WIRESHARK EVIDENCE ANALYSIS

Domain Targeted: Stormtheory[.]info

Infected Host IP: 10[.]2[.]23[.]231

Infected Host MAC Address: 00:11:0a:9f:c0:2d

Domain Controller: 10[.]2[.]23[.]2

Infected Hostname: FERGUSON-WIN-PC (10.2.23[.]231)

Other Host Observed: SUTTON-WIN-PC (10.2.23[.]109)

What Happened (Chronological PCAP summary)

The user logs in like normal (FERGUSON), conducting very normal activity. We see activity among msfnsci and isatap which seem to be normal networking behaviors. Another user, (SUTTON) also logs in and conducts normal activity. Later in the frames, we see that the user of Sutton-Win-PC gets hungry and attempts to access the domain rootcafeslc[.]com, which seems to be hosted on a Squarespace server and believed to be safe. At frame 3116, the host of FERGUSON-WIN-PC initiates a tcp handshake with malicious web server hosting the IP 209.141.55[.]226. After the connection was acknowledged, a steganographic JPEG troll11[.]jpg was requested by the host. This JPEG is believed to have maliciously embedded payloads coded within it and once executed, a C2 (Command & Control) connection is established.

The file troll1[.]jpg is classified as a trickbot/trick loader malware. This software infiltrates devices to deliver malicious payloads. The malware is capable of infecting victims' computers, analyzing their system information, and installing other types of threats, such as trojans and stealers as well as establishing persistence via C2 connections for further malware exploitation. The loaders are typically delivered through phishing emails and links and rely on social engineering to trick users into downloading what they believe to be images but in reality, is an executable. The malware utilizes advanced evasion and persistence tactics like code obfuscation or injecting themselves within legitimate processes (like iexplorer[.]exe) to avoid detection.

Once the attacker sent this malicious script embedded in what seemed to be a jpeg file, later in the frames we see a DNS request from the infected machine to dicarkadar[.]com. This web server has been flagged malicious and reported for C2 communications. We see a later query for cranetisti[.]com, another C2 using the same JA3 footprint as dicarkadar. The attacker communicates with the user over TLS encryption, pushing and pulling data until the connection dies because the infected machine can no longer reach it. The attacker seems to get a new IP and establishes a TCP connection before forwarding a malicious assembly file named tinx86. This has been reported for malware in past reports.......... to summarize everything else, the attacker used various domains under the same JA3 footprint (believed to be hosted by GoDaddy), used WebSocket connections to evade detection and establish persistence, attempted to exploit vulnerabilities in SMB server, data exfiltration, among other things.

Source: 10[.]2[.]23[.]231

Date Breach Discovered: 2/23/2019 at 7:24:36 PM

Date of Disclosure:

2/23/2019 at 7:49:16 PM (potential Outlook credentials leak)

2/23/2019 at 7:50:15 PM (domain info leak)

2/23/2019 at 7:50:44 PM (system info leak)

2/23/2019 at 7:49:13 PM (potential card info leak)

How Was Disclosure Discovered:

Followed and observed TCP stream of malicious traffic occurring between the IP 190[.]146[.]112[.]216 (suspected C2 server) and our infected machine 10[.]2[.]23[.]231 (FERGUSON-WIN-PC). The attacker made multiple POST requests via HTTP to the infected machine requesting outlook passwords, card/billing info, as well as network and system information.

Summary of Events:

The user makes a GET request to the malicious IP 209[.]141[.]55[.]226 for troll1[.]jpg. This jpeg uses maliciously embedded shellcode to execute what is believed to be vulnerabilities present in the user's browser and system (Windows 7). This eventually redirected the user to dicarkadar[.]com and cranetisti[.]com, two extensively reported C2 servers. From here, the user made two get requests, one for Tinx86[.]exe and one for Sw9JKmXqaSj[.]exe; Both have been extensively reported for malicious activity. After establishing a persistent connection with the machine with multiple backdoors; The attacker establishes WebSocket connections for uninterrupted persistence. We also found evidence of malicious SMB traffic with the attacker attempting to exploit shared folders and services such as samr, lsarpc, IPC$, NT rename, netlogon, and others using anonymous login attempts. The attacker also attempts to laterally move and escalate privileges, exfiltrate sensitive host data like sysinfo, card info, outlook passwords, etc. Much more information may have been exposed but due to the use of TLS and other encrypted communication methods, we were unable to determine what else was exposed/stolen.

Summary of Investigative Process and System Involved

IP ADDRESSES	**REMARKS**
10[.]2[.]23[.]2	Stormtheory.info Domain Controller
10[.]2[.]23[.]231	Infected Machine within Storm theory domain
209[.]141[.]55[.]226	Malicious Web Server
46[.]249[.]62[.]199	Malicious Web Server
87[.]236[.]22[.]142	Malicious Web Server
85[.]143[.]218[.]7	Malicious Web Server
213[.]226[.]68[.]112	Malicious Web Server
195[.]123[.]246[.]99	Malicious Web Server
190[.]146[.]112[.]216	Malicious Web Server

RESOLVED DOMAINS	REMARKS
Rootscafelc[.]com	Not malicious, but infected
dicarkadar[.]com	C2 Server
cranetisti[.]com	C2 Server
SUPERHAPS[.]PW	C2 Server
IPECHO[.]NET	Not malicious but used to return information about the user (browser identification, http headers, proxy detection etc.)

FILE NAME & EXECUTABLES	REMARKS	SHA256 HASH
Troll1[.]jpg	DLL executable	8cf2cddda8522975a22da3da429339be471234eacc0e11c099d6dcb732cf3cbb
Sw9JKmXqaSj[.]exe	DLL executable	d43159c8bf2e1bd866abdbb1687911e2282b1f98a7c063f85ffd53a7f51efed4
Tinx86_14[.]exe	DLL executable	f1b789be1126b557240dd0dfe98fc5f3ad6341bb1a5d8be0a954f65b486ad32a
win[.]png	Obfuscated	38c6c5b8d6fa71d9856758a5c0c2ac9d0a0a1450f75bb1004dd988e23d73a312
tin[.]png	Obfuscated	4c957072ab097d3474039f432466cd251d1dc7d91559b76d4e5ead4a8bd499d5
sin[.]png	Obfuscated	3abae6dd2ddae23b2de2ccbcc160a4a5773bef8934d0e6896d50197c3d3c417f

Methodology Summary

Our investigation focused on analyzing a captured PCAP file containing suspicious network traffic. The goal was to identify signs of malicious activity, determine the attack flow, and understand the potential impact.

1. Event Correlation Using Security Onion and Wireshark: We began by reviewing event logs in Security Onion documents to identify anomalous network behavior and possible indicators of compromise. These were correlated with packet-level details in Wireshark to verify the events and understand the sequence of communication, including suspicious domains, IPs, and file transfers.

2. Snapshotting and Network Isolation: During the investigation process, we took snapshots at key stages to preserve our progress and prevent loss of investigative data. Additionally, we analyzed the PCAP in an isolated environment, with the network disconnected, to ensure that no malicious content embedded in the traffic could be executed or affect the analysis system.

3. File Extraction and Hashing: Suspicious files observed in the PCAP (e.g., troll1.jpg, Sw9JKmXqaSj.exe) were extracted and saved rather than executed or downloaded. We then

generated SHA-256 hashes using the sha256sum command, allowing us to safely identify the files and investigate them further without executing any code.

4. Malware and Threat Intelligence Analysis: The generated hashes were submitted to VirusTotal for analysis. This provided threat intelligence including file reputation, malware classification, detection across antivirus engines, and associated malicious infrastructure (such as C2 servers and domains). Furthermore, AbuseIPDB, CrowdSec CTI, and urlscan[.]io reinforced our understanding of the intent of these malicious files/domains via MITRE ATT&CK techniques and behavioral history.

This methodology enabled a comprehensive and secure investigation of the PCAP file, helping us uncover the infection vector, attacker behavior, and scope of compromise without risking further contamination.

Obfuscation Techniques Observed:

Use of PADDINGX to evade detection during malware execution.

Obfuscated PE executables avoiding disk writes.

Code embedded in image files (e.g., PNGs) to bypass scanners.

Use of encrypted WebSocket and HTTPS connections to obscure payload delivery and C2 communications.

These findings suggest a coordinated and multi-phased attack using TrickBot and associated malware families, leveraging obfuscation, credential theft, system reconnaissance, and advanced persistence mechanisms.

Member(s) Impacted:

Ferguson-Win-PC[.]stormtheory[.]info

Sutton-Win-PC[.]stormtheory[.]info (Potentially impacted, present in logs but no interaction with malicious subjects was observed)

Type of PII/Confidential Data:

Potential leak of card and billing information (2/23/2019 at 7:49:13 PM)

Potential leak of Outlook Password (2/23/2019 at 7:49:16 PM)

Confirmed leak of Domain Information (2/23/2019 at 7:50:15 PM)

Confirmed leak of System Information (2/23/2019 at 7:50:44 PM)

Type of Incident:

Social Engineering

Where did the incident take place:

Utah (presumably north Utah)

Root Cause:

The host of FERGUSON-WIN-PC initiates a tcp handshake with a malicious web server hosting the IP 209.141.55[.]226. After acknowledgement, a steganographic JPEG troll11[.]jpg was requested by the host. This JPEG is believed to have maliciously embedded payloads coded within it and once executed, a C2 (Command & Control) connection is established.

Corrective Action:

None, Although, at 7:49:35, the user made multiple DNS queries for IP abused databases, the C2 connections persisted

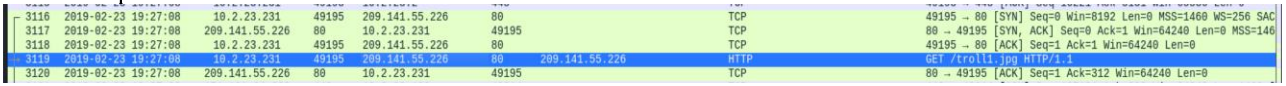
To effectively investigate and rid a system of malware:

1. Firstly, to see if a system is infected; Explore autoruns, use process explorer to see active/past processes run. Consider running netstat to view any open communications that may seem suspicious and use Wireshark to further analyze this suspicious traffic.
2. If the device is concluded to be infected, it should be disconnected or separated from the main network. If segregated, disable unnecessary ports as they could be hosting the gateway for C2 communications.
3. Identify stored credentials, consider changing them all if possible as they are all possibly exposed
4. Use FTK Imager or dd (forensic imagers) to create a forensic disk image. This image will be loaded into forensic analysis tools like Autopsy to investigate the presence of malicious files
5. Once evidence is collected and transferred to a device capable of forensic analysis, shutdown the machine and boot in safe mode (or equivalent) to clean drive of processes identified as malicious
6. If rootkit or persistent action is discovered during any part of the investigation, reimage or reinstall the operating system
7. Investigate other systems on network to mitigate the effects of a potential worm infection

Findings: (Split up into major events, referred to as Occurrences)

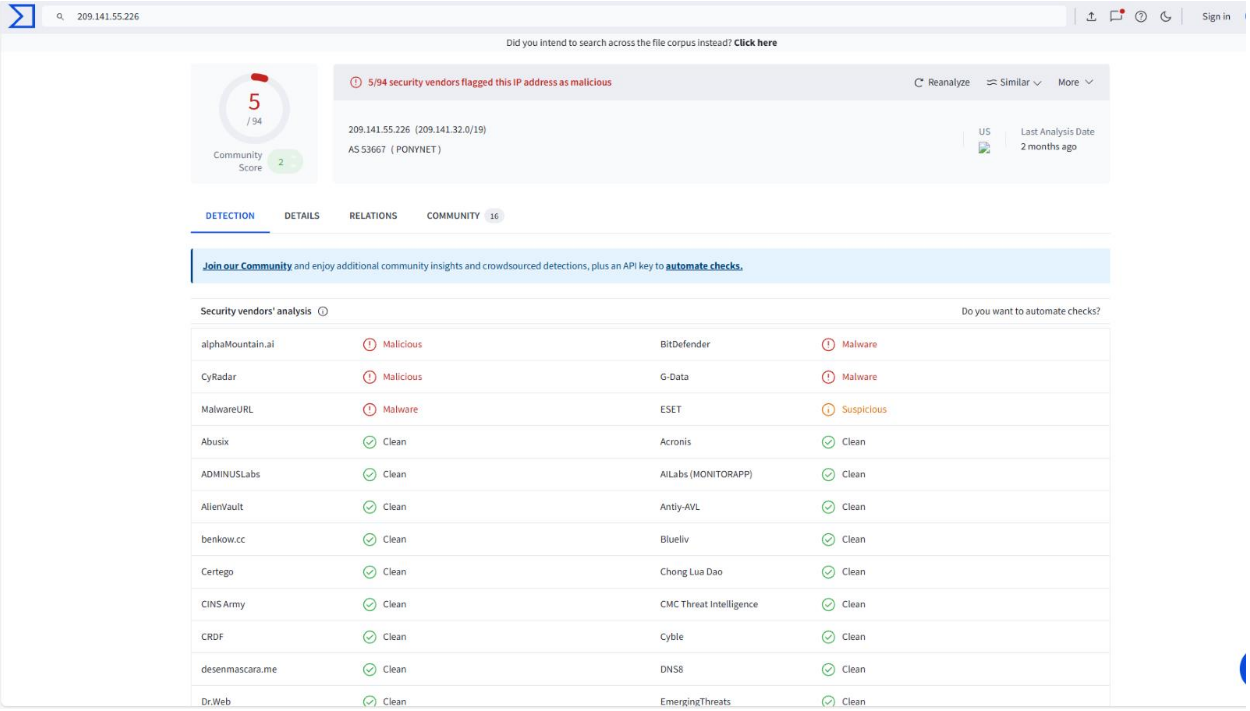
First Occurrence:
-Malicious TCP connection with 209[.]141[.]55[.]226

-GET request for malicious JPG file



```
3116  2019-02-23 19:27:08    10.2.23.231    49195  209.141.55.226   80                      TCP     49195 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SAC
3117  2019-02-23 19:27:08  209.141.55.226   80     10.2.23.231      49195                   TCP     80 → 49195 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=146
3118  2019-02-23 19:27:08    10.2.23.231    49195  209.141.55.226   80                      TCP     49195 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
3119  2019-02-23 19:27:08    10.2.23.231    49195  209.141.55.226   80     209.141.55.226   HTTP    GET /troll1.jpg HTTP/1.1
3120  2019-02-23 19:27:08  209.141.55.226   80     10.2.23.231      49195                   TCP     80 → 49195 [ACK] Seq=1 Ack=312 Win=64240 Len=0
```

Explanation: TCP Handshake with extensively reported IP



209.141.55.226

Did you intend to search across the file corpus instead? **Click here**

5 / 94

Community Score 2

5/94 security vendors flagged this IP address as malicious

Reanalyze | Similar | More

209.141.55.226 (209.141.32.0/19)

AS 53667 (PONYNET)

US

Last Analysis Date
2 months ago

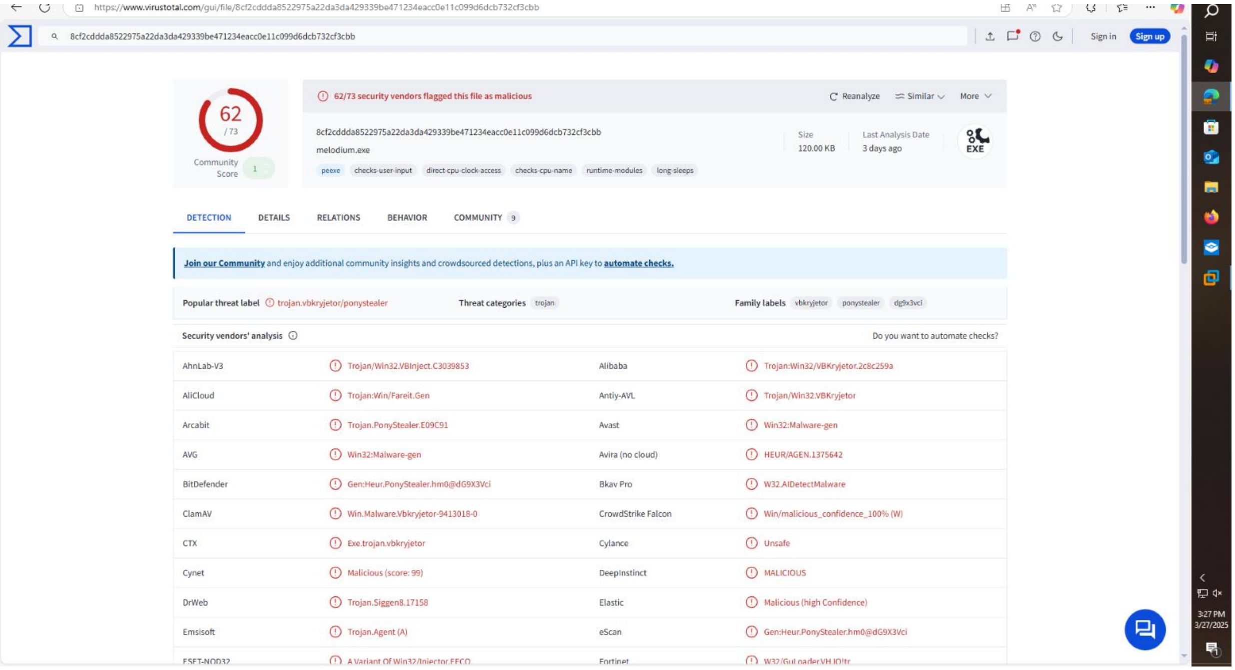
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to **automate checks.**

Security vendors' analysis

Do you want to automate checks?

alphaMountain.ai	Malicious	BitDefender	Malware
CyRadar	Malicious	G-Data	Malware
MalwareURL	Malware	ESET	Suspicious
Abusix	Clean	Acronis	Clean
ADMINUSLabs	Clean	AILabs (MONITORAPP)	Clean
AlienVault	Clean	Antiy-AVL	Clean
benkow.cc	Clean	Blueliv	Clean
Certego	Clean	Chong Lua Dao	Clean
CINS Army	Clean	CMC Threat Intelligence	Clean
CRDF	Clean	Cyble	Clean
desenmascara.me	Clean	DNS8	Clean
Dr.Web	Clean	EmergingThreats	Clean

Explanation: Results of VirusTotal lookup on IP



https://www.virustotal.com/gui/file/8cf2cddda8522975a22da3da429339be471234eacc0e11c099d6dcb732cf3cbb

8cf2cddda8522975a22da3da429339be471234eacc0e11c099d6dcb732cf3cbb

62 / 73

Community Score 1

62/73 security vendors flagged this file as malicious

Reanalyze | Similar | More

8cf2cddda8522975a22da3da429339be471234eacc0e11c099d6dcb732cf3cbb

melodium.exe

peexe | checks-user-input | direct-cpu-clock-access | checks-cpu-name | runtime-modules | long-sleeps

Size
120.00 KB

Last Analysis Date
3 days ago

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

Popular threat label trojan.vbkryjetor/ponystealer | Threat categories trojan | Family labels vbkryjetor ponystealer dg9x3vci

Security vendors' analysis

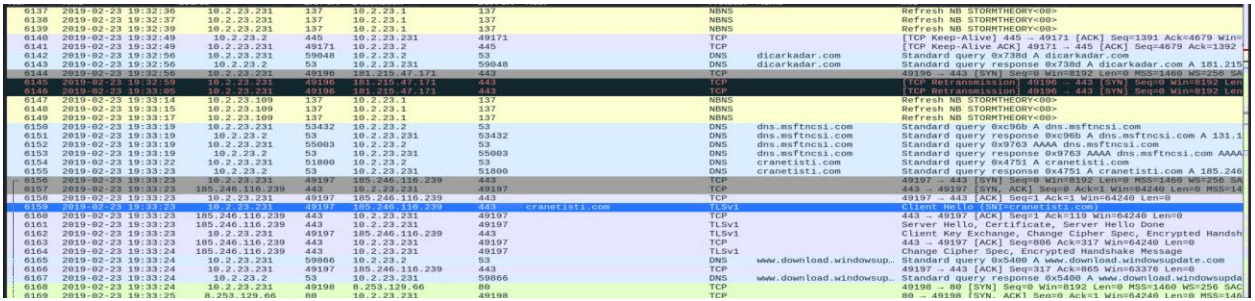
Do you want to automate checks?

AhnLab-V3	Trojan/Win32.VBInject.C3039853	Alibaba	Trojan:Win32/VBKryjetor.2c8c259a
AliCloud	Trojan:Win/Fareit.Gen	Antiy-AVL	Trojan/Win32.VBKryjetor
Arcabit	Trojan.PonyStealer.E09C91	Avast	Win32:Malware-gen
AVG	Win32:Malware-gen	Avira (no cloud)	HEUR/AGEN.1375642
BitDefender	Gen:Heur.PonyStealer.hm0@dG9X3Vci	Bkav Pro	W32.AIDetectMalware
ClamAV	Win.Malware.Vbkryjetor-9413018-0	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
CTX	Exe.trojan.vbkryjetor	Cylance	Unsafe
Cynet	Malicious (score: 99)	DeepInstinct	MALICIOUS
DrWeb	Trojan.Siggen8.17158	Elastic	Malicious (high Confidence)
Emsisoft	Trojan.Agent (A)	eScan	Gen:Heur.PonyStealer.hm0@dG9X3Vci
ESET-NOD32	A Variant Of Win32/Injector.EFCO	Fortinet	W32/GuLoader.VHJO!tr

Explanation: VirusTotal lookups on Troll1[.]jpg

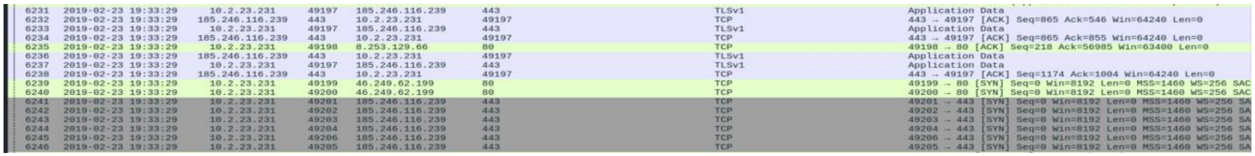
Second Occurrence:

-C2 communications with web servers dicarkadar[.]com and cranetisti[.]com
-C2 server IP: 185[.]246[.]116[.]239



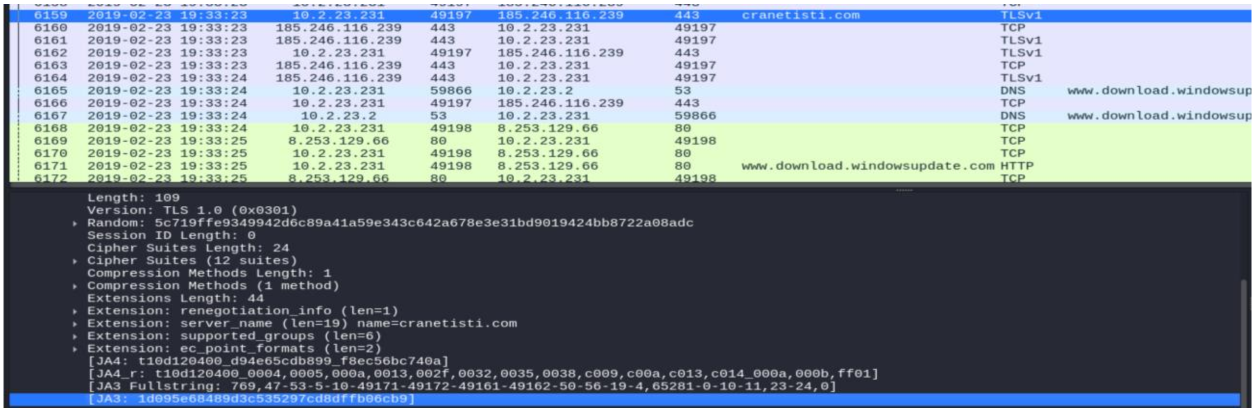
```
6137  2019-02-23 19:32:36    10.2.23.231     137    10.2.23.1        137                      NBNS                               Refresh NB STORMTHEORY<00>
6138  2019-02-23 19:32:37    10.2.23.231     137    10.2.23.1        137                      NBNS                               Refresh NB STORMTHEORY<00>
6139  2019-02-23 19:32:39    10.2.23.231     137    10.2.23.1        137                      NBNS                               Refresh NB STORMTHEORY<00>
6140  2019-02-23 19:32:49     10.2.23.2      445    10.2.23.231      49171                    TCP                                [TCP Keep-Alive] 445 → 49171 [ACK] Seq=1391 Ack=4679 Win=
6141  2019-02-23 19:32:49    10.2.23.231     49171  10.2.23.2        445                      TCP                                [TCP Keep-Alive ACK] 49171 → 445 [ACK] Seq=4679 Ack=1392
6142  2019-02-23 19:32:56    10.2.23.231     59048  10.2.23.2        53                       DNS     dicarkadar.com             Standard query 0x738d A dicarkadar.com
6143  2019-02-23 19:32:56     10.2.23.2      53     10.2.23.231      59048                    DNS     dicarkadar.com             Standard query response 0x738d A dicarkadar.com A 181.215
6144  2019-02-23 19:32:56    10.2.23.231     49196  181.215.47.171   443                      TCP                                49196 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SA
6145  2019-02-23 19:32:59    10.2.23.231     49196  181.215.47.171   443                      TCP                                [TCP Retransmission] 49196 → 443 [SYN] Seq=0 Win=8192 Len
6146  2019-02-23 19:33:05    10.2.23.231     49196  181.215.47.171   443                      TCP                                [TCP Retransmission] 49196 → 443 [SYN] Seq=0 Win=8192 Len
6147  2019-02-23 19:33:14    10.2.23.109     137    10.2.23.1        137                      NBNS                               Refresh NB STORMTHEORY<00>
6148  2019-02-23 19:33:15    10.2.23.109     137    10.2.23.1        137                      NBNS                               Refresh NB STORMTHEORY<00>
6149  2019-02-23 19:33:17    10.2.23.109     137    10.2.23.1        137                      NBNS                               Refresh NB STORMTHEORY<00>
6150  2019-02-23 19:33:19    10.2.23.231     53432  10.2.23.2        53                       DNS     dns.msftncsi.com           Standard query 0xc96b A dns.msftncsi.com
6151  2019-02-23 19:33:19     10.2.23.2      53     10.2.23.231      53432                    DNS     dns.msftncsi.com           Standard query response 0xc96b A dns.msftncsi.com A 131.1
6152  2019-02-23 19:33:19    10.2.23.231     55003  10.2.23.2        53                       DNS     dns.msftncsi.com           Standard query 0x9763 AAAA dns.msftncsi.com
6153  2019-02-23 19:33:19     10.2.23.2      53     10.2.23.231      55003                    DNS     dns.msftncsi.com           Standard query response 0x9763 AAAA dns.msftncsi.com AAAA
6154  2019-02-23 19:33:22    10.2.23.231     51800  10.2.23.2        53                       DNS     cranetisti.com             Standard query 0x4751 A cranetisti.com
6155  2019-02-23 19:33:23     10.2.23.2      53     10.2.23.231      51800                    DNS     cranetisti.com             Standard query response 0x4751 A cranetisti.com A 185.246
6156  2019-02-23 19:33:23    10.2.23.231     49197  185.246.116.239  443                      TCP                                49197 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SA
6157  2019-02-23 19:33:23  185.246.116.239   443    10.2.23.231      49197                    TCP                                443 → 49197 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=14
6158  2019-02-23 19:33:23    10.2.23.231     49197  185.246.116.239  443                      TCP                                49197 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
6159  2019-02-23 19:33:23    10.2.23.231     49197  185.246.116.239  443    cranetisti.com    TLSv1                              Client Hello (SNI=cranetisti.com)
6160  2019-02-23 19:33:23  185.246.116.239   443    10.2.23.231      49197                    TCP                                443 → 49197 [ACK] Seq=1 Ack=119 Win=64240 Len=0
6161  2019-02-23 19:33:23  185.246.116.239   443    10.2.23.231      49197                    TLSv1                              Server Hello, Certificate, Server Hello Done
6162  2019-02-23 19:33:23    10.2.23.231     49197  185.246.116.239  443                      TLSv1                              Client Key Exchange, Change Cipher Spec, Encrypted Handsh
6163  2019-02-23 19:33:23  185.246.116.239   443    10.2.23.231      49197                    TCP                                443 → 49197 [ACK] Seq=806 Ack=317 Win=64240 Len=0
6164  2019-02-23 19:33:24  185.246.116.239   443    10.2.23.231      49197                    TLSv1                              Change Cipher Spec, Encrypted Handshake Message
6165  2019-02-23 19:33:24    10.2.23.231     59866  10.2.23.2        53                       DNS     www.download.windowsup…    Standard query 0x5400 A www.download.windowsupdate.com
6166  2019-02-23 19:33:24    10.2.23.231     49197  185.246.116.239  443                      TCP                                49197 → 443 [ACK] Seq=317 Ack=865 Win=63376 Len=0
6167  2019-02-23 19:33:24     10.2.23.2      53     10.2.23.231      59866                    DNS     www.download.windowsup…    Standard query response 0x5400 A www.download.windowsupda
6168  2019-02-23 19:33:24    10.2.23.231     49198  8.253.129.66     80                       TCP                                49198 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SAC
6169  2019-02-23 19:33:25   8.253.129.66     80     10.2.23.231      49198                    TCP                                80 → 49198 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=146
```

Explanation: DNS Query for dicarkadar[.]com, TCP connection with cranetisti[.]com

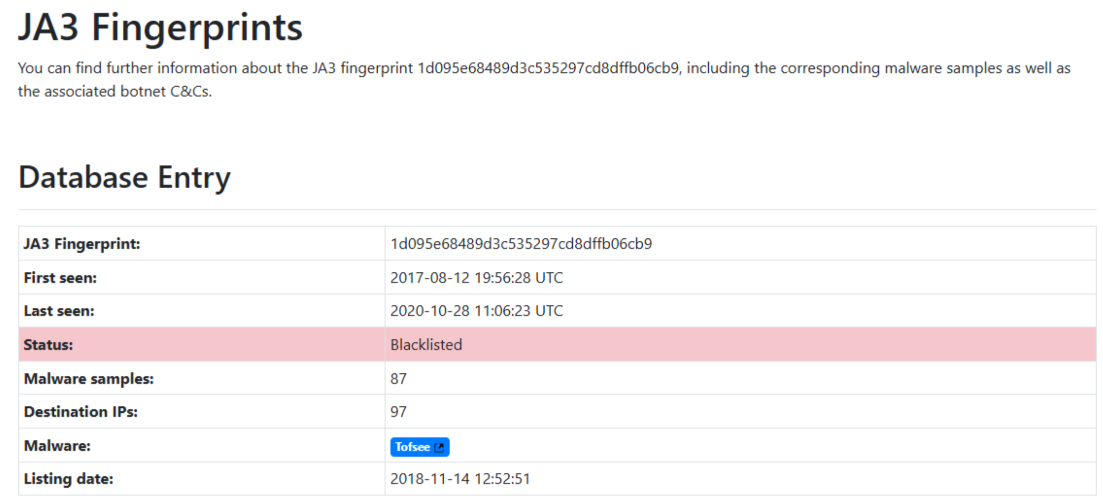


```
6231  2019-02-23 19:33:29    10.2.23.231     49197  185.246.116.239  443     TLSv1     Application Data
6232  2019-02-23 19:33:29  185.246.116.239   443    10.2.23.231      49197   TCP       443 → 49197 [ACK] Seq=865 Ack=546 Win=64240 Len=0
6233  2019-02-23 19:33:29    10.2.23.231     49197  185.246.116.239  443     TLSv1     Application Data
6234  2019-02-23 19:33:29  185.246.116.239   443    10.2.23.231      49197   TCP       443 → 49197 [ACK] Seq=865 Ack=855 Win=64240 Len=0
6235  2019-02-23 19:33:29    10.2.23.231     49198  8.253.129.66     80      TCP       49198 → 80 [ACK] Seq=218 Ack=56985 Win=63400 Len=0
6236  2019-02-23 19:33:29  185.246.116.239   443    10.2.23.231      49197   TLSv1     Application Data
6237  2019-02-23 19:33:29    10.2.23.231     49197  185.246.116.239  443     TLSv1     Application Data
6238  2019-02-23 19:33:29  185.246.116.239   443    10.2.23.231      49197   TCP       443 → 49197 [ACK] Seq=1174 Ack=1004 Win=64240 Len=0
6239  2019-02-23 19:33:29    10.2.23.231     49199  46.249.62.199    80      TCP       49199 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SAC
6240  2019-02-23 19:33:29    10.2.23.231     49200  46.249.62.199    80      TCP       49200 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SAC
6241  2019-02-23 19:33:29    10.2.23.231     49201  185.246.116.239  443     TCP       49201 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SA
6242  2019-02-23 19:33:29    10.2.23.231     49202  185.246.116.239  443     TCP       49202 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SA
6243  2019-02-23 19:33:29    10.2.23.231     49203  185.246.116.239  443     TCP       49203 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SA
6244  2019-02-23 19:33:29    10.2.23.231     49204  185.246.116.239  443     TCP       49204 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SA
6245  2019-02-23 19:33:29    10.2.23.231     49206  185.246.116.239  443     TCP       49206 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SA
6246  2019-02-23 19:33:29    10.2.23.231     49205  185.246.116.239  443     TCP       49205 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SA
```

Explanation: Application Data being sent from infected host to C2



```
6159  2019-02-23 19:33:23    10.2.23.231     49197  185.246.116.239  443    cranetisti.com                    TLSv1
6160  2019-02-23 19:33:23  185.246.116.239   443    10.2.23.231      49197                                    TCP
6161  2019-02-23 19:33:23  185.246.116.239   443    10.2.23.231      49197                                    TLSv1
6162  2019-02-23 19:33:23    10.2.23.231     49197  185.246.116.239  443                                      TLSv1
6163  2019-02-23 19:33:23  185.246.116.239   443    10.2.23.231      49197                                    TCP
6164  2019-02-23 19:33:24  185.246.116.239   443    10.2.23.231      49197                                    TLSv1
6165  2019-02-23 19:33:24    10.2.23.231     59866  10.2.23.2        53                                       DNS     www.download.windowsup
6166  2019-02-23 19:33:24    10.2.23.231     49197  185.246.116.239  443                                      TCP
6167  2019-02-23 19:33:24     10.2.23.2      53     10.2.23.231      59866                                    DNS     www.download.windowsup
6168  2019-02-23 19:33:24    10.2.23.231     49198  8.253.129.66     80                                       TCP
6169  2019-02-23 19:33:25   8.253.129.66     80     10.2.23.231      49198                                    TCP
6170  2019-02-23 19:33:25    10.2.23.231     49198  8.253.129.66     80                                       TCP
6171  2019-02-23 19:33:25    10.2.23.231     49198  8.253.129.66     80     www.download.windowsupdate.com    HTTP
6172  2019-02-23 19:33:25   8.253.129.66     80     10.2.23.231      49198                                    TCP

        Length: 109
        Version: TLS 1.0 (0x0301)
      ▸ Random: 5c719ffe9349942d6c89a41a59e343c642a678e3e31bd9019424bb8722a08adc
        Session ID Length: 0
        Cipher Suites Length: 24
      ▸ Cipher Suites (12 suites)
        Compression Methods Length: 1
      ▸ Compression Methods (1 method)
        Extensions Length: 44
      ▸ Extension: renegotiation_info (len=1)
      ▸ Extension: server_name (len=19) name=cranetisti.com
      ▸ Extension: supported_groups (len=6)
      ▸ Extension: ec_point_formats (len=2)
        [JA4: t10d120400_d94e65cdb899_f8ec56bc740a]
        [JA4_r: t10d120400_0004,0005,000a,0013,002f,0032,0035,0038,c009,c00a,c013,c014_000a,000b,ff01]
        [JA3 Fullstring: 769,47-53-5-10-49171-49172-49161-49162-50-56-19-4,65281-0-10-11,23-24,0]
        [JA3: 1d095e68489d3c535297cd8dffb06cb9]
```



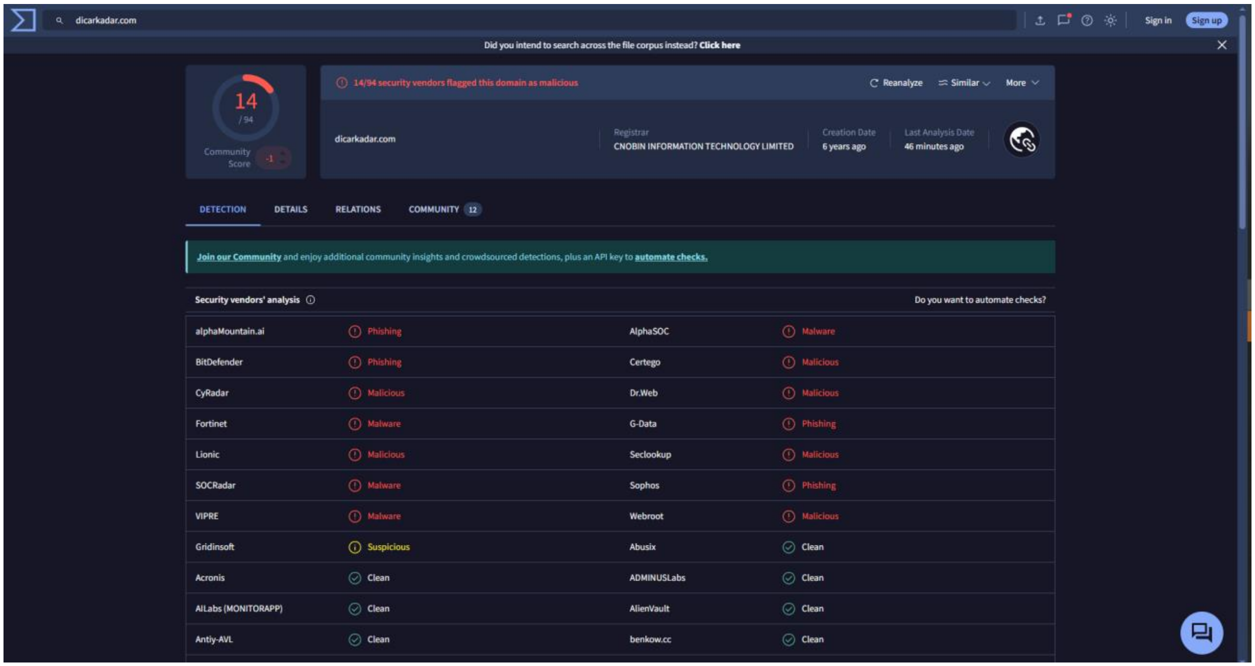
JA3 Fingerprints

You can find further information about the JA3 fingerprint 1d095e68489d3c535297cd8dffb06cb9, including the corresponding malware samples as well as the associated botnet C&Cs.

Database Entry

JA3 Fingerprint:	1d095e68489d3c535297cd8dffb06cb9
First seen:	2017-08-12 19:56:28 UTC
Last seen:	2020-10-28 11:06:23 UTC
Status:	Blacklisted
Malware samples:	87
Destination IPs:	97
Malware:	Tofsee
Listing date:	2018-11-14 12:52:51

Explanation: JA3 Footprint of C2 Web Server and proof it is blacklisted due to malware



14/94 security vendors flagged this domain as malicious

dicarkadar.com

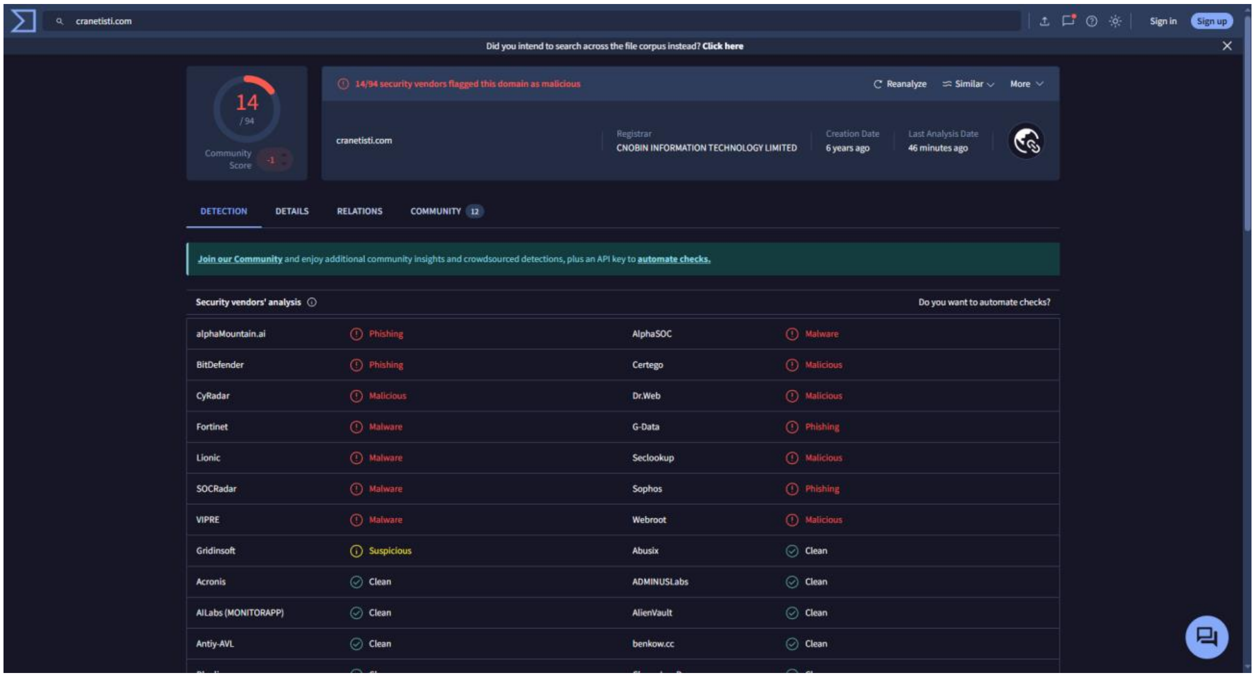
Registrar: CNOBIN INFORMATION TECHNOLOGY LIMITED
Creation Date: 6 years ago
Last Analysis Date: 46 minutes ago

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

Security vendors' analysis ⓘ — Do you want to automate checks?

alphaMountain.ai	Phishing	AlphaSOC	Malware
BitDefender	Phishing	Certego	Malicious
CyRadar	Malicious	Dr.Web	Malicious
Fortinet	Malware	G-Data	Phishing
Lionic	Malicious	Seclookup	Malicious
SOCRadar	Malware	Sophos	Phishing
VIPRE	Malware	Webroot	Malicious
Gridinsoft	Suspicious	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean
AILabs (MONITORAPP)	Clean	AlienVault	Clean
Antiy-AVL	Clean	benkow.cc	Clean

Explanation: Results of VirusTotal lookup on dicarkadar[.]com



14/94 security vendors flagged this domain as malicious

cranetisti.com

Registrar: CNOBIN INFORMATION TECHNOLOGY LIMITED
Creation Date: 6 years ago
Last Analysis Date: 46 minutes ago

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

Security vendors' analysis ⓘ — Do you want to automate checks?

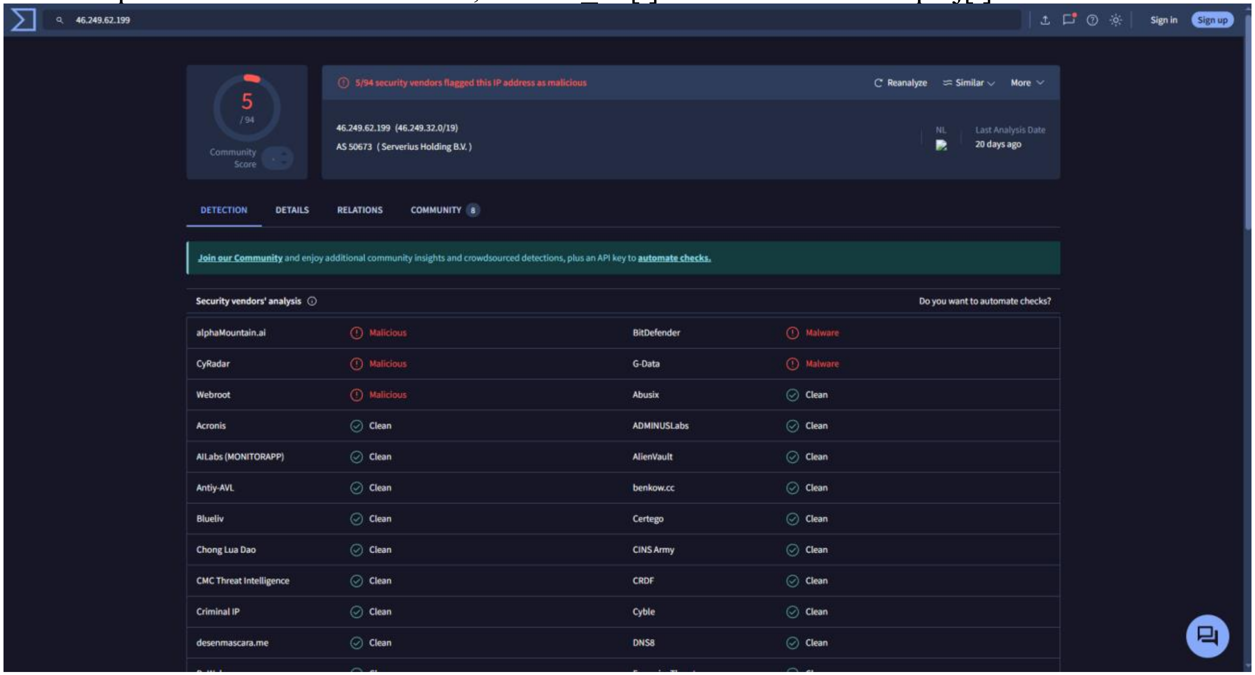
alphaMountain.ai	Phishing	AlphaSOC	Malware
BitDefender	Phishing	Certego	Malicious
CyRadar	Malicious	Dr.Web	Malicious
Fortinet	Malware	G-Data	Phishing
Lionic	Malware	Seclookup	Malicious
SOCRadar	Malware	Sophos	Phishing
VIPRE	Malware	Webroot	Malicious
Gridinsoft	Suspicious	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean
AILabs (MONITORAPP)	Clean	AlienVault	Clean
Antiy-AVL	Clean	benkow.cc	Clean

Explanation: Results of VirusTotal lookup on cranetisti[.]com

Third Occurrence:

-TCP connection with malicious web server 46[.]249[.]62[.]199

-GET request for two malicious files, Tinx86_14[.]exe and Sw9JKmXqaSj[.]exe



46.249.62.199

5/94 security vendors flagged this IP address as malicious

46.249.62.199 (46.249.32.0/19)
AS 50673 (Serverius Holding B.V.)

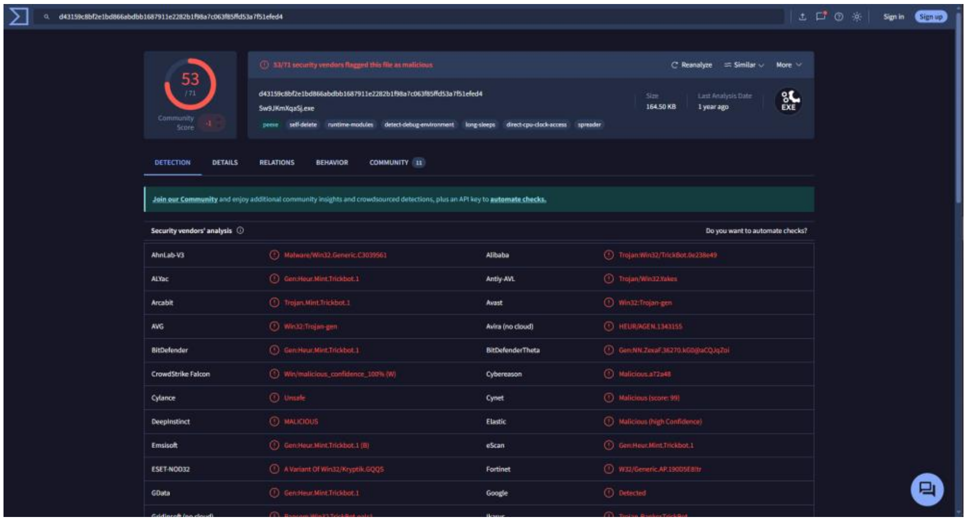
NL · Last Analysis Date: 20 days ago

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

Security vendors' analysis · Do you want to automate checks?

alphaMountain.ai	Malicious	BitDefender	Malware
CyRadar	Malicious	G-Data	Malware
Webroot	Malicious	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean
AILabs (MONITORAPP)	Clean	AlienVault	Clean
Antiy-AVL	Clean	benkow.cc	Clean
Blueliv	Clean	Certego	Clean
Chong Lua Dao	Clean	CINS Army	Clean
CMC Threat Intelligence	Clean	CRDF	Clean
Criminal IP	Clean	Cyble	Clean
desenmascara.me	Clean	DNS8	Clean

Explanation: Results of VirusTotal scan on Web Server 49[.]249[.]62[.]199



d43159c8bf2e1bd866abdbb1687911e2282b1f98a7c063f85ffd53a7f51efed4

53/71 security vendors flagged this file as malicious

d43159c8bf2e1bd866abdbb1687911e2282b1f98a7c063f85ffd53a7f51efed4
Sw9JKmXqaSj.exe

peexe · self-delete · runtime-modules · detect-debug-environment · long-sleeps · direct-cpu-clock-access · spreader

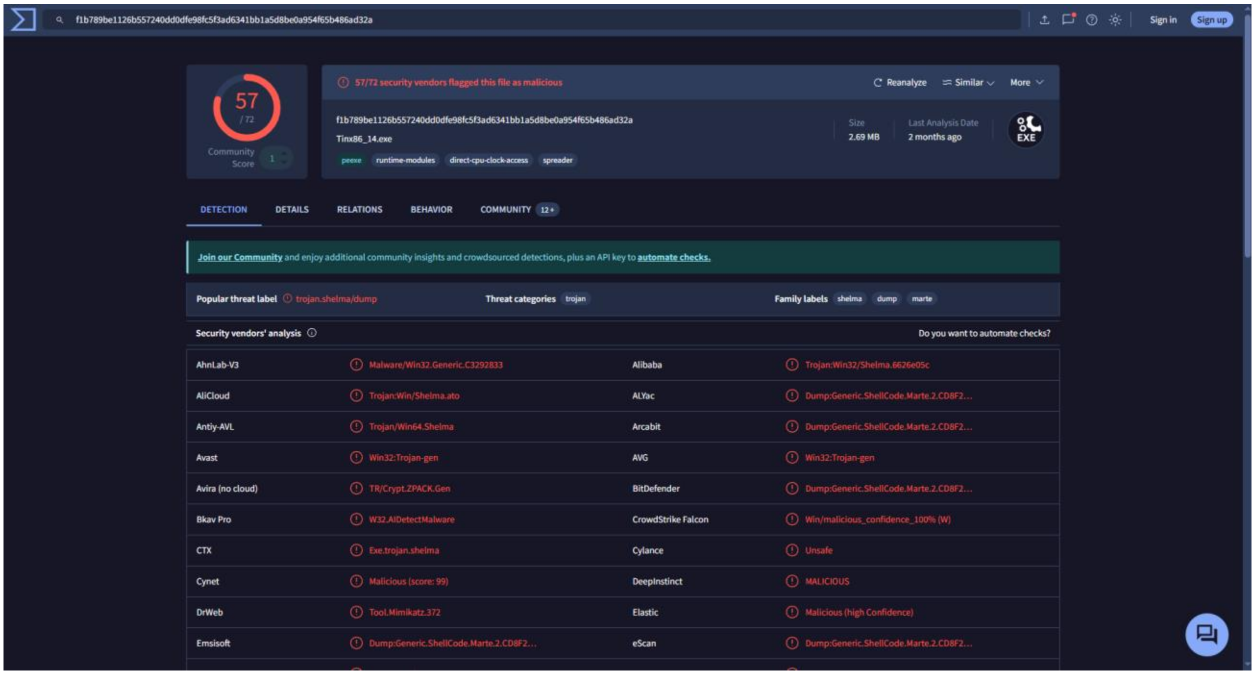
Size: 164.50 KB · Last Analysis Date: 1 year ago

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

Security vendors' analysis · Do you want to automate checks?

AhnLab-V3	Malware/Win32.Generic.C3039561	Alibaba	Trojan:Win32/TrickBot.0e238e49
ALYac	Gen:Heur.Mint.Trickbot.1	Antiy-AVL	Trojan/Win32.Yakes
Arcabit	Trojan.Mint.Trickbot.1	Avast	Win32:Trojan-gen
AVG	Win32:Trojan-gen	Avira (no cloud)	HEUR/AGEN.1343155
BitDefender	Gen:Heur.Mint.Trickbot.1	BitDefenderTheta	Gen:NN.ZexaF.36270.kG0@aCQJqZoi
CrowdStrike Falcon	Win/malicious_confidence_100% (W)	Cybereason	Malicious.a72a48
Cylance	Unsafe	Cynet	Malicious (score: 99)
DeepInstinct	MALICIOUS	Elastic	Malicious (high Confidence)
Emsisoft	Gen:Heur.Mint.Trickbot.1 (B)	eScan	Gen:Heur.Mint.Trickbot.1
ESET-NOD32	A Variant Of Win32/Kryptik.GQQS	Fortinet	W32/Generic.AP.190D5E8!tr
GData	Gen:Heur.Mint.Trickbot.1	Google	Detected

Explanation: Results of VirusTotal lookup for Sw9JKmXqaSj[.]exe hash



f1b789be1126b557240dd0dfe98fc5f3ad6341bb1a5d8be0a954f65b486ad32a

Sign in Sign up

57 / 72 Community Score 1

57/72 security vendors flagged this file as malicious

Reanalyze Similar More

f1b789be1126b557240dd0dfe98fc5f3ad6341bb1a5d8be0a954f65b486ad32a
Tinx86_14.exe

peexe runtime-modules direct-cpu-clock-access spreader

Size 2.69 MB

Last Analysis Date 2 months ago

EXE

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 12+

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

Popular threat label trojan.shelma/dump Threat categories trojan Family labels shelma dump marte

Security vendors' analysis

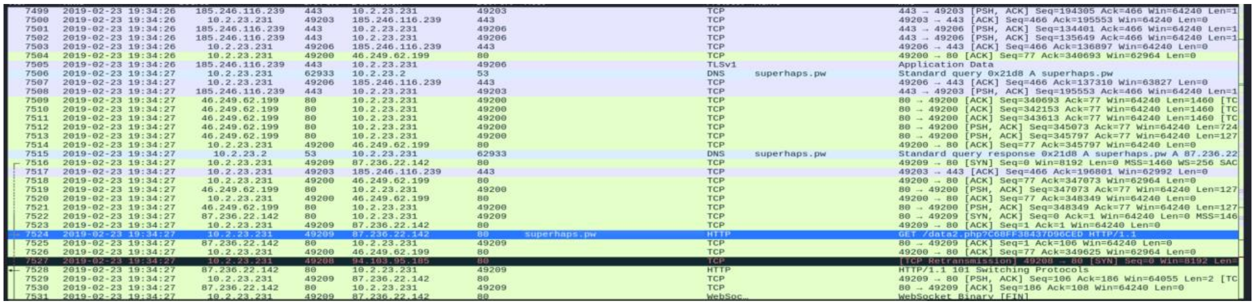
Do you want to automate checks?

AhnLab-V3	Malware/Win32.Generic.C3292833	Alibaba	Trojan:Win32/Shelma.6626e05c
AliCloud	Trojan:Win/Shelma.ato	ALYac	Dump:Generic.ShellCode.Marte.2.CD8F2...
Antiy-AVL	Trojan/Win64.Shelma	Arcabit	Dump:Generic.ShellCode.Marte.2.CD8F2...
Avast	Win32:Trojan-gen	AVG	Win32:Trojan-gen
Avira (no cloud)	TR/Crypt.ZPACK.Gen	BitDefender	Dump:Generic.ShellCode.Marte.2.CD8F2...
Bkav Pro	W32.AIDetectMalware	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
CTX	Exe.trojan.shelma	Cylance	Unsafe
Cynet	Malicious (score: 99)	DeepInstinct	MALICIOUS
DrWeb	Tool.Mimikatz.372	Elastic	Malicious (high Confidence)
Emsisoft	Dump:Generic.ShellCode.Marte.2.CD8F2...	eScan	Dump:Generic.ShellCode.Marte.2.CD8F2...

Explanation: Results of VirusTotal lookup for Tinx86_14[.]exe hash

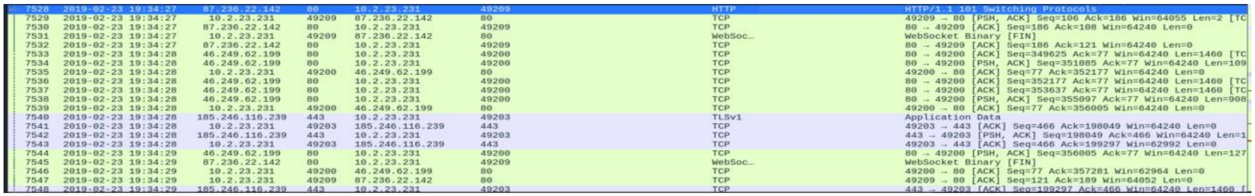
Fourth Occurrence:

-Interaction with IP 87[.]236[.]22[.]142 hosting C2 Server superhaps[.]pw
-Infected host makes GET request to this server, GET /data2[.]php?C68FF38437D96CED
-Use of WebSocket protocol for persistent, continuous, and uninterrupted connection



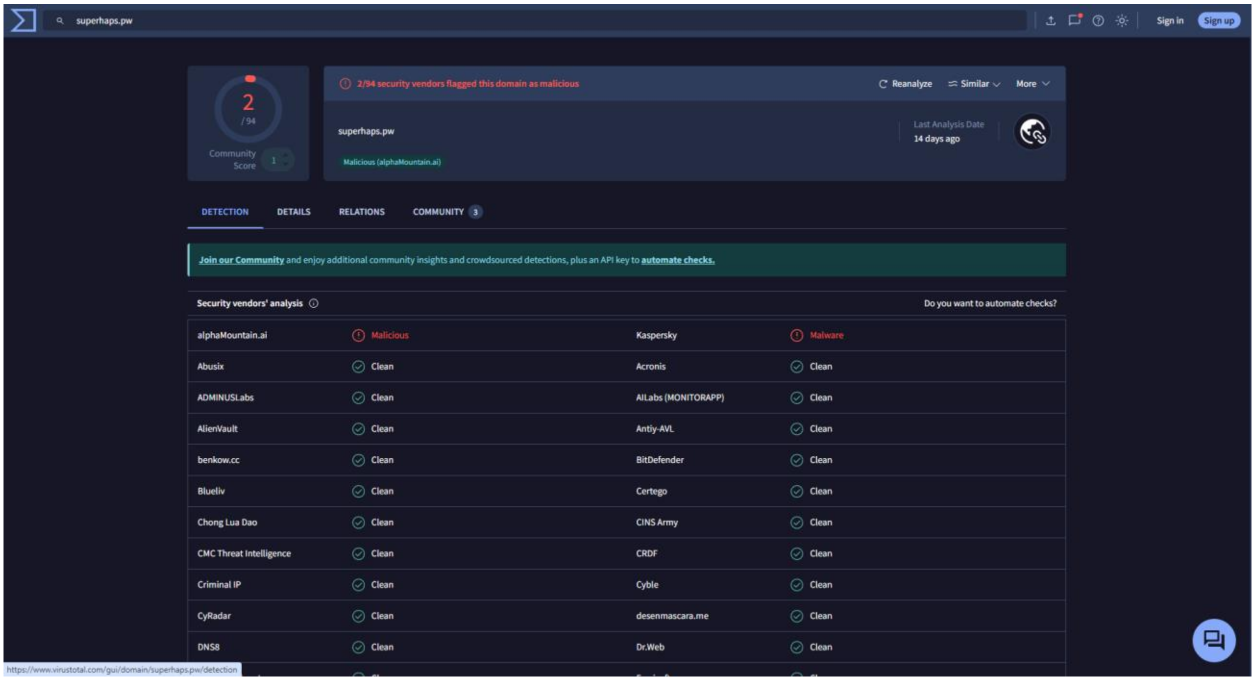
```
7499  2019-02-23 19:34:26  185.246.116.239  443    10.2.23.231      49203                TCP     443 → 49203 [PSH, ACK] Seq=194305 Ack=466 Win=64240 Len=1
7500  2019-02-23 19:34:26  10.2.23.231      49203  185.246.116.239  443                  TCP     49203 → 443 [ACK] Seq=466 Ack=195553 Win=64240 Len=0
7501  2019-02-23 19:34:26  185.246.116.239  443    10.2.23.231      49206                TCP     443 → 49206 [PSH, ACK] Seq=134401 Ack=466 Win=64240 Len=1
7502  2019-02-23 19:34:26  185.246.116.239  443    10.2.23.231      49206                TCP     443 → 49206 [PSH, ACK] Seq=135649 Ack=466 Win=64240 Len=1
7503  2019-02-23 19:34:26  10.2.23.231      49206  185.246.116.239  443                  TCP     49206 → 443 [ACK] Seq=466 Ack=136897 Win=64240 Len=0
7504  2019-02-23 19:34:26  10.2.23.231      49200  46.249.62.199    80                   TCP     49200 → 80 [ACK] Seq=77 Ack=340693 Win=62964 Len=0
7505  2019-02-23 19:34:26  185.246.116.239  443    10.2.23.231      49206                TLSv1   Application Data
7506  2019-02-23 19:34:27  10.2.23.231      62933  10.2.23.2        53                   DNS     superhaps.pw  Standard query 0x21d8 A superhaps.pw
7507  2019-02-23 19:34:27  10.2.23.231      49206  185.246.116.239  443                  TCP     49206 → 443 [ACK] Seq=466 Ack=137310 Win=63827 Len=0
7508  2019-02-23 19:34:27  185.246.116.239  443    10.2.23.231      49203                TCP     443 → 49203 [PSH, ACK] Seq=195553 Ack=466 Win=64240 Len=1
7509  2019-02-23 19:34:27  46.249.62.199    80     10.2.23.231      49200                TCP     80 → 49200 [ACK] Seq=340693 Ack=77 Win=64240 Len=1460 [TC
7510  2019-02-23 19:34:27  46.249.62.199    80     10.2.23.231      49200                TCP     80 → 49200 [ACK] Seq=342153 Ack=77 Win=64240 Len=1460 [TC
7511  2019-02-23 19:34:27  46.249.62.199    80     10.2.23.231      49200                TCP     80 → 49200 [ACK] Seq=343613 Ack=77 Win=64240 Len=1460 [TC
7512  2019-02-23 19:34:27  46.249.62.199    80     10.2.23.231      49200                TCP     80 → 49200 [PSH, ACK] Seq=345073 Ack=77 Win=64240 Len=724
7513  2019-02-23 19:34:27  46.249.62.199    80     10.2.23.231      49200                TCP     80 → 49200 [PSH, ACK] Seq=345797 Ack=77 Win=64240 Len=127
7514  2019-02-23 19:34:27  10.2.23.231      49200  46.249.62.199    80                   TCP     49200 → 80 [ACK] Seq=77 Ack=345797 Win=64240 Len=0
7515  2019-02-23 19:34:27  10.2.23.2        53     10.2.23.231      62933                DNS     superhaps.pw  Standard query response 0x21d8 A superhaps.pw A 87.236.22
7516  2019-02-23 19:34:27  10.2.23.231      49209  87.236.22.142    80                   TCP     49209 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SAC
7517  2019-02-23 19:34:27  10.2.23.231      49203  185.246.116.239  443                  TCP     49203 → 443 [ACK] Seq=466 Ack=196801 Win=62992 Len=0
7518  2019-02-23 19:34:27  10.2.23.231      49200  46.249.62.199    80                   TCP     49200 → 80 [ACK] Seq=77 Ack=347073 Win=62964 Len=0
7519  2019-02-23 19:34:27  46.249.62.199    80     10.2.23.231      49200                TCP     80 → 49200 [PSH, ACK] Seq=347073 Ack=77 Win=64240 Len=127
7520  2019-02-23 19:34:27  10.2.23.231      49200  46.249.62.199    80                   TCP     49200 → 80 [ACK] Seq=77 Ack=348349 Win=64240 Len=0
7521  2019-02-23 19:34:27  46.249.62.199    80     10.2.23.231      49200                TCP     80 → 49200 [PSH, ACK] Seq=348349 Ack=77 Win=64240 Len=127
7522  2019-02-23 19:34:27  87.236.22.142    80     10.2.23.231      49209                TCP     80 → 49209 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=146
7523  2019-02-23 19:34:27  10.2.23.231      49209  87.236.22.142    80                   TCP     49209 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
7524  2019-02-23 19:34:27  10.2.23.231      49209  87.236.22.142    80     superhaps.pw  HTTP    GET /data2.php?C68FF38437D96CED HTTP/1.1
7525  2019-02-23 19:34:27  87.236.22.142    80     10.2.23.231      49209                TCP     80 → 49209 [ACK] Seq=1 Ack=106 Win=64240 Len=0
7526  2019-02-23 19:34:27  10.2.23.231      49200  46.249.62.199    80                   TCP     49200 → 80 [ACK] Seq=77 Ack=349625 Win=62964 Len=0
7527  2019-02-23 19:34:27  10.2.23.231      49208  94.103.95.185    80                   TCP     [TCP Retransmission] 49208 → 80 [SYN] Seq=0 Win=8192 Len=
7528  2019-02-23 19:34:27  87.236.22.142    80     10.2.23.231      49209                HTTP    HTTP/1.1 101 Switching Protocols
7529  2019-02-23 19:34:27  10.2.23.231      49209  87.236.22.142    80                   TCP     49209 → 80 [PSH, ACK] Seq=106 Ack=186 Win=64055 Len=2 [TC
7530  2019-02-23 19:34:27  87.236.22.142    80     10.2.23.231      49209                TCP     80 → 49209 [ACK] Seq=186 Ack=108 Win=64240 Len=0
7531  2019-02-23 19:34:27  10.2.23.231      49209  87.236.22.142    80                   WebSoc… WebSocket Binary [FIN]
```

Explanation: TCP connection with superhaps[.]pw



```
7528  2019-02-23 19:34:27  87.236.22.142    80     10.2.23.231      49209   HTTP     HTTP/1.1 101 Switching Protocols
7529  2019-02-23 19:34:27  10.2.23.231      49209  87.236.22.142    80      TCP      49209 → 80 [PSH, ACK] Seq=106 Ack=186 Win=64055 Len=2 [TC
7530  2019-02-23 19:34:27  87.236.22.142    80     10.2.23.231      49209   TCP      80 → 49209 [ACK] Seq=186 Ack=108 Win=64240 Len=0
7531  2019-02-23 19:34:27  10.2.23.231      49209  87.236.22.142    80      WebSoc…  WebSocket Binary [FIN]
7532  2019-02-23 19:34:27  87.236.22.142    80     10.2.23.231      49209   TCP      80 → 49209 [ACK] Seq=186 Ack=121 Win=64240 Len=0
7533  2019-02-23 19:34:28  46.249.62.199    80     10.2.23.231      49200   TCP      80 → 49200 [ACK] Seq=349625 Ack=77 Win=64240 Len=1460 [TC
7534  2019-02-23 19:34:28  46.249.62.199    80     10.2.23.231      49200   TCP      80 → 49200 [PSH, ACK] Seq=351085 Ack=77 Win=64240 Len=109
7535  2019-02-23 19:34:28  10.2.23.231      49200  46.249.62.199    80      TCP      49200 → 80 [ACK] Seq=77 Ack=352177 Win=64240 Len=0
7536  2019-02-23 19:34:28  46.249.62.199    80     10.2.23.231      49200   TCP      80 → 49200 [ACK] Seq=352177 Ack=77 Win=64240 Len=1460 [TC
7537  2019-02-23 19:34:28  46.249.62.199    80     10.2.23.231      49200   TCP      80 → 49200 [ACK] Seq=353637 Ack=77 Win=64240 Len=1460 [TC
7538  2019-02-23 19:34:28  46.249.62.199    80     10.2.23.231      49200   TCP      80 → 49200 [PSH, ACK] Seq=355097 Ack=77 Win=64240 Len=908
7539  2019-02-23 19:34:28  10.2.23.231      49200  46.249.62.199    80      TCP      49200 → 80 [ACK] Seq=77 Ack=356005 Win=64240 Len=0
7540  2019-02-23 19:34:28  185.246.116.239  443    10.2.23.231      49203   TLSv1    Application Data
7541  2019-02-23 19:34:28  10.2.23.231      49203  185.246.116.239  443     TCP      49203 → 443 [ACK] Seq=466 Ack=198049 Win=64240 Len=0
7542  2019-02-23 19:34:28  185.246.116.239  443    10.2.23.231      49203   TCP      443 → 49203 [PSH, ACK] Seq=198049 Ack=466 Win=64240 Len=1
7543  2019-02-23 19:34:28  10.2.23.231      49203  185.246.116.239  443     TCP      49203 → 443 [ACK] Seq=466 Ack=199297 Win=62992 Len=0
7544  2019-02-23 19:34:29  46.249.62.199    80     10.2.23.231      49200   TCP      80 → 49200 [PSH, ACK] Seq=356005 Ack=77 Win=64240 Len=127
7545  2019-02-23 19:34:29  87.236.22.142    80     10.2.23.231      49209   WebSoc…  WebSocket Binary [FIN]
7546  2019-02-23 19:34:29  10.2.23.231      49200  46.249.62.199    80      TCP      49200 → 80 [ACK] Seq=77 Ack=357281 Win=62964 Len=0
7547  2019-02-23 19:34:29  10.2.23.231      49209  87.236.22.142    80      TCP      49209 → 80 [ACK] Seq=121 Ack=189 Win=64052 Len=0
7548  2019-02-23 19:34:29  185.246.116.239  443    10.2.23.231      49203   TCP      443 → 49203 [ACK] Seq=199297 Ack=466 Win=64240 Len=1460 [
```

Explanation: HTTP request from server to switch protocol to WebSocket connection



superhaps.pw

2/94 security vendors flagged this domain as malicious

2 / 94

Community Score 1

superhaps.pw

Malicious (alphaMountain.ai)

Last Analysis Date 14 days ago

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

Security vendors' analysis

Do you want to automate checks?

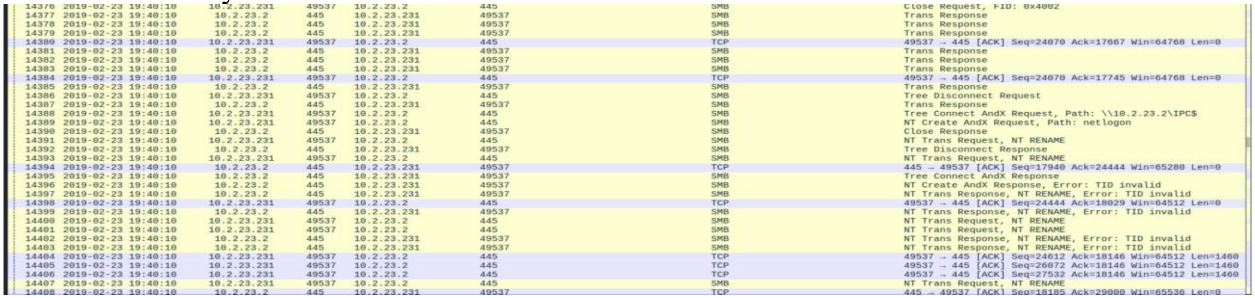
alphaMountain.ai	Malicious	Kaspersky	Malware
Abusix	Clean	Acronis	Clean
ADMINUSLabs	Clean	AILabs (MONITORAPP)	Clean
AlienVault	Clean	Antiy-AVL	Clean
benkow.cc	Clean	BitDefender	Clean
Blueliv	Clean	Certego	Clean
Chong Lua Dao	Clean	CINS Army	Clean
CMC Threat Intelligence	Clean	CRDF	Clean
Criminal IP	Clean	Cyble	Clean
CyRadar	Clean	desenmascara.me	Clean
DNS8	Clean	Dr.Web	Clean

https://www.virustotal.com/gui/domain/superhaps.pw/detection

Explanation: Results of VirusTotal lookup on superhaps[.]pw domain

Fifth Occurrence:

-Malicious SMB traffic interaction with infected host and domain controller
-Attacker attempts to find available SMB shares on network via Probing (IPC$ and netlogon)
-Checks to see if they can access IPC$ and Netlogon share for more system information and to explore vulnerabilities for possible exploitation attempts
-DC seems to have closed these shares and rejected malicious requests meaning attacker’s success was likely limited

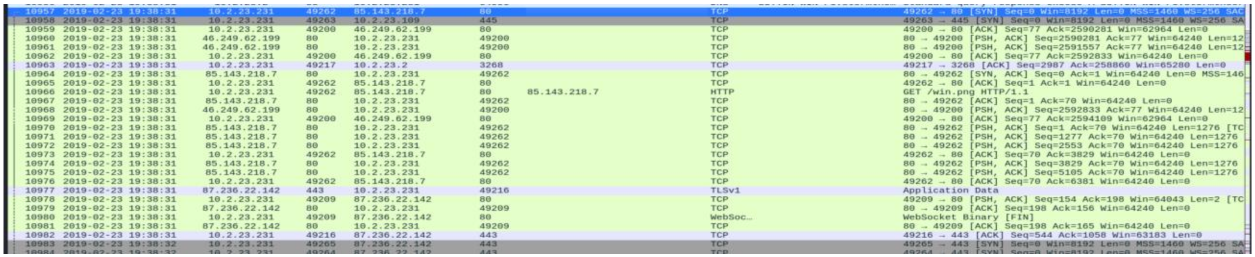


```
14376 2019-02-23 19:40:10  10.2.23.231  49537  10.2.23.2    445    SMB  Close Request, FID: 0x4002
14377 2019-02-23 19:40:10  10.2.23.2    445    10.2.23.231  49537  SMB  Trans Response
14378 2019-02-23 19:40:10  10.2.23.2    445    10.2.23.231  49537  SMB  Trans Response
14379 2019-02-23 19:40:10  10.2.23.2    445    10.2.23.231  49537  SMB  Trans Response
14380 2019-02-23 19:40:10  10.2.23.231  49537  10.2.23.2    445    TCP  49537 → 445 [ACK] Seq=24070 Ack=17667 Win=64768 Len=0
14381 2019-02-23 19:40:10  10.2.23.2    445    10.2.23.231  49537  SMB  Trans Response
14382 2019-02-23 19:40:10  10.2.23.2    445    10.2.23.231  49537  SMB  Trans Response
14383 2019-02-23 19:40:10  10.2.23.2    445    10.2.23.231  49537  SMB  Trans Response
14384 2019-02-23 19:40:10  10.2.23.231  49537  10.2.23.2    445    TCP  49537 → 445 [ACK] Seq=24070 Ack=17745 Win=64768 Len=0
14385 2019-02-23 19:40:10  10.2.23.2    445    10.2.23.231  49537  SMB  Trans Response
14386 2019-02-23 19:40:10  10.2.23.231  49537  10.2.23.2    445    SMB  Tree Disconnect Request
14387 2019-02-23 19:40:10  10.2.23.2    445    10.2.23.231  49537  SMB  Trans Response
14388 2019-02-23 19:40:10  10.2.23.231  49537  10.2.23.2    445    SMB  Tree Connect AndX Request, Path: \\10.2.23.2\IPC$
14389 2019-02-23 19:40:10  10.2.23.231  49537  10.2.23.2    445    SMB  NT Create AndX Request, Path: netlogon
14390 2019-02-23 19:40:10  10.2.23.2    445    10.2.23.231  49537  SMB  Close Response
14391 2019-02-23 19:40:10  10.2.23.231  49537  10.2.23.2    445    SMB  NT Trans Request, NT RENAME
14392 2019-02-23 19:40:10  10.2.23.2    445    10.2.23.231  49537  SMB  Tree Disconnect Response
14393 2019-02-23 19:40:10  10.2.23.231  49537  10.2.23.2    445    SMB  NT Trans Request, NT RENAME
14394 2019-02-23 19:40:10  10.2.23.2    445    10.2.23.231  49537  TCP  445 → 49537 [ACK] Seq=17940 Ack=24444 Win=65280 Len=0
14395 2019-02-23 19:40:10  10.2.23.2    445    10.2.23.231  49537  SMB  Tree Connect AndX Response
14396 2019-02-23 19:40:10  10.2.23.2    445    10.2.23.231  49537  SMB  NT Create AndX Response, Error: TID invalid
14397 2019-02-23 19:40:10  10.2.23.2    445    10.2.23.231  49537  SMB  NT Trans Response, NT RENAME, Error: TID invalid
14398 2019-02-23 19:40:10  10.2.23.231  49537  10.2.23.2    445    TCP  49537 → 445 [ACK] Seq=24444 Ack=18029 Win=64512 Len=0
14399 2019-02-23 19:40:10  10.2.23.2    445    10.2.23.231  49537  SMB  NT Trans Response, NT RENAME, Error: TID invalid
14400 2019-02-23 19:40:10  10.2.23.231  49537  10.2.23.2    445    SMB  NT Trans Request, NT RENAME
14401 2019-02-23 19:40:10  10.2.23.231  49537  10.2.23.2    445    SMB  NT Trans Request, NT RENAME
14402 2019-02-23 19:40:10  10.2.23.2    445    10.2.23.231  49537  SMB  NT Trans Response, NT RENAME, Error: TID invalid
14403 2019-02-23 19:40:10  10.2.23.2    445    10.2.23.231  49537  SMB  NT Trans Response, NT RENAME, Error: TID invalid
14404 2019-02-23 19:40:10  10.2.23.231  49537  10.2.23.2    445    TCP  49537 → 445 [ACK] Seq=24612 Ack=18146 Win=64512 Len=1460
14405 2019-02-23 19:40:10  10.2.23.231  49537  10.2.23.2    445    TCP  49537 → 445 [ACK] Seq=26072 Ack=18146 Win=64512 Len=1460
14406 2019-02-23 19:40:10  10.2.23.231  49537  10.2.23.2    445    TCP  49537 → 445 [ACK] Seq=27532 Ack=18146 Win=64512 Len=1460
14407 2019-02-23 19:40:10  10.2.23.231  49537  10.2.23.2    445    SMB  NT Trans Request, NT RENAME
14408 2019-02-23 19:40:10  10.2.23.2    445    10.2.23.231  49537  TCP  445 → 49537 [ACK] Seq=18185 Ack=29000 Win=65536 Len=0
```

Explanation: Malicious probing and reconnaissance of SMB server

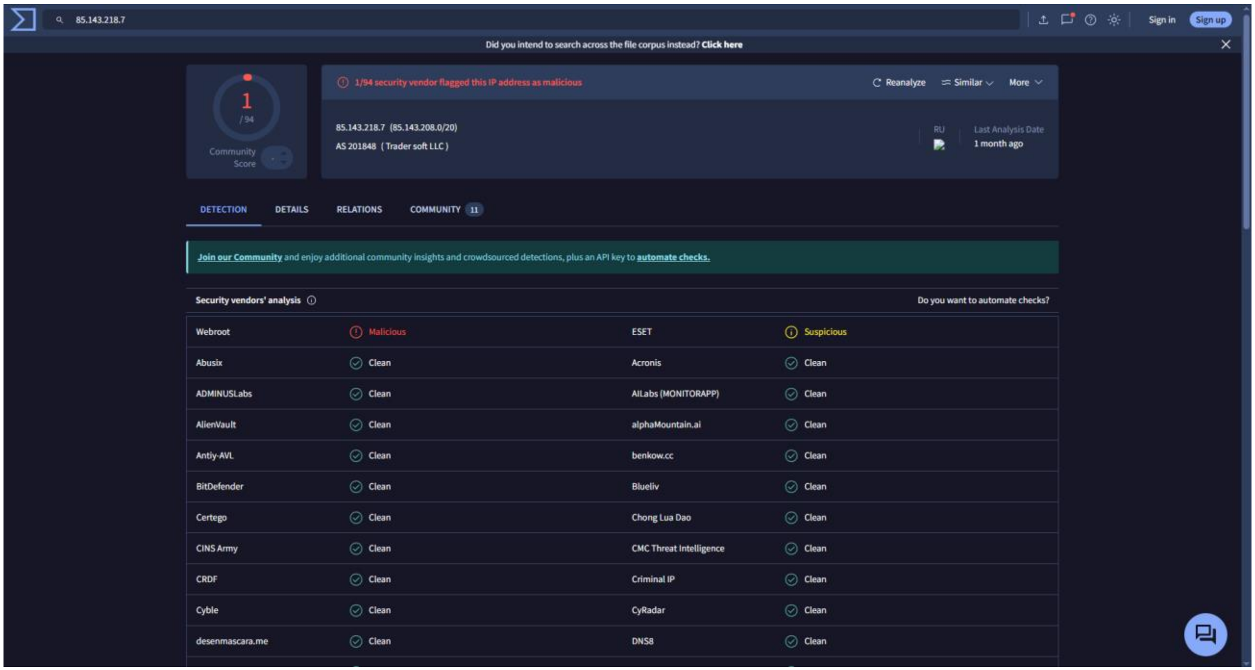
Sixth Occurrence:

-TCP connection with malicious web server 85[.]143[.]218[.]7
-Multiple GET requests to malicious PNGs from web server 85[.]143[.]218[.]7
-Malicious requests for: win[.]png, tin[.]png, sin[.]png
-Malicious server appears to send malicious SMB requests to infected host in attempt to understand internetwork processes



```
10957 2019-02-23 19:38:31   10.2.23.231    49262  85.143.218.7   80                   TCP     49262 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SAC
10958 2019-02-23 19:38:31   10.2.23.231    49263  10.2.23.109    445                  TCP     49263 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SA
10959 2019-02-23 19:38:31   10.2.23.231    49200  46.249.62.199  80                   TCP     49200 → 80 [ACK] Seq=77 Ack=2590281 Win=62964 Len=0
10960 2019-02-23 19:38:31  46.249.62.199   80     10.2.23.231    49200                TCP     80 → 49200 [PSH, ACK] Seq=2590281 Ack=77 Win=64240 Len=12
10961 2019-02-23 19:38:31  46.249.62.199   80     10.2.23.231    49200                TCP     80 → 49200 [PSH, ACK] Seq=2591557 Ack=77 Win=64240 Len=12
10962 2019-02-23 19:38:31   10.2.23.231    49200  46.249.62.199  80                   TCP     49200 → 80 [ACK] Seq=77 Ack=2592833 Win=64240 Len=0
10963 2019-02-23 19:38:31   10.2.23.231    49217  10.2.23.2      3268                 TCP     49217 → 3268 [ACK] Seq=2987 Ack=258860 Win=65280 Len=0
10964 2019-02-23 19:38:31   85.143.218.7   80     10.2.23.231    49262                TCP     80 → 49262 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=146
10965 2019-02-23 19:38:31   10.2.23.231    49262  85.143.218.7   80                   TCP     49262 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
10966 2019-02-23 19:38:31   10.2.23.231    49262  85.143.218.7   80    85.143.218.7   HTTP    GET /win.png HTTP/1.1
10967 2019-02-23 19:38:31   85.143.218.7   80     10.2.23.231    49262                TCP     80 → 49262 [ACK] Seq=1 Ack=70 Win=64240 Len=0
10968 2019-02-23 19:38:31  46.249.62.199   80     10.2.23.231    49200                TCP     80 → 49200 [PSH, ACK] Seq=2592833 Ack=77 Win=64240 Len=12
10969 2019-02-23 19:38:31   10.2.23.231    49200  46.249.62.199  80                   TCP     49200 → 80 [ACK] Seq=77 Ack=2594109 Win=62964 Len=0
10970 2019-02-23 19:38:31   85.143.218.7   80     10.2.23.231    49262                TCP     80 → 49262 [PSH, ACK] Seq=1 Ack=70 Win=64240 Len=1276 [TC
10971 2019-02-23 19:38:31   85.143.218.7   80     10.2.23.231    49262                TCP     80 → 49262 [PSH, ACK] Seq=1277 Ack=70 Win=64240 Len=1276
10972 2019-02-23 19:38:31   85.143.218.7   80     10.2.23.231    49262                TCP     80 → 49262 [PSH, ACK] Seq=2553 Ack=70 Win=64240 Len=1276
10973 2019-02-23 19:38:31   10.2.23.231    49262  85.143.218.7   80                   TCP     49262 → 80 [ACK] Seq=70 Ack=3829 Win=64240 Len=0
10974 2019-02-23 19:38:31   85.143.218.7   80     10.2.23.231    49262                TCP     80 → 49262 [PSH, ACK] Seq=3829 Ack=70 Win=64240 Len=1276
10975 2019-02-23 19:38:31   85.143.218.7   80     10.2.23.231    49262                TCP     80 → 49262 [PSH, ACK] Seq=5105 Ack=70 Win=64240 Len=1276
10976 2019-02-23 19:38:31   10.2.23.231    49262  85.143.218.7   80                   TCP     49262 → 80 [ACK] Seq=70 Ack=6381 Win=64240 Len=0
10977 2019-02-23 19:38:31  87.236.22.142   443    10.2.23.231    49216                TLSv1   Application Data
10978 2019-02-23 19:38:31   10.2.23.231    49209  87.236.22.142  80                   TCP     49209 → 80 [PSH, ACK] Seq=154 Ack=198 Win=64043 Len=2 [TC
10979 2019-02-23 19:38:31  87.236.22.142   80     10.2.23.231    49209                TCP     80 → 49209 [ACK] Seq=198 Ack=156 Win=64240 Len=0
10980 2019-02-23 19:38:31   10.2.23.231    49209  87.236.22.142  80                   WebSoc… WebSocket Binary [FIN]
10981 2019-02-23 19:38:31  87.236.22.142   80     10.2.23.231    49209                TCP     80 → 49209 [ACK] Seq=198 Ack=165 Win=64240 Len=0
10982 2019-02-23 19:38:31   10.2.23.231    49216  87.236.22.142  443                  TCP     49216 → 443 [ACK] Seq=544 Ack=1058 Win=63183 Len=0
10983 2019-02-23 19:38:32   10.2.23.231    49265  87.236.22.142  443                  TCP     49265 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SA
10984 2019-02-23 19:38:32   10.2.23.231    49264  87.236.22.142  443                  TCP     49264 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SA
```

Explanation: Beginning of TCP handshake with web server 85[.]143[.]218[.]7



Did you intend to search across the file corpus instead? **Click here**

1 / 94

Community Score

1/94 security vendor flagged this IP address as malicious

85.143.218.7 (85.143.208.0/20)

AS 201848 (Trader soft LLC)

RU

Last Analysis Date
1 month ago

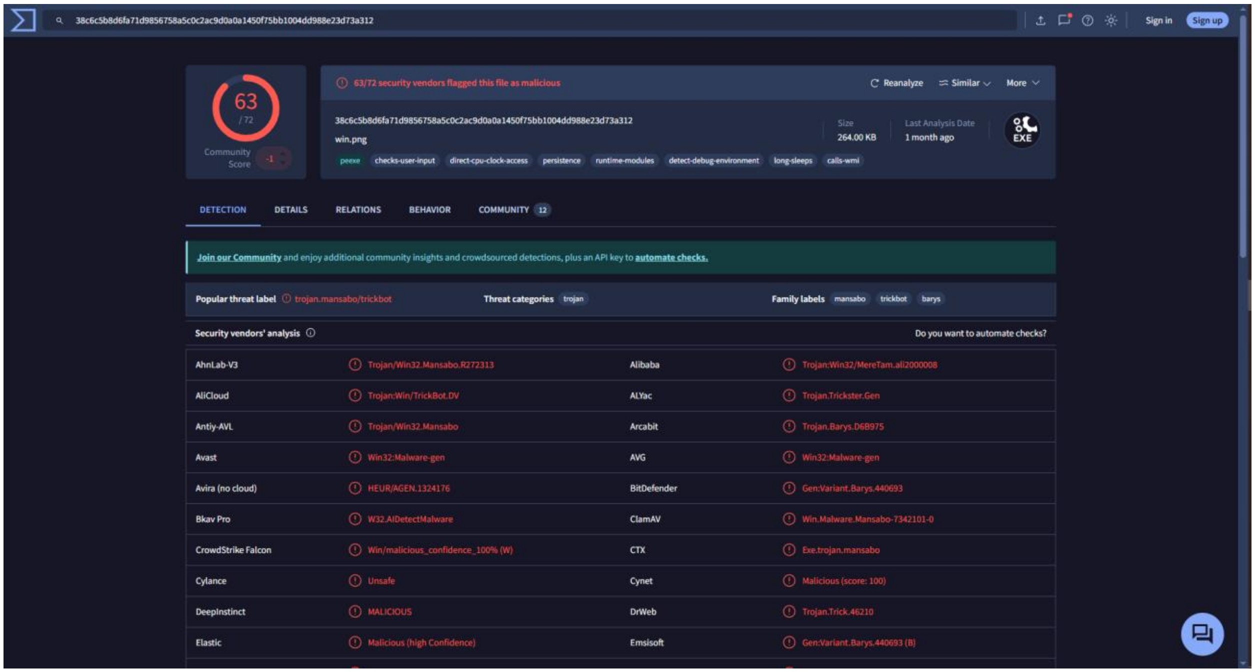
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to **automate checks.**

Security vendors' analysis

Do you want to automate checks?

Webroot	Malicious	ESET	Suspicious
Abusix	Clean	Acronis	Clean
ADMINUSLabs	Clean	AILabs (MONITORAPP)	Clean
AlienVault	Clean	alphaMountain.ai	Clean
Antiy-AVL	Clean	benkow.cc	Clean
BitDefender	Clean	Blueliv	Clean
Certego	Clean	Chong Lua Dao	Clean
CINS Army	Clean	CMC Threat Intelligence	Clean
CRDF	Clean	Criminal IP	Clean
Cyble	Clean	CyRadar	Clean
desenmascara.me	Clean	DNS8	Clean

Explanation: Results of VirusTotal lookup on IP 85[.]143[.]218[.]7 for the web server



38c6c5b8d6fa71d9856758a5c0c2ac9d0a0a1450f75bb1004dd988e23d73a312

63 / 72

63/72 security vendors flagged this file as malicious

38c6c5b8d6fa71d9856758a5c0c2ac9d0a0a1450f75bb1004dd988e23d73a312

win.png

peexe checks-user-input direct-cpu-clock-access persistence runtime-modules detect-debug-environment long-sleeps calls-wmi

Size 264.00 KB

Last Analysis Date 1 month ago

EXE

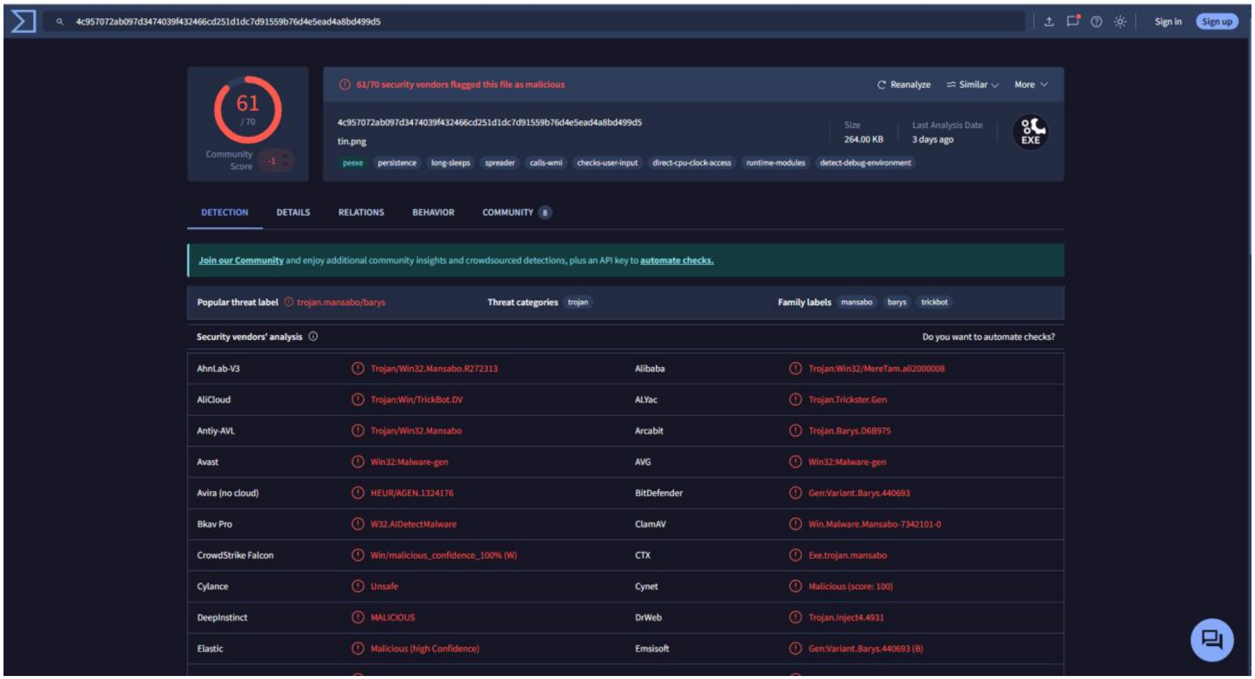
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.mansabo/trickbot Threat categories trojan Family labels mansabo trickbot barys

Security vendors' analysis Do you want to automate checks?

AhnLab-V3	Trojan/Win32.Mansabo.R272313	Alibaba	Trojan:Win32/MereTam.ali2000008
AliCloud	Trojan:Win/TrickBot.DV	ALYac	Trojan.Trickster.Gen
Antiy-AVL	Trojan/Win32.Mansabo	Arcabit	Trojan.Barys.D6B975
Avast	Win32:Malware-gen	AVG	Win32:Malware-gen
Avira (no cloud)	HEUR/AGEN.1324176	BitDefender	Gen:Variant.Barys.440693
Bkav Pro	W32.AIDetectMalware	ClamAV	Win.Malware.Mansabo-7342101-0
CrowdStrike Falcon	Win/malicious_confidence_100% (W)	CTX	Exe.trojan.mansabo
Cylance	Unsafe	Cynet	Malicious (score: 100)
DeepInstinct	MALICIOUS	DrWeb	Trojan.Trick.46210
Elastic	Malicious (high Confidence)	Emsisoft	Gen:Variant.Barys.440693 (B)

Explanation: Results of VirusTotal lookup on win[.]png



4c957072ab097d3474039f432466cd251d1dc7d91559b76d4e5ead4a8bd499d5

61 / 70

61/70 security vendors flagged this file as malicious

4c957072ab097d3474039f432466cd251d1dc7d91559b76d4e5ead4a8bd499d5

tin.png

peexe persistence long-sleeps spreader calls-wmi checks-user-input direct-cpu-clock-access runtime-modules detect-debug-environment

Size 264.00 KB

Last Analysis Date 3 days ago

EXE

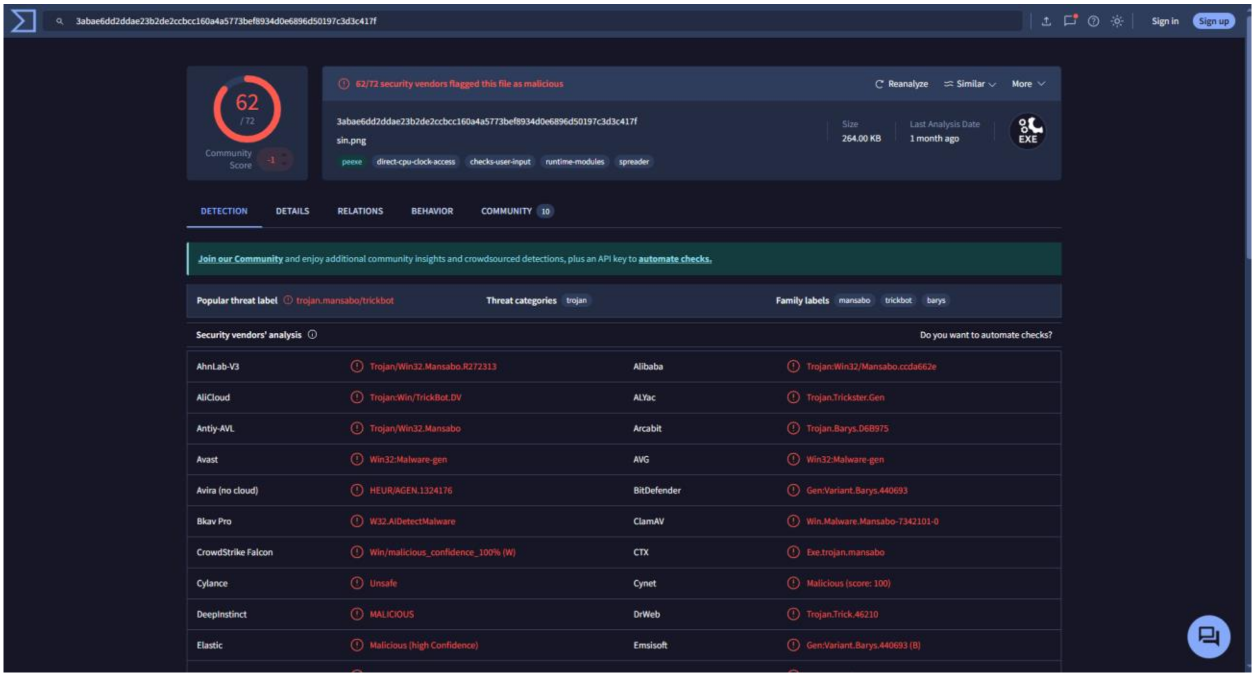
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.mansabo/barys Threat categories trojan Family labels mansabo barys trickbot

Security vendors' analysis Do you want to automate checks?

AhnLab-V3	Trojan/Win32.Mansabo.R272313	Alibaba	Trojan:Win32/MereTam.ali2000008
AliCloud	Trojan:Win/TrickBot.DV	ALYac	Trojan.Trickster.Gen
Antiy-AVL	Trojan/Win32.Mansabo	Arcabit	Trojan.Barys.D6B975
Avast	Win32:Malware-gen	AVG	Win32:Malware-gen
Avira (no cloud)	HEUR/AGEN.1324176	BitDefender	Gen:Variant.Barys.440693
Bkav Pro	W32.AIDetectMalware	ClamAV	Win.Malware.Mansabo-7342101-0
CrowdStrike Falcon	Win/malicious_confidence_100% (W)	CTX	Exe.trojan.mansabo
Cylance	Unsafe	Cynet	Malicious (score: 100)
DeepInstinct	MALICIOUS	DrWeb	Trojan.Inject4.4931
Elastic	Malicious (high Confidence)	Emsisoft	Gen:Variant.Barys.440693 (B)

Explanation: Results of VirusTotal lookup on tin[.]png



3abae6dd2ddae23b2de2ccbcc160a4a5773bef8934d0e6896d50197c3d3c417f

62 / 72 Community Score -1

62/72 security vendors flagged this file as malicious

3abae6dd2ddae23b2de2ccbcc160a4a5773bef8934d0e6896d50197c3d3c417f
sin.png
peexe direct-cpu-clock-access checks-user-input runtime-modules spreader

Size 264.00 KB
Last Analysis Date 1 month ago

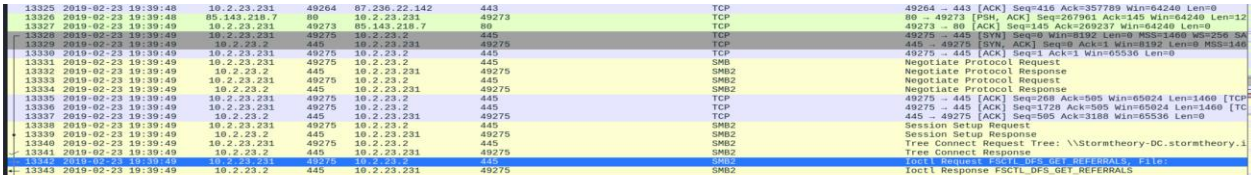
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.mansabo/trickbot · Threat categories trojan · Family labels mansabo trickbot barys

Security vendors' analysis · Do you want to automate checks?

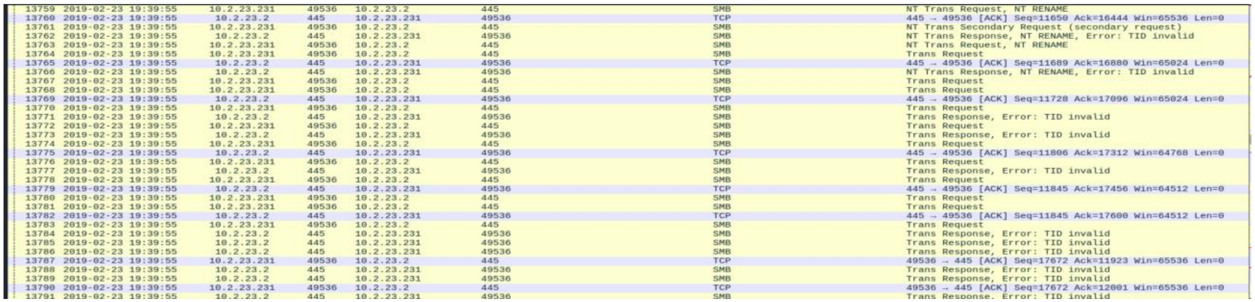
AhnLab-V3	Trojan/Win32.Mansabo.R272313	Alibaba	Trojan:Win32/Mansabo.ccda662e
AliCloud	Trojan:Win/TrickBot.DV	ALYac	Trojan.Trickster.Gen
Antiy-AVL	Trojan/Win32.Mansabo	Arcabit	Trojan.Barys.D6B975
Avast	Win32:Malware-gen	AVG	Win32:Malware-gen
Avira (no cloud)	HEUR/AGEN.1324176	BitDefender	Gen:Variant.Barys.440693
Bkav Pro	W32.AIDetectMalware	ClamAV	Win.Malware.Mansabo-7342101-0
CrowdStrike Falcon	Win/malicious_confidence_100% (W)	CTX	Exe.trojan.mansabo
Cylance	Unsafe	Cynet	Malicious (score: 100)
DeepInstinct	MALICIOUS	DrWeb	Trojan.Trick.46210
Elastic	Malicious (high Confidence)	Emsisoft	Gen:Variant.Barys.440693 (B)

Explanation: Results of VirusTotal lookup on sin[.]png



```
13325 2019-02-23 19:39:48  10.2.23.231   49264  87.236.22.142  443    TCP   49264 → 443 [ACK] Seq=416 Ack=357789 Win=64240 Len=0
13326 2019-02-23 19:39:48  85.143.218.7  80     10.2.23.231    49273  TCP   80 → 49273 [PSH, ACK] Seq=267961 Ack=145 Win=64240 Len=12
13327 2019-02-23 19:39:49  10.2.23.231   49273  85.143.218.7   80     TCP   49273 → 80 [ACK] Seq=145 Ack=269237 Win=64240 Len=0
13328 2019-02-23 19:39:49  10.2.23.231   49275  10.2.23.2      445    TCP   49275 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SA
13329 2019-02-23 19:39:49  10.2.23.2     445    10.2.23.231    49275  TCP   445 → 49275 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=146
13330 2019-02-23 19:39:49  10.2.23.231   49275  10.2.23.2      445    TCP   49275 → 445 [ACK] Seq=1 Ack=1 Win=65536 Len=0
13331 2019-02-23 19:39:49  10.2.23.231   49275  10.2.23.2      445    SMB   Negotiate Protocol Request
13332 2019-02-23 19:39:49  10.2.23.2     445    10.2.23.231    49275  SMB2  Negotiate Protocol Response
13333 2019-02-23 19:39:49  10.2.23.231   49275  10.2.23.2      445    SMB2  Negotiate Protocol Request
13334 2019-02-23 19:39:49  10.2.23.2     445    10.2.23.231    49275  SMB2  Negotiate Protocol Response
13335 2019-02-23 19:39:49  10.2.23.231   49275  10.2.23.2      445    TCP   49275 → 445 [ACK] Seq=268 Ack=505 Win=65024 Len=1460 [TCP
13336 2019-02-23 19:39:49  10.2.23.231   49275  10.2.23.2      445    TCP   49275 → 445 [ACK] Seq=1728 Ack=505 Win=65024 Len=1460 [TC
13337 2019-02-23 19:39:49  10.2.23.2     445    10.2.23.231    49275  TCP   445 → 49275 [ACK] Seq=505 Ack=3188 Win=65536 Len=0
13338 2019-02-23 19:39:49  10.2.23.231   49275  10.2.23.2      445    SMB2  Session Setup Request
13339 2019-02-23 19:39:49  10.2.23.2     445    10.2.23.231    49275  SMB2  Session Setup Response
13340 2019-02-23 19:39:49  10.2.23.231   49275  10.2.23.2      445    SMB2  Tree Connect Request Tree: \\Stormtheory-DC.stormtheory.i
13341 2019-02-23 19:39:49  10.2.23.2     445    10.2.23.231    49275  SMB2  Tree Connect Response
13342 2019-02-23 19:39:49  10.2.23.231   49275  10.2.23.2      445    SMB2  Ioctl Request FSCTL_DFS_GET_REFERRALS, File:
13343 2019-02-23 19:39:49  10.2.23.2     445    10.2.23.231    49275  SMB2  Ioctl Response FSCTL_DFS_GET_REFERRALS
```

Explanation: Malicious SMB request from malicious server through infected host



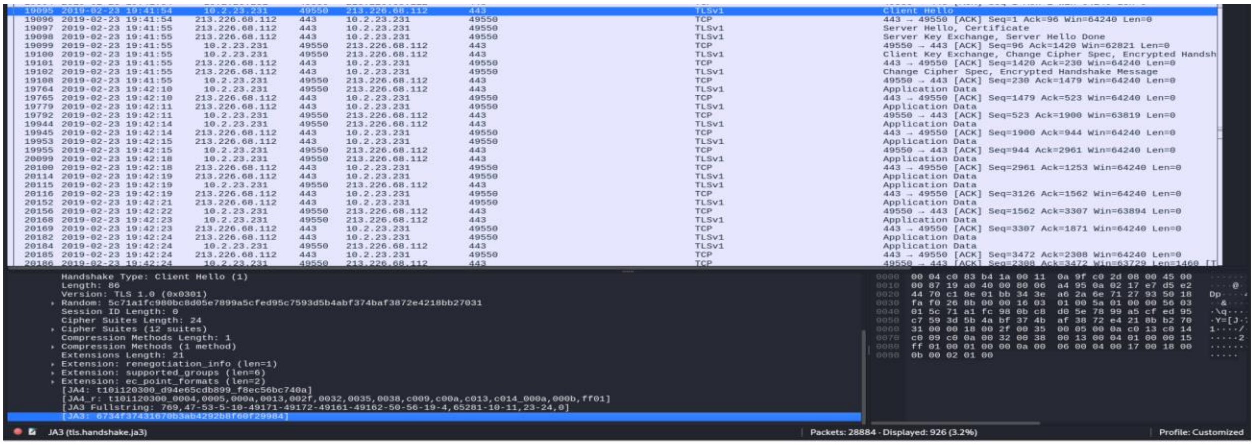
```
13759 2019-02-23 19:39:55  10.2.23.231  49536  10.2.23.2    445    SMB  NT Trans Request, NT RENAME
13760 2019-02-23 19:39:55  10.2.23.2    445    10.2.23.231  49536  TCP  445 → 49536 [ACK] Seq=11650 Ack=16444 Win=65536 Len=0
13761 2019-02-23 19:39:55  10.2.23.231  49536  10.2.23.2    445    SMB  NT Trans Secondary Request (secondary request)
13762 2019-02-23 19:39:55  10.2.23.2    445    10.2.23.231  49536  SMB  NT Trans Response, NT RENAME, Error: TID invalid
13763 2019-02-23 19:39:55  10.2.23.231  49536  10.2.23.2    445    SMB  NT Trans Request, NT RENAME
13764 2019-02-23 19:39:55  10.2.23.231  49536  10.2.23.2    445    SMB  Trans Request
13765 2019-02-23 19:39:55  10.2.23.2    445    10.2.23.231  49536  TCP  445 → 49536 [ACK] Seq=11689 Ack=16880 Win=65024 Len=0
13766 2019-02-23 19:39:55  10.2.23.2    445    10.2.23.231  49536  SMB  NT Trans Response, NT RENAME, Error: TID invalid
13767 2019-02-23 19:39:55  10.2.23.231  49536  10.2.23.2    445    SMB  Trans Request
13768 2019-02-23 19:39:55  10.2.23.231  49536  10.2.23.2    445    SMB  Trans Request
13769 2019-02-23 19:39:55  10.2.23.2    445    10.2.23.231  49536  TCP  445 → 49536 [ACK] Seq=11728 Ack=17096 Win=65024 Len=0
13770 2019-02-23 19:39:55  10.2.23.231  49536  10.2.23.2    445    SMB  Trans Request
13771 2019-02-23 19:39:55  10.2.23.2    445    10.2.23.231  49536  SMB  Trans Response, Error: TID invalid
13772 2019-02-23 19:39:55  10.2.23.231  49536  10.2.23.2    445    SMB  Trans Request
13773 2019-02-23 19:39:55  10.2.23.2    445    10.2.23.231  49536  SMB  Trans Response, Error: TID invalid
13774 2019-02-23 19:39:55  10.2.23.231  49536  10.2.23.2    445    SMB  Trans Request
13775 2019-02-23 19:39:55  10.2.23.2    445    10.2.23.231  49536  TCP  445 → 49536 [ACK] Seq=11806 Ack=17312 Win=64768 Len=0
13776 2019-02-23 19:39:55  10.2.23.231  49536  10.2.23.2    445    SMB  Trans Request
13777 2019-02-23 19:39:55  10.2.23.2    445    10.2.23.231  49536  SMB  Trans Response, Error: TID invalid
13778 2019-02-23 19:39:55  10.2.23.231  49536  10.2.23.2    445    SMB  Trans Request
13779 2019-02-23 19:39:55  10.2.23.2    445    10.2.23.231  49536  TCP  445 → 49536 [ACK] Seq=11845 Ack=17456 Win=64512 Len=0
13780 2019-02-23 19:39:55  10.2.23.231  49536  10.2.23.2    445    SMB  Trans Request
13781 2019-02-23 19:39:55  10.2.23.231  49536  10.2.23.2    445    SMB  Trans Request
13782 2019-02-23 19:39:55  10.2.23.2    445    10.2.23.231  49536  TCP  445 → 49536 [ACK] Seq=11845 Ack=17600 Win=64512 Len=0
13783 2019-02-23 19:39:55  10.2.23.231  49536  10.2.23.2    445    SMB  Trans Request
13784 2019-02-23 19:39:55  10.2.23.2    445    10.2.23.231  49536  SMB  Trans Response, Error: TID invalid
13785 2019-02-23 19:39:55  10.2.23.2    445    10.2.23.231  49536  SMB  Trans Response, Error: TID invalid
13786 2019-02-23 19:39:55  10.2.23.2    445    10.2.23.231  49536  SMB  Trans Response, Error: TID invalid
13787 2019-02-23 19:39:55  10.2.23.231  49536  10.2.23.2    445    TCP  49536 → 445 [ACK] Seq=17672 Ack=11923 Win=65536 Len=0
13788 2019-02-23 19:39:55  10.2.23.2    445    10.2.23.231  49536  SMB  Trans Response, Error: TID invalid
13789 2019-02-23 19:39:55  10.2.23.2    445    10.2.23.231  49536  SMB  Trans Response, Error: TID invalid
13790 2019-02-23 19:39:55  10.2.23.231  49536  10.2.23.2    445    TCP  49536 → 445 [ACK] Seq=17672 Ack=12001 Win=65536 Len=0
13791 2019-02-23 19:39:55  10.2.23.2    445    10.2.23.231  49536  SMB  Trans Response, Error: TID invalid
```

Explanation: Another screenshot of malicious SMB traffic

Seventh Occurrence:

-Communication with malicious web server 213[.]226[.]68[.]112

-Blacklisted SSL Certificate detected

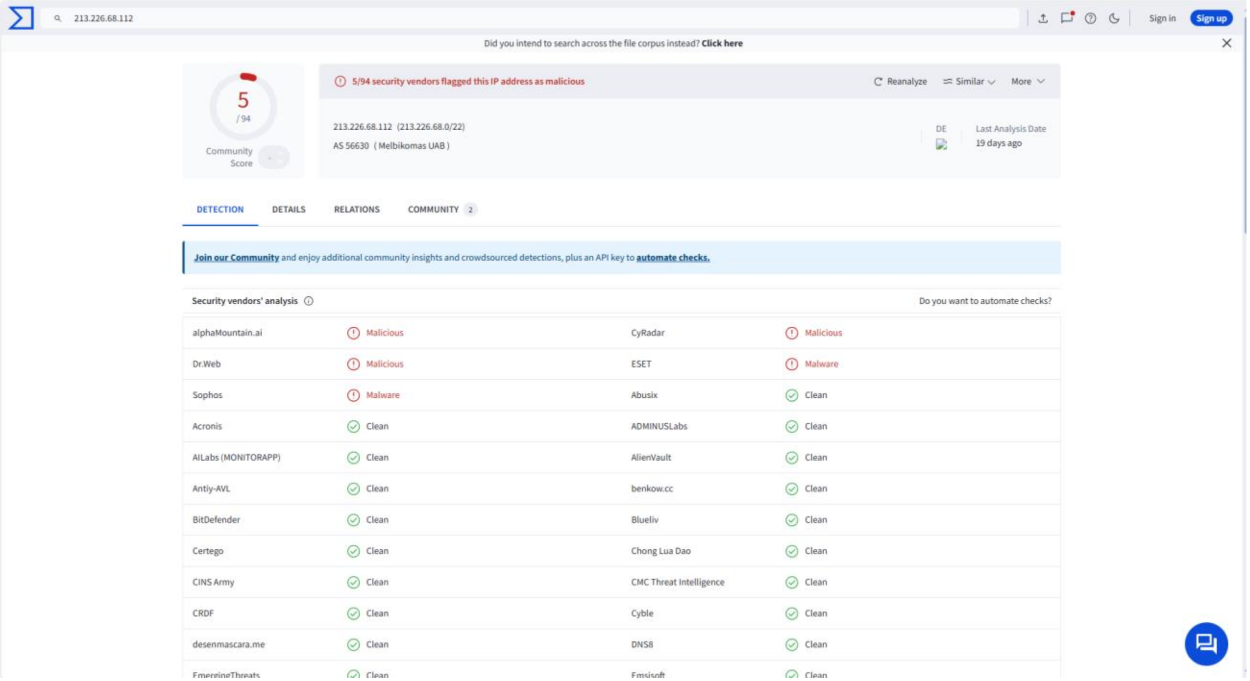


```
19095 2019-02-23 19:41:54    10.2.23.231     49550  213.226.68.112  443     TLSv1  Client Hello
19096 2019-02-23 19:41:54  213.226.68.112    443    10.2.23.231     49550   TCP    443 → 49550 [ACK] Seq=1 Ack=96 Win=64240 Len=0
19097 2019-02-23 19:41:55  213.226.68.112    443    10.2.23.231     49550   TLSv1  Server Hello, Certificate
19098 2019-02-23 19:41:55  213.226.68.112    443    10.2.23.231     49550   TLSv1  Server Key Exchange, Server Hello Done
19099 2019-02-23 19:41:55    10.2.23.231     49550  213.226.68.112  443     TCP    49550 → 443 [ACK] Seq=96 Ack=1420 Win=62821 Len=0
19100 2019-02-23 19:41:55    10.2.23.231     49550  213.226.68.112  443     TLSv1  Client Key Exchange, Change Cipher Spec, Encrypted Handsh
19101 2019-02-23 19:41:55  213.226.68.112    443    10.2.23.231     49550   TCP    443 → 49550 [ACK] Seq=1420 Ack=230 Win=64240 Len=0
19102 2019-02-23 19:41:55  213.226.68.112    443    10.2.23.231     49550   TLSv1  Change Cipher Spec, Encrypted Handshake Message
19108 2019-02-23 19:41:55    10.2.23.231     49550  213.226.68.112  443     TCP    49550 → 443 [ACK] Seq=230 Ack=1479 Win=64240 Len=0
19764 2019-02-23 19:42:10    10.2.23.231     49550  213.226.68.112  443     TLSv1  Application Data
19765 2019-02-23 19:42:10  213.226.68.112    443    10.2.23.231     49550   TCP    443 → 49550 [ACK] Seq=1479 Ack=523 Win=64240 Len=0
19779 2019-02-23 19:42:11  213.226.68.112    443    10.2.23.231     49550   TLSv1  Application Data
19792 2019-02-23 19:42:11    10.2.23.231     49550  213.226.68.112  443     TCP    49550 → 443 [ACK] Seq=523 Ack=1900 Win=63819 Len=0
19944 2019-02-23 19:42:14    10.2.23.231     49550  213.226.68.112  443     TLSv1  Application Data
19945 2019-02-23 19:42:14  213.226.68.112    443    10.2.23.231     49550   TCP    443 → 49550 [ACK] Seq=1900 Ack=944 Win=64240 Len=0
19953 2019-02-23 19:42:15  213.226.68.112    443    10.2.23.231     49550   TLSv1  Application Data
19955 2019-02-23 19:42:15    10.2.23.231     49550  213.226.68.112  443     TCP    49550 → 443 [ACK] Seq=944 Ack=2961 Win=64240 Len=0
20099 2019-02-23 19:42:18    10.2.23.231     49550  213.226.68.112  443     TLSv1  Application Data
20100 2019-02-23 19:42:18  213.226.68.112    443    10.2.23.231     49550   TCP    443 → 49550 [ACK] Seq=2961 Ack=1253 Win=64240 Len=0
20114 2019-02-23 19:42:19  213.226.68.112    443    10.2.23.231     49550   TLSv1  Application Data
20115 2019-02-23 19:42:19    10.2.23.231     49550  213.226.68.112  443     TLSv1  Application Data
20116 2019-02-23 19:42:19  213.226.68.112    443    10.2.23.231     49550   TCP    443 → 49550 [ACK] Seq=3126 Ack=1562 Win=64240 Len=0
20152 2019-02-23 19:42:21  213.226.68.112    443    10.2.23.231     49550   TLSv1  Application Data
20156 2019-02-23 19:42:22    10.2.23.231     49550  213.226.68.112  443     TCP    49550 → 443 [ACK] Seq=1562 Ack=3307 Win=63894 Len=0
20168 2019-02-23 19:42:23    10.2.23.231     49550  213.226.68.112  443     TLSv1  Application Data
20169 2019-02-23 19:42:23  213.226.68.112    443    10.2.23.231     49550   TCP    443 → 49550 [ACK] Seq=3307 Ack=1871 Win=64240 Len=0
20182 2019-02-23 19:42:24  213.226.68.112    443    10.2.23.231     49550   TLSv1  Application Data
20184 2019-02-23 19:42:24    10.2.23.231     49550  213.226.68.112  443     TLSv1  Application Data
20185 2019-02-23 19:42:24  213.226.68.112    443    10.2.23.231     49550   TCP    443 → 49550 [ACK] Seq=3472 Ack=2308 Win=64240 Len=0
20186 2019-02-23 19:42:24    10.2.23.231     49550  213.226.68.112  443     TCP    49550 → 443 [ACK] Seq=2308 Ack=3472 Win=63729 Len=1460 [T
```

```
      Handshake Type: Client Hello (1)
      Length: 86
      Version: TLS 1.0 (0x0301)
    ▸ Random: 5c71a1fc980bc8d05e7899a5cfed95c7593d5b4abf374baf3872e4218bb27031
      Session ID Length: 0
      Cipher Suites Length: 24
    ▸ Cipher Suites (12 suites)
      Compression Methods Length: 1
    ▸ Compression Methods (1 method)
      Extensions Length: 21
    ▸ Extension: renegotiation_info (len=1)
    ▸ Extension: supported_groups (len=6)
    ▸ Extension: ec_point_formats (len=2)
      [JA4: t10i120300_d94e65cdb899_f8ec56bc740a]
      [JA4_r: t10i120300_0004,0005,000a,0013,002f,0032,0035,0038,c009,c00a,c013,c014_000a,000b,ff01]
      [JA3 Fullstring: 769,47-53-5-10-49171-49172-49161-49162-50-56-19-4,65281-10-11,23-24,0]
      [JA3: 6734f37431670b3ab4292b8f60f29984]
```

```
0000  00 04 c0 83 b4 1a 00 11  0a 9f c0 2d 08 00 45 00   ······
0010  00 87 19 a0 40 00 80 06  a4 95 0a 02 17 e7 d5 e2   ····@·
0020  44 70 c1 8e 01 bb 34 3e  a6 2a 6e 71 27 93 50 18   Dp····
0030  fa f0 26 8b 00 00 16 03  01 00 5a 01 00 00 56 03   ··&···
0040  01 5c 71 a1 fc 98 0b c8  d0 5e 78 99 a5 cf ed 95   ·\q···
0050  c7 59 3d 5b 4a bf 37 4b  af 38 72 e4 21 8b b2 70   ·Y=[J·
0060  31 00 00 18 00 2f 00 35  00 05 00 0a c0 13 c0 14   1····/
0070  c0 09 c0 0a 00 32 00 38  00 13 00 04 01 00 00 15   ·····2
0080  ff 01 00 01 00 00 0a 00  06 00 04 00 17 00 18 00   ······
0090  0b 00 02 01 00                                     ·····
```

Explanation: Malicious traffic over HTTPS with web server



5/94 security vendors flagged this IP address as malicious

213.226.68.112 (213.226.68.0/22)
AS 56630 (Melbikomas UAB)

DE

Last Analysis Date
19 days ago

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

Security vendors' analysis

Do you want to automate checks?

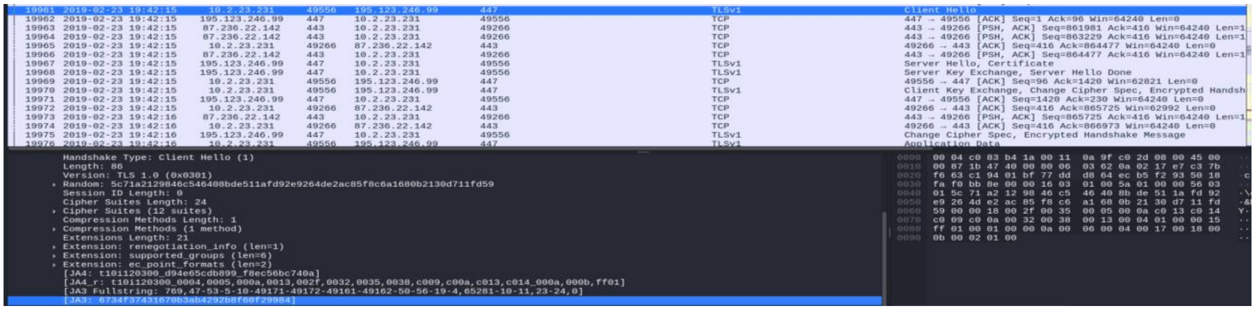
alphaMountain.ai	Malicious	CyRadar	Malicious
Dr.Web	Malicious	ESET	Malware
Sophos	Malware	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean
AILabs (MONITORAPP)	Clean	AlienVault	Clean
Antiy-AVL	Clean	benkow.cc	Clean
BitDefender	Clean	Blueliv	Clean
Certego	Clean	Chong Lua Dao	Clean
CINS Army	Clean	CMC Threat Intelligence	Clean
CRDF	Clean	Cyble	Clean
desenmascara.me	Clean	DNS8	Clean
EmergingThreats	Clean	Emsisoft	Clean

Explanation: VirusTotal lookup of web server 213[.]226[.]68[.]112

Eighth Occurrence:

-Malicious connection with web server 195[.]123[.]246[.]99

-Same JA3 footprint and VirusTotal profile as 213[.]226[.]68[.]112

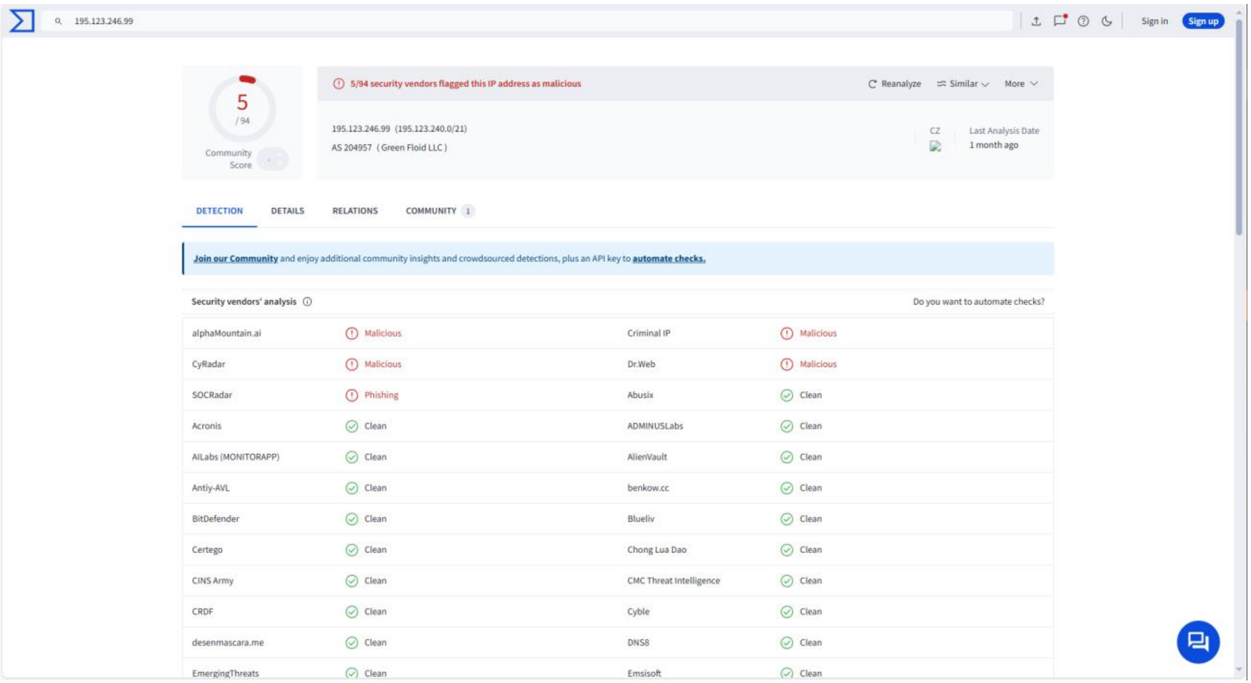


```
19961 2019-02-23 19:42:15   10.2.23.231     49556  195.123.246.99   447    TLSv1  Client Hello
19962 2019-02-23 19:42:15  195.123.246.99   447    10.2.23.231      49556  TCP    447 → 49556 [ACK] Seq=1 Ack=96 Win=64240 Len=0
19963 2019-02-23 19:42:15   87.236.22.142   443    10.2.23.231      49266  TCP    443 → 49266 [PSH, ACK] Seq=861981 Ack=416 Win=64240 Len=1
19964 2019-02-23 19:42:15   87.236.22.142   443    10.2.23.231      49266  TCP    443 → 49266 [PSH, ACK] Seq=863229 Ack=416 Win=64240 Len=1
19965 2019-02-23 19:42:15   10.2.23.231     49266  87.236.22.142    443    TCP    49266 → 443 [ACK] Seq=416 Ack=864477 Win=64240 Len=0
19966 2019-02-23 19:42:15   87.236.22.142   443    10.2.23.231      49266  TCP    443 → 49266 [PSH, ACK] Seq=864477 Ack=416 Win=64240 Len=1
19967 2019-02-23 19:42:15  195.123.246.99   447    10.2.23.231      49556  TLSv1  Server Hello, Certificate
19968 2019-02-23 19:42:15  195.123.246.99   447    10.2.23.231      49556  TLSv1  Server Key Exchange, Server Hello Done
19969 2019-02-23 19:42:15   10.2.23.231     49556  195.123.246.99   447    TCP    49556 → 447 [ACK] Seq=96 Ack=1420 Win=62821 Len=0
19970 2019-02-23 19:42:15   10.2.23.231     49556  195.123.246.99   447    TLSv1  Client Key Exchange, Change Cipher Spec, Encrypted Handsh
19971 2019-02-23 19:42:15  195.123.246.99   447    10.2.23.231      49556  TCP    447 → 49556 [ACK] Seq=1420 Ack=230 Win=64240 Len=0
19972 2019-02-23 19:42:15   10.2.23.231     49266  87.236.22.142    443    TCP    49266 → 443 [ACK] Seq=416 Ack=865725 Win=62992 Len=0
19973 2019-02-23 19:42:16   87.236.22.142   443    10.2.23.231      49266  TCP    443 → 49266 [PSH, ACK] Seq=865725 Ack=416 Win=64240 Len=1
19974 2019-02-23 19:42:16   10.2.23.231     49266  87.236.22.142    443    TCP    49266 → 443 [ACK] Seq=416 Ack=866973 Win=64240 Len=0
19975 2019-02-23 19:42:16  195.123.246.99   447    10.2.23.231      49556  TLSv1  Change Cipher Spec, Encrypted Handshake Message
19976 2019-02-23 19:42:16   10.2.23.231     49556  195.123.246.99   447    TLSv1  Application Data
```

```
    Handshake Type: Client Hello (1)
    Length: 86
    Version: TLS 1.0 (0x0301)
  ▸ Random: 5c71a2129846c546408bde511afd92e9264de2ac85f8c6a1680b2130d711fd59
    Session ID Length: 0
    Cipher Suites Length: 24
  ▸ Cipher Suites (12 suites)
    Compression Methods Length: 1
  ▸ Compression Methods (1 method)
    Extensions Length: 21
  ▸ Extension: renegotiation_info (len=1)
  ▸ Extension: supported_groups (len=6)
  ▸ Extension: ec_point_formats (len=2)
    [JA4: t10i120300_d94e65cdb899_f8ec56bc740a]
    [JA4_r: t10i120300_0004,0005,000a,0013,002f,0032,0035,0038,c009,c00a,c013,c014_000a,000b,ff01]
    [JA3 Fullstring: 769,47-53-5-10-49171-49172-49161-49162-50-56-19-4,65281-10-11,23-24,0]
    [JA3: 6734f37431670b3ab4292b8f60f29984]
```

```
0000  00 04 c0 83 b4 1a 00 11  0a 9f c0 2d 08 00 45 00   ··
0010  00 87 1b 47 40 00 80 06  03 62 0a 02 17 e7 c3 7b   ··
0020  f6 63 c1 94 01 bf 77 dd  d8 64 ec b5 f2 93 50 18   ·c
0030  fa f0 bb 8e 00 00 16 03  01 00 5a 01 00 00 56 03   ··
0040  01 5c 71 a2 12 98 46 c5  46 40 8b de 51 1a fd 92   ·\
0050  e9 26 4d e2 ac 85 f8 c6  a1 68 0b 21 30 d7 11 fd   ·&
0060  59 00 00 18 00 2f 00 35  00 05 00 0a c0 13 c0 14   Y·
0070  c0 09 c0 0a 00 32 00 38  00 13 00 04 01 00 00 15   ··
0080  ff 01 00 01 00 00 0a 00  06 00 04 00 17 00 18 00   ··
0090  0b 00 02 01 00                                      ··
```

Explanation: Malicious traffic between 195[.]123[.]246[.]99



5 / 94

Community Score

5/94 security vendors flagged this IP address as malicious

195.123.246.99 (195.123.240.0/21)
AS 204957 (Green Floid LLC)

CZ

Last Analysis Date
1 month ago

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

Security vendors' analysis

Do you want to automate checks?

alphaMountain.ai	Malicious	Criminal IP	Malicious
CyRadar	Malicious	Dr.Web	Malicious
SOCRadar	Phishing	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean
AILabs (MONITORAPP)	Clean	AlienVault	Clean
Antiy-AVL	Clean	benkow.cc	Clean
BitDefender	Clean	Blueliv	Clean
Certego	Clean	Chong Lua Dao	Clean
CINS Army	Clean	CMC Threat Intelligence	Clean
CRDF	Clean	Cyble	Clean
desenmascara.me	Clean	DNS8	Clean
EmergingThreats	Clean	Emsisoft	Clean

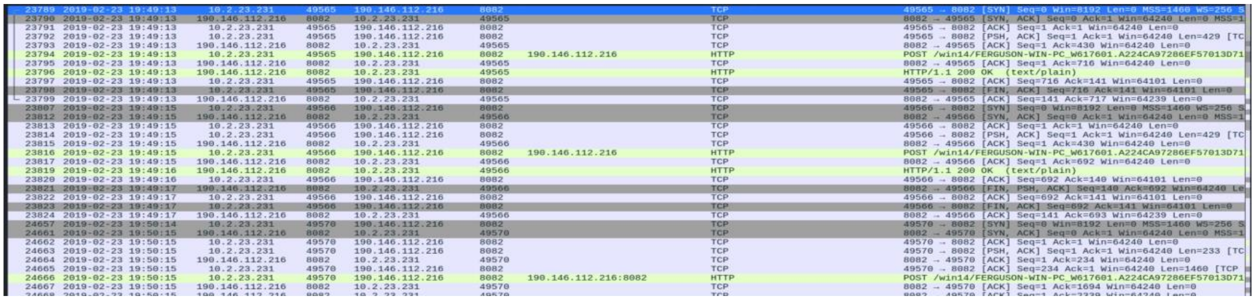
Explanation: Results of VirusTotal lookup on 195[.]123[.]246[.]99

Final Occurrence:

-Interaction with malicious web server 190[.]146[.]112[.]216

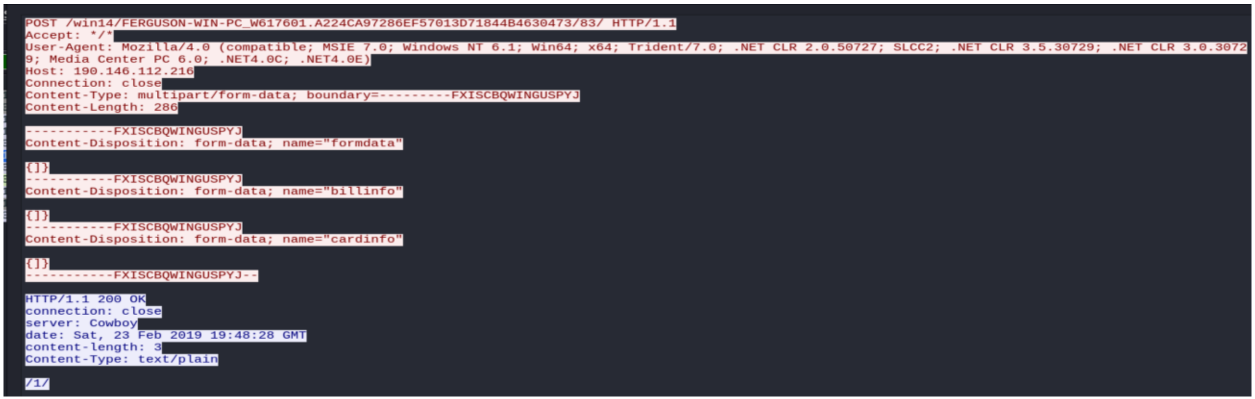
-Web server sends check in response along with 4 POST requests for information on the infected host device

-Made a request for financial data, one for domain information, one for network information and one for outlook credentials



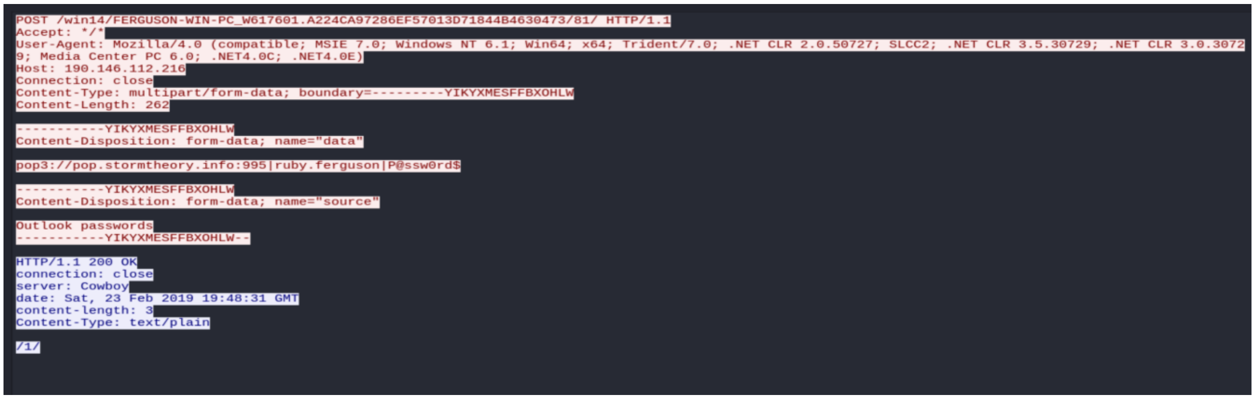
```
23789 2019-02-23 19:49:13    10.2.23.231    49565  190.146.112.216  8082                         TCP   49565 → 8082 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 S
23790 2019-02-23 19:49:13 190.146.112.216   8082   10.2.23.231      49565                        TCP   8082 → 49565 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1
23791 2019-02-23 19:49:13    10.2.23.231    49565  190.146.112.216  8082                         TCP   49565 → 8082 [ACK] Seq=1 Ack=1 Win=64240 Len=0
23792 2019-02-23 19:49:13    10.2.23.231    49565  190.146.112.216  8082                         TCP   49565 → 8082 [PSH, ACK] Seq=1 Ack=1 Win=64240 Len=429 [TC
23793 2019-02-23 19:49:13 190.146.112.216   8082   10.2.23.231      49565                        TCP   8082 → 49565 [ACK] Seq=1 Ack=430 Win=64240 Len=0
23794 2019-02-23 19:49:13    10.2.23.231    49565  190.146.112.216  8082   190.146.112.216       HTTP  POST /win14/FERGUSON-WIN-PC_W617601.A224CA97286EF57013D71
23795 2019-02-23 19:49:13 190.146.112.216   8082   10.2.23.231      49565                        TCP   8082 → 49565 [ACK] Seq=1 Ack=716 Win=64240 Len=0
23796 2019-02-23 19:49:13 190.146.112.216   8082   10.2.23.231      49565                        HTTP  HTTP/1.1 200 OK  (text/plain)
23797 2019-02-23 19:49:13    10.2.23.231    49565  190.146.112.216  8082                         TCP   49565 → 8082 [ACK] Seq=716 Ack=141 Win=64101 Len=0
23798 2019-02-23 19:49:13    10.2.23.231    49565  190.146.112.216  8082                         TCP   49565 → 8082 [FIN, ACK] Seq=716 Ack=141 Win=64101 Len=0
23799 2019-02-23 19:49:13 190.146.112.216   8082   10.2.23.231      49565                        TCP   8082 → 49565 [ACK] Seq=141 Ack=717 Win=64239 Len=0
23807 2019-02-23 19:49:15    10.2.23.231    49566  190.146.112.216  8082                         TCP   49566 → 8082 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 S
23812 2019-02-23 19:49:15 190.146.112.216   8082   10.2.23.231      49566                        TCP   8082 → 49566 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1
23813 2019-02-23 19:49:15    10.2.23.231    49566  190.146.112.216  8082                         TCP   49566 → 8082 [ACK] Seq=1 Ack=1 Win=64240 Len=0
23814 2019-02-23 19:49:15    10.2.23.231    49566  190.146.112.216  8082                         TCP   49566 → 8082 [PSH, ACK] Seq=1 Ack=1 Win=64240 Len=429 [TC
23815 2019-02-23 19:49:15 190.146.112.216   8082   10.2.23.231      49566                        TCP   8082 → 49566 [ACK] Seq=1 Ack=430 Win=64240 Len=0
23816 2019-02-23 19:49:15    10.2.23.231    49566  190.146.112.216  8082   190.146.112.216       HTTP  POST /win14/FERGUSON-WIN-PC_W617601.A224CA97286EF57013D71
23817 2019-02-23 19:49:15 190.146.112.216   8082   10.2.23.231      49566                        TCP   8082 → 49566 [ACK] Seq=1 Ack=692 Win=64240 Len=0
23819 2019-02-23 19:49:16 190.146.112.216   8082   10.2.23.231      49566                        HTTP  HTTP/1.1 200 OK  (text/plain)
23820 2019-02-23 19:49:16    10.2.23.231    49566  190.146.112.216  8082                         TCP   49566 → 8082 [ACK] Seq=692 Ack=140 Win=64101 Len=0
23821 2019-02-23 19:49:17 190.146.112.216   8082   10.2.23.231      49566                        TCP   8082 → 49566 [FIN, PSH, ACK] Seq=140 Ack=692 Win=64240 Le
23822 2019-02-23 19:49:17    10.2.23.231    49566  190.146.112.216  8082                         TCP   49566 → 8082 [ACK] Seq=692 Ack=141 Win=64101 Len=0
23823 2019-02-23 19:49:17    10.2.23.231    49566  190.146.112.216  8082                         TCP   49566 → 8082 [FIN, ACK] Seq=692 Ack=141 Win=64101 Len=0
23824 2019-02-23 19:49:17 190.146.112.216   8082   10.2.23.231      49566                        TCP   8082 → 49566 [ACK] Seq=141 Ack=693 Win=64239 Len=0
24657 2019-02-23 19:50:14    10.2.23.231    49570  190.146.112.216  8082                         TCP   49570 → 8082 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 S
24661 2019-02-23 19:50:15 190.146.112.216   8082   10.2.23.231      49570                        TCP   8082 → 49570 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1
24662 2019-02-23 19:50:15    10.2.23.231    49570  190.146.112.216  8082                         TCP   49570 → 8082 [ACK] Seq=1 Ack=1 Win=64240 Len=0
24663 2019-02-23 19:50:15    10.2.23.231    49570  190.146.112.216  8082                         TCP   49570 → 8082 [PSH, ACK] Seq=1 Ack=1 Win=64240 Len=233 [TC
24664 2019-02-23 19:50:15 190.146.112.216   8082   10.2.23.231      49570                        TCP   8082 → 49570 [ACK] Seq=1 Ack=234 Win=64240 Len=0
24665 2019-02-23 19:50:15    10.2.23.231    49570  190.146.112.216  8082                         TCP   49570 → 8082 [ACK] Seq=234 Ack=1 Win=64240 Len=1460 [TCP
24666 2019-02-23 19:50:15    10.2.23.231    49570  190.146.112.216  8082   190.146.112.216:8082  HTTP  POST /win14/FERGUSON-WIN-PC_W617601.A224CA97286EF57013D71
24667 2019-02-23 19:50:15 190.146.112.216   8082   10.2.23.231      49570                        TCP   8082 → 49570 [ACK] Seq=1 Ack=1694 Win=64240 Len=0
24668 2019-02-23 19:50:15 190.146.112.216   8082   10.2.23.231      49570                        TCP   8082 → 49570 [ACK] Seq=1 Ack=3339 Win=64240 Len=0
```

Explanation: Check-in response from web server 190[.]146[.]112[.]216



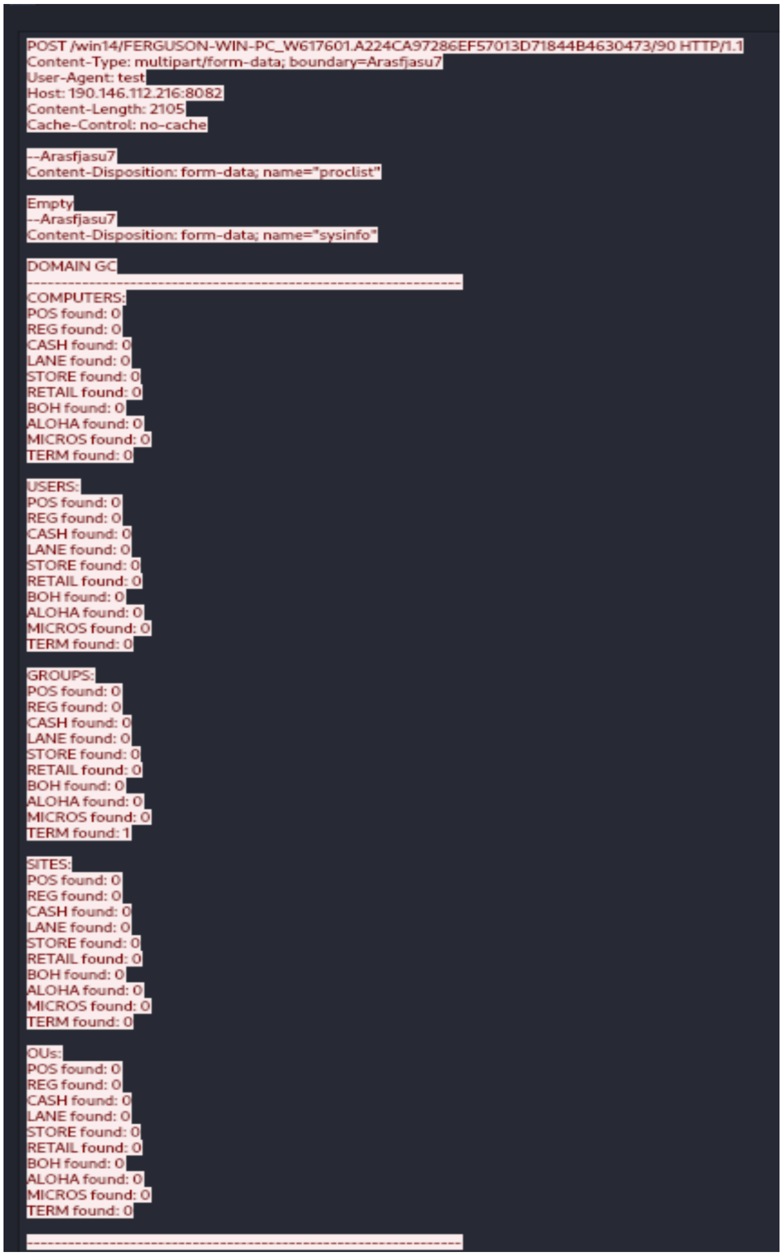
```
POST /win14/FERGUSON-WIN-PC_W617601.A224CA97286EF57013D71844B4630473/83/ HTTP/1.1
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.3072
9; Media Center PC 6.0; .NET4.0C; .NET4.0E)
Host: 190.146.112.216
Connection: close
Content-Type: multipart/form-data; boundary=---------FXISCBQWINGUSPYJ
Content-Length: 286

-----------FXISCBQWINGUSPYJ
Content-Disposition: form-data; name="formdata"

{[]}
-----------FXISCBQWINGUSPYJ
Content-Disposition: form-data; name="billinfo"

{[]}
-----------FXISCBQWINGUSPYJ
Content-Disposition: form-data; name="cardinfo"

{[]}
-----------FXISCBQWINGUSPYJ--

HTTP/1.1 200 OK
connection: close
server: Cowboy
date: Sat, 23 Feb 2019 19:48:28 GMT
content-length: 3
Content-Type: text/plain

/1/
```

Explanation: HTTP Stream of first post request for financial data being returned to the web server



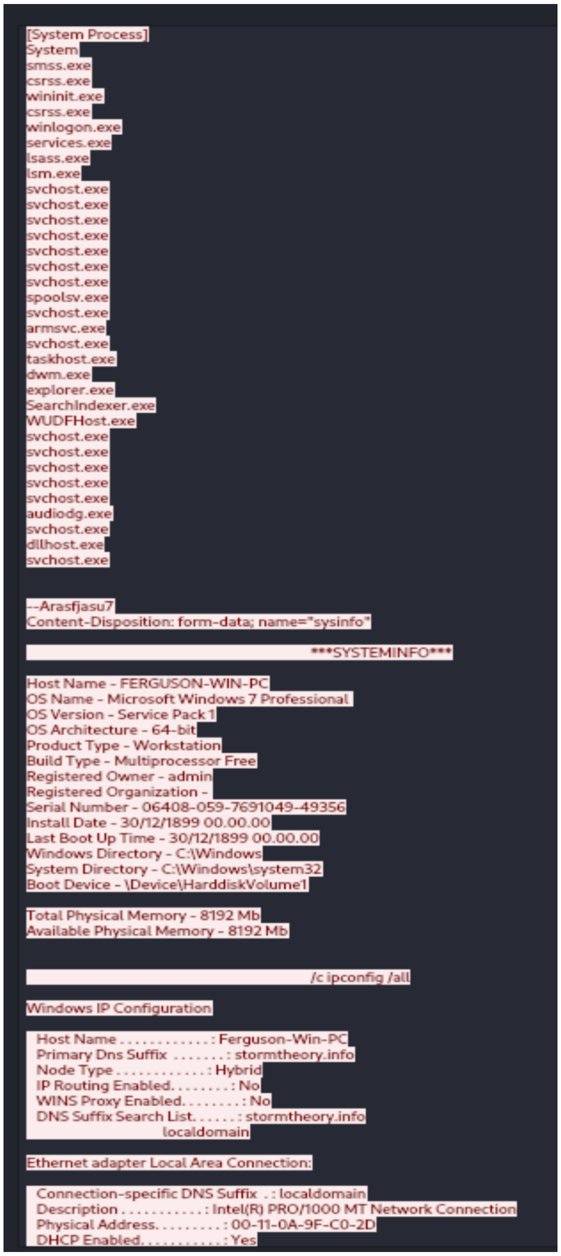
```
POST /win14/FERGUSON-WIN-PC_W617601.A224CA97286EF57013D71844B4630473/81/ HTTP/1.1
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.3072
9; Media Center PC 6.0; .NET4.0C; .NET4.0E)
Host: 190.146.112.216
Connection: close
Content-Type: multipart/form-data; boundary=---------YIKYXMESFFBXOHLW
Content-Length: 262

-----------YIKYXMESFFBXOHLW
Content-Disposition: form-data; name="data"

pop3://pop.stormtheory.info:995|ruby.ferguson|P@ssw0rd$

-----------YIKYXMESFFBXOHLW
Content-Disposition: form-data; name="source"

Outlook passwords
-----------YIKYXMESFFBXOHLW--

HTTP/1.1 200 OK
connection: close
server: Cowboy
date: Sat, 23 Feb 2019 19:48:31 GMT
content-length: 3
Content-Type: text/plain

/1/
```

Explanation: HTTP Stream of second post request for Outlook passwords being returned to web server



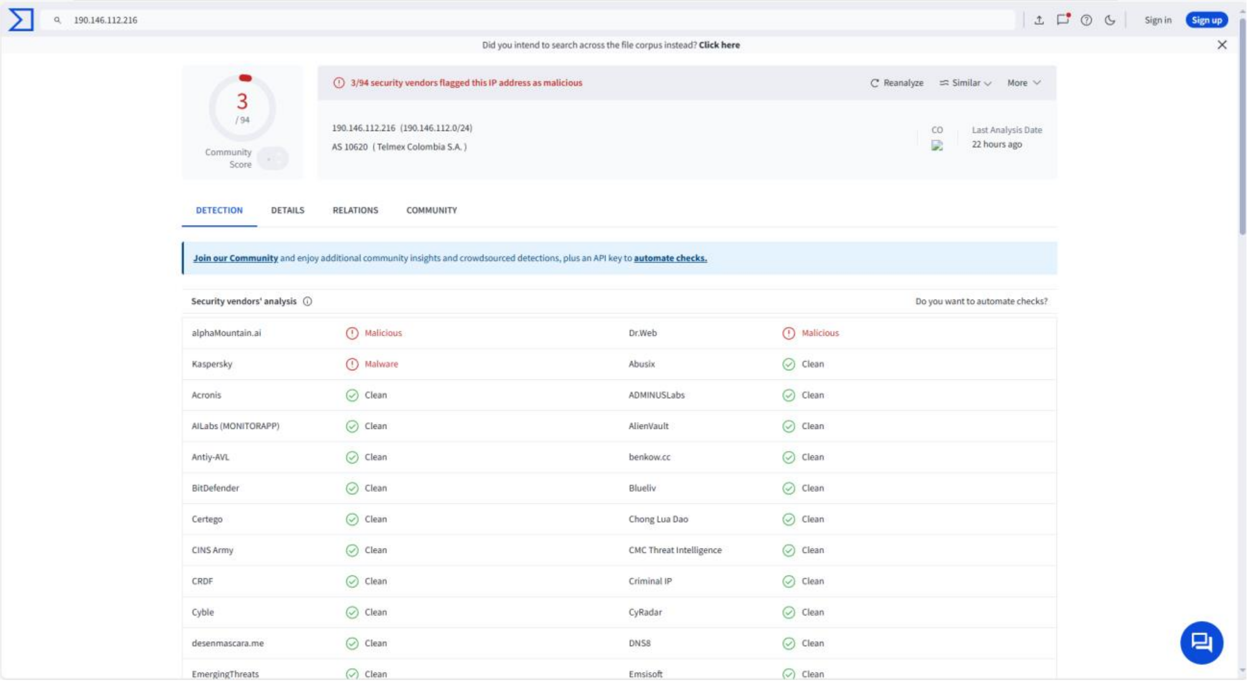
```
POST /win14/FERGUSON-WIN-PC_W617601.A224CA97286EF57013D71844B4630473/90 HTTP/1.1
Content-Type: multipart/form-data; boundary=Arasfjasu7
User-Agent: test
Host: 190.146.112.216:8082
Content-Length: 2105
Cache-Control: no-cache

--Arasfjasu7
Content-Disposition: form-data; name="proclist"

Empty
--Arasfjasu7
Content-Disposition: form-data; name="sysinfo"

DOMAIN GC
------------------------------------------------------------
COMPUTERS:
POS found: 0
REG found: 0
CASH found: 0
LANE found: 0
STORE found: 0
RETAIL found: 0
BOH found: 0
ALOHA found: 0
MICROS found: 0
TERM found: 0

USERS:
POS found: 0
REG found: 0
CASH found: 0
LANE found: 0
STORE found: 0
RETAIL found: 0
BOH found: 0
ALOHA found: 0
MICROS found: 0
TERM found: 0

GROUPS:
POS found: 0
REG found: 0
CASH found: 0
LANE found: 0
STORE found: 0
RETAIL found: 0
BOH found: 0
ALOHA found: 0
MICROS found: 0
TERM found: 1

SITES:
POS found: 0
REG found: 0
CASH found: 0
LANE found: 0
STORE found: 0
RETAIL found: 0
BOH found: 0
ALOHA found: 0
MICROS found: 0
TERM found: 0

OUs:
POS found: 0
REG found: 0
CASH found: 0
LANE found: 0
STORE found: 0
RETAIL found: 0
BOH found: 0
ALOHA found: 0
MICROS found: 0
TERM found: 0

------------------------------------------------------------
```

Explanation: HTTP stream of domain information of host network being returned to malicious web server



```
[System Process]
System
smss.exe
csrss.exe
wininit.exe
csrss.exe
winlogon.exe
services.exe
lsass.exe
lsm.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
spoolsv.exe
svchost.exe
armsvc.exe
svchost.exe
taskhost.exe
dwm.exe
explorer.exe
SearchIndexer.exe
WUDFHost.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
audiodg.exe
svchost.exe
dllhost.exe
svchost.exe


--Arasfjasu7
Content-Disposition: form-data; name="sysinfo"

                                                    ***SYSTEMINFO***

Host Name - FERGUSON-WIN-PC
OS Name - Microsoft Windows 7 Professional
OS Version - Service Pack 1
OS Architecture - 64-bit
Product Type - Workstation
Build Type - Multiprocessor Free
Registered Owner - admin
Registered Organization -
Serial Number - 06408-059-7691049-49356
Install Date - 30/12/1899 00.00.00
Last Boot Up Time - 30/12/1899 00.00.00
Windows Directory - C:\Windows
System Directory - C:\Windows\system32
Boot Device - \Device\HarddiskVolume1

Total Physical Memory - 8192 Mb
Available Physical Memory - 8192 Mb


                                                    /c ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : Ferguson-Win-PC
   Primary Dns Suffix  . . . . . . . : stormtheory.info
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : stormtheory.info
                                       localdomain

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : localdomain
   Description . . . . . . . . . . . : Intel(R) PRO/1000 MT Network Connection
   Physical Address. . . . . . . . . : 00-11-0A-9F-C0-2D
   DHCP Enabled. . . . . . . . . . . : Yes
```

Explanation: HTTP stream of system processes and network information pertaining to the host being returned to web server


190.146.112.216

Did you intend to search across the file corpus instead? **Click here**

3 /94

Community Score

3/94 security vendors flagged this IP address as malicious

Reanalyze | Similar | More

190.146.112.216 (190.146.112.0/24)
AS 10620 (Telmex Colombia S.A.)

CO

Last Analysis Date
22 hours ago

DETECTION | DETAILS | RELATIONS | COMMUNITY

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

Security vendors' analysis

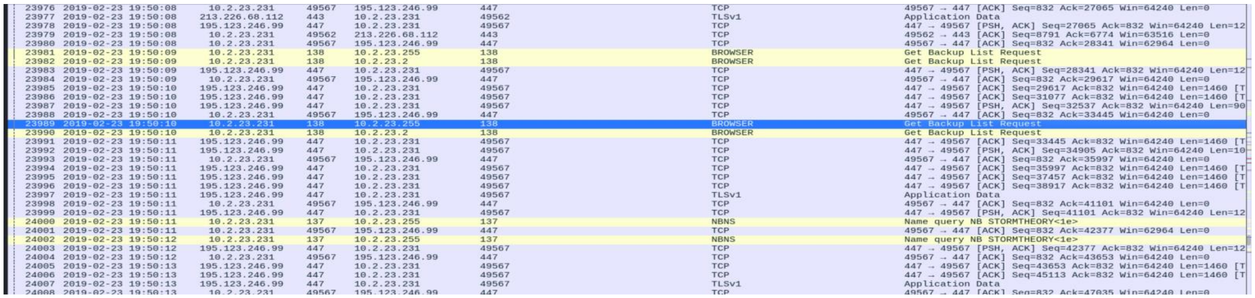
Do you want to automate checks?

alphaMountain.ai	Malicious	Dr.Web	Malicious
Kaspersky	Malware	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean
AILabs (MONITORAPP)	Clean	AlienVault	Clean
Antiy-AVL	Clean	benkow.cc	Clean
BitDefender	Clean	Blueliv	Clean
Certego	Clean	Chong Lua Dao	Clean
CINS Army	Clean	CMC Threat Intelligence	Clean
CRDF	Clean	Criminal IP	Clean
Cyble	Clean	CyRadar	Clean
desenmascara.me	Clean	DNS8	Clean
EmergingThreats	Clean	Emsisoft	Clean

Explanation: Results of VirusTotal lookup on IP 190[.]146[.]112[.]216

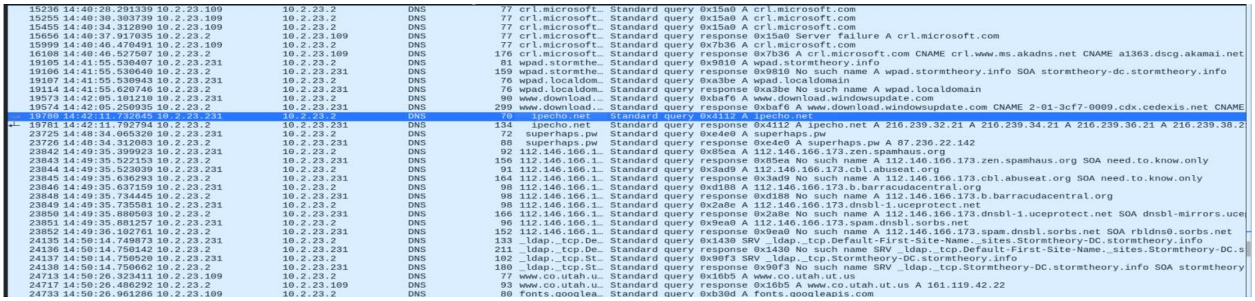
Noteworthy Mentions:

-Get Backup List Request which obtains information about other systems/computers on a network.


```
23976 2019-02-23 19:50:08   10.2.23.231     49567  195.123.246.99  447    TCP      49567 → 447 [ACK] Seq=832 Ack=27065 Win=64240 Len=0
23977 2019-02-23 19:50:08   213.226.68.112  443    10.2.23.231     49562  TLSv1    Application Data
23978 2019-02-23 19:50:08   195.123.246.99  447    10.2.23.231     49567  TCP      447 → 49567 [PSH, ACK] Seq=27065 Ack=832 Win=64240 Len=12
23979 2019-02-23 19:50:08   10.2.23.231     49562  213.226.68.112  443    TCP      49562 → 443 [ACK] Seq=8791 Ack=6774 Win=63516 Len=0
23980 2019-02-23 19:50:08   10.2.23.231     49567  195.123.246.99  447    TCP      49567 → 447 [ACK] Seq=832 Ack=28341 Win=62964 Len=0
23981 2019-02-23 19:50:09   10.2.23.231     138    10.2.23.255     138    BROWSER  Get Backup List Request
23982 2019-02-23 19:50:09   10.2.23.231     138    10.2.23.2       138    BROWSER  Get Backup List Request
23983 2019-02-23 19:50:09   195.123.246.99  447    10.2.23.231     49567  TCP      447 → 49567 [PSH, ACK] Seq=28341 Ack=832 Win=64240 Len=12
23984 2019-02-23 19:50:09   10.2.23.231     49567  195.123.246.99  447    TCP      49567 → 447 [ACK] Seq=832 Ack=29617 Win=64240 Len=0
23985 2019-02-23 19:50:10   195.123.246.99  447    10.2.23.231     49567  TCP      447 → 49567 [ACK] Seq=29617 Ack=832 Win=64240 Len=1460 [T
23986 2019-02-23 19:50:10   195.123.246.99  447    10.2.23.231     49567  TCP      447 → 49567 [ACK] Seq=31077 Ack=832 Win=64240 Len=1460 [T
23987 2019-02-23 19:50:10   195.123.246.99  447    10.2.23.231     49567  TCP      447 → 49567 [PSH, ACK] Seq=32537 Ack=832 Win=64240 Len=90
23988 2019-02-23 19:50:10   10.2.23.231     49567  195.123.246.99  447    TCP      49567 → 447 [ACK] Seq=832 Ack=33445 Win=64240 Len=0
23989 2019-02-23 19:50:10   10.2.23.231     138    10.2.23.255     138    BROWSER  Get Backup List Request
23990 2019-02-23 19:50:10   10.2.23.231     138    10.2.23.2       138    BROWSER  Get Backup List Request
23991 2019-02-23 19:50:11   195.123.246.99  447    10.2.23.231     49567  TCP      447 → 49567 [ACK] Seq=33445 Ack=832 Win=64240 Len=1460 [T
23992 2019-02-23 19:50:11   195.123.246.99  447    10.2.23.231     49567  TCP      447 → 49567 [PSH, ACK] Seq=34905 Ack=832 Win=64240 Len=10
23993 2019-02-23 19:50:11   10.2.23.231     49567  195.123.246.99  447    TCP      49567 → 447 [ACK] Seq=832 Ack=35997 Win=64240 Len=0
23994 2019-02-23 19:50:11   195.123.246.99  447    10.2.23.231     49567  TCP      447 → 49567 [ACK] Seq=35997 Ack=832 Win=64240 Len=1460 [T
23995 2019-02-23 19:50:11   195.123.246.99  447    10.2.23.231     49567  TCP      447 → 49567 [ACK] Seq=37457 Ack=832 Win=64240 Len=1460 [T
23996 2019-02-23 19:50:11   195.123.246.99  447    10.2.23.231     49567  TCP      447 → 49567 [ACK] Seq=38917 Ack=832 Win=64240 Len=1460 [T
23997 2019-02-23 19:50:11   195.123.246.99  447    10.2.23.231     49567  TLSv1    Application Data
23998 2019-02-23 19:50:11   10.2.23.231     49567  195.123.246.99  447    TCP      49567 → 447 [ACK] Seq=832 Ack=41101 Win=64240 Len=0
23999 2019-02-23 19:50:11   195.123.246.99  447    10.2.23.231     49567  TCP      447 → 49567 [PSH, ACK] Seq=41101 Ack=832 Win=64240 Len=12
24000 2019-02-23 19:50:11   10.2.23.231     137    10.2.23.255     137    NBNS     Name query NB STORMTHEORY<1e>
24001 2019-02-23 19:50:11   10.2.23.231     49567  195.123.246.99  447    TCP      49567 → 447 [ACK] Seq=832 Ack=42377 Win=62964 Len=0
24002 2019-02-23 19:50:12   10.2.23.231     137    10.2.23.255     137    NBNS     Name query NB STORMTHEORY<1e>
24003 2019-02-23 19:50:12   195.123.246.99  447    10.2.23.231     49567  TCP      447 → 49567 [PSH, ACK] Seq=42377 Ack=832 Win=64240 Len=12
24004 2019-02-23 19:50:12   10.2.23.231     49567  195.123.246.99  447    TCP      49567 → 447 [ACK] Seq=832 Ack=43653 Win=64240 Len=0
24005 2019-02-23 19:50:13   195.123.246.99  447    10.2.23.231     49567  TCP      447 → 49567 [ACK] Seq=43653 Ack=832 Win=64240 Len=1460 [T
24006 2019-02-23 19:50:13   195.123.246.99  447    10.2.23.231     49567  TCP      447 → 49567 [ACK] Seq=45113 Ack=832 Win=64240 Len=1460 [T
24007 2019-02-23 19:50:13   195.123.246.99  447    10.2.23.231     49567  TLSv1    Application Data
24008 2019-02-23 19:50:13   10.2.23.231     49567  195.123.246.99  447    TCP      49567 → 447 [ACK] Seq=832 Ack=47035 Win=64240 Len=0
```

Explanation: Get Backup List Request from malicious host

-ipecho[.]net visited by infected host to return more host information to C2 server (browser identification, proxy detection, etc.)



```
15236 14:40:28.291339 10.2.23.109   10.2.23.2     DNS   77 crl.microsoft… Standard query 0x15a0 A crl.microsoft.com
15255 14:40:30.303739 10.2.23.109   10.2.23.2     DNS   77 crl.microsoft… Standard query 0x15a0 A crl.microsoft.com
15455 14:40:34.312890 10.2.23.109   10.2.23.2     DNS   77 crl.microsoft… Standard query 0x15a0 A crl.microsoft.com
15656 14:40:37.917035 10.2.23.2     10.2.23.109   DNS   77 crl.microsoft… Standard query response 0x15a0 Server failure A crl.microsoft.com
15999 14:40:46.470491 10.2.23.109   10.2.23.2     DNS   77 crl.microsoft… Standard query 0x7b36 A crl.microsoft.com
16108 14:40:46.527507 10.2.23.2     10.2.23.109   DNS  176 crl.microsoft… Standard query response 0x7b36 A crl.microsoft.com CNAME crl.www.ms.akadns.net CNAME a1363.dscg.akamai.net
19105 14:41:55.530407 10.2.23.231   10.2.23.2     DNS   81 wpad.stormthe… Standard query 0x9810 A wpad.stormtheory.info
19106 14:41:55.530640 10.2.23.2     10.2.23.231   DNS  159 wpad.stormthe… Standard query response 0x9810 No such name A wpad.stormtheory.info SOA stormtheory-dc.stormtheory.info
19107 14:41:55.530943 10.2.23.231   10.2.23.2     DNS   76 wpad.localdom… Standard query 0xa3be A wpad.localdomain
19114 14:41:55.620746 10.2.23.2     10.2.23.231   DNS   76 wpad.localdom… Standard query response 0xa3be No such name A wpad.localdomain
19573 14:42:05.101210 10.2.23.231   10.2.23.2     DNS   90 www.download.… Standard query 0xbaf6 A www.download.windowsupdate.com
19574 14:42:05.250935 10.2.23.2     10.2.23.231   DNS  299 www.download.… Standard query response 0xbaf6 A www.download.windowsupdate.com CNAME 2-01-3cf7-0009.cdx.cedexis.net CNAME
19780 14:42:11.732645 10.2.23.231   10.2.23.2     DNS   70  ipecho.net    Standard query 0x4112 A ipecho.net
19781 14:42:11.792794 10.2.23.2     10.2.23.231   DNS  134  ipecho.net    Standard query response 0x4112 A ipecho.net A 216.239.32.21 A 216.239.34.21 A 216.239.36.21 A 216.239.38.2
23725 14:48:34.065320 10.2.23.231   10.2.23.2     DNS   72  superhaps.pw  Standard query 0xe4e0 A superhaps.pw
23726 14:48:34.312083 10.2.23.2     10.2.23.231   DNS   88  superhaps.pw  Standard query response 0xe4e0 A superhaps.pw A 87.236.22.142
23842 14:49:35.399923 10.2.23.231   10.2.23.2     DNS   92 112.146.166.1… Standard query 0x85ea A 112.146.166.173.zen.spamhaus.org
23843 14:49:35.522153 10.2.23.2     10.2.23.231   DNS  156 112.146.166.1… Standard query response 0x85ea No such name A 112.146.166.173.zen.spamhaus.org SOA need.to.know.only
23844 14:49:35.523039 10.2.23.231   10.2.23.2     DNS   91 112.146.166.1… Standard query 0x3ad9 A 112.146.166.173.cbl.abuseat.org
23845 14:49:35.636293 10.2.23.2     10.2.23.231   DNS  164 112.146.166.1… Standard query response 0x3ad9 No such name A 112.146.166.173.cbl.abuseat.org SOA need.to.know.only
23846 14:49:35.637159 10.2.23.231   10.2.23.2     DNS   98 112.146.166.1… Standard query 0xd188 A 112.146.166.173.b.barracudacentral.org
23848 14:49:35.734445 10.2.23.2     10.2.23.231   DNS   98 112.146.166.1… Standard query response 0xd188 No such name A 112.146.166.173.b.barracudacentral.org
23849 14:49:35.735581 10.2.23.231   10.2.23.2     DNS   98 112.146.166.1… Standard query 0x2a8e A 112.146.166.173.dnsbl-1.uceprotect.net
23850 14:49:35.880503 10.2.23.2     10.2.23.231   DNS  166 112.146.166.1… Standard query response 0x2a8e No such name A 112.146.166.173.dnsbl-1.uceprotect.net SOA dnsbl-mirrors.uce
23851 14:49:35.881257 10.2.23.231   10.2.23.2     DNS   96 112.146.166.1… Standard query 0x9ea0 A 112.146.166.173.spam.dnsbl.sorbs.net
23852 14:49:36.102761 10.2.23.2     10.2.23.231   DNS  152 112.146.166.1… Standard query response 0x9ea0 No such name A 112.146.166.173.spam.dnsbl.sorbs.net SOA rbldns0.sorbs.net
24135 14:50:14.749873 10.2.23.231   10.2.23.2     DNS  133 _ldap._tcp.De… Standard query 0x1430 SRV _ldap._tcp.Default-First-Site-Name._sites.Stormtheory-DC.stormtheory.info
24136 14:50:14.750142 10.2.23.2     10.2.23.231   DNS  211 _ldap._tcp.De… Standard query response 0x1430 No such name SRV _ldap._tcp.Default-First-Site-Name._sites.Stormtheory-DC.s
24137 14:50:14.750520 10.2.23.231   10.2.23.2     DNS  102 _ldap._tcp.St… Standard query 0x90f3 SRV _ldap._tcp.Stormtheory-DC.stormtheory.info
24138 14:50:14.750662 10.2.23.2     10.2.23.231   DNS  180 _ldap._tcp.St… Standard query response 0x90f3 No such name SRV _ldap._tcp.Stormtheory-DC.stormtheory.info SOA stormtheory
24713 14:50:26.323411 10.2.23.109   10.2.23.2     DNS   77 www.co.utah.u… Standard query 0x16b5 A www.co.utah.ut.us
24717 14:50:26.486292 10.2.23.2     10.2.23.109   DNS   93 www.co.utah.u… Standard query response 0x16b5 A www.co.utah.ut.us A 161.119.42.22
24733 14:50:26.961286 10.2.23.109   10.2.23.2     DNS   80 fonts.googlea… Standard query 0xb30d A fonts.googleapis.com
```

Explanation: snippet of Host visiting IP service

References and Resources Used:

https://www.virustotal.com/gui/home/upload

https://sslbl.abuse.ch/ja3-fingerprints/

https://any.run/malware-trends/trickbot

https://medium.com/@0x0vid/malware-analysis-trickbot-part-3-network-collector-dll-1940741c7ac3

https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-076a

https://www.netsecurity.com/trickbot-malware-analysis/

https://chatgpt.com/

https://app.crowdsec.net/cti

https://www.abuseipdb.com/

https://urlscan.io/