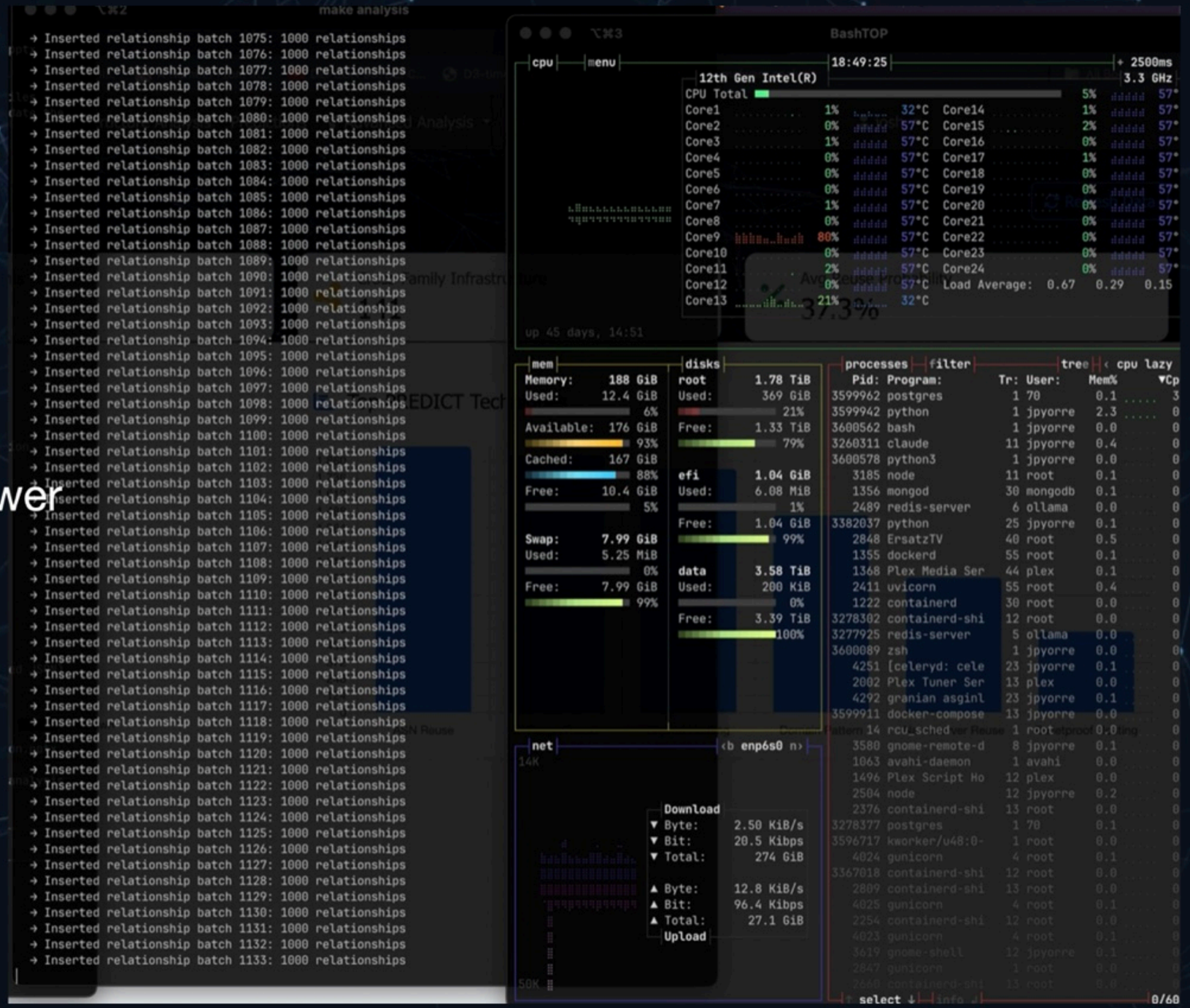
Calculate Relationships

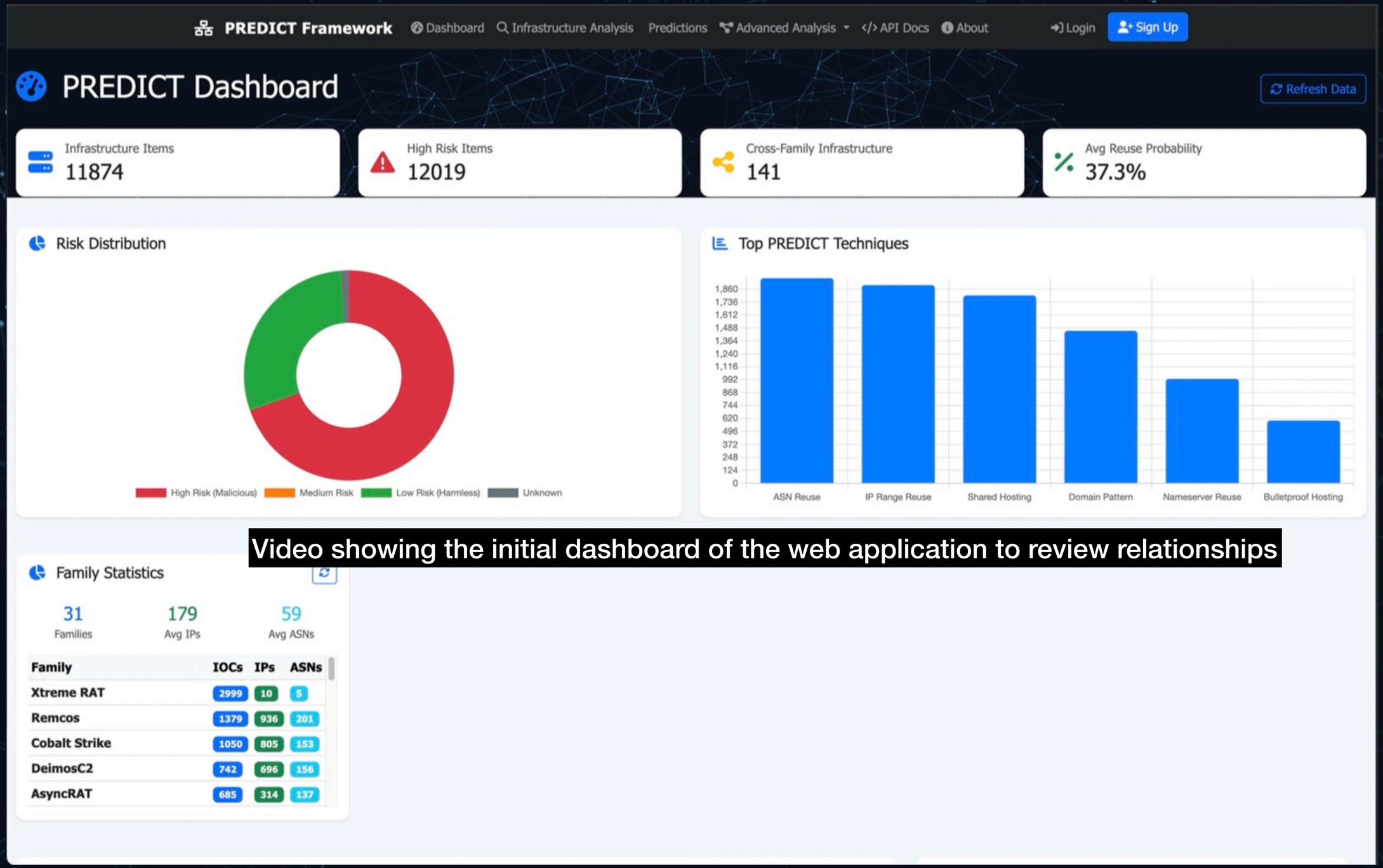


Populate Database

Building Network

- Multi-threaded
- Doesn’t need much power
- Takes a few minutes




PREDICT Framework
Dashboard
Infrastructure Analysis
Predictions
Advanced Analysis
API Docs
About
Login
Sign Up
PREDICT Dashboard
Refresh Data
Infrastructure Items
11874
High Risk Items
12019
Cross-Family Infrastructure
141
Avg Reuse Probability
37.3%
Risk Distribution
High Risk (Malicious)
Medium Risk
Low Risk (Harmless)
Unknown
Top PREDICT Techniques
1,860
1,736
1,612
1,488
1,364
1,240
1,116
992
868
744
620
496
372
248
124
0
ASN Reuse
IP Range Reuse
Shared Hosting
Domain Pattern
Nameserver Reuse
Bulletproof Hosting
Video showing the initial dashboard of the web application to review relationships
Family Statistics
31
Families
179
Avg IPs
59
Avg ASNs
Family
IOCs
IPs
ASNs
Xtreme RAT
2999
10
5
Remcos
1379
936
201
Cobalt Strike
1050
805
153
DeimosC2
742
696
156
AsyncRAT
685
314
137

Map Filtering

Threat Level:

All IOCs

Malware Family:

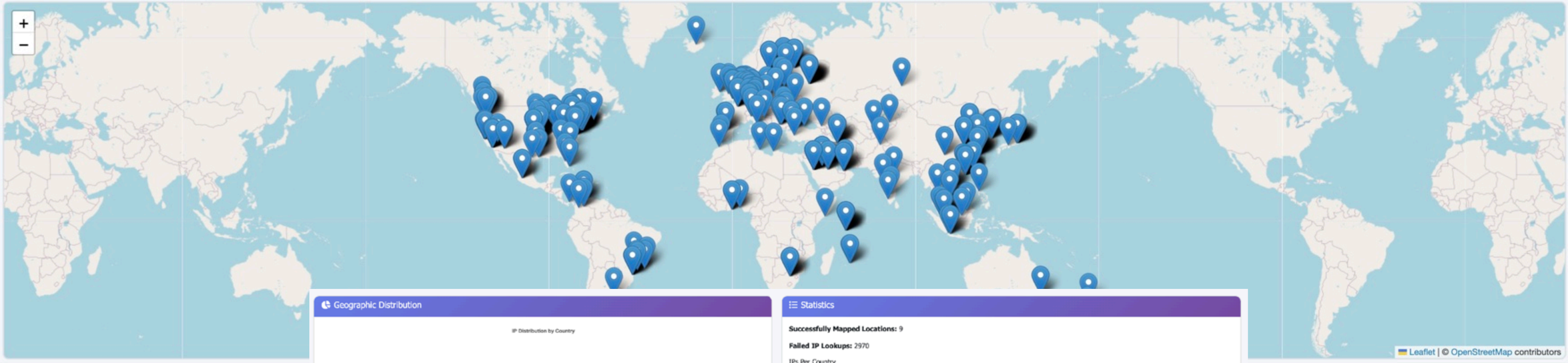
All Families

✓ Apply Filters | Get Statistics

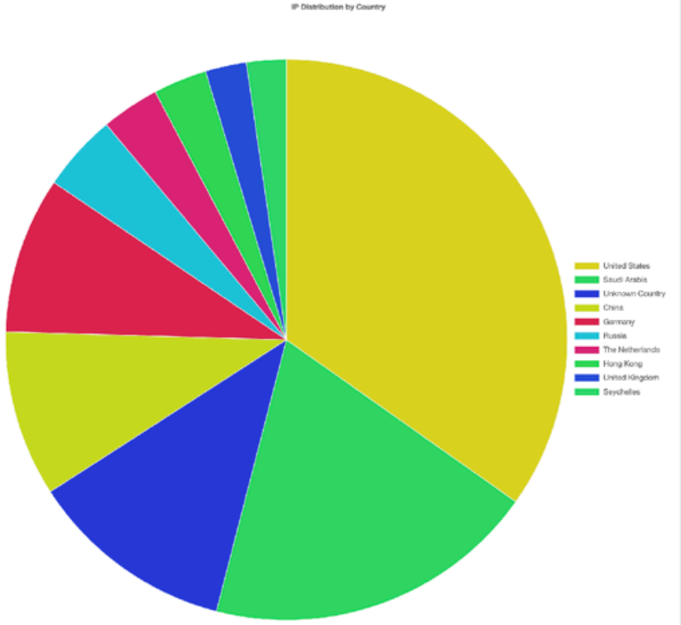
Map Generated Successfully!

Showing 20034 of 20034 locations (filtered for all IOCs).

More info on the web interface



Geographic Distribution



Statistics

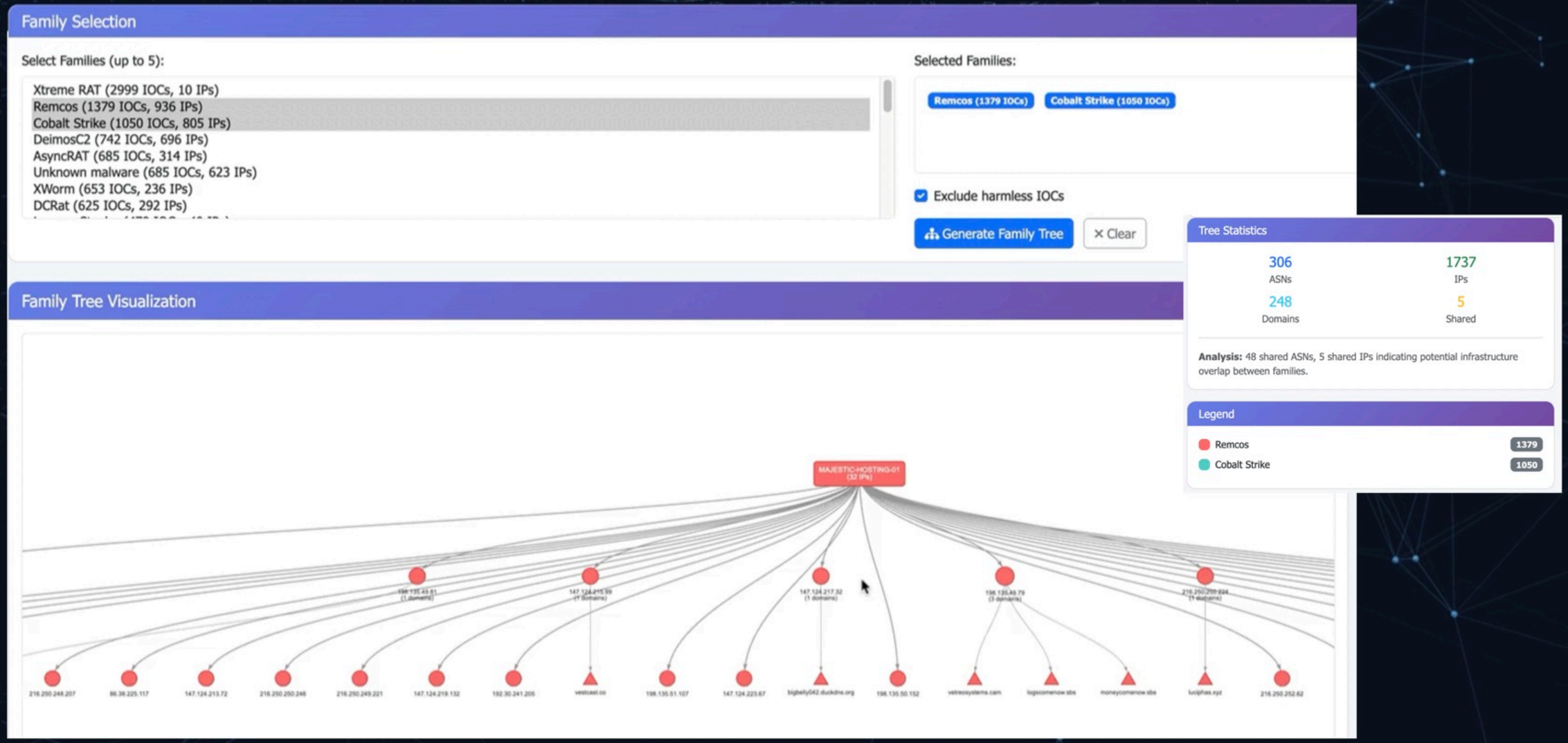
Successfully Mapped Locations: 9

Failed IP Lookups: 2970

IPs Per Country

- United States: **5431** IPs
- Saudi Arabia: **3001** IPs
- Unknown Country: **1853** IPs
- China: **1493** IPs
- Germany: **1409** IPs
- Russia: **694** IPs
- The Netherlands: **521** IPs
- Hong Kong: **482** IPs
- United Kingdom: **369** IPs
- Seychelles: **357** IPs

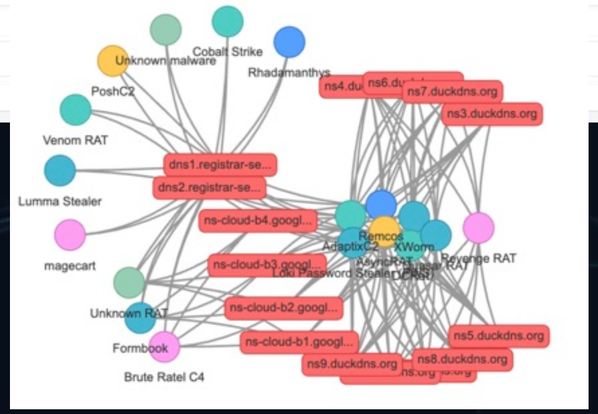
Family Tree Analysis



DNS Analysis

DNS Relationship Analysis

Nameserver	Shared Families	Families	Shared Domains
dns1.registrar-servers.com	14	Cobalt Strike, Formbook, Unknown RAT +11 more	48
dns2.registrar-servers.com	14	Cobalt Strike, Formbook, Unknown RAT +11 more	48
ns1.duckdns.org	8	Remcos, XWorm, AdaptixC2 +5 more	173
ns2.duckdns.org	8	Remcos, XWorm, AdaptixC2 +5 more	173
ns3.duckdns.org	8	Remcos, XWorm, AdaptixC2 +5 more	173
ns4.duckdns.org	8	Remcos, XWorm, AdaptixC2 +5 more	173
ns5.duckdns.org	8	Remcos, XWorm, AdaptixC2 +5 more	173
ns6.duckdns.org	8	Remcos, XWorm, AdaptixC2 +5 more	173
ns7.duckdns.org	8	Remcos, XWorm, AdaptixC2 +5 more	173
ns8.duckdns.org	8	Remcos, XWorm, AdaptixC2 +5 more	173
ns9.duckdns.org	8	Remcos, XWorm, AdaptixC2 +5 more	173
ns-cloud-b1.googledomains.com	8	Formbook, Unknown RAT, Remcos +5 more	50
ns-cloud-b2.googledomains.com	8	Formbook, Unknown RAT, Remcos +5 more	50
ns-cloud-b3.googledomains.com	8	Formbook, Unknown RAT, Remcos +5 more	50
ns-cloud-b4.googledomains.com	8	Formbook, Unknown RAT, Remcos +5 more	50
ns1.playit-dns.com	8	Unknown RAT, Remcos, XWorm +5 more	180
ns2.playit-dns.com	8	Unknown RAT, Remcos, XWorm +5 more	180
ns1.playit.cloud	8	Unknown RAT, Remcos, XWorm +5 more	179
ns67.domaincontrol.com	8		179
ns68.domaincontrol.com	8		179



Infrastructure Evolution

Analysis Configuration

Malware Family: Cobalt Strike (1050 IOCs)

Time Window (days): 90 days

Exclude harmless IOCs

Analyze Evolution

9.24	1,050	0.092	90 days
Evolution Score	Total IOCs	Diversity Score	Analysis Period

Infrastructure Persistence

Average Persistence: 1.1%

Hangzhou Alibaba Advertising Co.,Ltd. — 20.8%
asn: 218 uses

Shenzhen Tencent Computer Systems Company Limited — 17.2%
asn: 181 uses

PEG-HK — 5.0%
asn: 53 uses

Huawei Cloud Service data center — 4.5%
asn: 47 uses

Tencent Building, Kejizhongyi Avenue — 3.3%
asn: 35 uses

Migration Patterns

153	41
Unique ASNs	Countries

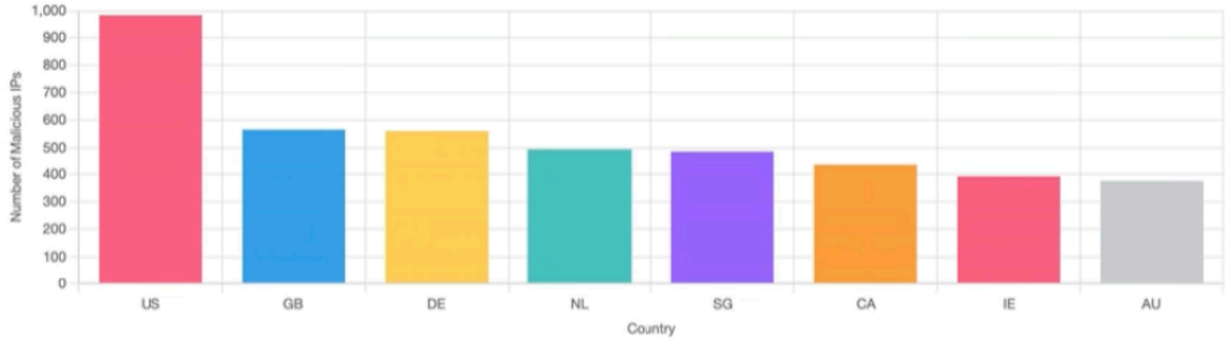
Analysis: Infrastructure spread across 153 ASNs and 41 countries indicates the scope of infrastructure utilization.

Evolution Timeline

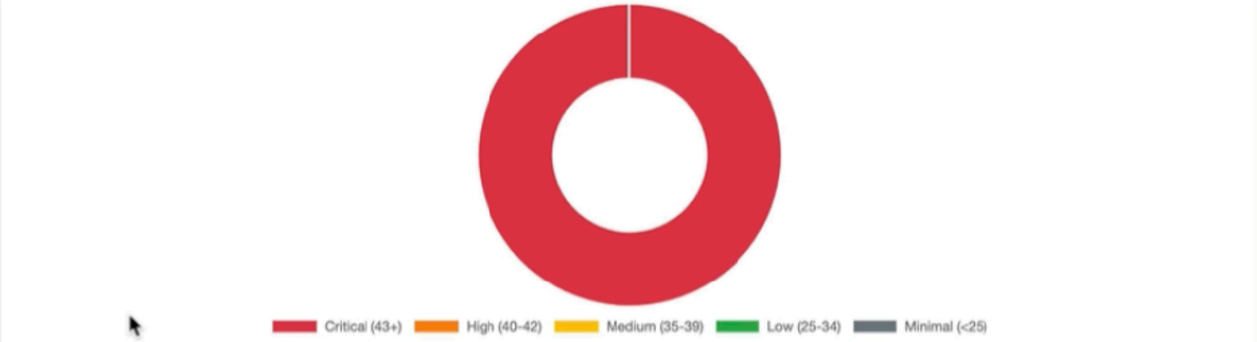
BulletProof Hosting

AS62005	BlueVPS OU	100	Cobalt Strike, AdaptixC2, Unknown malware...	10

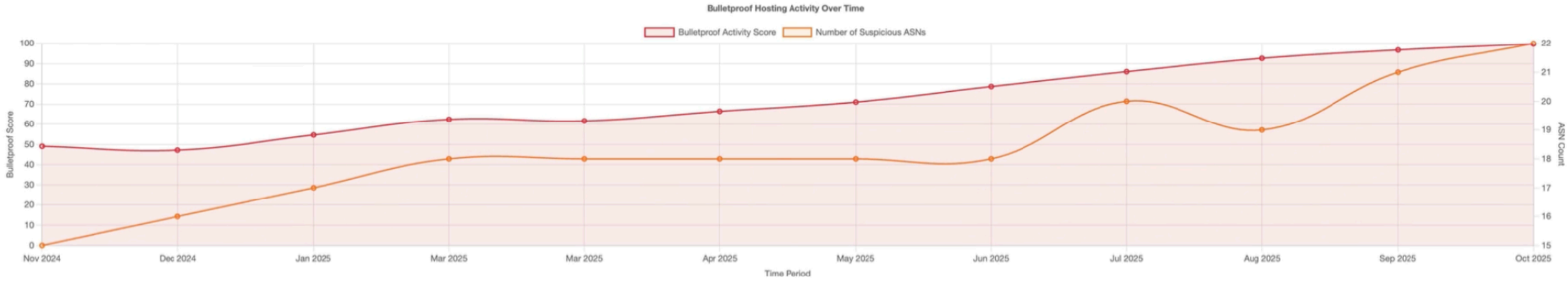
Geographic Distribution Chart



Provider Risk Distribution



Bulletproof Hosting Evolution Timeline



Bulletproof Hosting Indicators

20

20

100%

BulletProof Hosting

ASN	Provider	Risk Score	Families	IPs
AS401116	NYBULA	100	Cobalt Strike, Remcos, XWorm...	66
AS51167	Contabo GmbH	100	Cobalt Strike, Remcos, XWorm...	44
AS36352	AS-COLOCROSSING	100	Cobalt Strike, Remcos, XWorm...	196
AS14061	DIGITALOCEAN-ASN	100	Cobalt Strike, PoshC2, Remcos...	118
AS132203	Tencent Building, Kejizhongyi Avenue	100	Cobalt Strike, XWorm, AdaptixC2...	38
AS9009	M247 Europe SRL	100	Cobalt Strike, Unknown RAT, Remcos...	150
AS396982	GOOGLE-CLOUD-PLATFORM	100	Cobalt Strike, Formbook, Unknown RAT...	47
AS213230, AS24940	Hetzner Online GmbH	100	Cobalt Strike, Unknown RAT, magecart...	169
AS8075	MICROSOFT-CORP-MSN-AS-BLOCK	100	Cobalt Strike, PoshC2, Remcos...	46
AS40021	CONTABO-40021	100	Remcos, XWorm, AdaptixC2...	11

BulletProof Hosting

ASN	Provider			IPs
AS401116	NYBULA	100	Cobalt Strike, Remcos, XWorm...	66
AS51167	Contabo GmbH	100	Cobalt Strike, Remcos, XWorm...	44
AS36352	[illegible]	100	Cobalt Strike, [illegible]emcos, XWorm...	196
AS14061	DIGITALOCEAN-ASN	100	Cobalt Strike, PoshC2, Remcos...	118
AS132203	Tencent Building, Kejizhongyi Avenue	100	Cobalt Strike, XWorm, AdaptixC2...	38
AS9009	M247 Europe SRL	100	Cobalt Strike, Unknown RAT, Remcos...	150
AS396982	GOOGLE-CLOUD-PLATFORM	100	Cobalt Strike, Formbook, Unknown RAT...	47
AS213230, AS24940	Hetzner Online GmbH	100	Cobalt Strike, Unknown RAT, magecart...	169
AS8075	MICROSOFT-CORP-MSN-AS-BLOCK	100	Cobalt Strike, PoshC2, Remcos...	46
AS40021	CONTABO-40021	100	Remcos, XWorm, AdaptixC2...	11

Looking at information in the source CSV to show the value of the web interface

```
→ infrastructure_files cat * | grep "396982"
```

BulletProof Hosting

Findings up to date at time of presentation

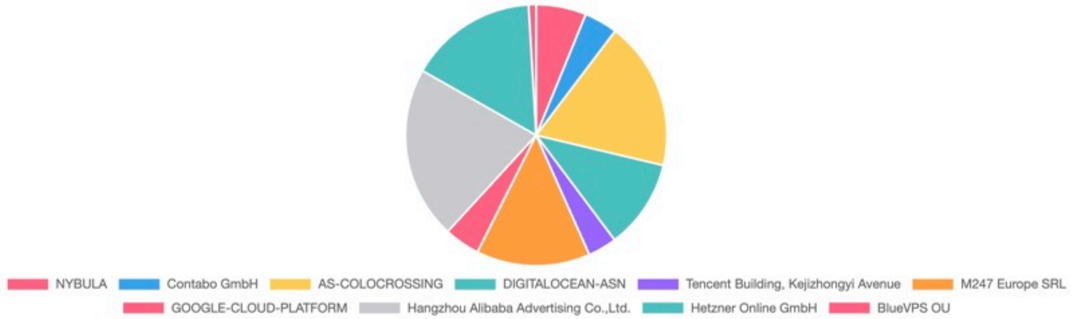
Various Findings

Infrastructure Reuse Patterns

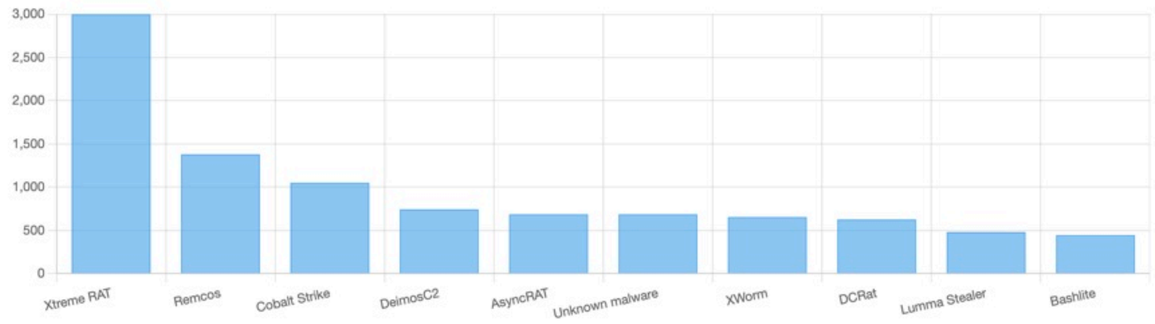
43,634 IOCs across 32 malware types

- 📊 43,634 IOCs analyzed across 32 malware types
- 🔴 15,102 malicious IOCs identified
- 🌐 5,357 unique malicious IPs discovered
- 🔄 3.3% IP reuse rate (infrastructure recycling)
- 📡 39.8% ASN reuse rate (provider patterns)
- 🔗 20 IPs serve multiple malware types
- 🏢 830 unique ASNs hosting malicious infrastructure

Infrastructure Distribution



Family Activity Trends



Risk Assessment

100

Overall Risk Score

20	0	0
High Risk	Medium Risk	Low Risk

Infrastructure Correlations

328

Shared ASNs

2.2

Avg Families per ASN

Infrastructure Sharing Level

Predictive Insights

100%

Prediction Confidence

20	15
ASN Predictions	Country Predictions

Ready for Deployment

Top ASNs by Activity

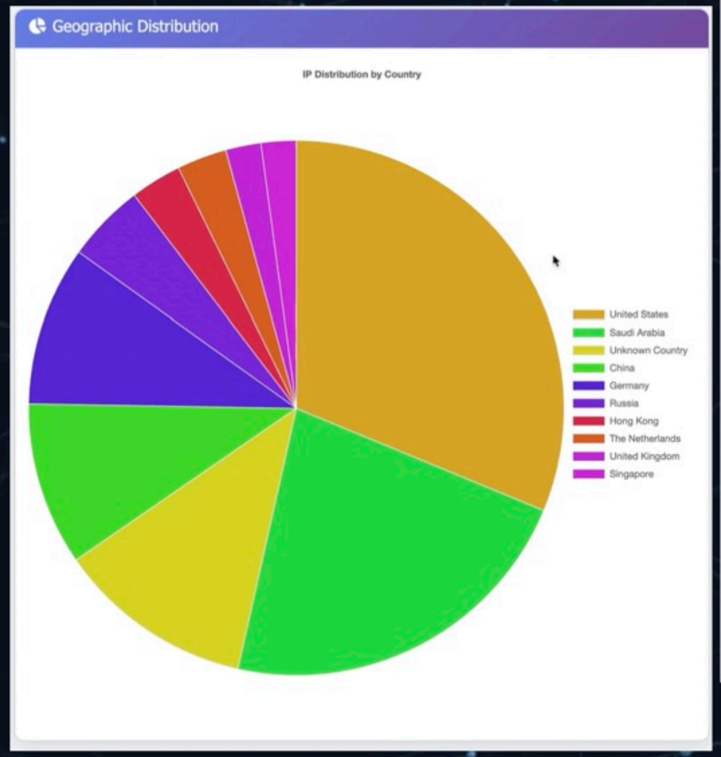
ASN	Provider	IPs	Families	Score
AS401116	NYBULA	66	13	100
AS51167	Contabo GmbH	44	11	100
AS36352	AS-COLOCROSSING	196	17	100
AS14061	DIGITALOCEAN-ASN	118	16	100
AS132203	Tencent Building, Kejizhongyi Avenue	38	8	100
AS9009	M247 Europe SRL	150	15	100
AS396982	GOOGLE-CLOUD-PLATFORM	47	13	100
AS37963	Hangzhou Alibaba Advertising Co.,Ltd.	228	13	100

Most Active Families

Family	IOCs	IPs	ASNs	Countries
Xtreme RAT	2999	10	5	undefined
Remcos	1379	936	201	undefined
Cobalt Strike	1050	805	153	undefined
DeimosC2	742	696	156	undefined
AsyncRAT	685	314	137	undefined
Unknown malware	685	623	213	undefined
XWorm	653	236	123	undefined
DCRat	625	292	111	undefined

Geo Overview

20,034 IOCs across 32 malware types



Statistics

IPs Per Country

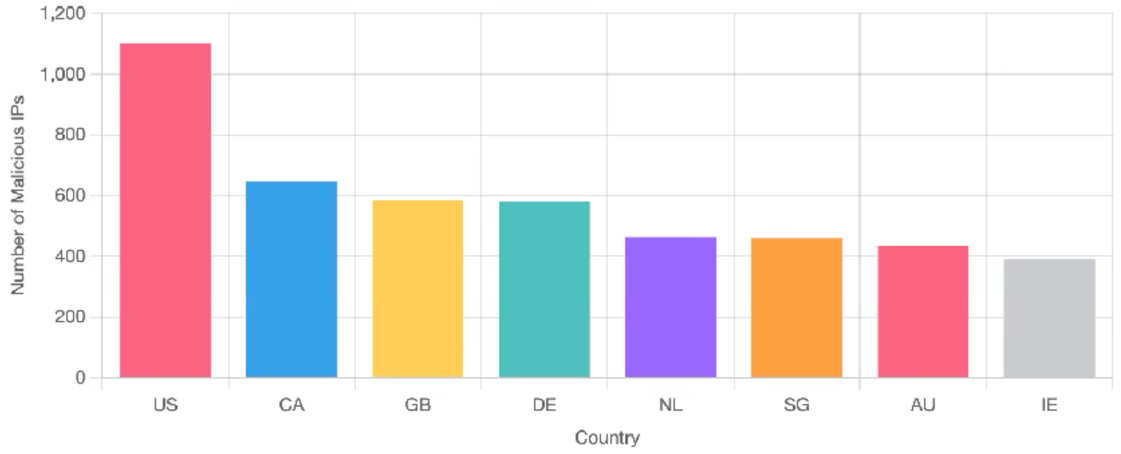
- United States: **5431** IPs
- Saudi Arabia: **3001** IPs
- Unknown Country: **1853** IPs
- China: **1493** IPs
- Germany: **1409** IPs
- Russia: **694** IPs
- The Netherlands: **521** IPs
- Hong Kong: **482** IPs
- United Kingdom: **369** IPs
- Seychelles: **357** IPs

Top “Bulletproof” Hosting Candidates

Suspicious Hosting Providers

ASN	Provider	Risk Score	Families	IPs
AS51167	Contabo GmbH	100	Bashlite, Remcos, Unknown malware...	44
AS36352	AS-COLOCROSSING	100	Bashlite, Venom RAT, MooBot...	196
AS14061	DIGITALOCEAN-ASN	100	Bashlite, MooBot, PoshC2...	118
AS132203	Tencent Building, Kejizhongyi Avenue	100	XWorm, Unknown malware, FatalRat...	38
AS9009	M247 Europe SRL	100	Bashlite, PureLogs Stealer, Remcos...	150
AS396982	GOOGLE-CLOUD-PLATFORM	100	MooBot, Remcos, Unknown malware...	47
AS37963	Hangzhou Alibaba Advertising Co.,Ltd.	100	Xtreme RAT, MooBot, Remcos...	228
AS213230, AS24940	Hetzner Online GmbH	100	Bashlite, magecart, Venom RAT...	169
AS62005	BlueVPS OU	100	Bashlite, Unknown malware, AdaptixC2...	10
AS8075	MICROSOFT-CORP-MSN-AS-BLOCK	100	PoshC2, Remcos, Unknown malware...	46

Geographic Distribution Chart



Geographic Distribution

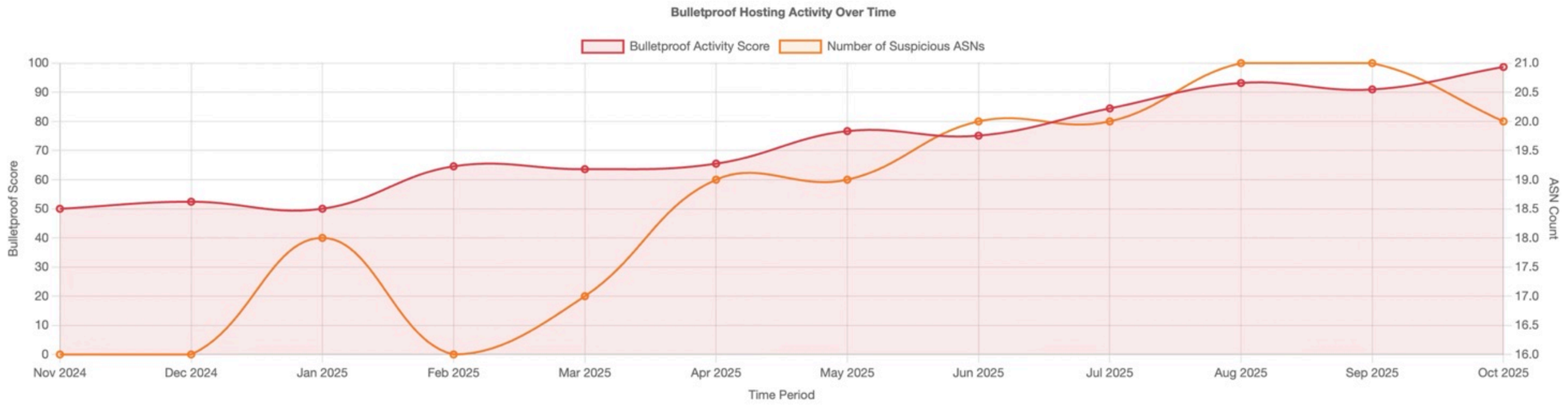
10

Countries with suspicious hosting

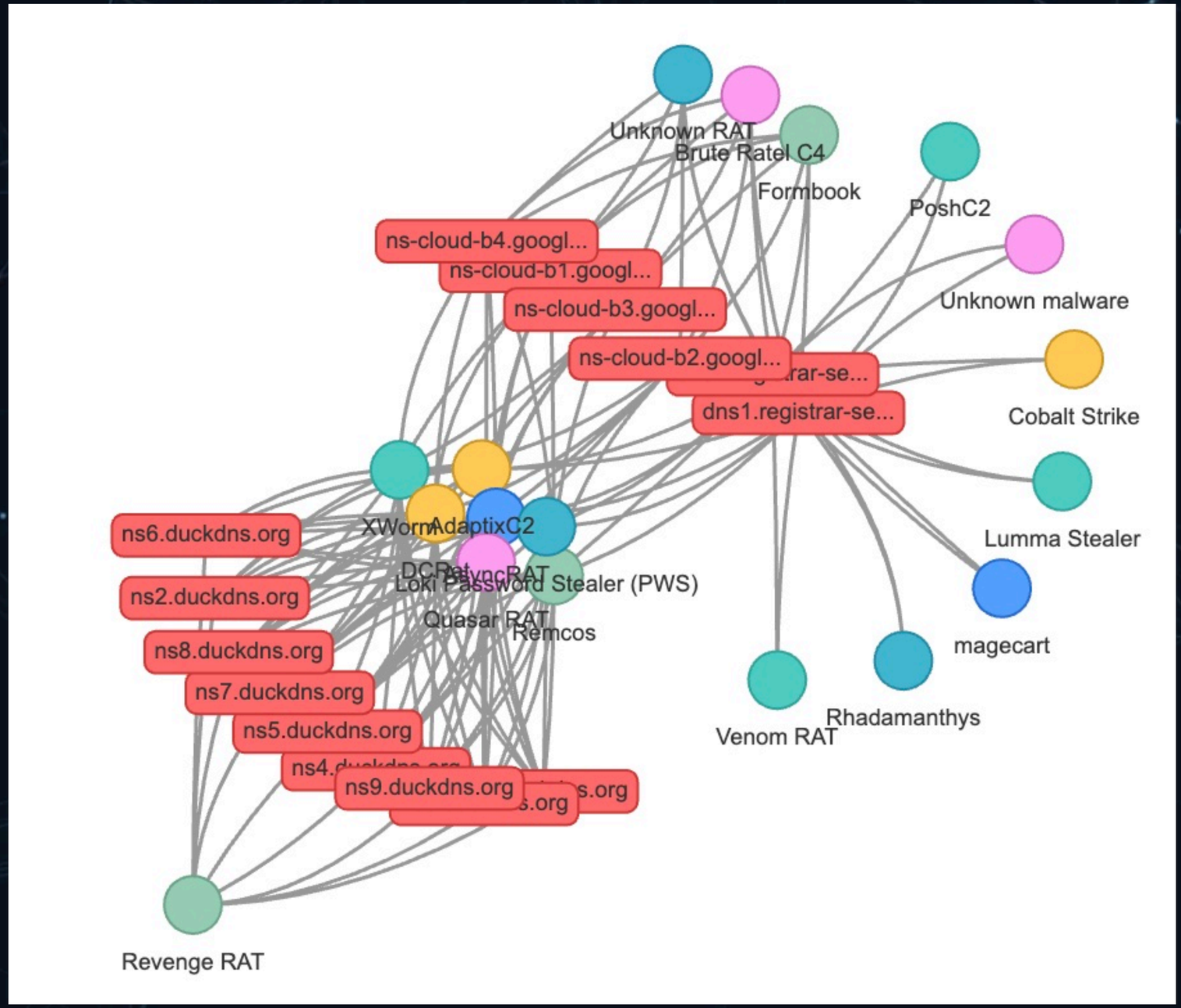
US	14 ASNs
GB	9 ASNs
NL	9 ASNs
DE	7 ASNs
CA	7 ASNs
SG	6 ASNs
AU	5 ASNs
IN	5 ASNs
JP	5 ASNs
FR	4 ASNs

... and 30 more

Bulletproof Hosting Evolution Timeline



NS Relationships



NS Relationships

Nameserver	Shared Families	Families	Shared Domains
dns1.registrar-servers.com	14	PoshC2 Rhadamanthys Formbook +11 more	48
dns2.registrar-servers.com	14	PoshC2 Rhadamanthys Formbook +11 more	48
ns1.duckdns.org	8	XWorm AdaptixC2 Revenge RAT +5 more	173
ns2.duckdns.org	8	XWorm AdaptixC2 Revenge RAT +5 more	173
ns3.duckdns.org	8	XWorm AdaptixC2 Revenge RAT +5 more	173
ns4.duckdns.org	8	XWorm AdaptixC2 Revenge RAT +5 more	173
ns5.duckdns.org	8	XWorm AdaptixC2 Revenge RAT +5 more	173
ns6.duckdns.org	8	XWorm AdaptixC2 Revenge RAT +5 more	173
ns7.duckdns.org	8	XWorm AdaptixC2 Revenge RAT +5 more	173
ns8.duckdns.org	8	XWorm AdaptixC2 Revenge RAT +5 more	173
ns9.duckdns.org	8	XWorm AdaptixC2 Revenge RAT +5 more	173
ns-cloud-b1.googledomains.com	8	XWorm Formbook Unknown RAT +5 more	50
ns-cloud-b2.googledomains.com	8	XWorm Formbook Unknown RAT +5 more	50
ns-cloud-b3.googledomains.com	8	XWorm Formbook Unknown RAT +5 more	50
ns-cloud-b4.googledomains.com	8	XWorm Formbook Unknown RAT +5 more	50
ns1.playit-dns.com	8	XWorm Quasar RAT RedLine Stealer +5 more	180
ns2.playit-dns.com	8	XWorm Quasar RAT RedLine Stealer +5 more	180
ns1.playit.cloud	8	XWorm Quasar RAT RedLine Stealer +5 more	179
ns67.domaincontrol.com	8	XWorm Quasar RAT RedLine Stealer +5 more	179
ns68.domaincontrol.com	8	XWorm Quasar RAT RedLine Stealer +5 more	179


Using
Predict

Cross-Family Infrastructure Examples

IPs Serving Multiple Malware Families

104.21.112.1 → RAT + Post-Exploitation + Social_Engineering + Infostealer

104.21.16.1 → RAT + Post-Exploitation + Social_Engineering + Infostealer

104.21.32.1 → RAT + Post-Exploitation + Social_Engineering + Infostealer

104.21.48.1 → RAT + Post-Exploitation + Social_Engineering + Infostealer

104.21.64.1 → RAT + Post-Exploitation + Social_Engineering + Infostealer

The Soft Block…

Not quite blocking

Potentially Malicious Endpoints

Soft Block Recommendations

High-Risk Infrastructure

10 High-Risk ASNs require monitoring

15 Suspicious Network Ranges identified

Soft Block Recommendations

Top Priority ASNs

Hangzhou Alibaba Advertising Co.,Ltd. (Score: 248.5)

Hetzner Online GmbH (Score: 230.8)

CLOUDFLARENET (Score: 230.2)

Shenzhen Tencent Computer Systems Company Limited (Score: 185.4)

AS-COLOCROSSING (Score: 159.3)

Soft Block Recommendations

Monitoring Rules

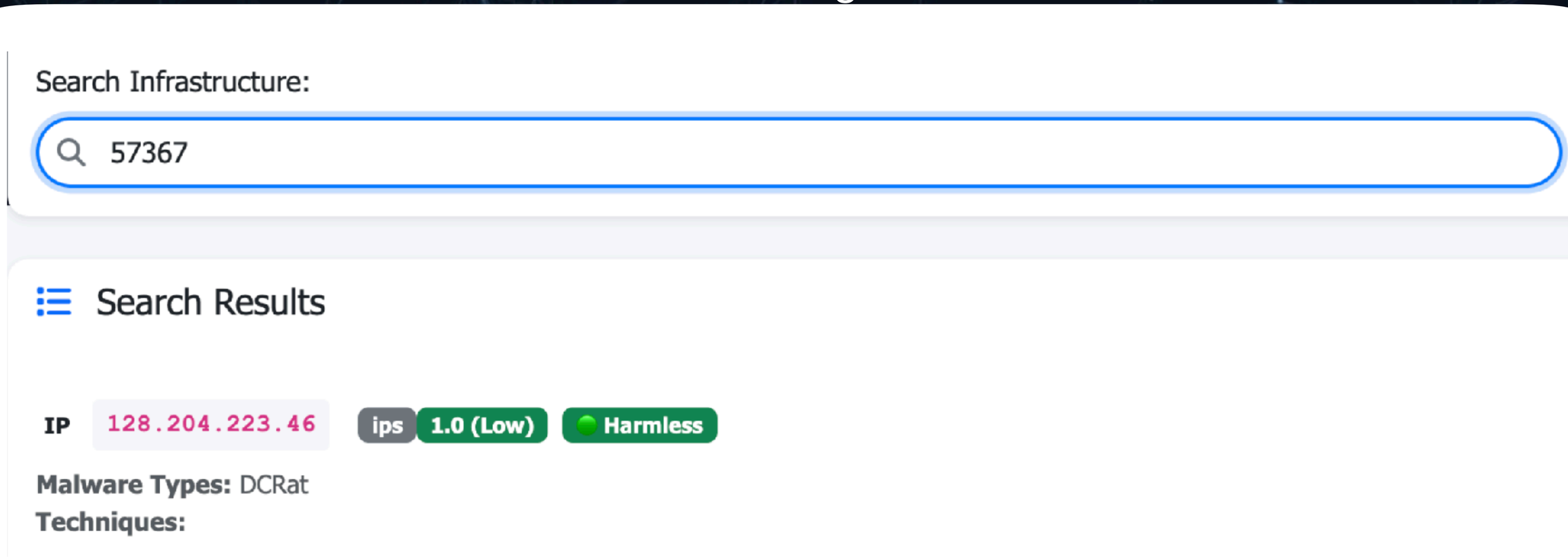
If beacon destination is in high-risk ASN → SOFT_BLOCK

If beacon destination is in suspicious network range → SOFT_BLOCK

If beacon destination matches historical malware IP pattern → SOFT_BLOCK

ASN Search

ASN for IP associated with DCRat that is benign



Malicious IPs on one ASN (BulletProof Hoster) Compared to Google ASN

Search Infrastructure:

42708

Search Results

IP 46.246.12.7 ips 100.0 (Critical) Malicious
Malware Types: DCRat
Techniques: H01

IP 46.246.6.14 ips 100.0 (Critical) Malicious
Malware Types: DCRat
Techniques: H01

IP 46.246.86.6 ips 100.0 (Critical) Malicious
Malware Types: DCRat
Techniques: H01

IP 46.246.6.16 ips 100.0 (Critical) Malicious
Malware Types: DCRat
Techniques: H01

IP 46.246.82.12 ips 100.0 (Critical) Malicious
Malware Types: DCRat
Techniques: H01

IP 46.246.82.2 ips 100.0 (Critical) Malicious

Search Infrastructure:

15169

Search Results

IP 8.8.8.8 ips 100.0 (Critical) Harmless
Malware Types: DCRat
Techniques:

IP 142.250.107.84 ips 100.0 (Critical) Harmless
Malware Types: DCRat
Techniques:

IP 173.194.202.94 ips 100.0 (Critical) Harmless
Malware Types: DCRat
Techniques:

IP 192.178.163.100 ips 100.0 (Critical) Harmless
Malware Types: DCRat
Techniques:

IP 192.178.163.101 ips 100.0 (Critical) Harmless
Malware Types: DCRat
Techniques:

IP 192.178.163.102 ips 100.0 (Critical) Harmless
Malware Types: DCRat
Techniques:

URL/Domain Search

DCRat Exact URL

Search Infrastructure:

http://a1167258.xsph.ru/cc3a74f8.php

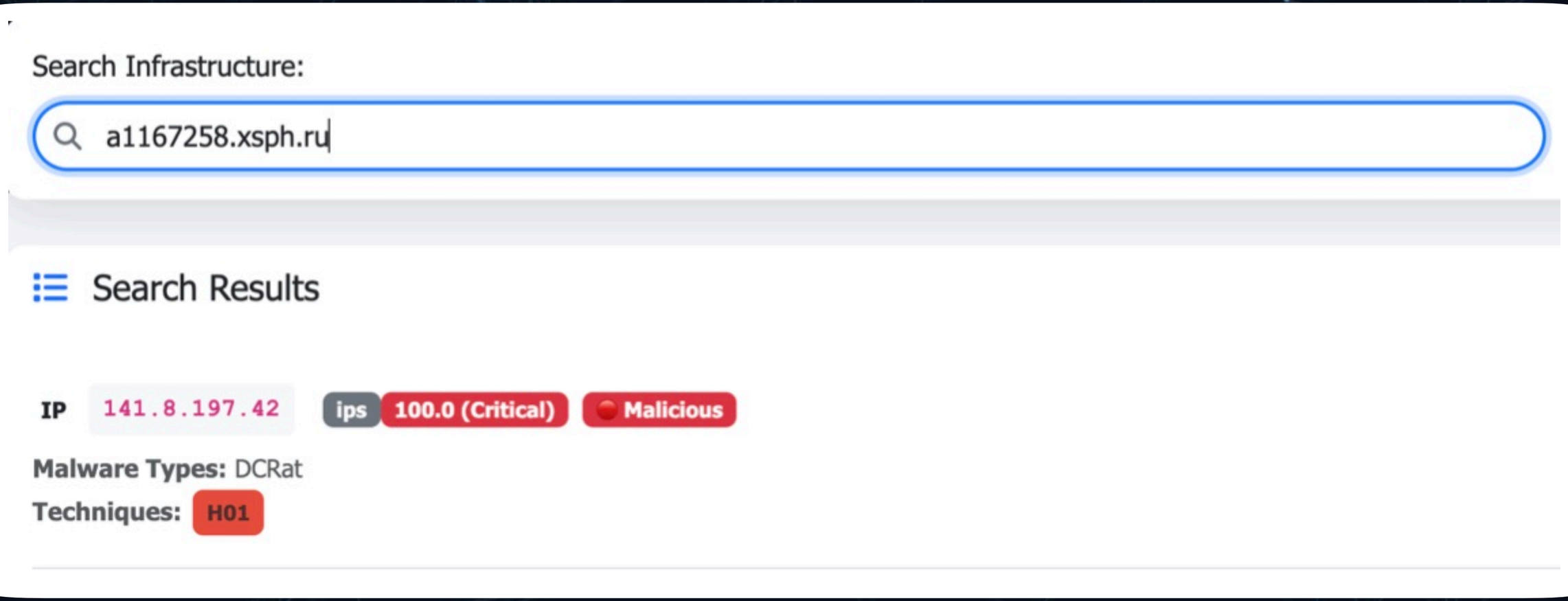
Search Results

IP 141.8.197.42 ips 100.0 (Critical) Malicious

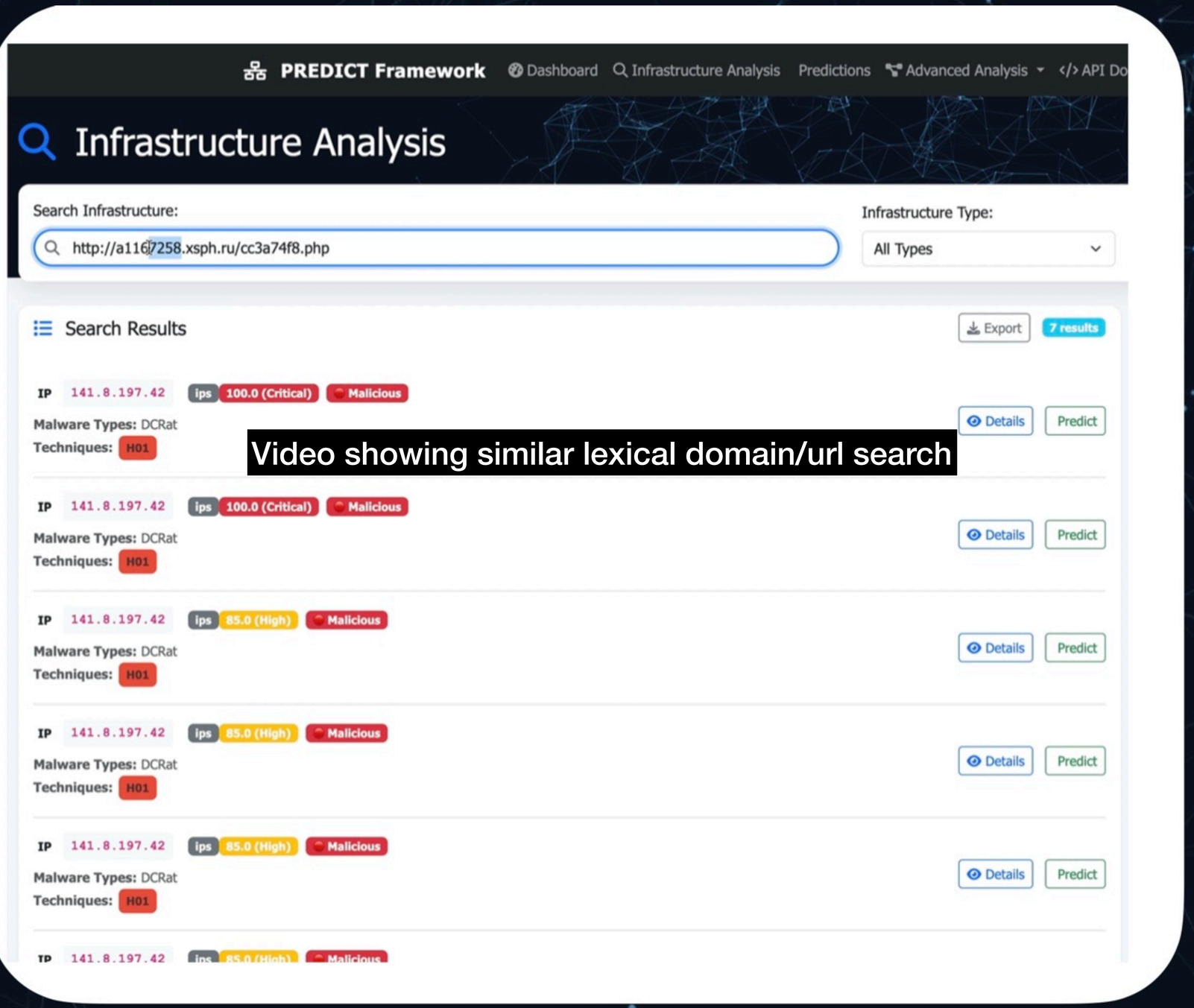
Malware Types: DCRat

Techniques: H01

DCRat Exact domain

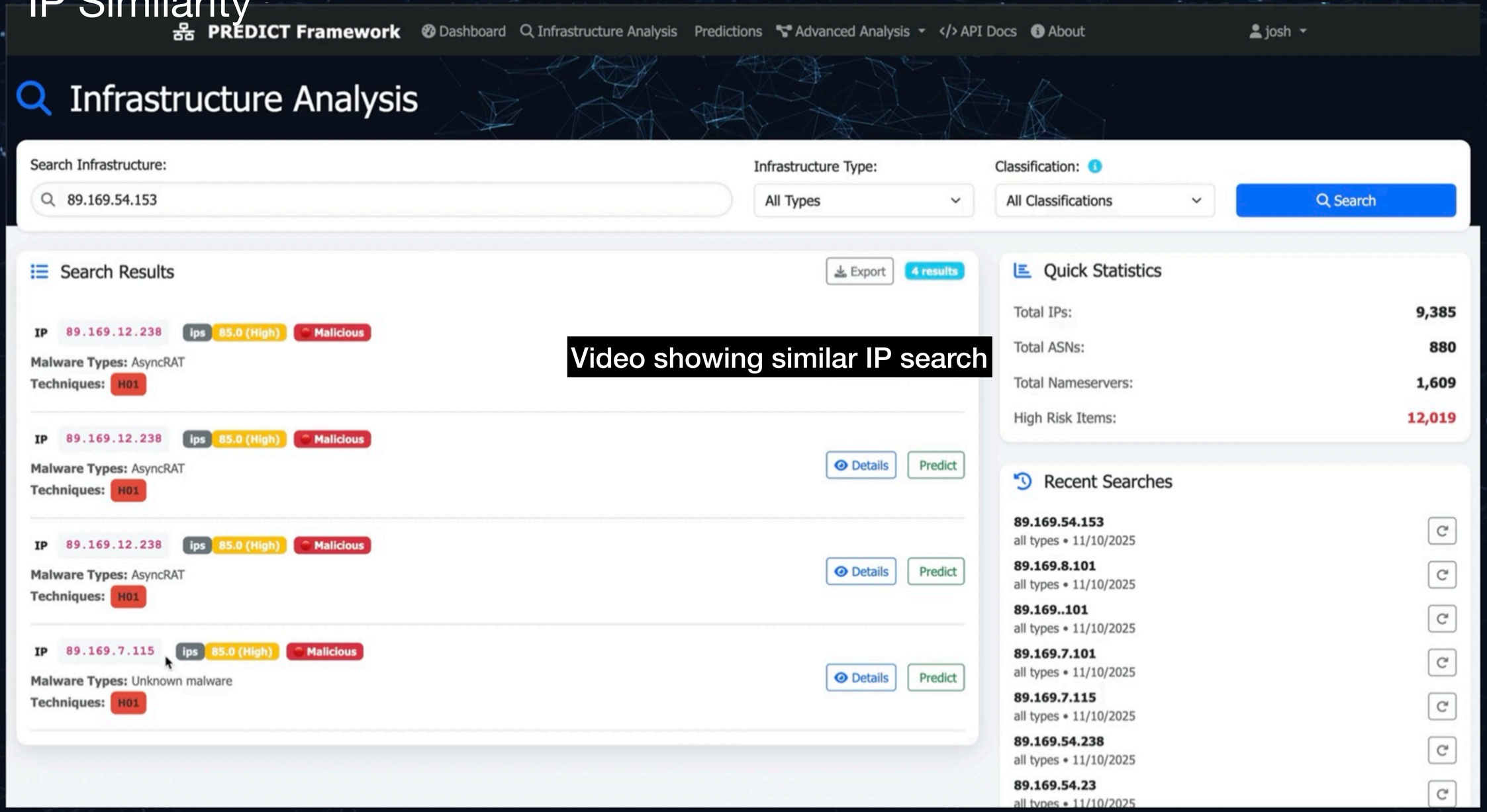


URL/Domain Similarities



- **IP Relationships**

IP Similarity



Other Ways to Use Relationship Data

- **XDR**
- **Stored Passive DNS**
- **Active DNS Queries**

XDR

TRILLION!

1,033,772,959,529 Total XDR Events

25,606,206 associated with malicious infrastructure (.002477% of total events)

TRILLION!

1,033,772,959,529 Total XDR Events

25,606,206 associated with malicious infrastructure (.002477% of total events)

Row Labels
104.21.112.1
["Social_Engineering","Unknown","Infostealer","RAT"]
104.21.16.1
["Unknown","RAT","Infostealer","Social_Engineering"]
104.21.32.1
["Unknown","Social_Engineering","RAT","Infostealer"]
104.21.48.1
["RAT","Infostealer","Unknown","Social_Engineering"]
104.21.64.1
["Social_Engineering","Unknown","Infostealer","RAT"]
104.21.80.1
["Unknown","Social_Engineering","RAT","Infostealer"]
104.21.96.1
["RAT","Unknown","Social_Engineering","Infostealer"]
13.248.169.48
["Infostealer","Unknown"]
15.197.148.33
["Unknown","Infostealer"]
162.159.36.2
["RAT","Infostealer"]
199.59.243.228
["Unknown"]

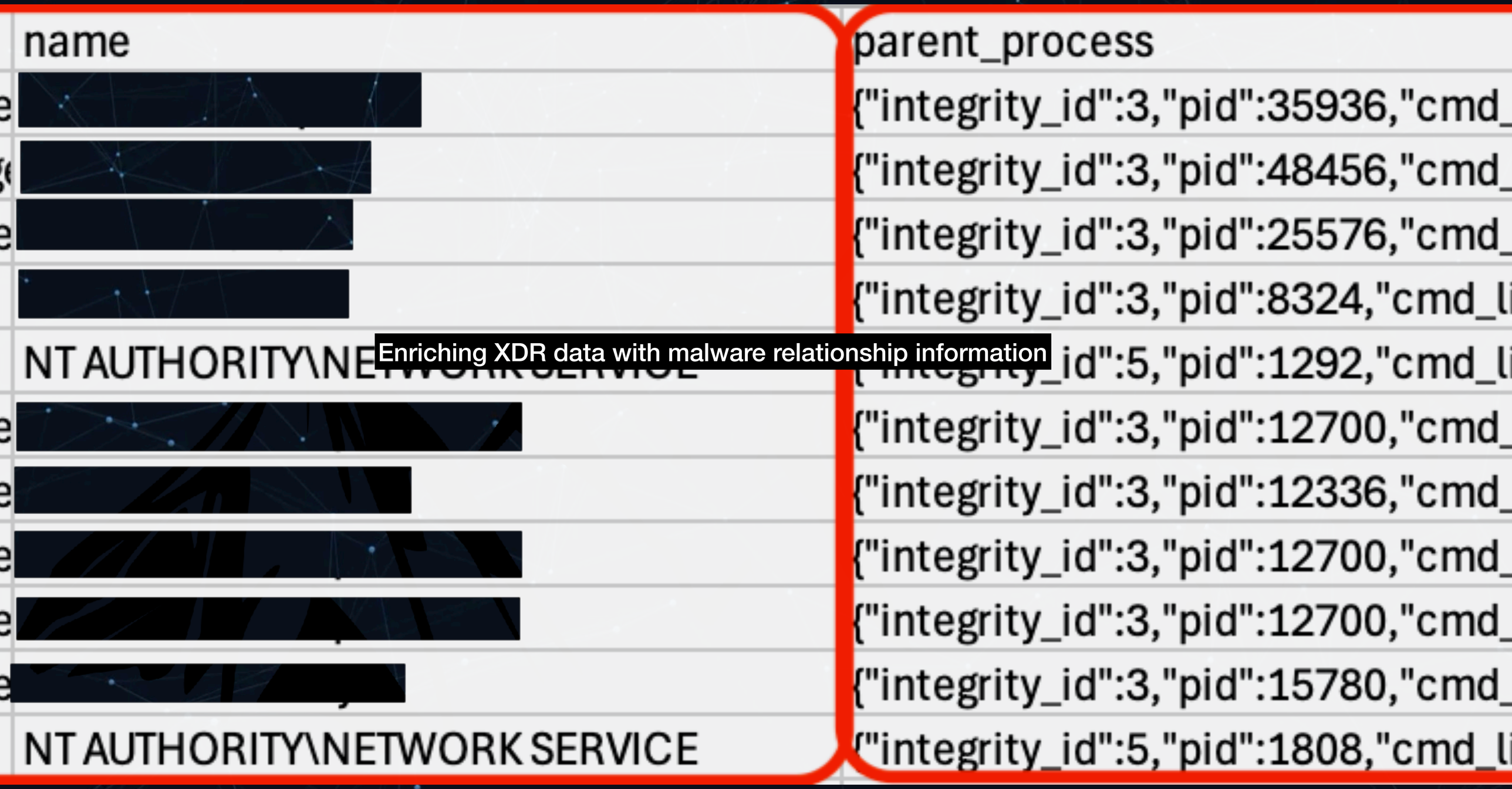
Grouped Destination IPs
and the malware they relate to

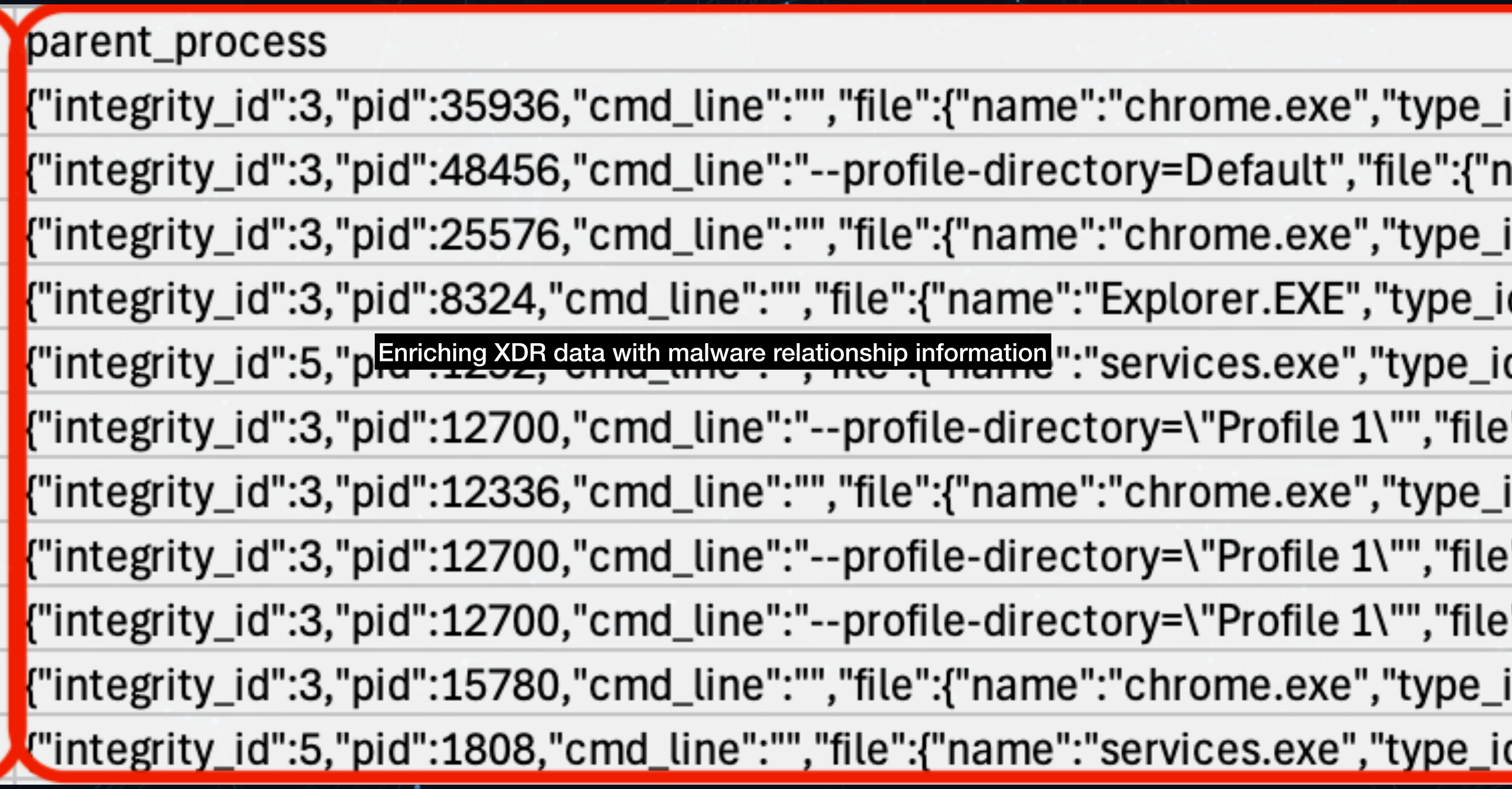
hostname	ip	port	owner
cdn-v2.reelup.io	104.21.48.1	443	null
www.dmcaforce.com	104.21.64.1	443	null
www.hiveworkshop.com	104.21.112.1	443	null
clearout.io	104.21.96.1	443	null
		53	null
playcode.io	104.21.32.1	443	null
tagsrv.swayer.io	104.21.48.1	443	null
playcode.io	104.21.64.1	443	null
playcode.io	104.21.64.1	443	null
audienceexposure.com	199.59.243.2	443	null
	162.159.36.2	53	null

Enriching XDR data with malware relationship information

cmd_line	name	path
--type=utility	chrome.exe	C:\Program Files\Google\Chrome\Application\ch
--type=utility	msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Applicatio
--type=utility	chrome.exe	C:\Program Files\Google\Chrome\Application\ch
	firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
	svchost.exe	C:\Windows\System32\svchost.exe
--type=utility	chrome.exe	C:\Program Files\Google\Chrome\Application\ch
--type=utility	chrome.exe	C:\Program Files\Google\Chrome\Application\ch
--type=utility	chrome.exe	C:\Program Files\Google\Chrome\Application\ch
--type=utility	chrome.exe	C:\Program Files\Google\Chrome\Application\ch
--type=utility	chrome.exe	C:\Program Files\Google\Chrome\Application\ch
#NAME?	svchost.exe	C:\Windows\System32\svchost.exe

Enriching XDR data with malware relationship information


name
parent_process
{"integrity_id":3,"pid":35936,"cmd_
{"integrity_id":3,"pid":48456,"cmd_
{"integrity_id":3,"pid":25576,"cmd_
{"integrity_id":3,"pid":8324,"cmd_l
Enriching XDR data with malware relationship information
id":5,"pid":1292,"cmd_l
{"integrity_id":3,"pid":12700,"cmd_
{"integrity_id":3,"pid":12336,"cmd_
{"integrity_id":3,"pid":12700,"cmd_
{"integrity_id":3,"pid":12700,"cmd_
{"integrity_id":3,"pid":15780,"cmd_
NT AUTHORITY\NETWORK SERVICE
{"integrity_id":5,"pid":1808,"cmd_l



Enriching XDR data with malware relationship information

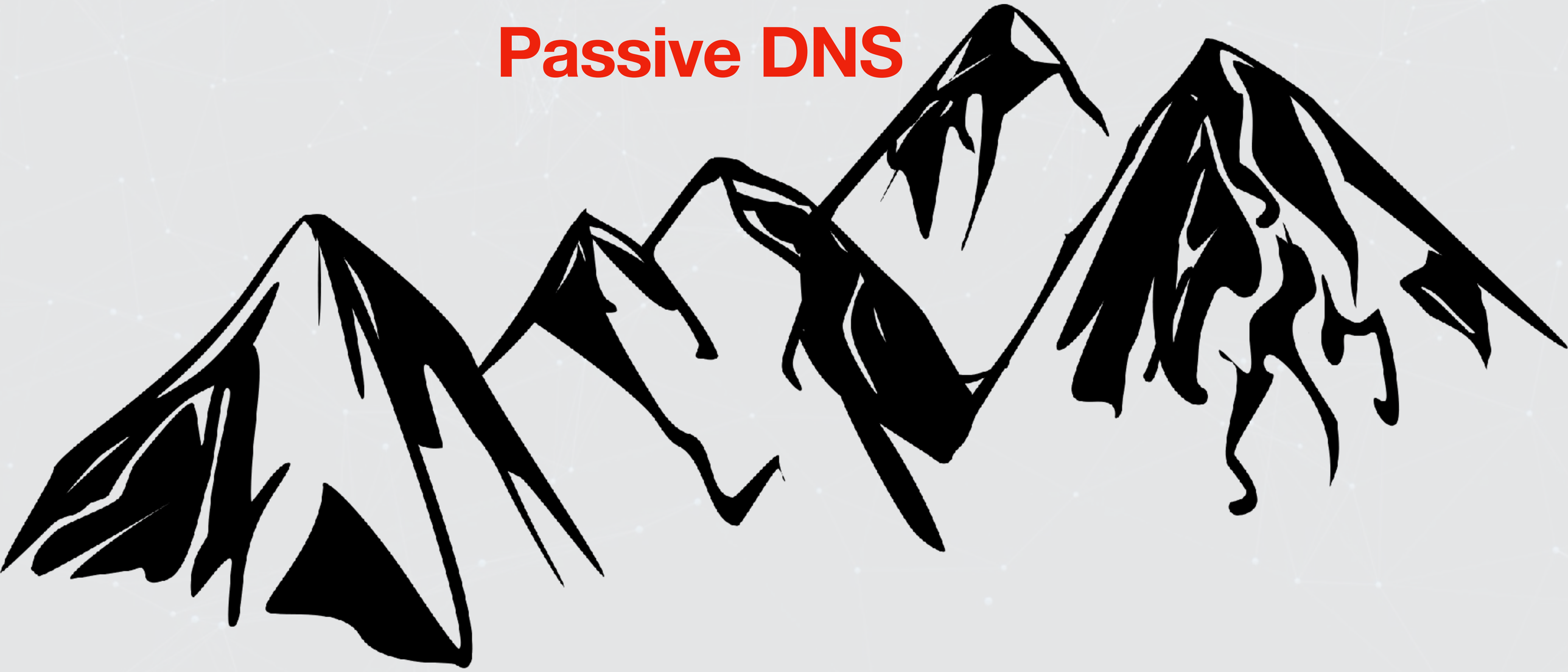
malware_ip_	malware_ip_	malware_ip_families	m
275	critical	["RAT","Infostealer","Unknown","Social_Engineering	
269	critical	["Social_Engineering","Unknown","Infostealer","RAT	
272	critical	["Social_Engineering","Unknown","Infostealer","RAT	
270	critical	["RAT","Unknown","Social_Engineering","Infostealer	
61	critical	["RAT","Infostealer"]	
279	critical	["Unknown","Social_Engineering","RAT","Infostealer	
275	critical	["RAT","Infostealer","Unknown","Social_Engineering	
269	critical	["Social_Engineering","Unknown","Infostealer","RAT	
269	critical	["Social_Engineering","Unknown","Infostealer","RAT	
14	medium	["Unknown"]	
61	critical	["RAT","Infostealer"]	

Enriching XDR data with malware relationship information

	malware_ip_	malware_ma	malware_hig	malware_is_suspicious	
l_Engineering	4	275	critical	TRUE	
stealer","RAT	4	269	critical	TRUE	
stealer","RAT	4	272	critical	TRUE	
g","Infostealer	4	270	critical	TRUE	
	2	61	critical	TRUE	
r","Infostealer	4	279	critical	TRUE	
l_Engineering	4	275	critical	TRUE	
stealer","RAT	4	269	critical	TRUE	
stealer","RAT	4	269	critical	TRUE	
	1	14	medium	TRUE	
	2	61	critical	TRUE	

Enriching XDR data with malware relationship information

Passive DNS



BILLION!

48,813,835,544 Total Passive DNS of Newly Seen Domains

3,369,173,682 associated with malicious infrastructure (6.90%)

```
4 display(pdns_tree.limit(5))
```

▸ (1) Spark Jobs

▸ pdns_tree: pyspark.sql.connect.dataframe.DataFrame = [hourstamp: long, domain: string ... 5 more fields]

Table +

	type	rr	name	name_server	name_server_backup
2	-0-0-0-0-0-0-0-57-0-0-0-0-0-0-0-0-0-0-0-0-0-0-0.info	A	54.85.87.184	0-0-2-3-4-1-7-4-5-4-6-4-4-1-6-2-0-7-3-0-4-7-0-7-1-8-0-3-1-7-1-.0-0-0-0-0-0-0-0-0-0-0-0-0-57-0-0-0-0-0-0-0-0...	ns3.csof.net.	null
3	-0-0-0-0-0-0-0-57-0-0-0-0-0-0-0-0-0-0-0-0-0-0-0.info	A	54.85.87.184	0-0-3-0-6-0-1-3-3-5-3-1-3-7-1-4-0-1-5-5-0-5-0-0-2-4-5-3-3-3-6-.0-0-0-0-0-0-0-0-0-0-0-0-0-57-0-0-0-0-0-0-0-0...	ns1.csof.net.	null
4		AAAA	2a00:d70:0:b:2002:0:d91a:3650	0-100-0.ch.	ns3.hostpoint.ch.	null
5	s.net	TXT	"v=spf1 include:mx.ovh.com ~all"	0-100editions.net.	dns110.ovh.net.	null

▶ ✓ 11:27 AM (9s) 11 SQL

```
1 %sql
2 select * from enriched_pdns_tree
3 where malware_is_suspicious = 'true'
```

▸ (3) Spark Jobs

▸ _sqldf: pyspark.sql.connect.dataframe.DataFrame = [hourstamp: long, domain: string ... 18 more fields]

Table +

Enriching passive DNS data with malware relationship information

	hourstamp	domain	type	rr	name	name_server	name_server_backup	malware_ip_score	malware_ip_risk	malware_ip_families
1	1752537600	000027s.cn	A	104.21.112.1	exyeczwflyn.000027s.cn.	albert.ns.cloudflare.com.	null	272	critical	["Social_Engineering","Unknown","I
2	1752537600	000027s.cn	A	104.21.112.1	pexiby.000027s.cn.	marissa.ns.cloudflare.com.	null	272	critical	["Social_Engineering","Unknown","I
3	1752537600	000027s.cn	A	104.21.112.1	zydkmi.000027s.cn.	albert.ns.cloudflare.com.	null	272	critical	["Social_Engineering","Unknown","I
4	1752537600	000027s.cn	A	104.21.16.1	exyeczwflyn.000027s.cn.	albert.ns.cloudflare.com.	null	279	critical	["Unknown","RAT","Infostealer","So
5	1752537600	000027s.cn	A	104.21.16.1	pexiby.000027s.cn.	marissa.ns.cloudflare.com.	null	279	critical	["Unknown","RAT","Infostealer","So
6	1752537600	000027s.cn	A	104.21.16.1	zydkmi.000027s.cn.	albert.ns.cloudflare.com.	null	279	critical	["Unknown","RAT","Infostealer","So
7	1752537600	000027s.cn	A	104.21.32.1	exyeczwflyn.000027s.cn.	albert.ns.cloudflare.com.	null	279	critical	["Unknown","Social_Engineering","I
8	1752537600	000027s.cn	A	104.21.32.1	pexiby.000027s.cn.	marissa.ns.cloudflare.com.	null	279	critical	["Unknown","Social_Engineering","I
9	1752537600	000027s.cn	A	104.21.32.1	zydkmi.000027s.cn.	albert.ns.cloudflare.com.	null	279	critical	["Unknown","Social_Engineering","I
10	1752537600	00006018.com	A	15.197.148.33	00006018.com.	ns35.domaincontrol.com.	null	77	critical	["Unknown","Infostealer"]
11	1752537600	000lf.shop	A	13.248.213.45	000lf.shop.	ns75.domaincontrol.com.	null	19	medium	["Unknown"]
12	1752537600	0033.xyz	A	13.248.169.48	0033.xyz.	ns2.afternic.com.	null	107	critical	["Infostealer","Unknown"]
13	1752537600	005.ai	A	13.248.169.48	*.005.ai.	ns2.dan.com.	null	107	critical	["Infostealer","Unknown"]
14	1752537600	005.ai	A	13.248.169.48	test.005.ai.	ns2.dan.com.	null	107	critical	["Infostealer","Unknown"]

Active Monitoring

Logs, DNS, etc

Active Monitoring

Logs, DNS, etc

```
Nov  2 00:29:17 dnsmasq[16371]: cached 1337x.to is 2606:4700:3035::6815:28c1
Nov  2 00:29:17 dnsmasq[16371]: cached 1337x.to is 2606:4700:3032::ac43:bc43
Nov  2 00:29:17 dnsmasq[16371]: reply apibay.org is 104.21.62.171
Nov  2 00:29:17 dnsmasq[16371]: reply apibay.org is 172.67.137.143
Nov  2 00:29:17 dnsmasq[16371]: reply apibay.org is 2606:4700:3037::6815:3eab
Nov  2 00:29:17 dnsmasq[16371]: reply apibay.org is 2606:4700:3033::ac43:898f
Nov  2 00:29:17 dnsmasq[16371]: reply 1337x.to is 104.21.40.193
Nov  2 00:29:17 dnsmasq[16371]: reply 1337x.to is 172.67.188.67
Nov  2 00:30:00 dnsmasq[16371]: failed to send UDP request: Network unreachable
Nov  2 00:30:00 dnsmasq[16371]: failed to send UDP request: Network unreachable
Nov  2 00:40:29 dnsmasq[16371]: failed to send UDP request: Network unreachable
Nov  2 00:40:29 dnsmasq[16371]: failed to send UDP request: Network unreachable
Nov  2 00:45:20 dnsmasq[16371]: query[A] acg.rip from 192.168.1.24
Nov  2 00:45:20 dnsmasq[16371]: cached-stale acg.rip is 194.127.164.6
Nov  2 00:45:20 dnsmasq[16371]: forwarded acg.rip to 208.67.220.220
Nov  2 00:45:20 dnsmasq[16371]: query[AAAA] acg.rip from 192.168.1.24
Nov  2 00:45:20 dnsmasq[16371]: cached-stale acg.rip is NODATA-IPv6
Nov  2 00:45:20 dnsmasq[16371]: forwarded acg.rip to 208.67.220.220
Nov  2 00:45:20 dnsmasq[16371]: query[A] eztvx.to from 192.168.1.24
Nov  2 00:45:20 dnsmasq[16371]: cached-stale eztvx.to is 172.67.194.150
Nov  2 00:45:20 dnsmasq[16371]: cached-stale eztvx.to is 104.21.68.109
Nov  2 00:45:20 dnsmasq[16371]: forwarded eztvx.to to 208.67.220.220
Nov  2 00:45:20 dnsmasq[16371]: query[AAAA] eztvx.to from 192.168.1.24
Nov  2 00:45:20 dnsmasq[16371]: cached-stale eztvx.to is 2606:4700:3033::6815:446d
                                ed-stale eztvx.to is 2606:4700:3031::ac43:c296
                                arded eztvx.to to 208.67.220.220
Nov  2 00:45:20 dnsmasq[16371]: query[A] apibay.org from 192.168.1.24
Nov  2 00:45:20 dnsmasq[16371]: cached-stale apibay.org is 104.21.62.171
Nov  2 00:45:20 dnsmasq[16371]: cached-stale apibay.org is 172.67.137.143
Nov  2 00:45:20 dnsmasq[16371]: forwarded apibay.org to 208.67.220.220
Nov  2 00:45:20 dnsmasq[16371]: query[AAAA] apibay.org from 192.168.1.24
Nov  2 00:45:20 dnsmasq[16371]: cached-stale apibay.org is 2606:4700:3037::6815:3eab
Nov  2 00:45:20 dnsmasq[16371]: cached-stale apibay.org is 2606:4700:3033::ac43:898f
Nov  2 00:45:20 dnsmasq[16371]: forwarded apibay.org to 208.67.220.220
Nov  2 00:45:20 dnsmasq[16371]: reply acg.rip is NODATA-IPv6
Nov  2 00:45:20 dnsmasq[16371]: reply acg.rip is 194.127.164.6
Nov  2 00:45:20 dnsmasq[16371]: reply eztvx.to is 104.21.68.109
Nov  2 00:45:20 dnsmasq[16371]: reply eztvx.to is 172.67.194.150
Nov  2 00:45:20 dnsmasq[16371]: reply eztvx.to is 2606:4700:3031::ac43:c296
Nov  2 00:45:20 dnsmasq[16371]: reply eztvx.to is 2606:4700:3033::6815:446d
Nov  2 00:45:20 dnsmasq[16371]: reply apibay.org is 104.21.62.171
Nov  2 00:45:20 dnsmasq[16371]: reply apibay.org is 172.67.137.143
Nov  2 00:45:20 dnsmasq[16371]: reply apibay.org is 2606:4700:3033::ac43:898f
Nov  2 00:45:20 dnsmasq[16371]: reply apibay.org is 2606:4700:3037::6815:3eab
Nov  2 00:45:50 dnsmasq[16371]: query[A] diag.meethue.com from 192.168.1.17
Nov  2 00:45:50 dnsmasq[16371]:
```

Live monitoring of a networks DNS traffic

```
2025-11-02 22:46:57,221 - elastic_transport.transport - INFO - HEAD http://localhost:9200/predict-results [status:200 duration:0.004s]
2025-11-02 22:46:57,221 - __main__ - INFO - Parsing DNS log file...

Extracted IOCs from DNS log:
  - Domains: 13
  - IPs: 30

Domains found: ping.ui.com, feed.flightradar24.com, 1337x.to, similardomain.bg, testbaddomain.com, nissi2.bg, rutracker.org, 2.pool.ntp.org, 1.pool.ntp.org, scrobbles.plex.tv
  ... and 3 more

IPs found: 35.172.142.61, 172.64.151.205, 104.18.98.112, 66.118.228.14, 67.217.246.204, 45.83.234.123, 137.110.222.27, 104.21.32.39, 162.159.200.1, 23.150.41.122
  ... and 20 more

============================================================
Performing API lookups for 43 unique IOCs...
============================================================
  ℹ  LOW-MEDIUM RISK: nissi2.bg (Similar: 1, Related: 1) | Malware: AdaptixC2
2025-11-02 22:46:57,284 - elastic_transport.transport - INFO - POST http://localhost:9200/predict-results/_doc [status:201 duration:0.002s]
2025-11-02 22:46:57,284 - __main__ - INFO - Indexed domain nissi2.bg - Matches: 0, Related: 1
  Progress: 10/43 IOCs processed...
  ℹ  LOW RISK: nissi.bg (Exact: 1, Similar: 20, Related: 37) | Malware: AdaptixC2, Bashlite, BlackCat Ransomware
2025-11-02 22:46:57,327 - elastic_transport.transport - INFO - POST http://localhost:9200/predict-results/_doc [status:201 duration:0.003s]
2025-11-02 22:46:57,327 - __main__ - INFO - Indexed domain nissi.bg - Matches: 1, Related: 37
  Progress: 20/43 IOCs processed...
  ▲  MEDIUM RISK: 104.167.215.195 (Exact: 0, Similar: 1, Related: 1) | Malware: AdaptixC2
2025-11-02 22:46:57,433 - elastic_transport.transport - INFO - POST http://localhost:9200/predict-results/_doc [status:201 duration:0.002s]
2025-11-02 22:46:57,433 - __main__ - INFO - Indexed ip 104.167.215.195 - Matches: 0, Related: 1
  Progress: 30/43 IOCs processed...
  ▲  MEDIUM RISK: 23.95.35.34 (Exact: 0, Similar: 2, Related: 2) | Malware: Bashlite
2025-11-02 22:46:57,487 - elastic_transport.transport - INFO - POST http://localhost:9200/predict-results/_doc [status:201 duration:0.002s]
2025-11-02 22:46:57,488 - __main__ - INFO - Indexed ip 23.95.35.34 - Matches: 0, Related: 2
  ⚠️  HIGH RISK: 128.199.219.80 (Exact: 1, Similar: 22, Related: 42) | Malware: AdaptixC2, Bashlite
2025-11-02 22:46:57,530 - elastic_transport.transport - INFO - POST http://localhost:9200/predict-results/_doc [status:201 duration:0.002s]
2025-11-02 22:46:57,530 - __main__
  Progress: 40/43 IOCs processed...
  Progress: 43/43 IOCs processed...

============================================================
Analysis Complete - Summary
============================================================
Total IOCs analyzed: 43
Found in PREDICT DB: 5
Not found: 38

Risk Distribution:
  - High Risk: 1
  - Medium Risk: 2
  - Low Risk: 1
  - Low-Medium Risk: 1

Elasticsearch Indexing:
  - Successfully indexed: 5
  - Failed to index: 0
2025-11-02 22:46:57,559 - elastic_transport.transport - INFO - POST http://localhost:9200/predict-results/_count [status:200 duration:0.002s]
2025-11-02 22:46:57,561 - elastic_transport.transport - INFO - POST http://localhost:9200/predict-results/_search [status:200 duration:0.002s]

Elasticsearch Index 'predict-results' Statistics:
  - Total documents: 25
  - Documents with API data: 25

✓ Results have been indexed to Elasticsearch index: 'predict-results'
✓ You can view them in Kibana at: http://localhost:5601
```

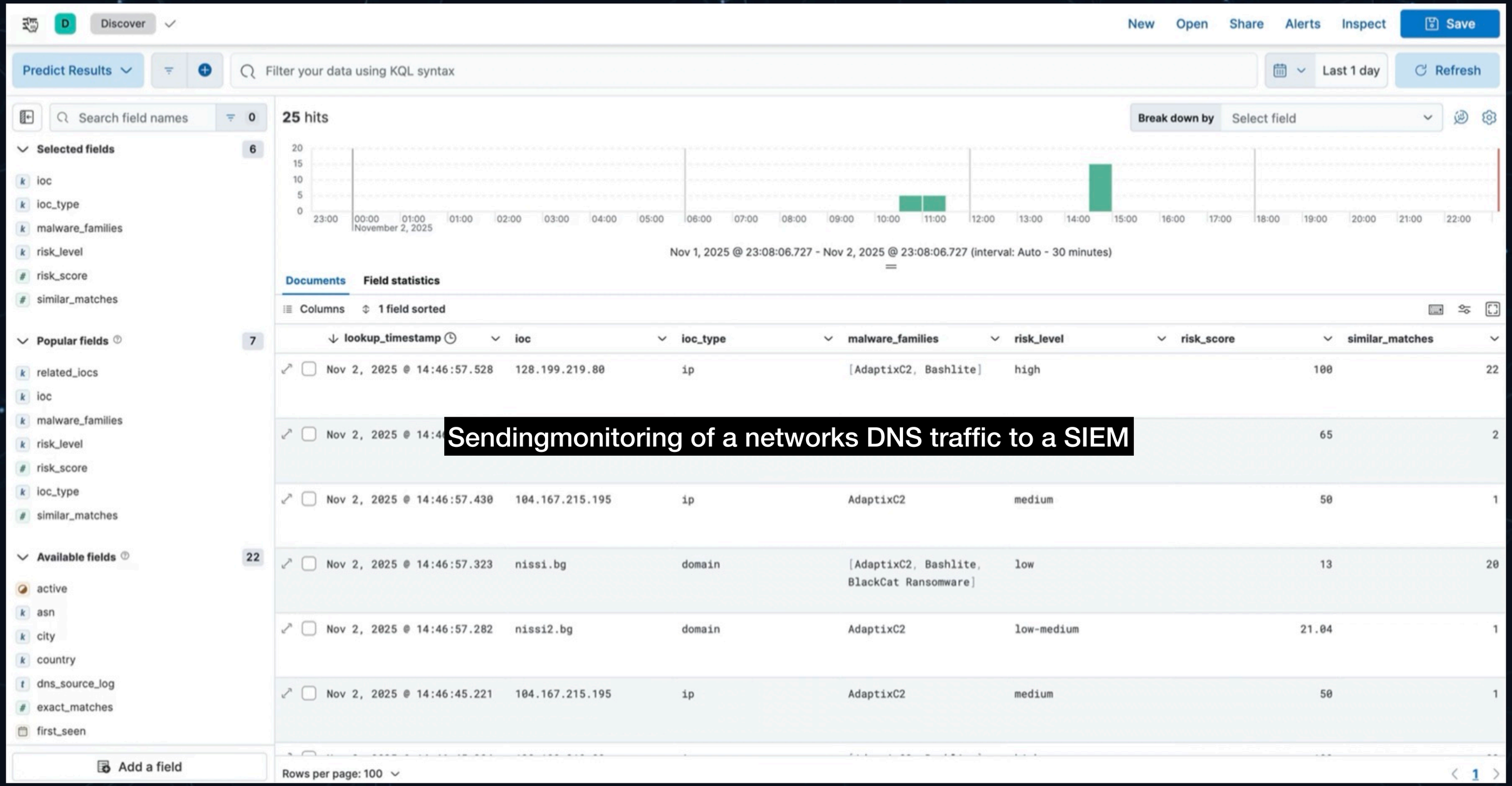
Live monitoring of a networks DNS traffic

Live monitoring of a networks DNS traffic

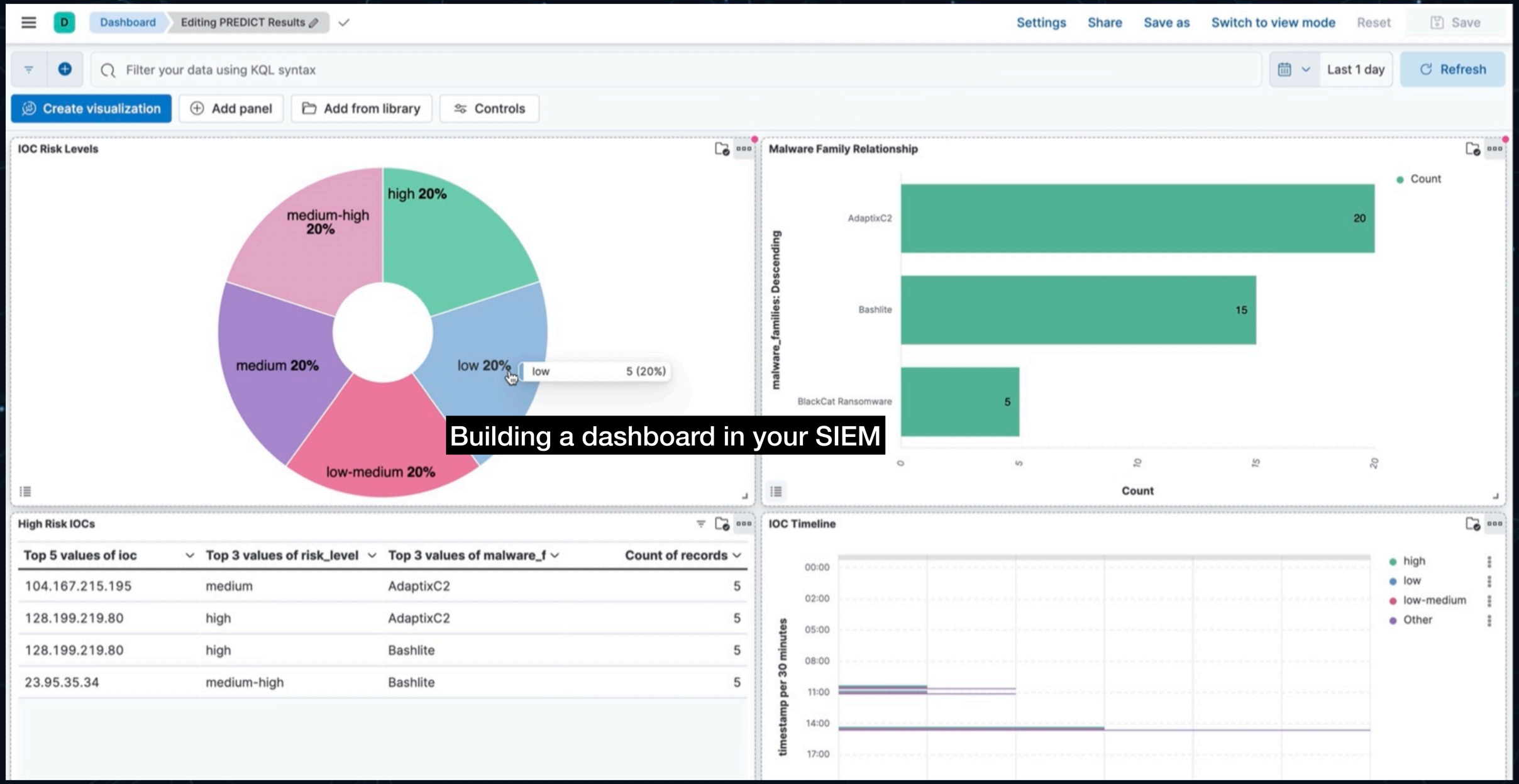
```
============================================================
Performing API lookups for 43 unique IOCs...
============================================================
  ℹ  LOW-MEDIUM RISK: nissi2.bg (Similar: 1, Related: 1) | Malware: AdaptixC2
2025-11-02 22:46:57,284 - elastic_transport.transport - INFO - POST http://localhost:9200/predict-results/_doc [status:201 duration:0.002s]
2025-11-02 22:46:57,284 - __main__ - INFO - Indexed domain nissi2.bg - Matches: 0, Related: 1
  Progress: 10/43 IOCs processed...
  ℹ  LOW RISK: nissi.bg (Exact: 1, Similar: 20, Related: 37) | Malware: AdaptixC2, Bashlite, BlackCat Ransomware
2025-11-02 22:46:57,327 - elastic_transport.transport - INFO - POST http://localhost:9200/predict-results/_doc [status:201 duration:0.003s]
2025-11-02 22:46:57,327 - __main__ - INFO - Indexed domain nissi.bg - Matches: 1, Related: 37
  Progress: 20/43 IOCs processed...
  ⚠  MEDIUM RISK: 104.167.215.195 (Exact: 0, Similar: 1, Related: 1) | Malware: AdaptixC2
2025-11-02 22:46:57,433 - elastic_transport.transport - INFO - POST http://localhost:9200/predict-results/_doc [status:201 duration:0.002s]
2025-11-02 22:46:57,433 - __main__ - INFO - Indexed ip 104.167.215.195 - Matches: 0, Related: 1
  Progress: 30/43 IOCs processed...
  ⚠  MEDIUM RISK: 23.95.35.34 (Exact: 0, Similar: 2, Related: 2) | Malware: Bashlite
2025-11-02 22:46:57,487 - elastic_transport.transport - INFO - POST http://localhost:9200/predict-results/_doc [status:201 duration:0.002s]
2025-11-02 22:46:57,488 - __main__ - INFO - Indexed ip 23.95.35.34 - Matches: 0, Related: 2
  ⚠️  HIGH RISK: 128.199.219.80 (Exact: 1, Similar: 22, Related: 42) | Malware: AdaptixC2, Bashlite
2025-11-02 22:46:57,530 - elastic_transport.transport - INFO - POST http://localhost:9200/predict-results/_doc [status:201 duration:0.002s]
2025-11-02 22:46:57,530 - __main__ - INFO - Indexed ip 128.199.219.80 - Matches: 1, Related: 42
```

Live monitoring of a networks DNS traffic

```
============================================================
Analysis Complete - Summary
============================================================
Total IOCs analyzed: 43
Found in PREDICT DB: 5
Not found: 38

Risk Distribution:
  - High Risk: 1
  - Medium Risk: 2
  - Low Risk: 1
  - Low-Medium Risk: 1

Elasticsearch Indexing:
  - Successfully indexed: 5
  - Failed to index: 0
2025-11-02 22:46:57,559 - elastic_transport.transport - INFO - POST http://localhost:9200/predict-results/_count [status:200 duration:0.002s]
2025-11-02 22:46:57,561 - elastic_transport.transport - INFO - POST http://localhost:9200/predict-results/_search [status:200 duration:0.002s]

Elasticsearch Index 'predict-results' Statistics:
  - Total documents: 25
  - Documents with API data: 25
```



Sendingmonitoring of a networks DNS traffic to a SIEM


Dashboard
Editing PREDICT Results
Settings
Share
Save as
Switch to view mode
Reset
Save
Filter your data using KQL syntax
Last 1 day
Refresh
Create visualization
Add panel
Add from library
Controls
IOC Risk Levels
high 20%
medium-high 20%
medium 20%
low 20%
low-medium 20%
low 5 (20%)
Malware Family Relationship
Count
AdaptixC2
Bashlite
BlackCat Ransomware
malware_families: Descending
20
15
5
0
5
10
15
20
Count
Building a dashboard in your SIEM
High Risk IOCs
Top 5 values of ioc
Top 3 values of risk_level
Top 3 values of malware_f
Count of records
104.167.215.195 medium AdaptixC2 5
128.199.219.80 high AdaptixC2 5
128.199.219.80 high Bashlite 5
23.95.35.34 medium-high Bashlite 5
IOC Timeline
timestamp per 30 minutes
00:00
02:00
05:00
08:00
11:00
14:00
17:00
high
low
low-medium
Other

</> API Documentation

REST API for Infrastructure Analysis and IOC Lookup

Quick Navigation

Quick Links

Get API Key

↑ Upgrade Plan

Overview

The PREDICT Infrastructure Analyzer API provides programmatic access to our malware infrastructure analysis and IOC lookup capabilities.

Base URL: `http://localhost:5001/api`

Content-Type: `application/json`

Response Format: JSON

Authentication: Required via API Key (see Authentication section)

Quick Start Example:

```
# Get your API key from /account, then:
export PREDICT_API_KEY="predict_your_api_key_here"

# Test it out:
curl -H "X-API-Key: $PREDICT_API_KEY" \
     "http://localhost:5001/api/ioc/lookup/8.8.8.8"
```

Supported

API Docs included

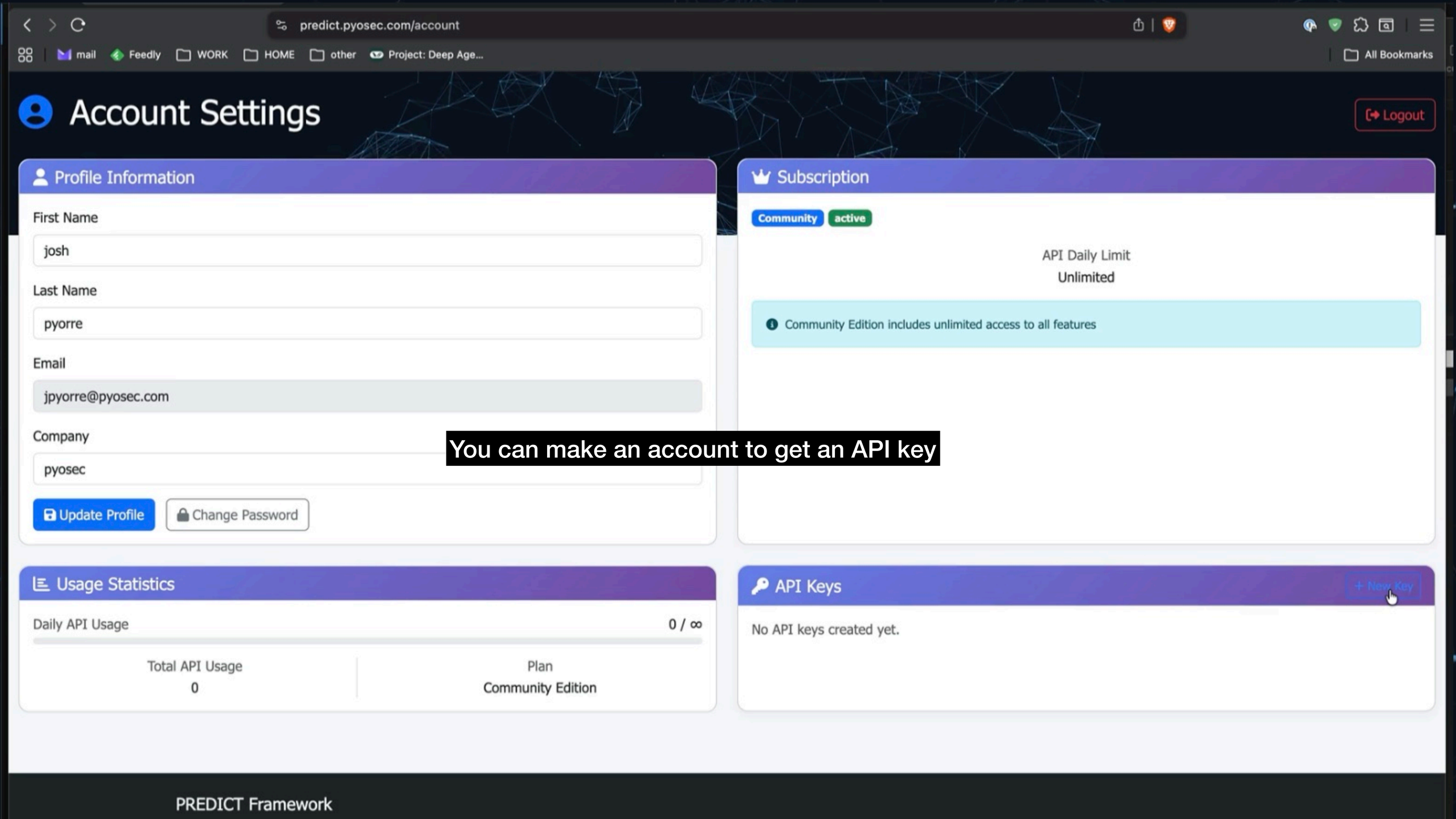
- IP Addr
- Domain Names
- CIDR Blocks
- URLs
- Hashes (MD5, SHA1, SHA256)
- Nameservers

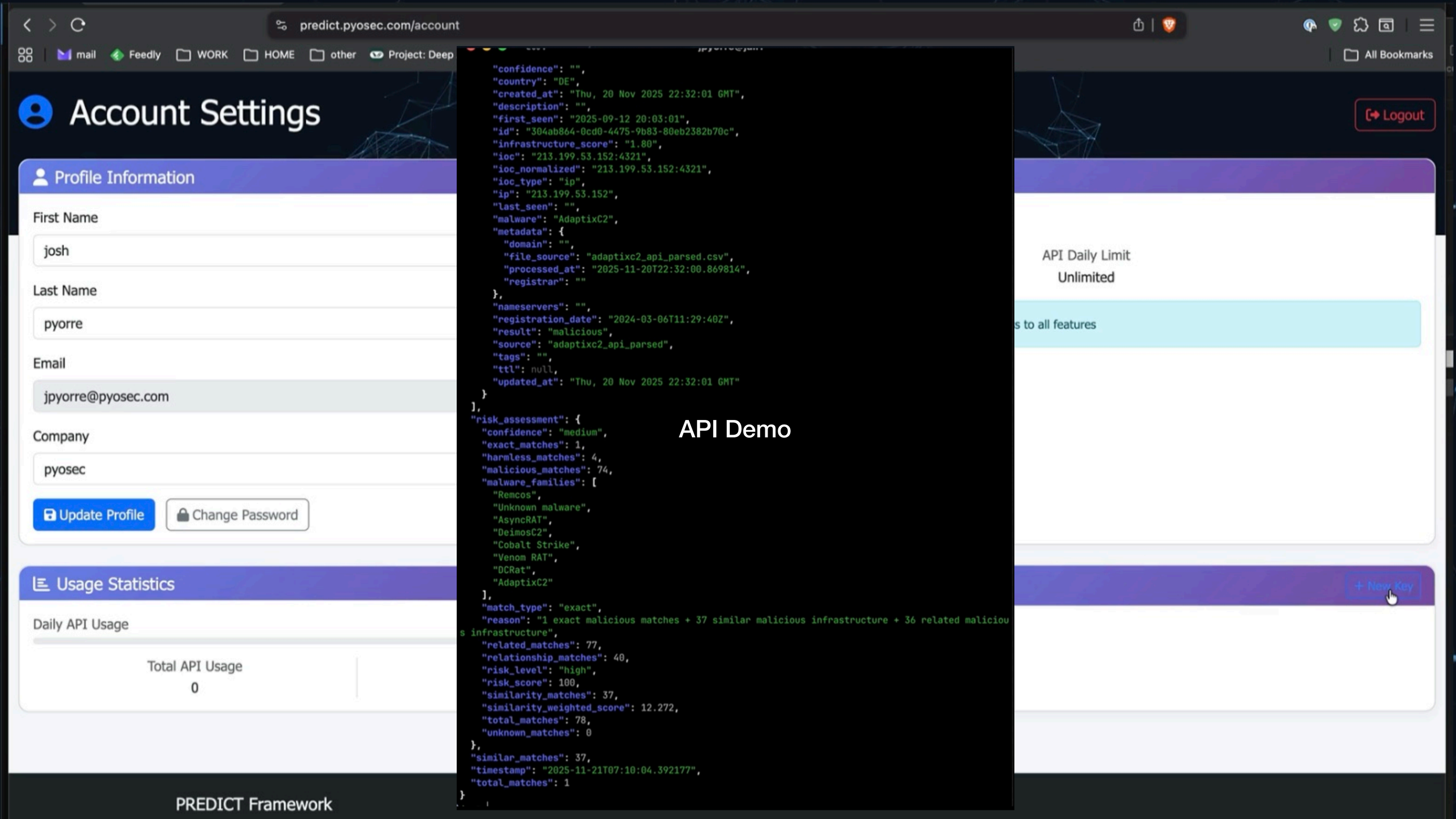
Authentication

All API requests require authentication via API key. Web interface access uses session-based authentication.

Getting Your API Key:

1. Log in to your account
2. Navigate to Account Settings
3. Click "New Key" in the API Keys section
4. Copy and securely store your API key


predict.pyosec.com/account
mail
Feedly
WORK
HOME
other
Project: Deep Age...
All Bookmarks
Account Settings
Logout
Profile Information
First Name
josh
Last Name
pyorre
Email
jpyorre@pyosec.com
Company
pyosec
Update Profile
Change Password
Subscription
Community
active
API Daily Limit
Unlimited
Community Edition includes unlimited access to all features
You can make an account to get an API key
Usage Statistics
Daily API Usage
0 / ∞
Total API Usage
0
Plan
Community Edition
API Keys
+ New Key
No API keys created yet.
PREDICT Framework

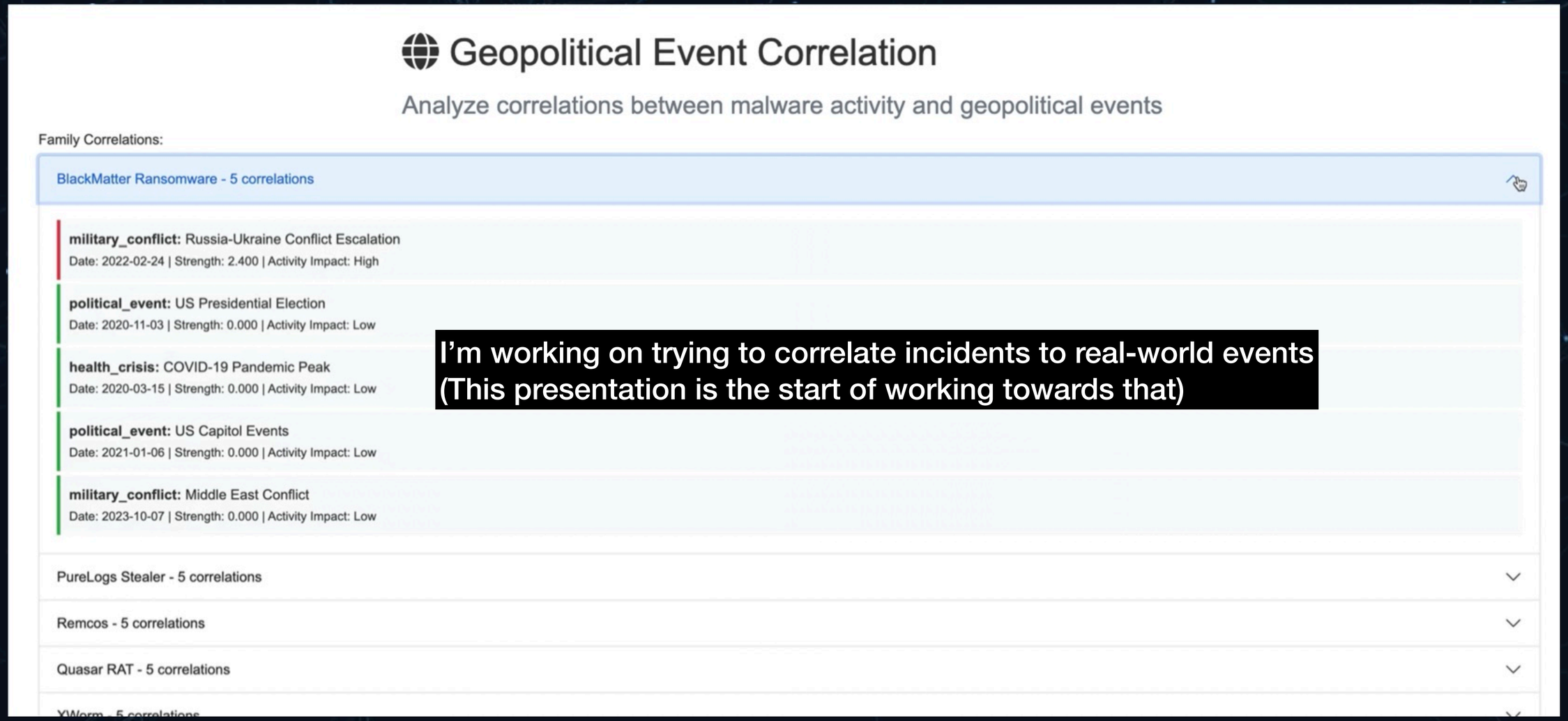

predict.pyosec.com/account
mail
Feedly
WORK
HOME
other
Project: Deep
All Bookmarks
Account Settings
Logout
Profile Information
First Name
josh
Last Name
pyorre
Email
jpyorre@pyosec.com
Company
pyosec
Update Profile
Change Password
Usage Statistics
Daily API Usage
Total API Usage
0
API Daily Limit
Unlimited
s to all features
+ New Key
PREDICT Framework
"confidence": "",
"country": "DE",
"created_at": "Thu, 20 Nov 2025 22:32:01 GMT",
"description": "",
"first_seen": "2025-09-12 20:03:01",
"id": "304ab864-0cd0-4475-9b83-80eb2382b70c",
"infrastructure_score": "1.80",
"ioc": "213.199.53.152:4321",
"ioc_normalized": "213.199.53.152:4321",
"ioc_type": "ip",
"ip": "213.199.53.152",
"last_seen": "",
"malware": "AdaptixC2",
"metadata": {
"domain": "",
"file_source": "adaptixc2_api_parsed.csv",
"processed_at": "2025-11-20T22:32:00.869814",
"registrar": ""
},
"nameservers": "",
"registration_date": "2024-03-06T11:29:40Z",
"result": "malicious",
"source": "adaptixc2_api_parsed",
"tags": "",
"ttl": null,
"updated_at": "Thu, 20 Nov 2025 22:32:01 GMT"
}
],
"risk_assessment": {
"confidence": "medium",
"exact_matches": 1,
"harmless_matches": 4,
"malicious_matches": 74,
"malware_families": [
"Remcos",
"Unknown malware",
"AsyncRAT",
"DeimosC2",
"Cobalt Strike",
"Venom RAT",
"DCRat",
"AdaptixC2"
],
"match_type": "exact",
"reason": "1 exact malicious matches + 37 similar malicious infrastructure + 36 related maliciou
s infrastructure",
"related_matches": 77,
"relationship_matches": 40,
"risk_level": "high",
"risk_score": 100,
"similarity_matches": 37,
"similarity_weighted_score": 12.272,
"total_matches": 78,
"unknown_matches": 0
},
"similar_matches": 37,
"timestamp": "2025-11-21T07:10:04.392177",
"total_matches": 1
}
API Demo

Take Action

- Notify on Results
- Soft-block (monitor)
- Actual Block (DNS sinkhole, Firewall, etc…)

Future Work

Future Work

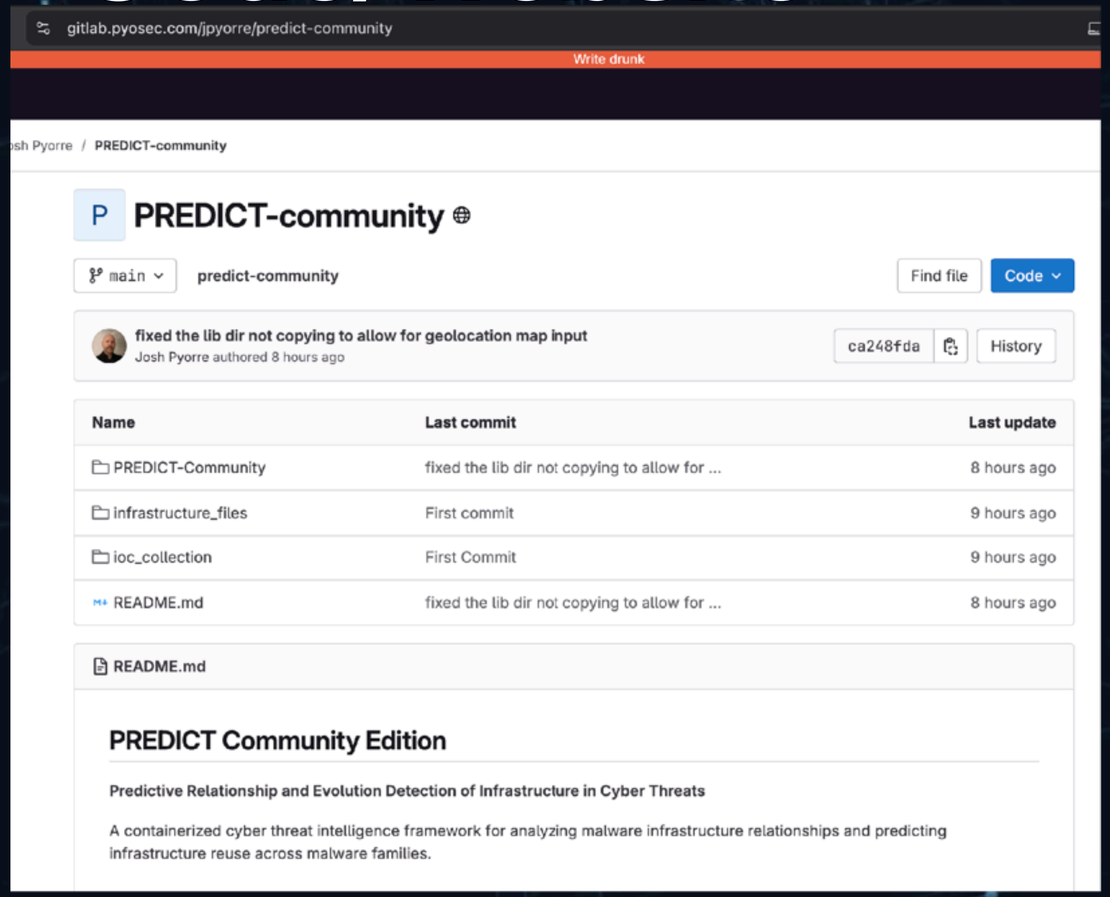


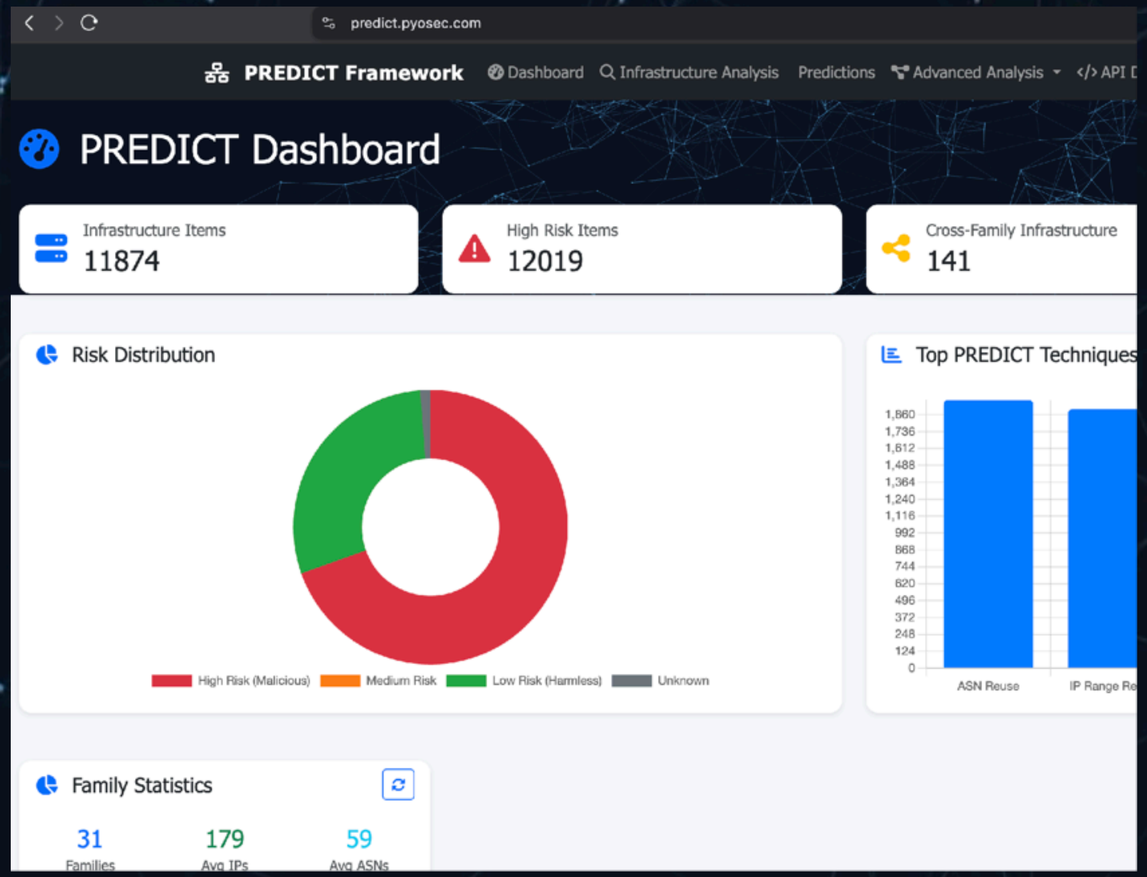
I'm working on trying to correlate incidents to real-world events
(This presentation is the start of working towards that)

Future Work

- Create my very own VirusTotal
- Rebuild my malware lab (the 10 year old MacBook battery started to swell)
- explore TLD similarities and fast flux

Code/Website





- Install it yourself: https://gitlab.pyosec.com/jpyorre/predict-community
- Try it with all the data I've collected: https://predict.pyosec.com

Thank you!

- Install it yourself: https://gitlab.pyosec.com/jpyorre/predict-community
- Try it with all the data I've collected: https://predict.pyosec.com

- If you like dark electronic music: https://dievortex.com