OSINT – Open-source Intelligence

COS30015 IT Security- Week 8

Troy Cao

CONTENT

01 Introduction of OSINT

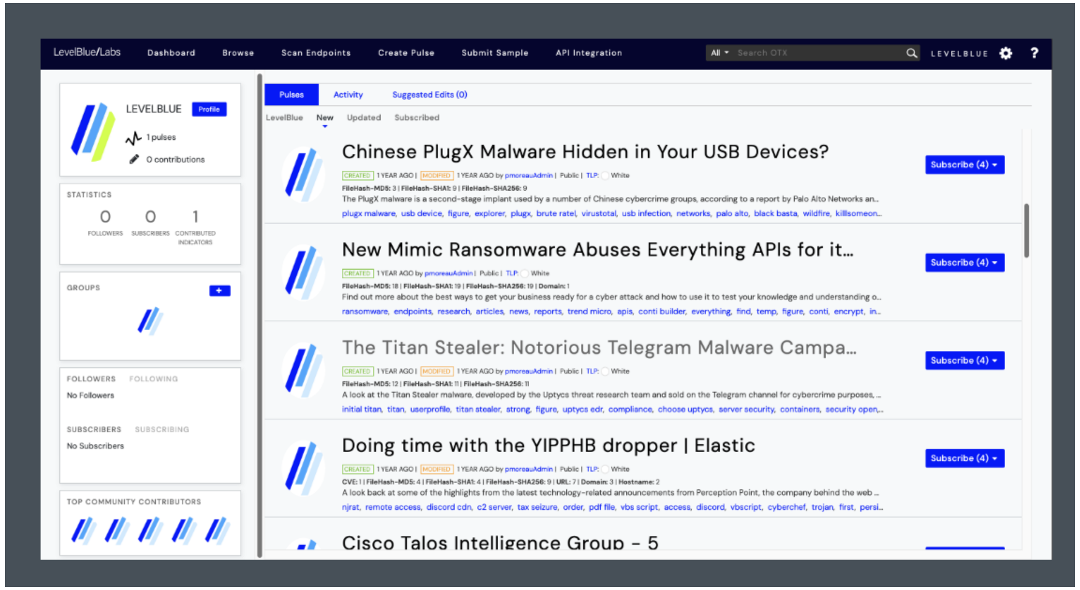
02 Open-sourced Intelligence (OSINT) Tools

03 Indicator of Compromise (IoC)

04 Case Study

SWINBURNE UNIVERSITY OF TECHNOLOGY

What is OSINT?



Chinese PlugX Malware Hidden in Your USB Devices?

CREATED 1 YEAR AGO | MODIFIED 1 YEAR AGO by pmoreauAdmin | Public | TLP: White

FileHash-MD5: 3 | FileHash-SHA1: 9 | FileHash-SHA256: 9

The PlugX malware is a second-stage implant used by a number of Chinese cybercrime groups, according to a report by Palo Alto Networks an...

plugx malware, usb device, figure, explorer, plugx, brute ratel, virustotal, usb infection, networks, palo alto, black basta, wildfire, killsomeon...

New Mimic Ransomware Abuses Everything APIs for it...

CREATED 1 YEAR AGO by pmoreauAdmin | Public | TLP: White

FileHash-MD5: 18 | FileHash-SHA1: 19 | FileHash-SHA256: 19 | Domain: 1

Find out more about the best ways to get your business ready for a cyber attack and how to use it to test your knowledge and understanding o...

ransomware, endpoints, research, articles, news, reports, trend micro, apis, conti builder, everything, find, temp, figure, conti, encrypt, in...

The Titan Stealer: Notorious Telegram Malware Campa...

CREATED 1 YEAR AGO | MODIFIED 1 YEAR AGO by pmoreauAdmin | Public | TLP: White

FileHash-MD5: 12 | FileHash-SHA1: 11 | FileHash-SHA256: 11

A look at the Titan Stealer malware, developed by the Uptycs threat research team and sold on the Telegram channel for cybercrime purposes, ...

initial titan, titan, userprofile, titan stealer, strong, figure, uptycs edr, compliance, choose uptycs, server security, containers, security open,...

Doing time with the YIPPHB dropper | Elastic

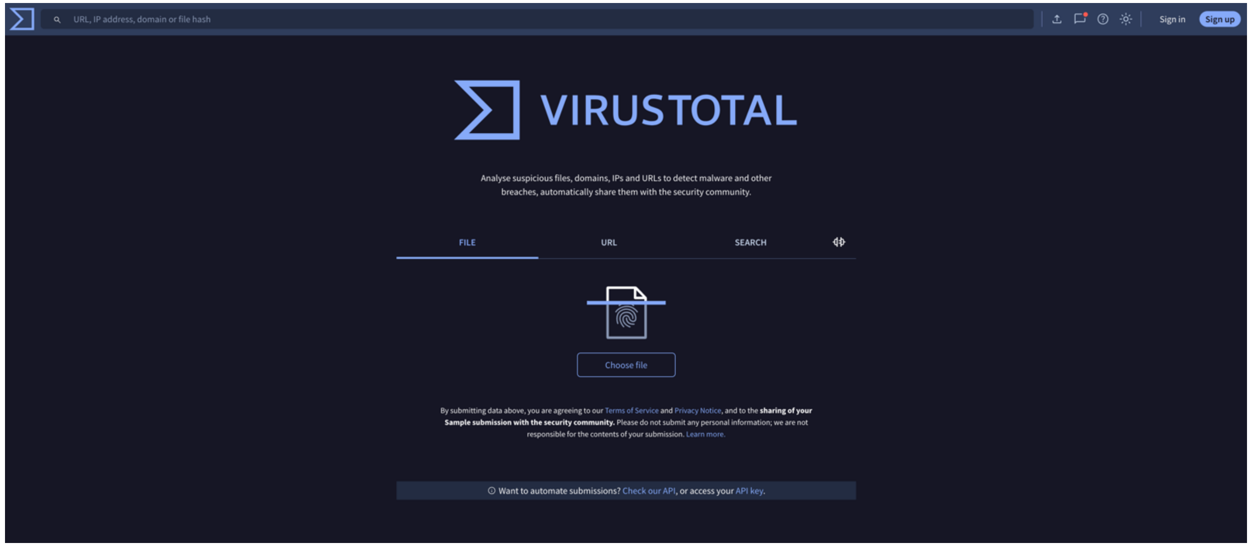
CREATED 1 YEAR AGO | MODIFIED 1 YEAR AGO by pmoreauAdmin | Public | TLP: White

CVE: 1 | FileHash-MD5: 4 | FileHash-SHA1: 4 | FileHash-SHA256: 9 | URL: 7 | Domain: 3 | Hostname: 2

A look back at some of the highlights from the latest technology-related announcements from Perception Point, the company behind the web ...

njrat, remote access, discord cdn, c2 server, tax seizure, order, pdf file, vbs script, access, discord, vbscript, cyberchef, trojan, first, persi...

Cisco Talos Intelligence Group – 5



Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.

By submitting data above, you are agreeing to our Terms of Service and Privacy Notice, and to the **sharing of your Sample submission with the security community.** Please do not submit any personal information; we are not responsible for the contents of your submission. Learn more.

ⓘ Want to automate submissions? Check our API, or access your API key.

- **Open source intelligence (OSINT)** is the act of gathering and analysing publicly available data for intelligence purposes.

- In the cybersecurity realm, intelligence researchers and analysts leverage open-source data to **better understand the threat landscape** and help **defend** organizations and individuals from **known risks** within their IT environment.

- There are two common use cases for OSINT:
  - Measuring the risk to your own organization;
  - Understanding the actor, tactics and targets;

Source: https://www.virustotal.com/gui/home/upload; https://otx.alienvault.com/ ; https://www.crowdstrike.com/cybersecurity-101/osint-open-source-intelligence/

CONTENT

01 Introduction of OSINT

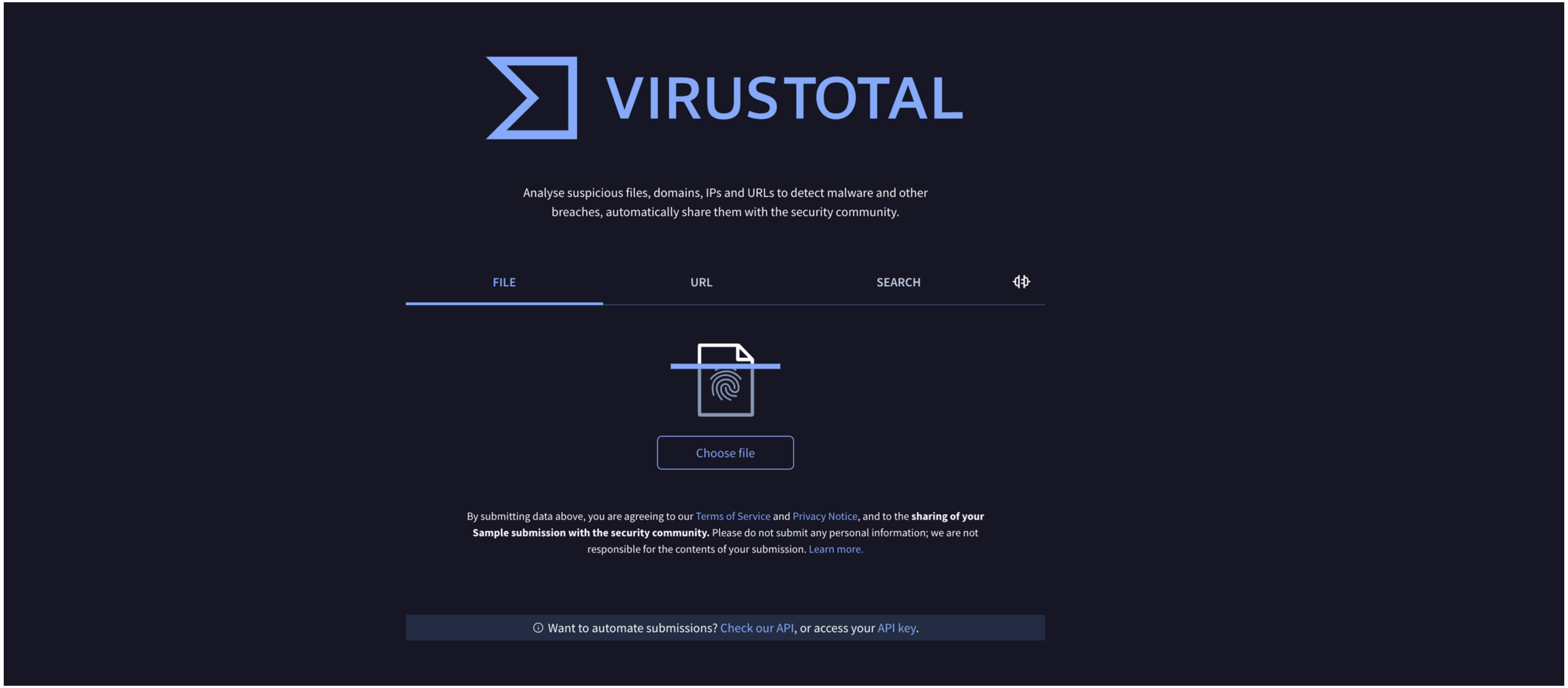
02 **Open-sourced Intelligence (OSINT) Tools**

03 Indicator of Compromise (IoC)

04 Case Study

SWINBURNE UNIVERSITY OF TECHNOLOGY

VIRUSTOTAL

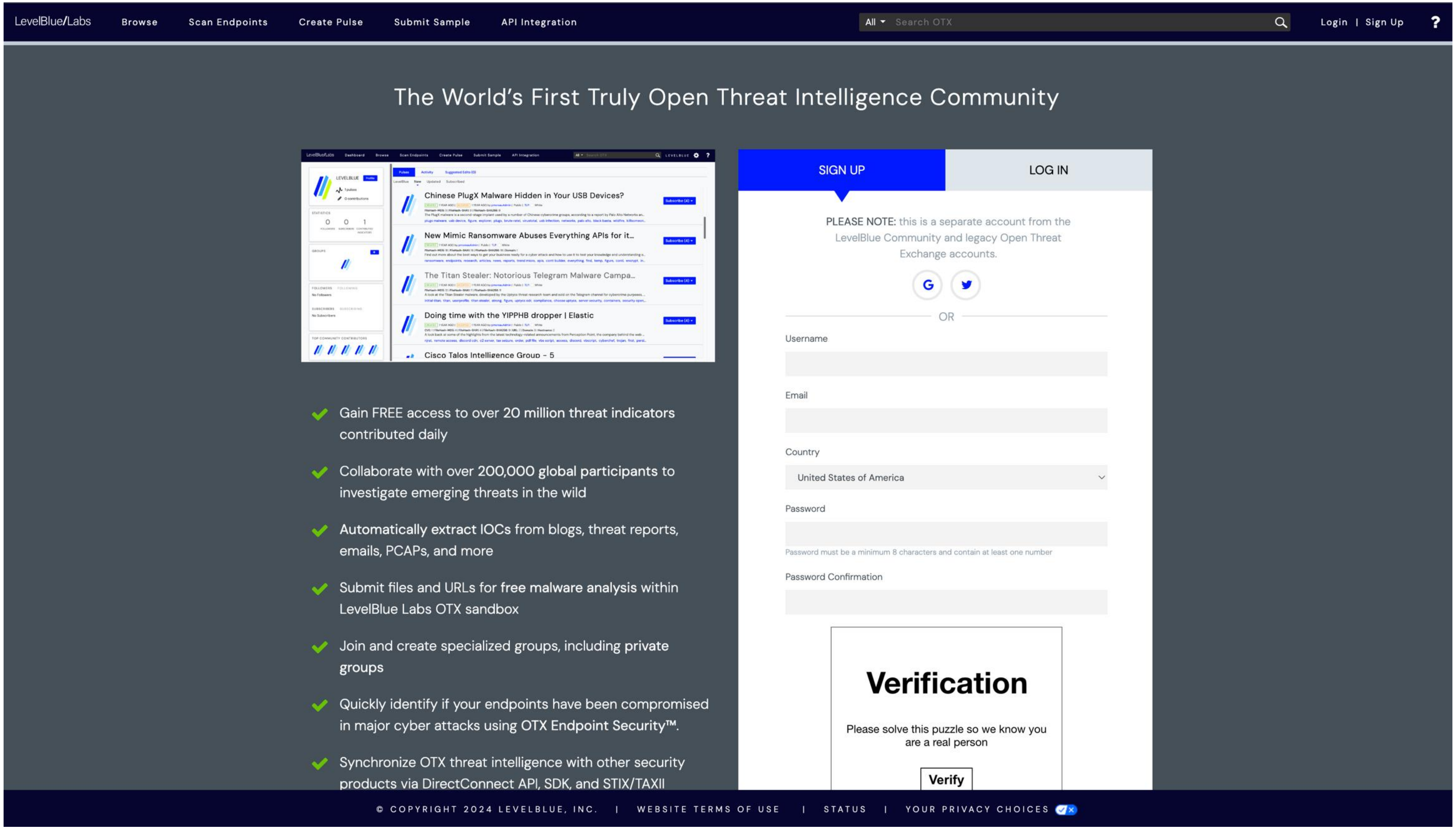


Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.

By submitting data above, you are agreeing to our Terms of Service and Privacy Notice, and to the **sharing of your Sample submission with the security community.** Please do not submit any personal information; we are not responsible for the contents of your submission. Learn more.

ⓘ Want to automate submissions? Check our API, or access your API key.

ALIENVAULT



LevelBlue/Labs | Browse | Scan Endpoints | Create Pulse | Submit Sample | API Integration | All | Search OTX | Login | Sign Up | ?

The World's First Truly Open Threat Intelligence Community

Chinese PlugX Malware Hidden in Your USB Devices?

New Mimic Ransomware Abuses Everything APIs for it...

The Titan Stealer: Notorious Telegram Malware Campa...

Doing time with the YIPPHB dropper | Elastic

Cisco Talos Intelligence Group – 5

- Gain FREE access to over 20 million threat indicators contributed daily
- Collaborate with over 200,000 global participants to investigate emerging threats in the wild
- Automatically extract IOCs from blogs, threat reports, emails, PCAPs, and more
- Submit files and URLs for free malware analysis within LevelBlue Labs OTX sandbox
- Join and create specialized groups, including private groups
- Quickly identify if your endpoints have been compromised in major cyber attacks using OTX Endpoint Security™.
- Synchronize OTX threat intelligence with other security products via DirectConnect API, SDK, and STIX/TAXII

SIGN UP | LOG IN

PLEASE NOTE: this is a separate account from the LevelBlue Community and legacy Open Threat Exchange accounts.

G

OR

Username

Email

Country

United States of America

Password

Password must be a minimum 8 characters and contain at least one number

Password Confirmation

Verification

Please solve this puzzle so we know you are a real person

Verify

© COPYRIGHT 2024 LEVELBLUE, INC. | WEBSITE TERMS OF USE | STATUS | YOUR PRIVACY CHOICES

CONTENT

01 Introduction of OSINT

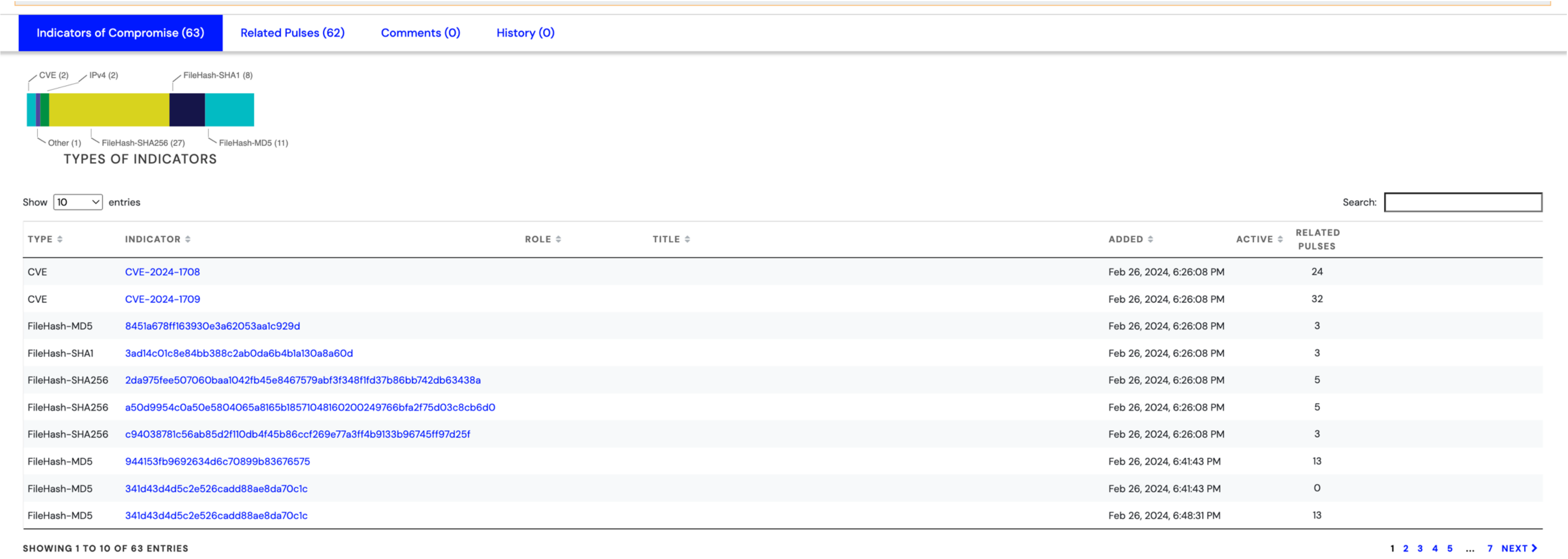
02 Open-sourced Intelligence (OSINT) Tools

03 Indicator of Compromise (IoC)

04 Case Study

SWINBURNE UNIVERSITY OF TECHNOLOGY

Indicator of Compromise - IoC



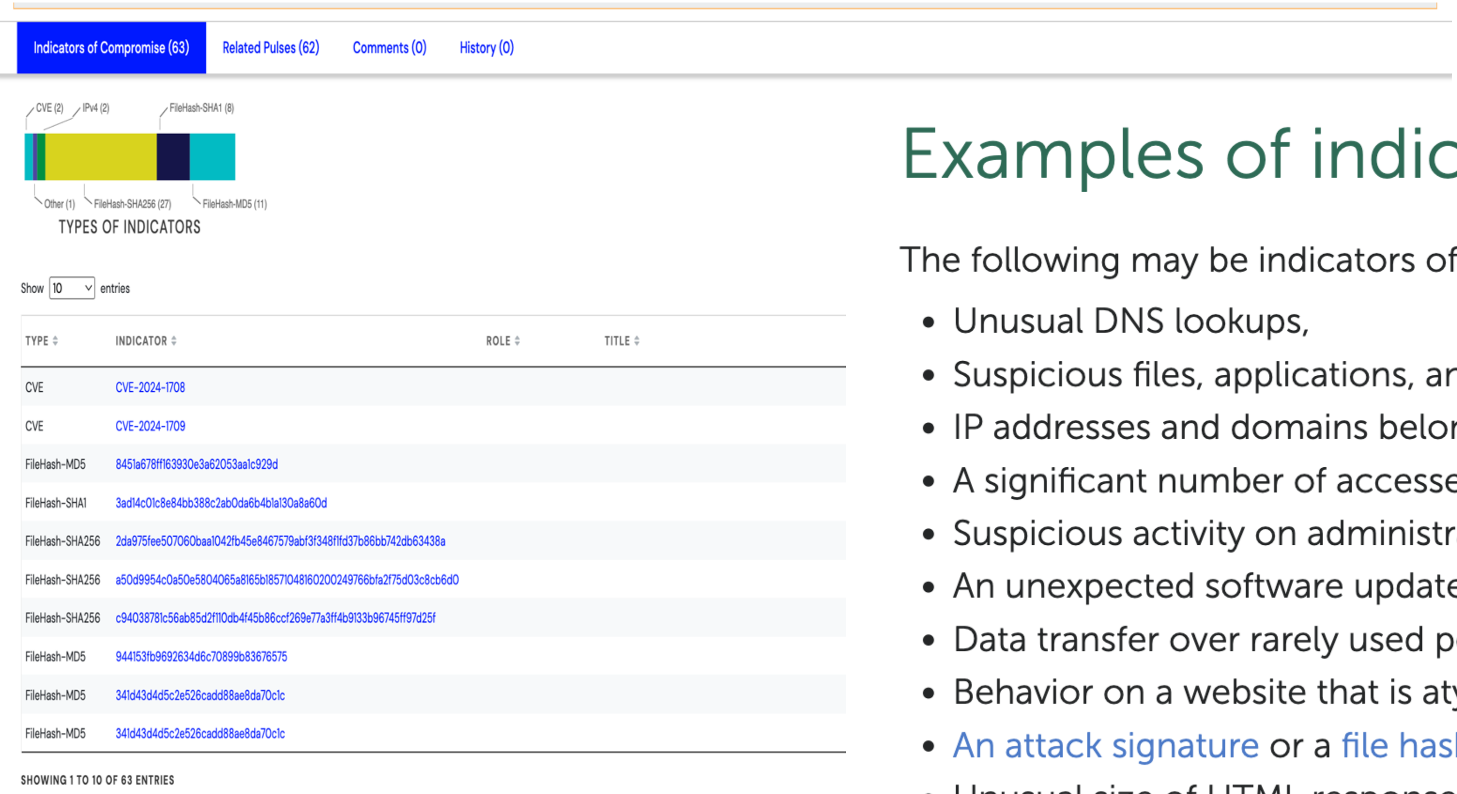
TYPE	INDICATOR	ROLE	TITLE	ADDED	ACTIVE	RELATED PULSES
CVE	CVE-2024-1708			Feb 26, 2024, 6:26:08 PM		24
CVE	CVE-2024-1709			Feb 26, 2024, 6:26:08 PM		32
FileHash-MD5	8451a678ff163930e3a62053aa1c929d			Feb 26, 2024, 6:26:08 PM		3
FileHash-SHA1	3ad14c01c8e84bb388c2ab0da6b4b1a130a8a60d			Feb 26, 2024, 6:26:08 PM		3
FileHash-SHA256	2da975fee507060baa1042fb45e8467579abf3f348f1fd37b86bb742db63438a			Feb 26, 2024, 6:26:08 PM		5
FileHash-SHA256	a50d9954c0a50e5804065a8165b18571048160200249766bfa2f75d03c8cb6d0			Feb 26, 2024, 6:26:08 PM		5
FileHash-SHA256	c94038781c56ab85d2f110db4f45b86ccf269e77a3ff4b9133b96745ff97d25f			Feb 26, 2024, 6:26:08 PM		3
FileHash-MD5	944153fb9692634d6c70899b83676575			Feb 26, 2024, 6:41:43 PM		13
FileHash-MD5	341d43d4d5c2e526cadd88ae8da70c1c			Feb 26, 2024, 6:41:43 PM		0
FileHash-MD5	341d43d4d5c2e526cadd88ae8da70c1c			Feb 26, 2024, 6:48:31 PM		13

SHOWING 1 TO 10 OF 63 ENTRIES

- In the field of computer security, an **Indicator of compromise (IoC)** is an object or activity that, observed on a network or on a device, indicates a high probability of unauthorized access to the system.

Source: https://otx.alienvault.com/ ; https://encyclopedia.kaspersky.com/

Indicator of Compromise - IoC

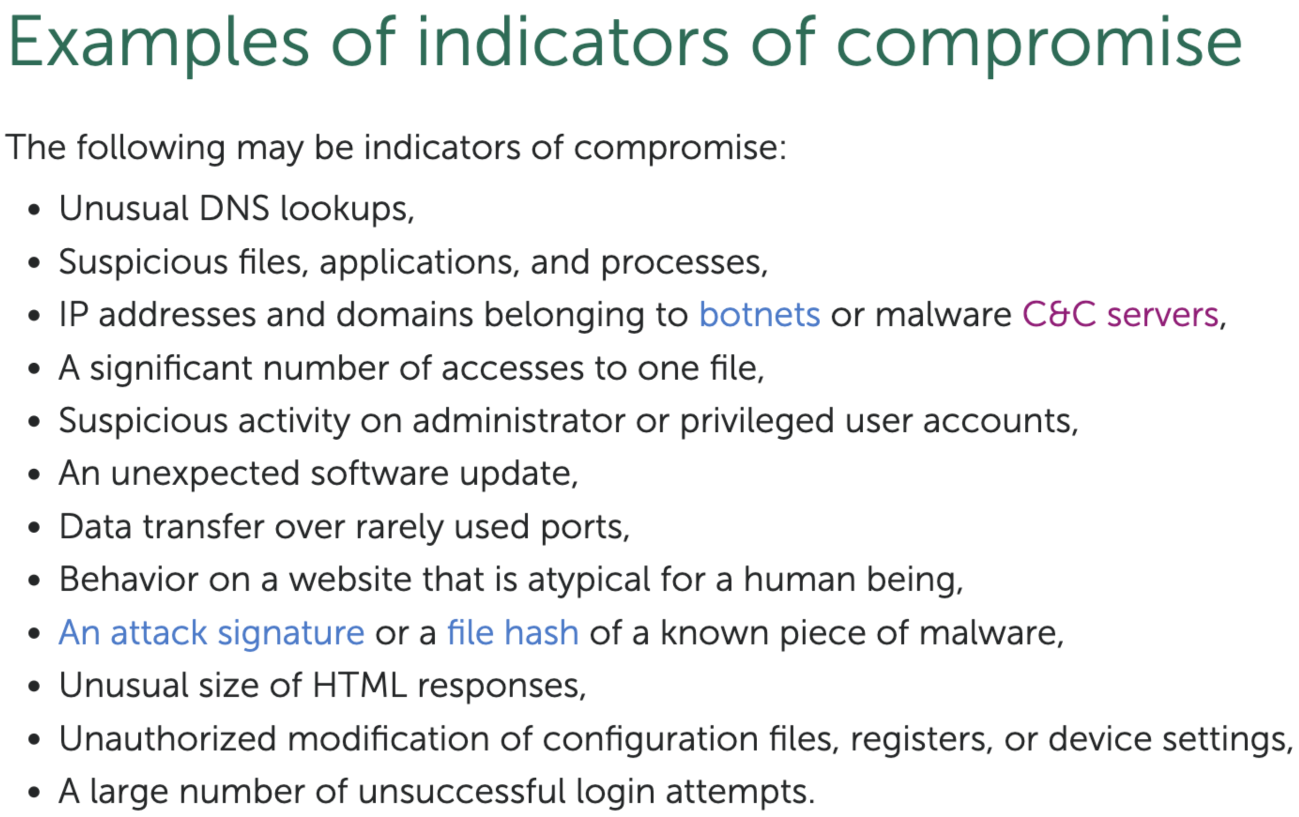


TYPES OF INDICATORS

Show 10 entries

TYPE	INDICATOR	ROLE	TITLE
CVE	CVE-2024-1708		
CVE	CVE-2024-1709		
FileHash-MD5	8451a678ff163930e3a62053aa1c929d		
FileHash-SHA1	3ad14c01c8e84bb388c2ab0da6b4b1a130a8a60d		
FileHash-SHA256	2da975fee507060baa1042fb45e8467579abf3f348f1fd37b86bb742db63438a		
FileHash-SHA256	a50d9954c0a50e5804065a8165b18571048160200249766bfa2f75d03c8cb6d0		
FileHash-SHA256	c94038781c56ab85d2f110db4f45b86ccf269e77a3ff4b9133b96745ff97d25f		
FileHash-MD5	944153fb9692634d6c70899b83676575		
FileHash-MD5	341d43d4d5c2e526cadd88ae8da70c1c		
FileHash-MD5	341d43d4d5c2e526cadd88ae8da70c1c		

SHOWING 1 TO 10 OF 63 ENTRIES



Examples of indicators of compromise

The following may be indicators of compromise:

- Unusual DNS lookups,
- Suspicious files, applications, and processes,
- IP addresses and domains belonging to botnets or malware C&C servers,
- A significant number of accesses to one file,
- Suspicious activity on administrator or privileged user accounts,
- An unexpected software update,
- Data transfer over rarely used ports,
- Behavior on a website that is atypical for a human being,
- An attack signature or a file hash of a known piece of malware,
- Unusual size of HTML responses,
- Unauthorized modification of configuration files, registers, or device settings,
- A large number of unsuccessful login attempts.

Source: https://otx.alienvault.com/ ; https://encyclopedia.kaspersky.com/

CONTENT

01 Introduction of OSINT

02 Open-sourced Intelligence (OSINT) Tools

03 Indicator of Compromise (IoC)

04 **Case Study**

SWINBURNE UNIVERSITY OF TECHNOLOGY

Fanging & Defanging

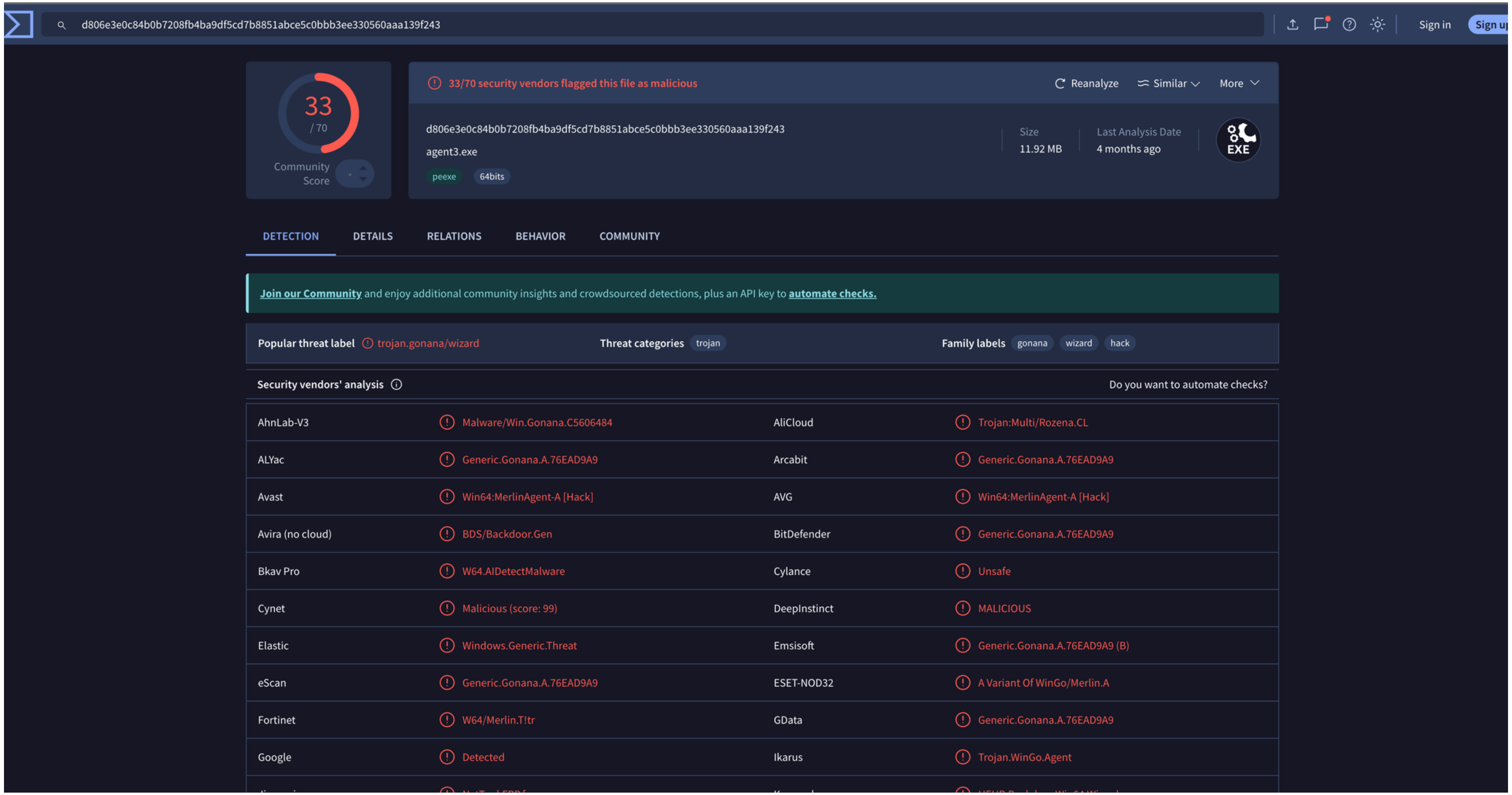
- **Fanging:** Restoring an indicator of compromise to its original form, with no artifacts from defanging.
  - ❖ e.g. example[.]com => example.com

- **Defanging:** Adding text to an indicator of compromise so that it does not become a link when presented in any medium (in an email, on a website, in a pdf, etc).
  - ❖ e.g. example.com => example[.]com

- Why use Fanging (or DeFanging)?
  - ❖ Making sure indicators are properly and fully defanged so malicious links are not accidentally distributed;
  - ❖ Making it easy for automated scripts to fang indicators so that security professionals can collect and investigate data easily..

Source: https://github.com/Ne0nd0g/merlin

Case Study - Merlin C2



33/70 security vendors flagged this file as malicious

d806e3e0c84b0b7208fb4ba9df5cd7b8851abce5c0bbb3ee330560aaa139f243

agent3.exe

peexe 64bits

Size: 11.92 MB

Last Analysis Date: 4 months ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label: trojan.gonana/wizard

Threat categories: trojan

Family labels: gonana wizard hack

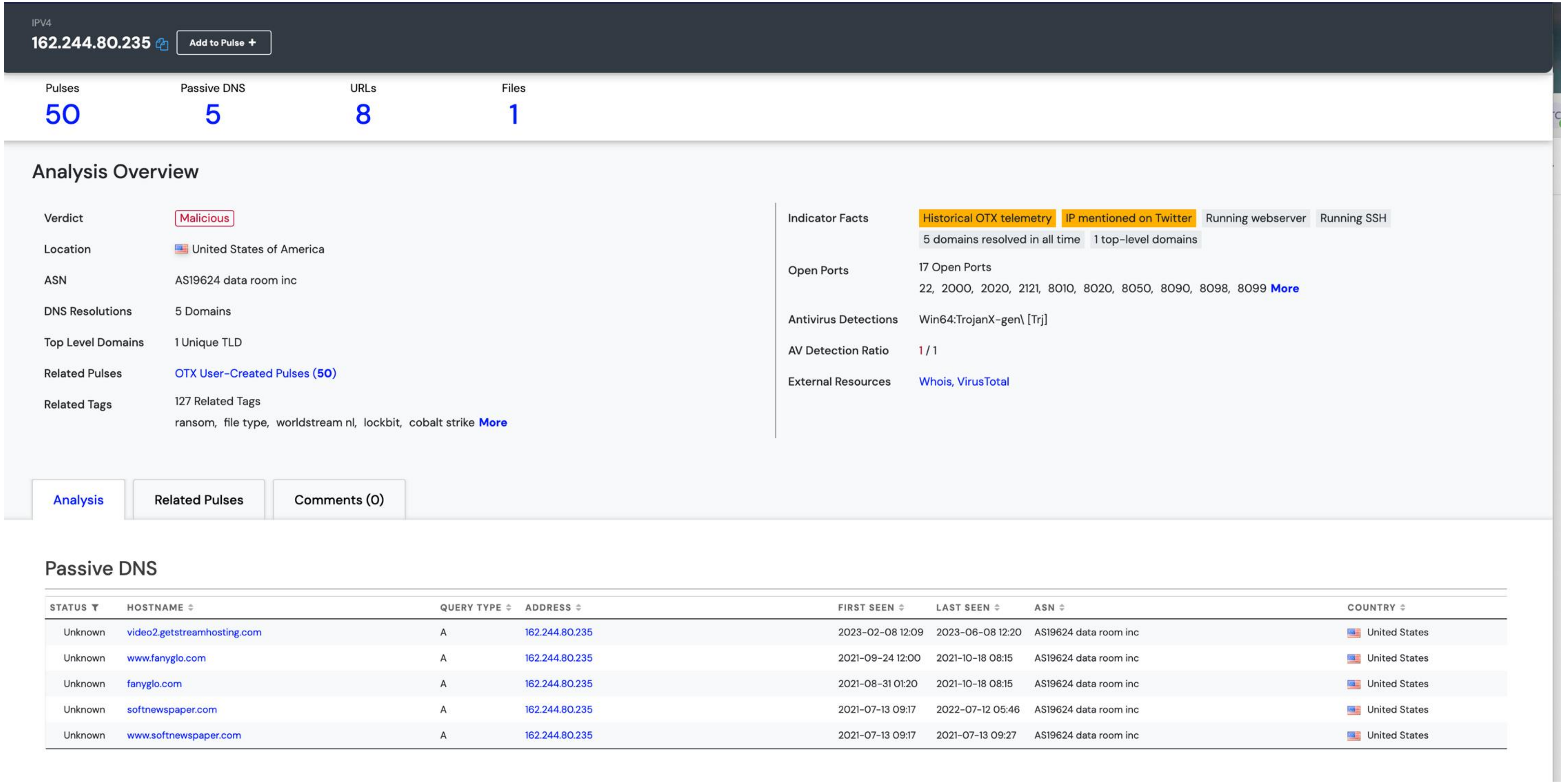
Security vendors' analysis

Do you want to automate checks?

AhnLab-V3	Malware/Win.Gonana.C5606484	AliCloud	Trojan:Multi/Rozena.CL
ALYac	Generic.Gonana.A.76EAD9A9	Arcabit	Generic.Gonana.A.76EAD9A9
Avast	Win64:MerlinAgent-A [Hack]	AVG	Win64:MerlinAgent-A [Hack]
Avira (no cloud)	BDS/Backdoor.Gen	BitDefender	Generic.Gonana.A.76EAD9A9
Bkav Pro	W64.AIDetectMalware	Cylance	Unsafe
Cynet	Malicious (score: 99)	DeepInstinct	MALICIOUS
Elastic	Windows.Generic.Threat	Emsisoft	Generic.Gonana.A.76EAD9A9 (B)
eScan	Generic.Gonana.A.76EAD9A9	ESET-NOD32	A Variant Of WinGo/Merlin.A
Fortinet	W64/Merlin.T!tr	GData	Generic.Gonana.A.76EAD9A9
Google	Detected	Ikarus	Trojan.WinGo.Agent

Source: https://github.com/Ne0nd0g/merlin

Case Study – Conti Ransomware



162.244.80.235

Pulses	Passive DNS	URLs	Files
50	5	8	1

Analysis Overview

Verdict	Malicious
Location	United States of America
ASN	AS19624 data room inc
DNS Resolutions	5 Domains
Top Level Domains	1 Unique TLD
Related Pulses	OTX User-Created Pulses (50)
Related Tags	127 Related Tags ransom, file type, worldstream nl, lockbit, cobalt strike More

Indicator Facts	Historical OTX telemetry IP mentioned on Twitter Running webserver Running SSH 5 domains resolved in all time 1 top-level domains
Open Ports	17 Open Ports 22, 2000, 2020, 2121, 8010, 8020, 8050, 8090, 8098, 8099 More
Antivirus Detections	Win64:TrojanX-gen\ [Trj]
AV Detection Ratio	1 / 1
External Resources	Whois, VirusTotal

Passive DNS

STATUS	HOSTNAME	QUERY TYPE	ADDRESS	FIRST SEEN	LAST SEEN	ASN	COUNTRY
Unknown	video2.getstreamhosting.com	A	162.244.80.235	2023-02-08 12:09	2023-06-08 12:20	AS19624 data room inc	United States
Unknown	www.fanyglo.com	A	162.244.80.235	2021-09-24 12:00	2021-10-18 08:15	AS19624 data room inc	United States
Unknown	fanyglo.com	A	162.244.80.235	2021-08-31 01:20	2021-10-18 08:15	AS19624 data room inc	United States
Unknown	softnewspaper.com	A	162.244.80.235	2021-07-13 09:17	2022-07-12 05:46	AS19624 data room inc	United States
Unknown	www.softnewspaper.com	A	162.244.80.235	2021-07-13 09:17	2021-07-13 09:27	AS19624 data room inc	United States

Source: https://otx.alienvault.com/

Thanks for Watching

Troy Cao