Hi Mr. Cobblepot,

Based on my analysis of the cyber threat event, i have gathered some info.

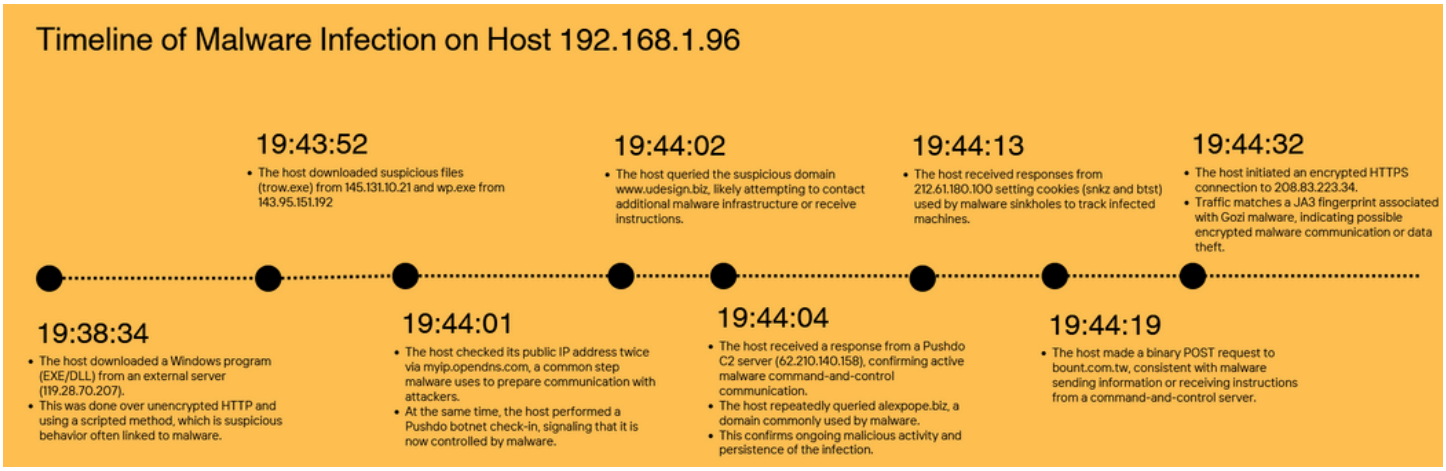
A workstation(internal host 192.168.1.96) within the corporate network has been confirmed to be compromised by a multi-stage malware infection involving *Pushdo* and a *Gozi* component. The system has engaged in unauthorized external communications, including contact with known command-and-control(C2) infrastructure, attempts to exfiltrate data and repeated efforts to download additional malicious payloads from untrusted external servers. The observed activity indicates that the host has become part of a botnet and is active in malicious operations outside the organizations control.

This is a significant security breach and these are the immediate recommendations:

- Isolate and forensically assess the affected host
- Block identified malicious infrastructure and review network exposure

Below is more information about the case.

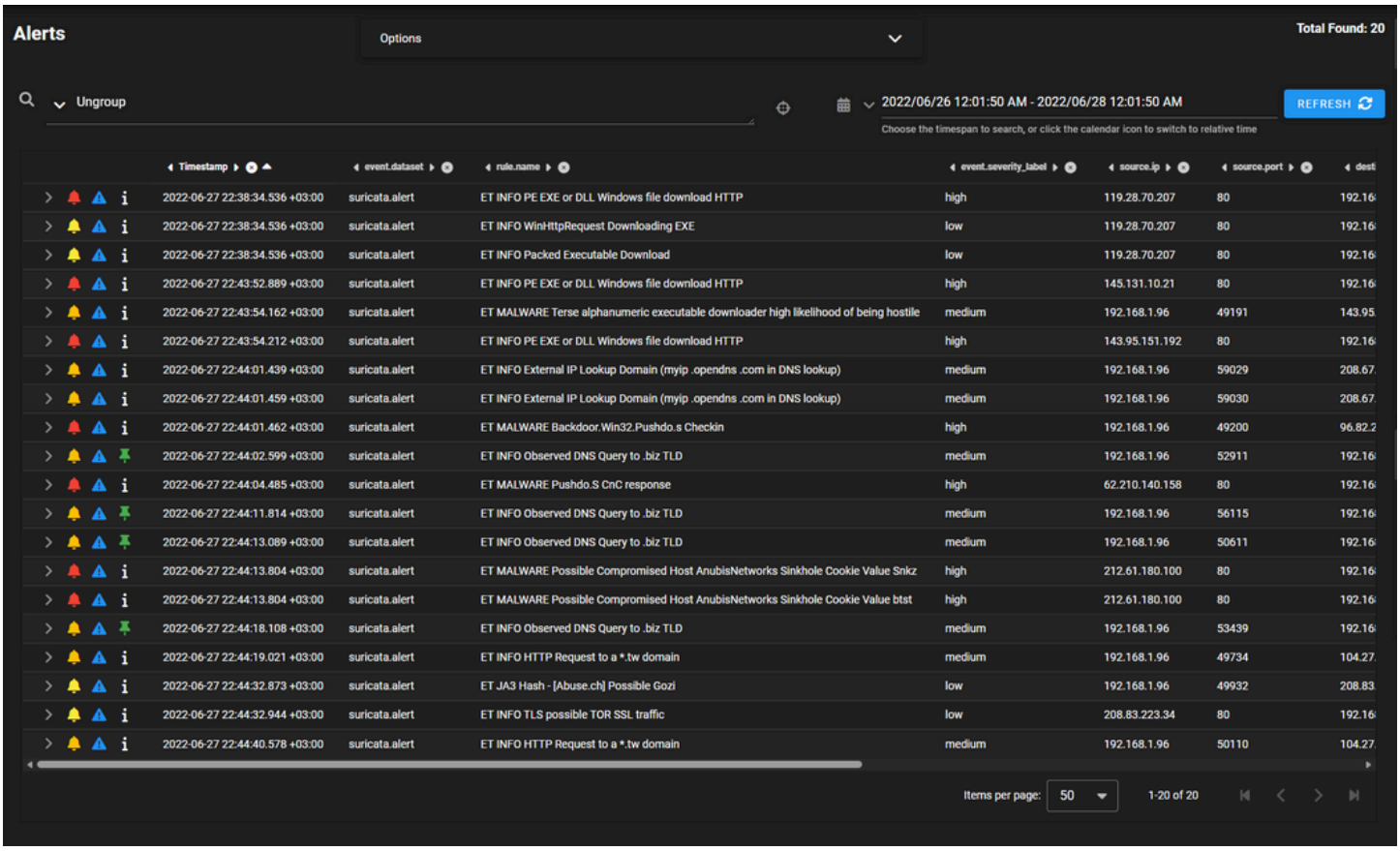
Analyzing the intrusion



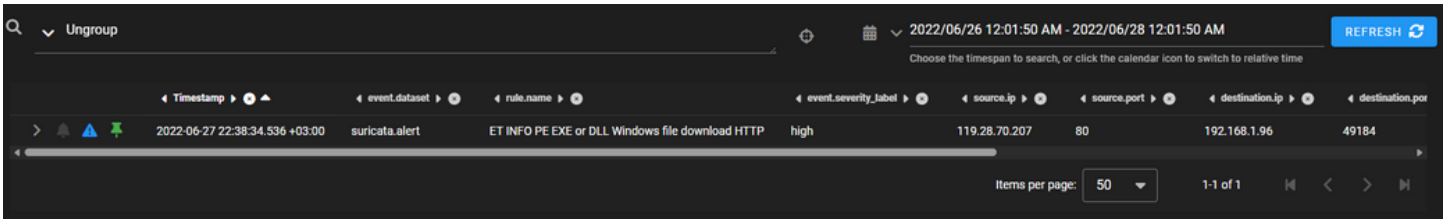
Proof of findings

Security Onion

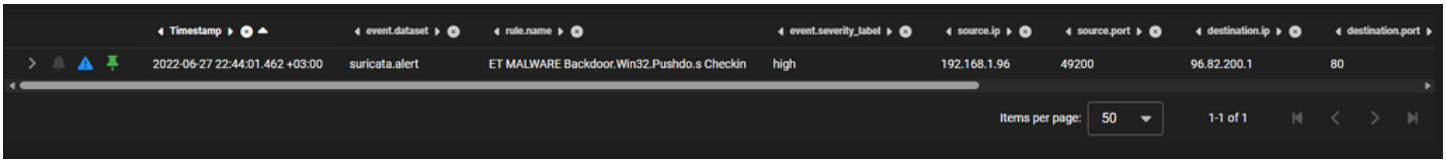
Picture of SO Alert page showing the whole attack.



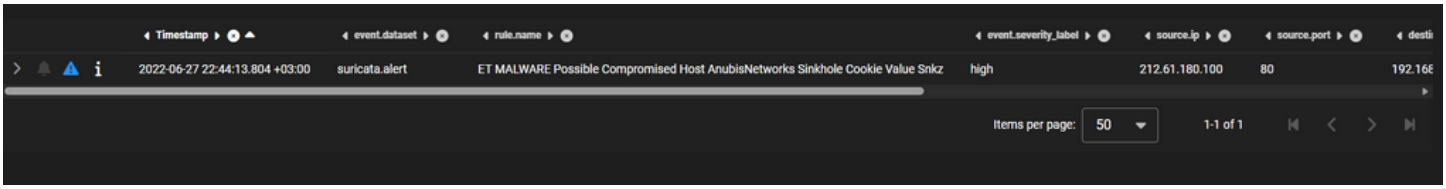
SO image of .exe-file downloaded HTTP



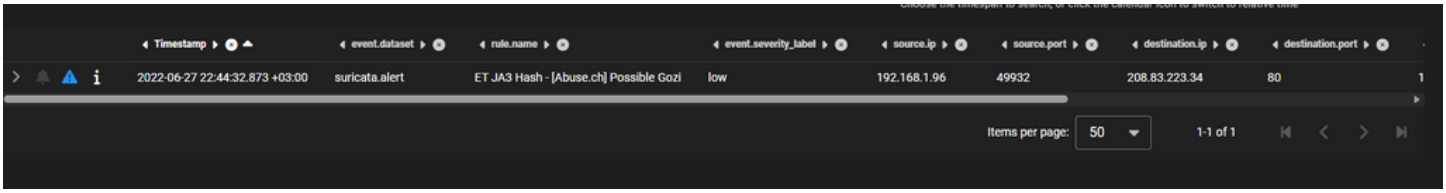
SO image of Pushdo/Cutwail botnet(backdoor) activity detected



SO image of AnubisNetworks sinkhole activity

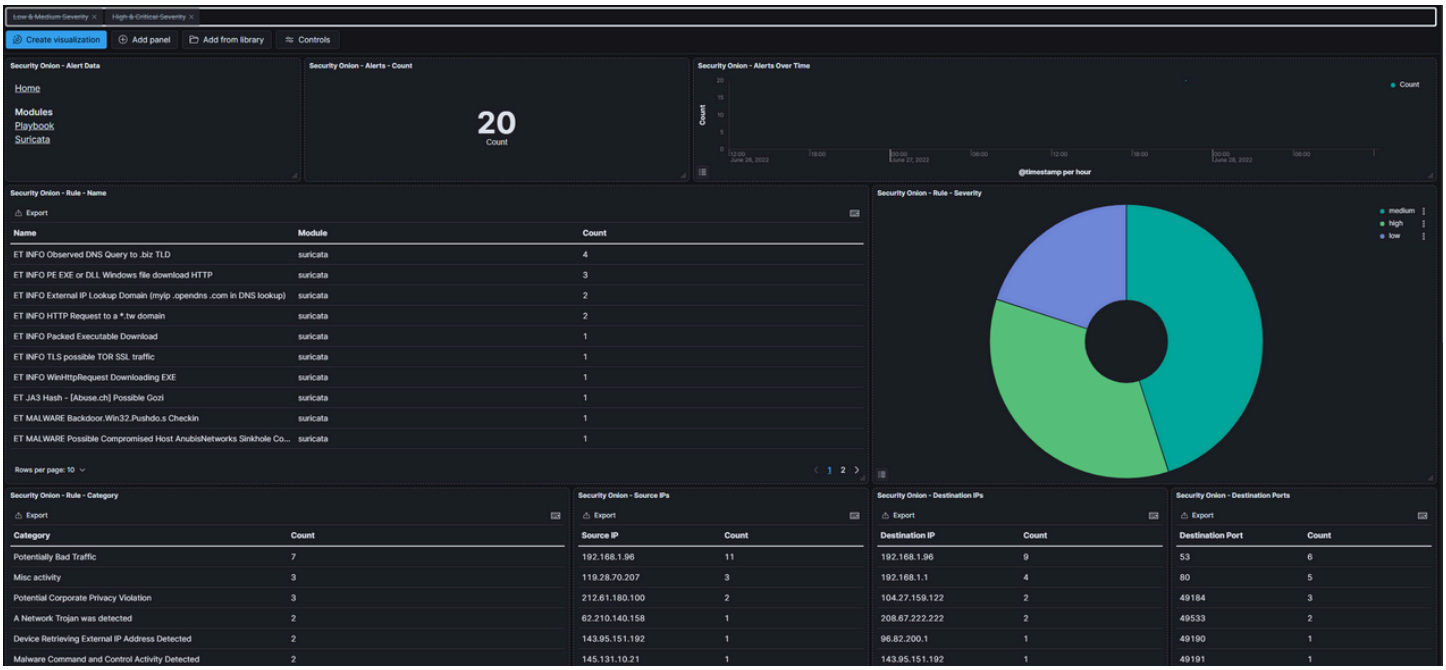


SO image of JA3 fingerprint Gozi malware.

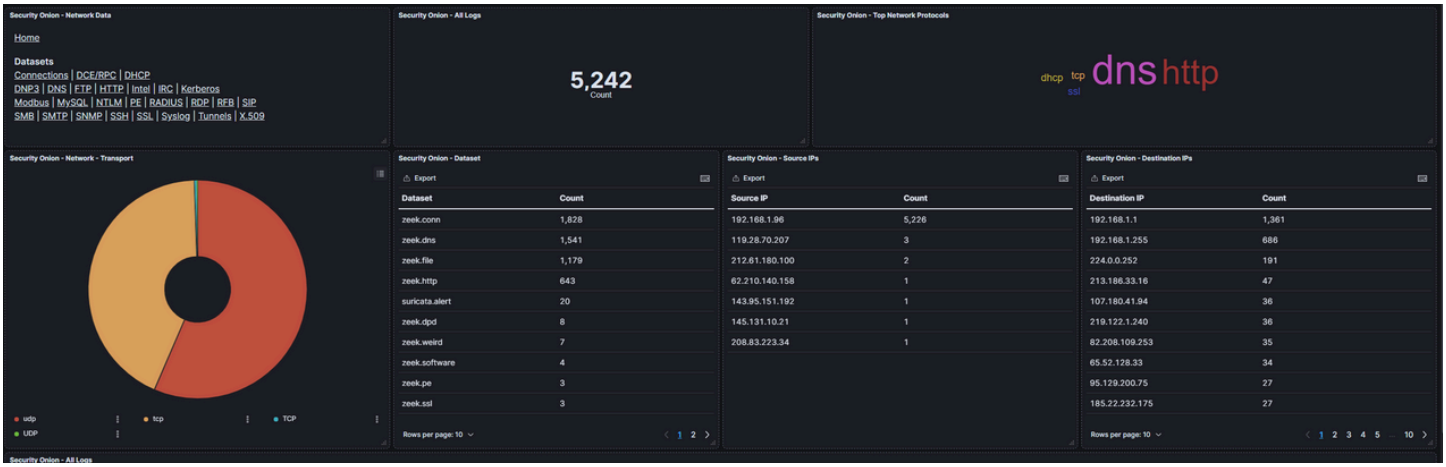


Kibana

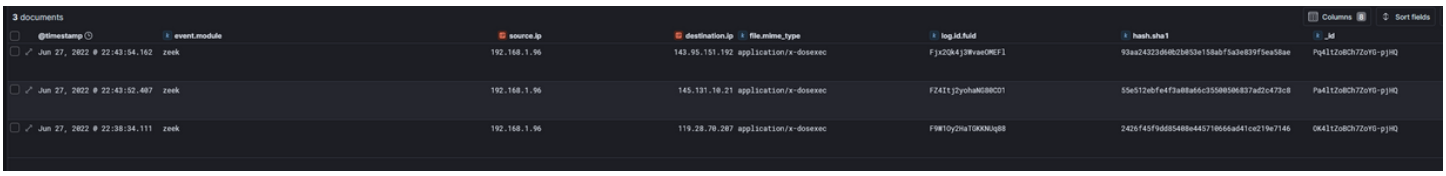
Overview of Alerts in Kibana.



Kibana’s network traffic overview.



Kibana image of malicious files.



Wireshark

Wireshark image of http/1.1 filter showing GET of malicious files and botnet/c2 activity

http.request.version == "HTTP/1.1"

No.	Time	Source	Destination	Protocol	Length	Info
6	2022-06-27 22:38:32.652026	192.168.1.96	119.28.70.207	HTTP	230	GET /gerv.gun HTTP/1.1
298	2022-06-27 22:43:50.222947	192.168.1.96	119.28.70.207	HTTP	560	POST /auth/ajax/847598782/?min=data HTTP/1.1 (application/x-www-form-urlencoded)
304	2022-06-27 22:43:51.070180	192.168.1.96	119.28.70.207	HTTP	662	POST /auth/min/828949448/ HTTP/1.1 (application/x-www-form-urlencoded)
313	2022-06-27 22:43:52.243381	192.168.1.96	145.131.10.21	HTTP	200	GET /oud/trow.exe HTTP/1.1
667	2022-06-27 22:43:54.128138	192.168.1.96	143.95.151.192	HTTP	202	GET /wp.exe HTTP/1.1
866	2022-06-27 22:43:58.714716	192.168.1.96	59.106.164.230	HTTP	169	GET /img/t64.bin HTTP/1.1
1423	2022-06-27 22:44:01.381384	192.168.1.96	198.1.85.250	HTTP	881	POST / HTTP/1.1
1427	2022-06-27 22:44:01.389770	192.168.1.96	96.82.200.1	HTTP	857	POST / HTTP/1.1
1436	2022-06-27 22:44:01.401240	192.168.1.96	64.125.133.18	HTTP	848	POST / HTTP/1.1
1439	2022-06-27 22:44:01.410587	192.168.1.96	184.168.47.225	HTTP	890	POST / HTTP/1.1
1460	2022-06-27 22:44:01.461139	192.168.1.96	148.251.33.194	HTTP	849	POST / HTTP/1.1
1471	2022-06-27 22:44:01.473367	192.168.1.96	80.74.154.6	HTTP	861	POST / HTTP/1.1
1476	2022-06-27 22:44:01.478809	192.168.1.96	82.201.61.230	HTTP	899	POST / HTTP/1.1
1481	2022-06-27 22:44:01.485102	192.168.1.96	64.125.133.18	HTTP	848	POST / HTTP/1.1
1489	2022-06-27 22:44:01.492940	192.168.1.96	193.77.149.5	HTTP	869	POST / HTTP/1.1
1492	2022-06-27 22:44:01.495129	192.168.1.96	210.188.201.166	HTTP	873	POST / HTTP/1.1
1572	2022-06-27 22:44:01.652802	192.168.1.96	219.122.1.240	HTTP	869	POST / HTTP/1.1

SSL Blacklist

Picture of Gozi malware's JA3 fingerprint

SSL blacklist from ABUSE.ch | SPAMHAUS

SSL Certificates | JA3 Fingerprints | Blacklist | Statistics | About

JA3 Fingerprint / Browse

JA3 Fingerprints

You can find further information about the JA3 fingerprint c201b92f8b483fa388be174d6689f534, including the corresponding malware samples as well as the associated botnet C&Cs.

Database Entry

JA3 Fingerprint:	c201b92f8b483fa388be174d6689f534
First seen:	2018-03-12 13:43:52 UTC
Last seen:	2021-01-28 06:17:06 UTC
Status:	Blacklisted
Malware samples:	68
Destination IPs:	1'555
Malware:	Gozi
Listing date:	2018-11-14 00:00:00

Malware Samples

The table below documents all malware samples associated with this JA3 Fingerprint.

Timestamp (UTC)	Malware Sample (MD5 hash)	VT	Botnet C&C (IP:port)
2025-09-06 03:56:54	42e3fe07f3b4f46db7079c45036fd828	n/a	171.25.193.9:80
2025-09-03 01:35:52	d92114533145be94bf0a1f02f84a1c25	n/a	193.23.244.244:443
2025-09-02 22:44:21	d223ac7fb64b644a543bca360dffd84d	n/a	193.23.244.244:443
2025-08-31 04:46:45	84ce6c634d80ac265d02cfb097558cd7	n/a	193.23.244.244:443
2025-08-20 08:04:45	e26a6e2a00b757d7b67069787274ffb2	n/a	171.25.193.9:80
2025-08-20 05:43:57	cfd6b93939d1702ebe9b2c6470a32e59	n/a	193.23.244.244:443

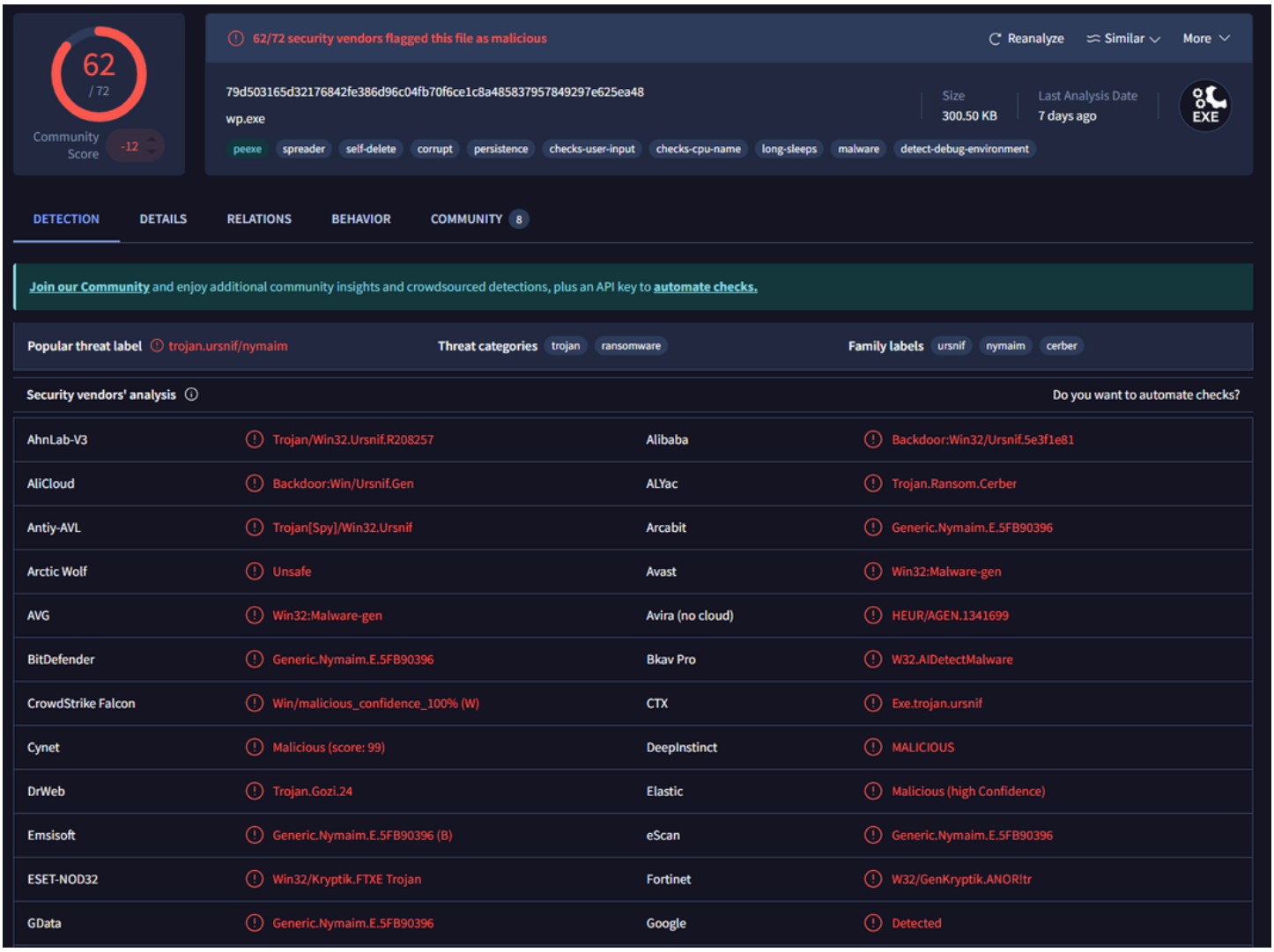
Table of IP-addresses

IP-address	AbuseIPdb	Country	Domain	Details
119.28.70.207	no	Hong Kong	tencent.com	...
143.95.151.192	no	United States of America	vantagepointtechnologies.com	...
145.131.10.21	no	Netherlands	argeweb.nl	...
62.210.140.158	no	France	scaleway.com	C2-Server
208.83.223.34	no	United States of America	appliedops.net	Possible Gozi
212.61.180.100	no	Netherlands	claranet.com	AnubisNetworks Sinkhole Cookie

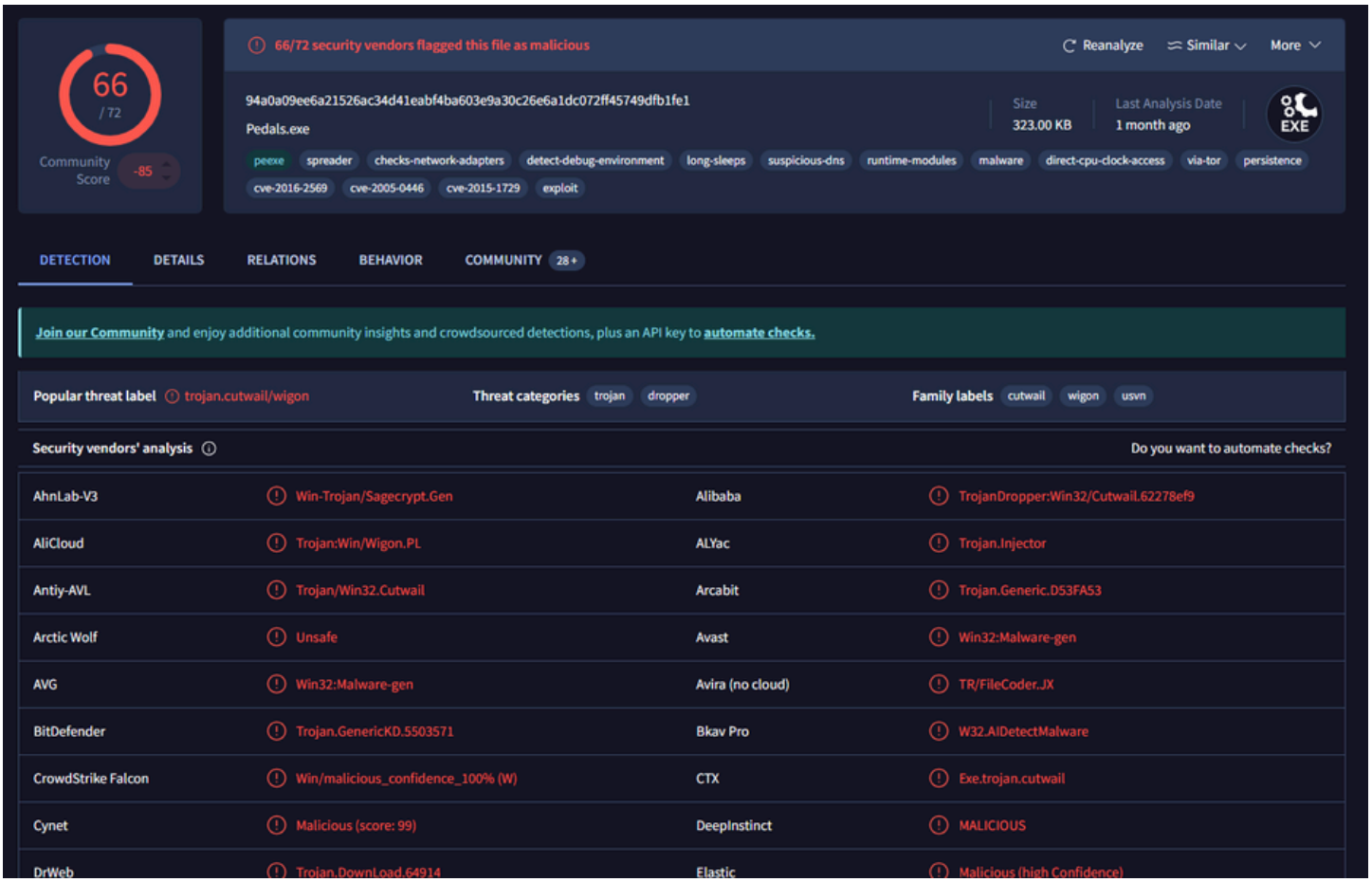
Table of malicious files and VirusTotal analysis

Filename	Source IP	Destination IP	Details	SHA1-hashvalue	Virustotal PoC
wp.exe	192.168.1.96	143.95.151.192	Trojan-Ransomware	93aa24323d60b2b053e158abf5a3e839f5ea58ae	Picture 1
trow.exe(Pedals.exe)	192.168.1.96	145.131.10.21	Trojan-Dropper	55e512ebfe4f3a08a66c35500506837ad2c473c8	Picture 2
gerv.gun	192.168.1.96	119.28.70.207	Trojan-Banker-Ransomware	2426f45f9dd85408e445710666ad41ce219e7146	Picture 3

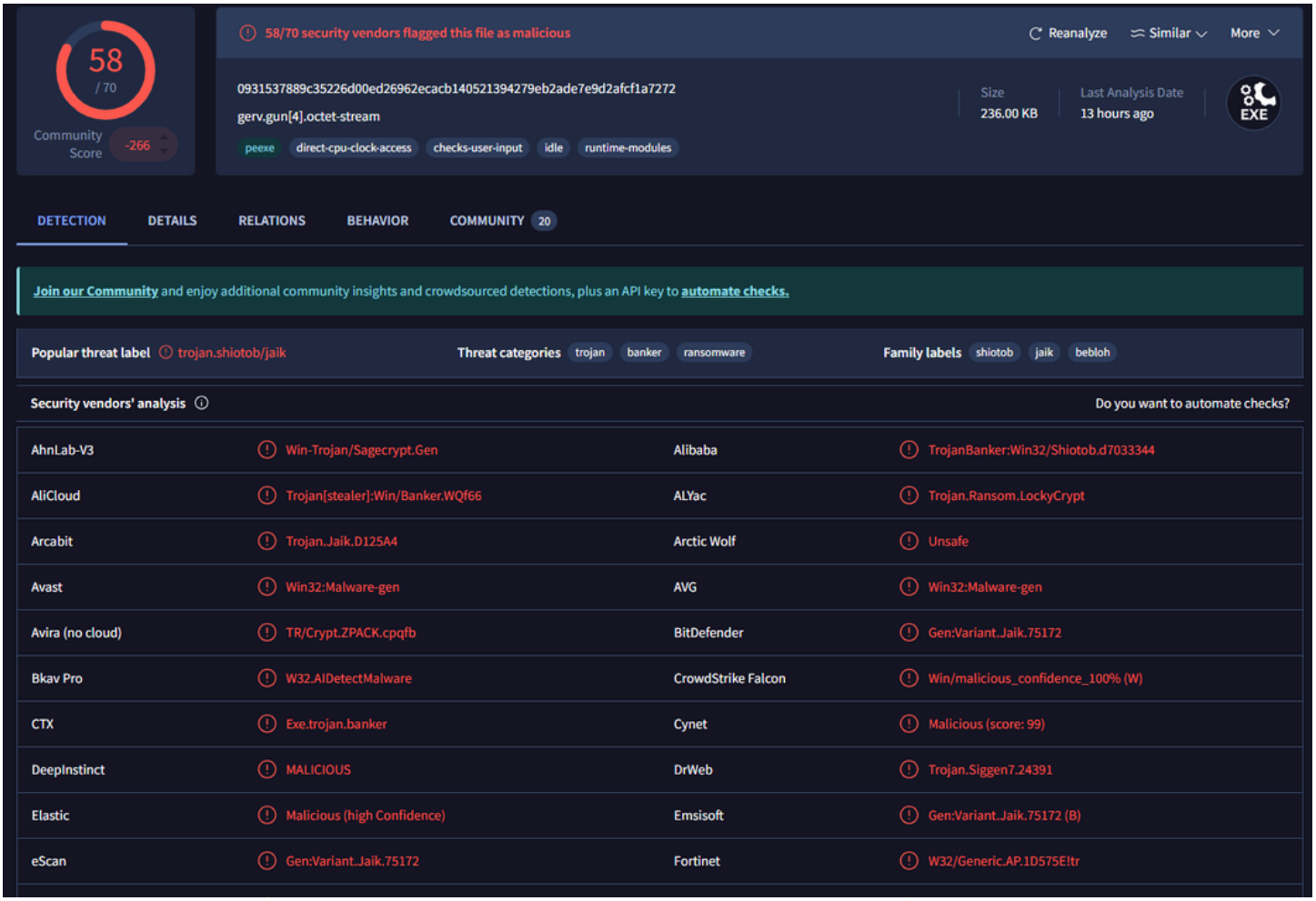
Picture 1.


62
/ 72
Community Score
-12
62/72 security vendors flagged this file as malicious
Reanalyze
Similar
More
79d503165d32176842fe386d96c04fb70f6ce1c8a485837957849297e625ea48
wp.exe
Size
300.50 KB
Last Analysis Date
7 days ago
EXE
peexe
spreader
self-delete
corrupt
persistence
checks-user-input
checks-cpu-name
long-sleeps
malware
detect-debug-environment
DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY 8
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Popular threat label trojan.ursnif/nymaim
Threat categories trojan ransomware
Family labels ursnif nymaim cerber
Security vendors' analysis
Do you want to automate checks?
AhnLab-V3 Trojan/Win32.Ursnif.R208257
Alibaba Backdoor:Win32/Ursnif.5e3f1e81
AliCloud Backdoor:Win/Ursnif.Gen
ALYac Trojan.Ransom.Cerber
Antiy-AVL Trojan[Spy]/Win32.Ursnif
Arcabit Generic.Nymaim.E.5FB90396
Arctic Wolf Unsafe
Avast Win32:Malware-gen
AVG Win32:Malware-gen
Avira (no cloud) HEUR/AGEN.1341699
BitDefender Generic.Nymaim.E.5FB90396
Bkav Pro W32.AIDetectMalware
CrowdStrike Falcon Win/malicious_confidence_100% (W)
CTX Exe.trojan.ursnif
Cynet Malicious (score: 99)
DeepInstinct MALICIOUS
DrWeb Trojan.Gozi.24
Elastic Malicious (high Confidence)
Emsisoft Generic.Nymaim.E.5FB90396 (B)
eScan Generic.Nymaim.E.5FB90396
ESET-NOD32 Win32/Kryptik.FTXE Trojan
Fortinet W32/GenKryptik.ANOR!tr
GData Generic.Nymaim.E.5FB90396
Google Detected

Picture 2.


66
/ 72
Community Score
-85
66/72 security vendors flagged this file as malicious
Reanalyze
Similar
More
94a0a09ee6a21526ac34d41eabf4ba603e9a30c26e6a1dc072ff45749dfb1fe1
Pedals.exe
Size
323.00 KB
Last Analysis Date
1 month ago
EXE
peexe
spreader
checks-network-adapters
detect-debug-environment
long-sleeps
suspicious-dns
runtime-modules
malware
direct-cpu-clock-access
via-tor
persistence
cve-2016-2569
cve-2005-0446
cve-2015-1729
exploit
DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY 28+
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Popular threat label trojan.cutwail/wigon
Threat categories trojan dropper
Family labels cutwail wigon usvn
Security vendors' analysis
Do you want to automate checks?
AhnLab-V3 Win-Trojan/Sagecrypt.Gen
Alibaba TrojanDropper:Win32/Cutwail.62278ef9
AliCloud Trojan:Win/Wigon.PL
ALYac Trojan.Injector
Antiy-AVL Trojan/Win32.Cutwail
Arcabit Trojan.Generic.D53FA53
Arctic Wolf Unsafe
Avast Win32:Malware-gen
AVG Win32:Malware-gen
Avira (no cloud) TR/FileCoder.JX
BitDefender Trojan.GenericKD.5503571
Bkav Pro W32.AIDetectMalware
CrowdStrike Falcon Win/malicious_confidence_100% (W)
CTX Exe.trojan.cutwail
Cynet Malicious (score: 99)
DeepInstinct MALICIOUS
DrWeb Trojan.DownLoad.64914
Elastic Malicious (high Confidence)

Picture 3.


58
/ 70
Community Score
-266
58/70 security vendors flagged this file as malicious
Reanalyze
Similar
More
0931537889c35226d00ed26962ecacb140521394279eb2ade7e9d2afcf1a7272
gerv.gun[4].octet-stream
Size
236.00 KB
Last Analysis Date
13 hours ago
EXE
peexe
direct-cpu-clock-access
checks-user-input
idle
runtime-modules
DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY 20
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Popular threat label trojan.shiotob/jaik
Threat categories trojan banker ransomware
Family labels shiotob jaik bebloh
Security vendors' analysis
Do you want to automate checks?
AhnLab-V3 Win-Trojan/Sagecrypt.Gen
Alibaba TrojanBanker:Win32/Shiotob.d7033344
AliCloud Trojan[stealer]:Win/Banker.WQf66
ALYac Trojan.Ransom.LockyCrypt
Arcabit Trojan.Jaik.D125A4
Arctic Wolf Unsafe
Avast Win32:Malware-gen
AVG Win32:Malware-gen
Avira (no cloud) TR/Crypt.ZPACK.cpqfb
BitDefender Gen:Variant.Jaik.75172
Bkav Pro W32.AIDetectMalware
CrowdStrike Falcon Win/malicious_confidence_100% (W)
CTX Exe.trojan.banker
Cynet Malicious (score: 99)
DeepInstinct MALICIOUS
DrWeb Trojan.Siggen7.24391
Elastic Malicious (high Confidence)
Emsisoft Gen:Variant.Jaik.75172 (B)
eScan Gen:Variant.Jaik.75172
Fortinet W32/Generic.AP.1D575E!tr

Tools

Used tools in a list:

- Wireshark
- Security Onion
- Kibana
- Virustotal
- Canva
- ChatGPT(Summarize text and analyze alert messages)
- AbuseDB
- SSL Blacklist

JJ, JO