PCAP Threat Analysis Report – Exercise 1

Lutho Mboniswa 25 April 2025

1. Introduction

This report summarizes the analysis of a PCAP file provided for the CTF challenge hosted by Snode Technologies at the Security Summit Ideathon event in preparation for the Security Summit hackathon. The goal of this challenge was to identify and investigate a suspicious IP address, correlate it with known threat intelligence sources and tools, and provide recommendations to mitigate similar threats in the future.

2. Tools and Methods Used

The following tools and methodologies were used to inspect the PCAP and identify the threat:
- **Wireshark**: To inspect raw traffic, identify suspicious connections, and analyze packet-level behavior.
- **VirusTotal**: For open-source threat intelligence, used to check IP reputation.
- **Wireshark Filters:** Custom filters applied such as `ip.addr == `x.x.x.x`, `tcp.port == 443`, `tcp`, and `tls` to isolate traffic and investigate further.

Traffic analysis focused on TCP connections over port 443. Each IP connecting over this protocol was noted and cross-referenced against public threat intelligence tools for IP reputation.

3. Identified Malicious IP Address

Suspicious IP Address: *51.124.78[.]146*

Evidence from PCAP:
The suspicious IP was not the initiator of the connection; instead, it was contacted by an internal host, which then initiated the three-way handshake. The traffic consisted mainly of TCP ACK packets and encrypted TLS traffic, lacking application-layer data such as HTTP

headers. This behavior indicates a possible Command and Control (C2) beacon, data exfiltration attempt, or crypto-mining activity, often seen in malware communications.

The crypto-mining behavior is indicated by the repetitive sessions opened by the internal host to incrementing host numbers, which indicates possible automation.

Screenshots and specific timestamps are available in appendix A.

4. IP Intelligence (VirusTotal Analysis)

- VirusTotal Report URL: https://www.virustotal.com/gui/ip-address/51.124.78.146/community
- Threat Classification: Cryptocurrency Miner
- Associated Tags: Suspicious
- Last Seen: *2025-05-06 13:53:32*
- Related Files/Domains (if any): (Appendix, figure 4x)

5. Link to Malicious Activity

The endpoint `51.124.78.146` demonstrates persistent, overlapping connections over HTTPS port 43, initiated from incrementing ports on the client side, meaning this host maintains multiple concurrent sessions to the same external IP without terminating previous ones. This behavior suggests automated background activity which is not indicative of normal user behavior.

This IP is flagged as malicious on Virustotal (Figure Vx) and listed as a top IOC in a GitHub report exposing a CrowdStrike-themed crypto-mining and phishing campaign. (Figure Gx)

Alternative scans of the over OTX AlienVault indicate the IP to be linked to the CrowdStrike Crypt-mining campaign as well.

The network behavior combined with open-source intelligence suggests this is not a false positive, but rather a confirmed malicious IOC, warranting isolation, further forensic investigation, and IOC-based detection across the environment.

6. Recommendations

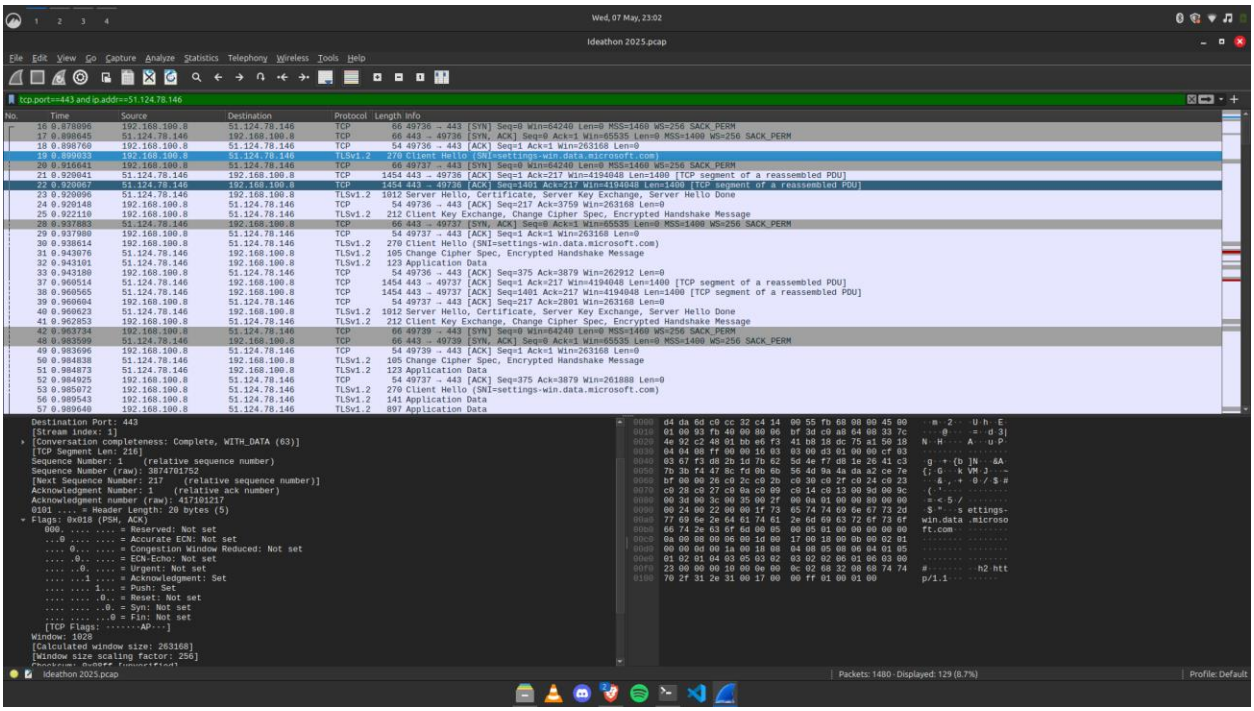
- Implement strict outbound traffic filtering to block unauthorized external communications.
- Deploy network behavior analysis tools to detect unusual traffic patterns such as repeated TLS sessions to rare IPs.
- Use endpoint detection and response (EDR) solutions to monitor and contain infected devices.
- Incorporate threat intelligence feeds into firewalls and SIEMs to block known malicious IPs in real-time.
- Educate users on phishing and other initial infection vectors that might result in similar communication.

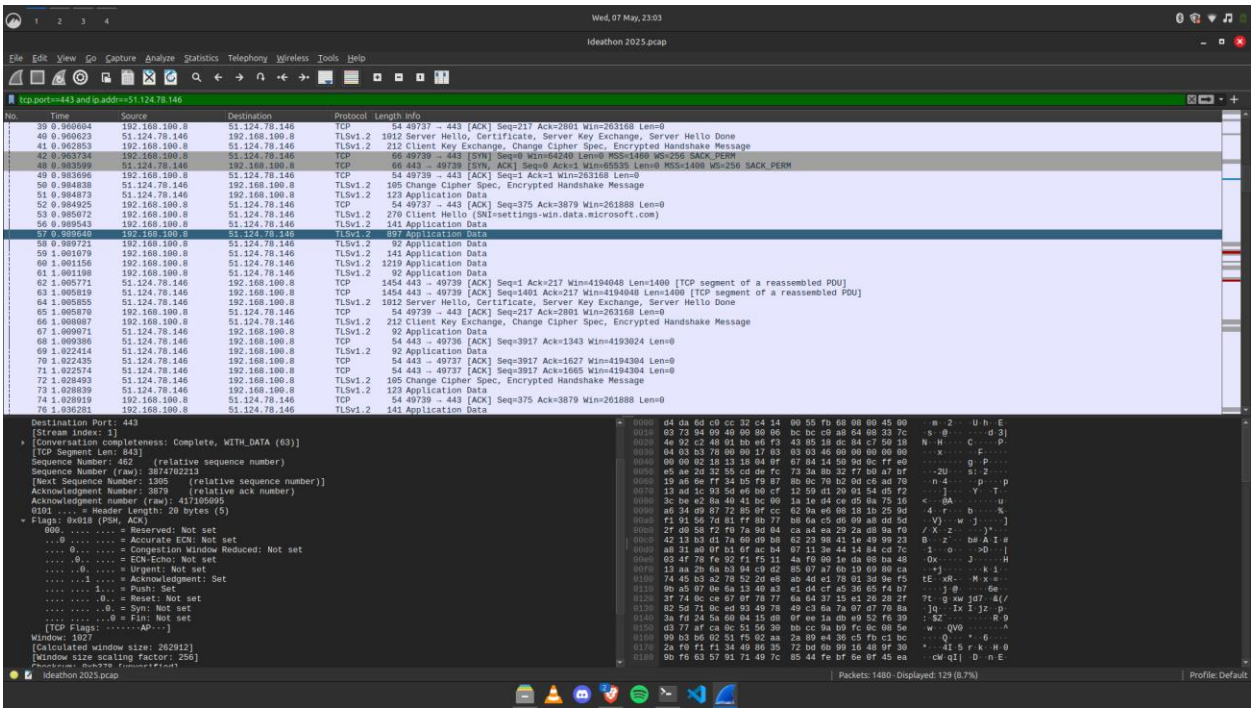
7. Conclusion

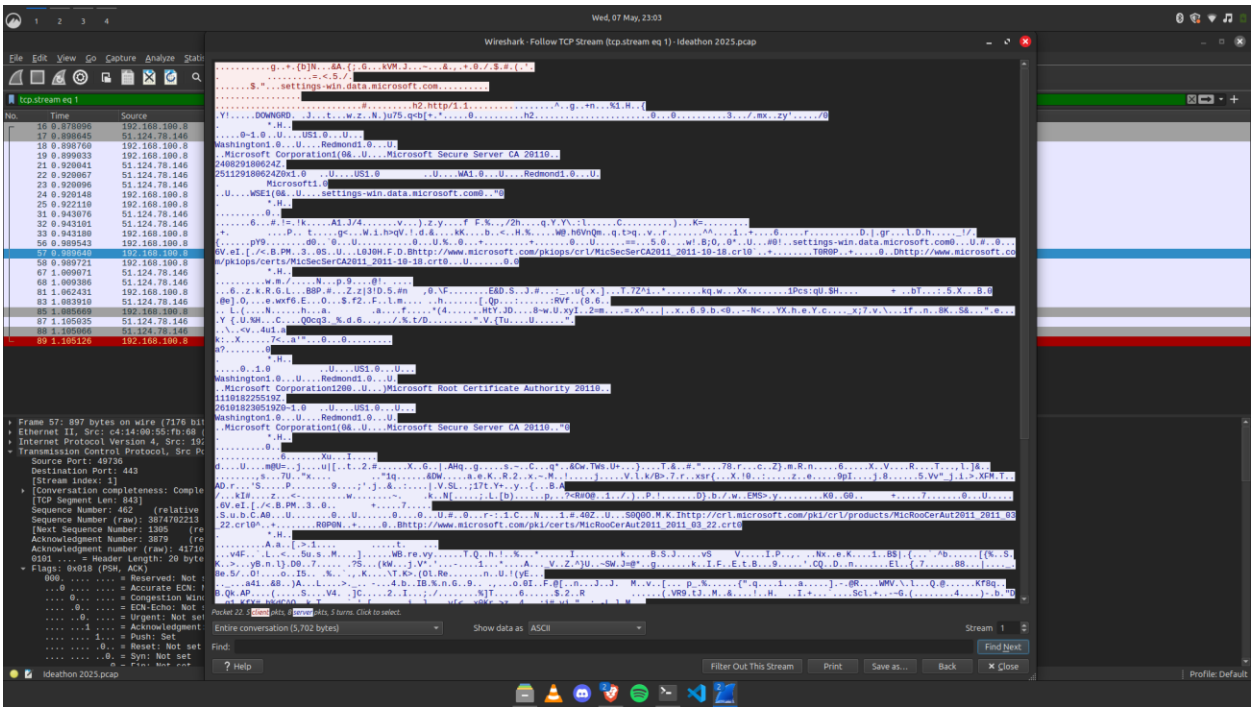
The PCAP analysis revealed outbound encrypted traffic to a known suspicious IP, indicative of potential crypto-mining activity. Though packet content was encrypted, the traffic patterns and threat intelligence link this behavior to a likely Crypto-mining and phishing campaign. Implementing the recommended controls can help prevent, detect, and respond to such threats more effectively in a real-world scenario.

8. Appendix: Screenshots & Filters Used

A. Wireshark Screenshots


Wed, 07 May, 23:02
Ideathon 2025.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.port==443 and ip.addr==51.124.78.146
No. Time Source Destination Protocol Length Info
16 0.878096 192.168.100.8 51.124.78.146 TCP 66 49736 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
17 0.898645 51.124.78.146 192.168.100.8 TCP 66 443 → 49736 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 WS=256 SACK_PERM
18 0.898760 192.168.100.8 51.124.78.146 TCP 54 49736 → 443 [ACK] Seq=1 Ack=1 Win=263168 Len=0
19 0.899033 192.168.100.8 51.124.78.146 TLSv1.2 270 Client Hello (SNI=settings-win.data.microsoft.com)
20 0.916641 192.168.100.8 51.124.78.146 TCP 66 49737 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
21 0.920041 51.124.78.146 192.168.100.8 TCP 1454 443 → 49736 [ACK] Seq=1 Ack=217 Win=4194048 Len=1400 [TCP segment of a reassembled PDU]
22 0.920067 51.124.78.146 192.168.100.8 TCP 1454 443 → 49736 [ACK] Seq=1401 Ack=217 Win=4194048 Len=1400 [TCP segment of a reassembled PDU]
23 0.920096 51.124.78.146 192.168.100.8 TLSv1.2 1012 Server Hello, Certificate, Server Key Exchange, Server Hello Done
24 0.920148 192.168.100.8 51.124.78.146 TCP 54 49736 → 443 [ACK] Seq=217 Ack=3759 Win=263168 Len=0
25 0.922110 192.168.100.8 51.124.78.146 TLSv1.2 212 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
28 0.937883 51.124.78.146 192.168.100.8 TCP 66 443 → 49737 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 WS=256 SACK_PERM
29 0.937980 192.168.100.8 51.124.78.146 TCP 54 49737 → 443 [ACK] Seq=1 Ack=1 Win=263168 Len=0
30 0.938614 192.168.100.8 51.124.78.146 TLSv1.2 270 Client Hello (SNI=settings-win.data.microsoft.com)
31 0.943076 51.124.78.146 192.168.100.8 TLSv1.2 105 Change Cipher Spec, Encrypted Handshake Message
32 0.943101 51.124.78.146 192.168.100.8 TLSv1.2 123 Application Data
33 0.943180 192.168.100.8 51.124.78.146 TCP 54 49736 → 443 [ACK] Seq=375 Ack=3879 Win=262912 Len=0
37 0.960514 51.124.78.146 192.168.100.8 TCP 1454 443 → 49737 [ACK] Seq=1 Ack=217 Win=4194048 Len=1400 [TCP segment of a reassembled PDU]
38 0.960565 51.124.78.146 192.168.100.8 TCP 1454 443 → 49737 [ACK] Seq=1401 Ack=217 Win=4194048 Len=1400 [TCP segment of a reassembled PDU]
39 0.960604 192.168.100.8 51.124.78.146 TCP 54 49737 → 443 [ACK] Seq=217 Ack=2801 Win=263168 Len=0
40 0.960623 51.124.78.146 192.168.100.8 TLSv1.2 1012 Server Hello, Certificate, Server Key Exchange, Server Hello Done
41 0.962853 192.168.100.8 51.124.78.146 TLSv1.2 212 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
42 0.963734 192.168.100.8 51.124.78.146 TCP 66 49739 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
48 0.983599 51.124.78.146 192.168.100.8 TCP 66 443 → 49739 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 WS=256 SACK_PERM
49 0.983696 192.168.100.8 51.124.78.146 TCP 54 49739 → 443 [ACK] Seq=1 Ack=1 Win=263168 Len=0
50 0.984838 51.124.78.146 192.168.100.8 TLSv1.2 105 Change Cipher Spec, Encrypted Handshake Message
51 0.984873 51.124.78.146 192.168.100.8 TLSv1.2 123 Application Data
52 0.984925 192.168.100.8 51.124.78.146 TCP 54 49737 → 443 [ACK] Seq=375 Ack=3879 Win=261888 Len=0
53 0.985072 192.168.100.8 51.124.78.146 TLSv1.2 270 Client Hello (SNI=settings-win.data.microsoft.com)
56 0.989543 51.124.78.146 192.168.100.8 TLSv1.2 141 Application Data
57 0.989640 192.168.100.8 51.124.78.146 TLSv1.2 897 Application Data
Destination Port: 443
[Stream index: 1]
[Conversation completeness: Complete, WITH_DATA (63)]
[TCP Segment Len: 216]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 3874701752
[Next Sequence Number: 217 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 417101217
0101 .... = Header Length: 20 bytes (5)
Flags: 0x018 (PSH, ACK)
000. .... = Reserved: Not set
...0 .... = Accurate ECN: Not set
.... 0... .... = Congestion Window Reduced: Not set
.... .0.. .... = ECN-Echo: Not set
.... ..0. .... = Urgent: Not set
....1 .... = Acknowledgment: Set
.... 1... = Push: Set
.... .0.. = Reset: Not set
....0. = Syn: Not set
....0 = Fin: Not set
[TCP Flags: ·····AP···]
Window: 1028
[Calculated window size: 263168]
[Window scaling factor: 256]
0000 d4 da 6d c0 cc 32 c4 14 00 55 fb 68 08 00 45 00 ··m··2··· ·U·h··E·
0010 01 00 93 fb 40 00 80 06 bf 3d c0 a8 64 08 33 7c ····@···· ·=··d·3|
0020 4e 92 c2 48 01 bb e6 f3 41 b8 18 dc 75 a1 50 18 N··H···· A···u·P·
0030 04 04 08 ff 00 00 16 03 03 00 d3 01 00 00 cf 03 ···••••• ••••••••
0040 03 67 f3 d8 2b 1d 7b 62 5d 4e f7 d8 1e 26 41 c3 ·g··+·{b]N···&A·
0050 7b 3b f4 47 8c fd 00 6b 56 4d 9a 4a da a2 ce 7e {;·G···k VM·J···~
0060 bf 00 00 26 c0 2c c0 2b c0 30 c0 2f c0 24 c0 23 ···&·,·+ ·0·/·$·#
0070 c0 28 c0 27 c0 0a c0 09 c0 14 c0 13 00 9d 00 9c ·(·'···· ········
0080 00 3d 00 3c 00 35 00 2f 00 0a 01 00 00 80 00 00 ·=·<·5·/ ········
0090 00 24 00 22 00 00 1f 73 65 74 74 69 6e 67 73 2d ·$·"···s ettings-
00a0 77 69 6e 2e 64 61 74 61 2e 6d 69 63 72 6f 73 6f win.data .microso
00b0 66 74 2e 63 6f 6d 00 05 00 05 01 00 00 00 00 00 ft.com·· ········
00c0 0a 00 08 00 06 00 1d 00 17 00 18 00 19 00 01 00 ········ ········
00d0 00 00 0d 00 1a 00 18 08 04 08 05 08 06 04 01 05 ········ ········
00e0 01 02 01 04 03 05 03 02 03 02 02 06 01 00 03 00 ········ ········
00f0 23 00 00 00 10 00 0e 00 0c 02 68 32 08 68 74 74 #·····h2·htt
0100 70 2f 31 2e 31 00 17 00 00 ff 01 00 01 00 p/1.1··· ····
Ideathon 2025.pcap
Packets: 1480 · Displayed: 129 (8.7%)
Profile: Default


Wed, 07 May, 23:03
Ideathon 2025.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.port==443 and ip.addr==51.124.78.146
No. Time Source Destination Protocol Length Info
39 0.960604 192.168.100.8 51.124.78.146 TCP 54 49737 → 443 [ACK] Seq=217 Ack=2801 Win=263168 Len=0
40 0.960623 51.124.78.146 192.168.100.8 TLSv1.2 1012 Server Hello, Certificate, Server Key Exchange, Server Hello Done
41 0.962853 192.168.100.8 51.124.78.146 TLSv1.2 212 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
42 0.963734 192.168.100.8 51.124.78.146 TCP 66 49739 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
48 0.983599 51.124.78.146 192.168.100.8 TCP 66 443 → 49739 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 WS=256 SACK_PERM
49 0.983696 192.168.100.8 51.124.78.146 TCP 54 49739 → 443 [ACK] Seq=1 Ack=1 Win=263168 Len=0
50 0.984838 51.124.78.146 192.168.100.8 TLSv1.2 105 Change Cipher Spec, Encrypted Handshake Message
51 0.984873 51.124.78.146 192.168.100.8 TLSv1.2 123 Application Data
52 0.984925 192.168.100.8 51.124.78.146 TCP 54 49737 → 443 [ACK] Seq=375 Ack=3879 Win=261888 Len=0
53 0.985072 192.168.100.8 51.124.78.146 TLSv1.2 270 Client Hello (SNI=settings-win.data.microsoft.com)
56 0.989543 51.124.78.146 192.168.100.8 TLSv1.2 141 Application Data
57 0.989640 192.168.100.8 51.124.78.146 TLSv1.2 897 Application Data
58 0.989721 192.168.100.8 51.124.78.146 TLSv1.2 92 Application Data
59 1.001079 192.168.100.8 51.124.78.146 TLSv1.2 141 Application Data
60 1.001156 192.168.100.8 51.124.78.146 TLSv1.2 1219 Application Data
61 1.001198 192.168.100.8 51.124.78.146 TLSv1.2 92 Application Data
62 1.005771 51.124.78.146 192.168.100.8 TCP 1454 443 → 49739 [ACK] Seq=1 Ack=217 Win=4194048 Len=1400 [TCP segment of a reassembled PDU]
63 1.005819 51.124.78.146 192.168.100.8 TCP 1454 443 → 49739 [ACK] Seq=1401 Ack=217 Win=4194048 Len=1400 [TCP segment of a reassembled PDU]
64 1.005855 51.124.78.146 192.168.100.8 TLSv1.2 1012 Server Hello, Certificate, Server Key Exchange, Server Hello Done
65 1.005870 192.168.100.8 51.124.78.146 TCP 54 49739 → 443 [ACK] Seq=217 Ack=2801 Win=263168 Len=0
66 1.009087 192.168.100.8 51.124.78.146 TLSv1.2 212 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
67 1.009971 51.124.78.146 192.168.100.8 TLSv1.2 92 Application Data
68 1.009386 51.124.78.146 192.168.100.8 TCP 54 443 → 49736 [ACK] Seq=3917 Ack=1343 Win=4193024 Len=0
69 1.022414 51.124.78.146 192.168.100.8 TLSv1.2 92 Application Data
70 1.022435 51.124.78.146 192.168.100.8 TCP 54 443 → 49737 [ACK] Seq=3917 Ack=1627 Win=4194304 Len=0
71 1.022574 51.124.78.146 192.168.100.8 TCP 54 443 → 49737 [ACK] Seq=3917 Ack=1665 Win=4194304 Len=0
72 1.028493 51.124.78.146 192.168.100.8 TLSv1.2 105 Change Cipher Spec, Encrypted Handshake Message
73 1.028839 51.124.78.146 192.168.100.8 TLSv1.2 123 Application Data
74 1.028919 192.168.100.8 51.124.78.146 TCP 54 49739 → 443 [ACK] Seq=375 Ack=3879 Win=261888 Len=0
76 1.036281 192.168.100.8 51.124.78.146 TLSv1.2 141 Application Data
Destination Port: 443
[Stream index: 1]
[Conversation completeness: Complete, WITH_DATA (63)]
[TCP Segment Len: 843]
Sequence Number: 462 (relative sequence number)
Sequence Number (raw): 3874702213
[Next Sequence Number: 1305 (relative sequence number)]
Acknowledgment Number: 3879 (relative ack number)
Acknowledgment number (raw): 417105095
0101 .... = Header Length: 20 bytes (5)
Flags: 0x018 (PSH, ACK)
000. .... = Reserved: Not set
...0 .... = Accurate ECN: Not set
.... 0... .... = Congestion Window Reduced: Not set
.... .0.. .... = ECN-Echo: Not set
.... ..0. .... = Urgent: Not set
....1 .... = Acknowledgment: Set
.... 1... = Push: Set
.... .0.. = Reset: Not set
....0. = Syn: Not set
....0 = Fin: Not set
[TCP Flags: ·····AP···]
Window: 1027
[Calculated window size: 262912]
[Window size scaling factor: 256]
0000 d4 da 6d c0 cc 32 c4 14 00 55 fb 68 08 00 45 00 ··m··2··· ·U·h··E·
0010 03 73 94 09 40 00 80 06 bc c9 a8 64 08 33 7c ·s··@···· ···d·3|
0020 4e 92 c2 48 01 bb e6 f3 43 85 18 dc 84 c7 50 18 N··H···· C·····P·
0030 04 03 b3 78 00 00 17 03 03 03 46 00 00 00 00 00 ···x···· ··F·····
0040 00 00 02 18 13 18 04 0f 67 84 14 50 9d 0c ff e0 ········ g··P····
0050 e5 ae 2d 32 55 cd de fc 73 3a 8b 32 f7 b0 a7 bf ··-2U··· s:·2····
0060 19 a6 6e ff 34 b5 f9 87 8b 0c 70 b2 0d c6 ad 70 ··n·4··· ··p····p
0070 13 ad 1c 93 5d e6 b0 cf 12 59 d1 20 91 54 d5 f2 ····]··· ·Y· ·T··
0080 3c be e2 8a 40 41 bc 00 1a 1e d4 ce d5 0a 75 16 <···@A·· ·····u·
0090 a6 34 d9 87 72 85 0f cc 62 9a e6 08 18 1b 25 9d ·4··r··· b·····%·
00a0 f1 91 56 7d 81 ff 8b 77 b8 6a c5 d6 09 a8 dd 5d ··V}···w ·j·····]
00b0 2f d0 58 f2 f0 7a 9d 04 ca a4 ea 29 2a d8 9a f0 /·X··z·· ···)*···
00c0 42 13 b3 d1 7a 60 d9 b8 62 23 98 41 1e 49 99 23 B···z`·· b#·A·I·#
00d0 a8 31 a0 0f b1 6f ac b4 07 11 3e 44 14 84 cd 7c ·1···o·· ··>D···|
00e0 03 4f 78 fe 92 f5 f5 11 4a f0 80 1e da 08 ba 48 ·Ox····· J·····H
00f0 13 aa 2b 6a b3 94 c9 d2 85 07 a7 6b 10 69 80 ca ··+j···· ···k·i··
0100 74 45 b3 a2 78 52 2d e8 ab 4d e1 78 01 3d 9e f5 tE··xR-· ·M·x·=··
0110 9b a5 07 0e 6a 13 40 a3 e1 dd cf a5 36 65 f4 b7 ····j·@· ····6e··
0120 3f 74 0c ce 67 0f 78 77 6a 64 37 15 e1 26 28 2f ?t··g·xw jd7··&(/
0130 82 5d 71 0c ed 93 49 78 49 c3 6a 7a 07 d7 70 8a ·]q···Ix I·jz··p·
0140 3a fd 24 5a 60 04 15 d8 0f ee 1a db e9 52 f6 39 :·$Z`··· ·····R·9
0150 d3 77 af ca 0c 51 56 30 bb cc 9a b9 fc 0c 08 5e ·w···QV0 ·····^
0160 99 b3 b6 02 51 f5 02 aa 2a 89 e4 36 c5 fb c1 bc ····Q··· *··6····
0170 2a f0 f1 f1 34 49 86 35 72 bd 6b 99 16 48 9f 30 *···4I·5 r·k··H·0
0180 9b f6 63 57 81 71 49 7c 85 44 fe bf 6e 0f 45 ea ··cW·qI| ·D··n·E·
Ideathon 2025.pcap
Packets: 1480 · Displayed: 129 (8.7%)
Profile: Default



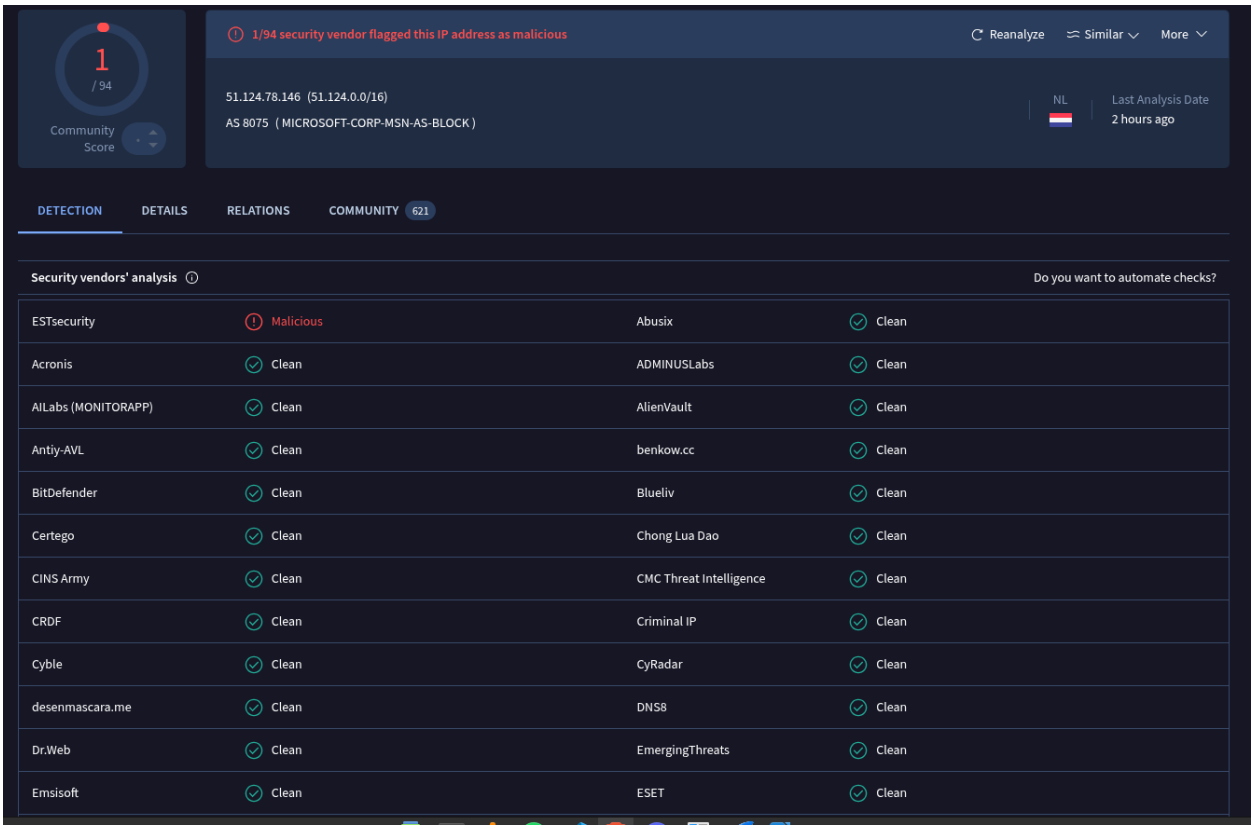
B. Filters Used

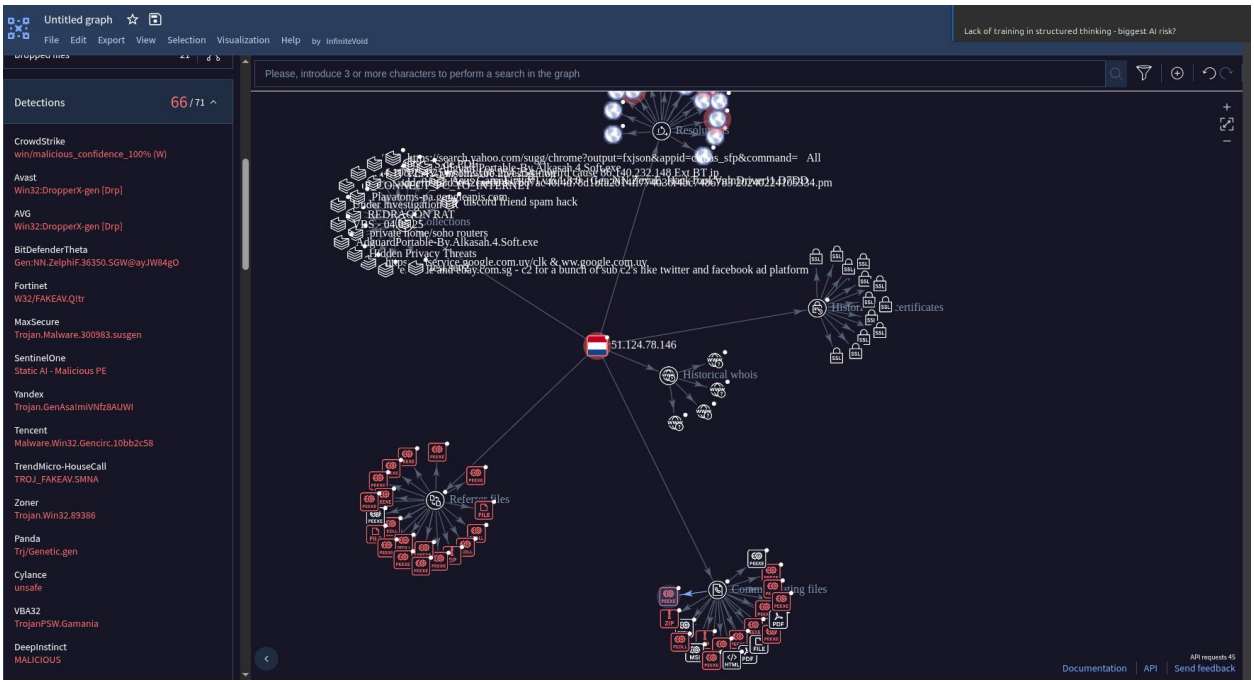
- ip.addr == 51.124.78.146

- ip.addr == 51.124.78.146 and tcp.port==443
  - tcp
  - tls

- tcp.port == 443

B. Captured Screenshots


1
/ 94
Community Score
1/94 security vendor flagged this IP address as malicious
Reanalyze
Similar
More
51.124.78.146 (51.124.0.0/16)
AS 8075 (MICROSOFT-CORP-MSN-AS-BLOCK)
NL
Last Analysis Date
2 hours ago
DETECTION
DETAILS
RELATIONS
COMMUNITY 621
Security vendors' analysis
Do you want to automate checks?
ESTsecurity Malicious
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
EmergingThreats Clean
Emsisoft Clean
ESET Clean


Untitled graph
File Edit Export View Selection Visualization Help by InfiniteVoid
Lack of training in structured thinking - biggest AI risk?
Please, introduce 3 or more characters to perform a search in the graph
Detections 66 / 71
CrowdStrike win/malicious_confidence_100% (W)
Avast Win32:DropperX-gen [Drp]
AVG Win32:DropperX-gen [Drp]
BitDefenderTheta Gen:NN.ZelphiF.36350.SGW@ayJW84gO
Fortinet W32/FAKEAV.QItr
MaxSecure Trojan.Malware.300983.susgen
SentinelOne Static AI - Malicious PE
Yandex Trojan.GenAsa!miVNfz8AUWI
Tencent Malware.Win32.Gencirc.10bb2c58
TrendMicro-HouseCall TROJ_FAKEAV.SMNA
Zoner Trojan.Win32.89386
Panda Trj/Genetic.gen
Cylance unsafe
VBA32 TrojanPSW.Gamania
DeepInstinct MALICIOUS
Resolu
discord friend spam hack
private home/soho routers
Hidden Privacy Threats
51.124.78.146
Historical whois
Hist
certificates
Referre files
Comm
ating files
Documentation
API
Send feedback

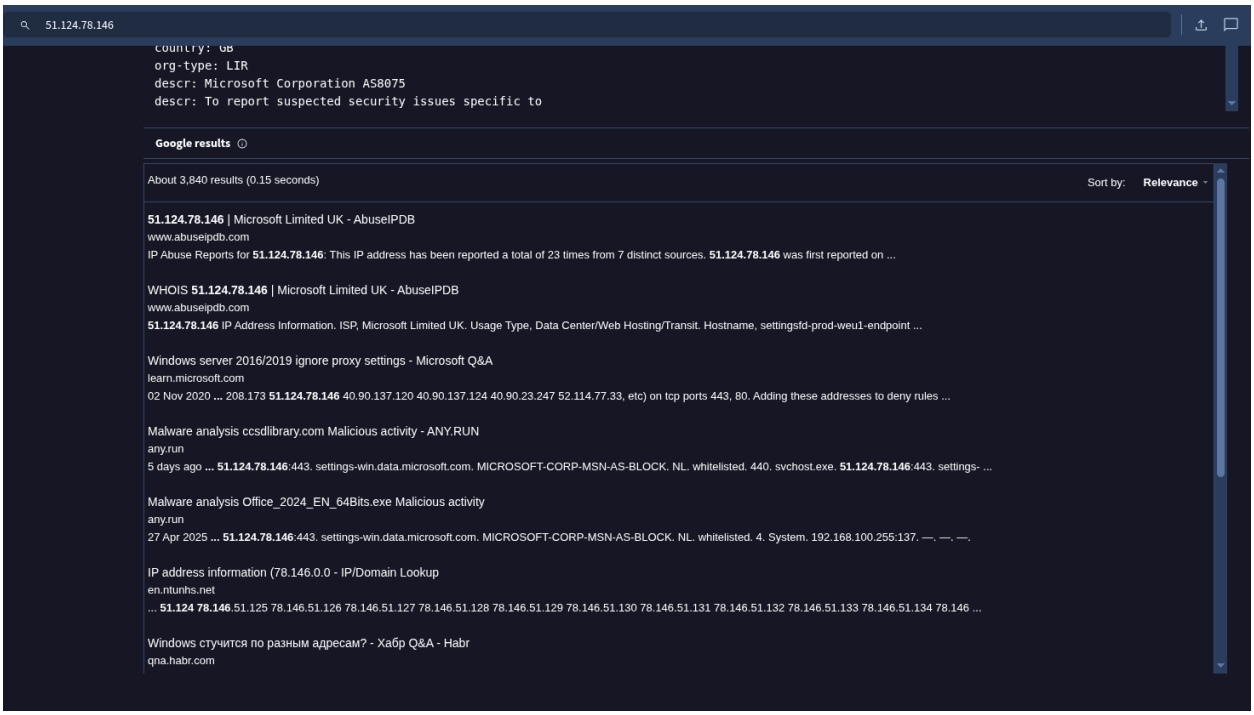


Figure 1A-C – Virus Total screenshots.

ANY.RUN
INTERACTIVE MALWARE ANALYSIS

General | Behavior | MalConf | Static information | Video | Screenshots | System events | Network

General Info

Add for printing

URL:	ccsdlibrary.com
Full analysis:	https://app.any.run/tasks/70ead222-c79d-42d8-b1a1-8c520d8412c0
Verdict:	Malicious activity
Analysis date:	May 02, 2025 at 23:14:41
OS:	Windows 10 Professional (build: 19044, 64 bit)
Tags:	phishing storm1747
Indicators:	
MD5:	B4B26F8E68FF2976DF8C09B50D111EB3
SHA1:	16F504C3C495B4D9E5F98DB902D98504D260AD18
SHA256:	0673033724C093C00E786B9D9217B121640071D8CC4EC95A5A3DA535734CAF3A
SSDEEP:	3:5HU1:5q

ANY.RUN is an interactive service which provides full access to the guest system. Information in this report could be distorted by user actions and is provided for user acknowledgement as it is. ANY.RUN does not guarantee maliciousness or safety of the content.

Software environment set and analysis options

Behavior activities

Add for printing

MALICIOUS	SUSPICIOUS	INFO
PHISHING has been detected (SURICATA) • msedge.exe (PID: 1396)	No suspicious indicators.	No info indicators.

Find more information about signature artifacts and mapping to MITRE ATT&CK™ MATRIX at the full report

Files activity

Add for printing

Executable files	Suspicious files	Text files	Unknown types
0	12	0	0

Dropped files

PID	Process	Filename	Type
1396	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Network\Network Persistent State~RF138f04.TMP **MD5:** 50823AF426E5FA5F5641C1004F470D3E **SHA256:** 599163927CC9E5640C868AEDD3B0B6EC79E6513970504124E417922D8AAAB7C3	binary
1396	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Network\6602b46f-e536-482f-981b-f69e79059359.tmp **MD5:** C81B26B263724393070728337A7E6624 **SHA256:** 8748F2310C2A8DF6E377413370792376F1DAE0DC02501C49EDE80F817EEBCDA8	binary
1396	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_0000ba **MD5:** A620A68D8F00E5C4F2803E686D6F7514 **SHA256:** 44A8F499F80F75FBD07885DBB5BDAF97BD9BE7B0B8DBC0C769960F7F6EF5E22D	binary
1396	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Network\a5788b42-4130-41c7-a877-a2a426bdaf8c.tmp **MD5:** 3140CB797498137E330D3CAE1AD5970A **SHA256:** B4C87E65FB18FF2E4028E934653089C7DE70D854E7D861D9A1063189C5212119	binary
1396	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Network\Network Persistent State **MD5:** 3140CB797498137E330D3CAE1AD5970A **SHA256:** B4C87E65FB18FF2E4028E934653089C7DE70D854E7D861D9A1063189C5212119	binary
1396	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_0000bb **MD5:** D17B5A55EC9D8608C1D2B531CCB6DE88 **SHA256:** DC2A3600C7CDFAEA40DB03757D6915D67518215DB51397C8A5BB3F132AE89A49	binary
1396	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Network\TransportSecurity **MD5:** C81B26B263724393070728337A7E6624 **SHA256:** 8748F2310C2A8DF6E377413370792376F1DAE0DC02501C49EDE80F817EEBCDA8	binary
1396	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Network\TransportSecurity~RF139b88.TMP **MD5:** 15D26FA4E16467BE658F42074AC0DBAA **SHA256:** D287407BD901A32E3F38F4392984507184D596C3694FAA69DD0B2E68F9F3A8FE	binary
1396	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_0000bc **MD5:** 10B84D6DDEFB33D0D3F0615CA3E91C5A **SHA256:** C69A6E50A300D39721F9AE8FC5B40600DD90093F65E3A4650C9540C58C071144	compressed
1396	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Network\TransportSecurity~RF1496df.TMP **MD5:** C81B26B263724393070728337A7E6624 **SHA256:** 8748F2310C2A8DF6E377413370792376F1DAE0DC02501C49EDE80F817EEBCDA8	binary
1396	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Network\40c41af4-436e-4b71-a113-b2fe0668baca.tmp **MD5:** FD930EA07B2198ED04C66708BB0DD8BB **SHA256:** F4A08DB9E835A9B3B412E8BFECBA88212742F38DC7DC5E1FABBC7BA1280CCA21	binary

Network activity

Add for printing

HTTP(S) requests	TCP/UDP connections	DNS requests	Threats
54	64	45	2

HTTP requests

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
–	–	GET	200	23.35.229.160:80	http://www.microsoft.com/pkiops/crl/MicSecSerCA2011_2011-10-18.crl	unknown	–	–	whitelisted
–	–	GET	200	23.35.229.160:80	http://www.microsoft.com/pkiops/crl/MicSecSerCA2011_2011-10-18.crl	unknown	–	–	whitelisted
–	–	GET	302	192.168.1.2:443	https://ccsdlibrary.com/	unknown	–	–	–
2564	RUXIMICS.exe	GET	200	23.48.23.158:80	http://crl.microsoft.com/pki/crl/products/MicRooCerAut2011_2011_03_22.crl	unknown	–	–	whitelisted
3080	MoUsoCoreWorker.exe	GET	200	23.48.23.158:80	http://crl.microsoft.com/pki/crl/products/MicRooCerAut2011_2011_03_22.crl	unknown	–	–	whitelisted
–	–	POST	200	40.126.32.134:443	https://login.live.com/RST2.srf	unknown	xml	1.24 Kb	whitelisted
440	svchost.exe	GET	200	23.48.23.158:80	http://crl.microsoft.com/pki/crl/products/MicRooCerAut2011_2011_03_22.crl	unknown	–	–	whitelisted
–	–	POST	403	23.35.229.160:443	https://go.microsoft.com/fwlink/?LinkID=2257403&clcid=0x409	unknown	html	384 b	whitelisted
–	–	POST	200	20.190.159.129:443	https://login.live.com/ppsecure/deviceaddcredential.srf	unknown	text	16.7 Kb	whitelisted
–	–	GET	404	88.198.109.229:443	https://copaxso.xyz/favicon.ico	unknown	html	555 b	–
–	–	POST	200	40.126.31.130:443	https://login.live.com/RST2.srf	unknown	xml	10.3 Kb	whitelisted
–	–	GET	304	52.149.20.212:443	https://slscr.update.microsoft.com/SLS/%7B522D76A4-93E1-47F8-B8CE-07C937AD1A1E%7D/x64/10.0.19045.4046/0?CH=686&L=en-US&P=&PT=0x30&WUA=10.0.19041.3996&MK=DELL&MD=DELL	unknown	–	–	–
–	–	POST	403	23.35.229.160:443	https://go.microsoft.com/fwlink/?LinkID=2257403&clcid=0x409	unknown	html	384 b	whitelisted
–	–	GET	200	23.35.229.160:80	http://www.microsoft.com/pkiops/crl/Microsoft%20Update%20Signing%20CA%202.1.crl	unknown	–	–	whitelisted

Connections

PID	Process	IP	Domain	ASN	CN	Reputation
2564	RUXIMICS.exe	51.124.78.146:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	whitelisted
–	–	239.255.255.250:1900	–	–	–	whitelisted
3080	MoUsoCoreWorker.exe	51.124.78.146:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	whitelisted
440	svchost.exe	51.124.78.146:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	whitelisted
1396	msedge.exe	92.123.104.34:443	www.bing.com	Akamai International B.V.	DE	whitelisted
1396	msedge.exe	103.224.212.213:443	ccsdlibrary.com	Trellian Pty. Limited	AU	unknown
6124	svchost.exe	40.126.32.74:443	login.live.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	whitelisted
1396	msedge.exe	103.224.182.206:443	ofijii.com	Trellian Pty. Limited	AU	unknown
2564	RUXIMICS.exe	23.48.23.158:80	crl.microsoft.com	Akamai International B.V.	DE	whitelisted
3080	MoUsoCoreWorker.exe	23.48.23.158:80	crl.microsoft.com	Akamai International B.V.	DE	whitelisted
440	svchost.exe	23.48.23.158:80	crl.microsoft.com	Akamai International B.V.	DE	whitelisted
–	–	23.35.229.160:80	www.microsoft.com	AKAMAI-AS	DE	whitelisted
–	–	103.224.182.206:443	ofijii.com	Trellian Pty. Limited	AU	unknown
–	–	69.192.162.125:443	go.microsoft.com	AKAMAI-AS	DE	whitelisted
–	–	40.127.240.158:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	whitelisted
–	–	88.198.109.229:443	copaxso.xyz	Hetzner Online GmbH	DE	unknown
–	–	13.107.246.45:443	xpaywalletcdn.azureedge.net	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
–	–	40.126.32.74:443	login.live.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	whitelisted
–	–	224.0.0.251:5353	–	–	–	unknown

–	–	GET	200	92.123.104.33:443	https://www.bing.com/bloomfilterfiles/ExpandedDomainsFilterGlobal.json	unknown	binary	654 Kb	whitelisted
–	–	GET	200	23.48.23.192:80	http://crl.microsoft.com/pki/crl/products/MicRooCerAut_2010-06-23.crl	unknown	–	–	whitelisted
–	–	GET	200	23.35.229.160:80	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Update%20Signing%20CA%202.1.crl	unknown	–	–	whitelisted
–	–	GET	200	88.198.109.229:443	https://copaxso.xyz/landers/9aa988e9-8cdc-4a3d-b4a8-d27ee144b14a/product.png	unknown	image	13.8 Kb	–
–	–	GET	200	13.107.246.45:443	https://edgeassetservice.azureedge.net/assets/edge_hub_apps_manifest_gz/4.10.36/asset?assetgroup=Shoreline	unknown	binary	1.78 Mb	whitelisted
–	–	GET	200	23.35.229.160:80	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Product%20Root%20Certificate%20Authority%202018.crl	unknown	–	–	whitelisted
–	–	GET	200	20.242.39.171:443	https://fe3cr.delivery.mp.microsoft.com/clientwebservice/ping	unknown	–	–	–
–	–	GET	200	23.48.23.192:80	http://crl.microsoft.com/pki/crl/products/MicTimStaPCA_2010-07-01.crl	unknown	–	–	whitelisted
–	–	GET	200	52.149.20.212:443	https://slscr.update.microsoft.com/SLS/%7B522D76A4-93E1-47F8-B8CE-07C937AD1A1E%7D/x64/10.0.19045.4046/0?CH=686&L=en-US&P=&PT=0x30&WUA=10.0.19041.3996&MK=DELL&MD=DELL	unknown	–	–	–
–	–	GET	304	52.149.20.212:443	https://slscr.update.microsoft.com/SLS/%7BE7A50285-D08D-499D-9FF8-180FDC2332BC%7D/x64/10.0.19045.4046/0?CH=686&L=en-US&P=&PT=0x30&WUA=10.0.19041.3996&MK=DELL&MD=DELL	unknown	–	–	–
–	–	GET	200	52.149.20.212:443	https://slscr.update.microsoft.com/SLS/%7BE7A50285-D08D-499D-9FF8-180FDC2332BC%7D/x64/10.0.19045.4046/0?CH=686&L=en-US&P=&PT=0x30&WUA=10.0.19041.3996&MK=DELL&MD=DELL	unknown	–	–	–
–	–	GET	200	23.35.229.160:80	http://www.microsoft.com/pkiops/crl/MicSecSerCA2011_2011-10-18.crl	unknown	–	–	whitelisted
–	–	GET	304	52.149.20.212:443	https://slscr.update.microsoft.com/SLS/%7B522D76A4-93E1-47F8-B8CE-07C937AD1A1E%7D/x64/10.0.19045.4046/0?CH=686&L=en-US&P=&PT=0x30&WUA=10.0.19041.3996&MK=DELL&MD=DELL	unknown	–	–	–
–	–	GET	200	52.149.20.212:443	https://slscr.update.microsoft.com/sls/ping	unknown	–	–	–
–	–	POST	403	23.35.229.160:443	https://go.microsoft.com/fwlink/?LinkID=2257403&clcid=0x409	unknown	html	384 b	whitelisted

–	–	POST	200	20.190.159.68:443	https://login.live.com/RST2.srf	unknown	xml	11.1 Kb	whitelisted
–	–	GET	200	92.123.104.26:443	https://edgeservices.bing.com/edgesvc/userstatus	unknown	binary	381 b	whitelisted
–	–	POST	400	20.190.159.68:443	https://login.live.com/ppsecure/deviceaddcredential.srf	unknown	text	203 b	whitelisted
–	–	POST	500	40.91.76.224:443	https://activation-v2.sls.microsoft.com/SLActivateProduct/SLActivateProduct.asmx?configextension=Retail	unknown	xml	512 b	whitelisted
–	–	GET	401	13.107.6.158:443	https://business.bing.com/work/api/v2/tenant/my/settingswithflights?&clienttype=edge-omnibox	unknown	binary	585 b	whitelisted
–	–	GET	200	88.198.109.229:443	https://copaxso.xyz/landers/9aa988e9-8cdc-4a3d-b4a8-d27ee144b14a/product.png	unknown	image	13.8 Kb	–
–	–	GET	200	52.149.20.212:443	https://slscr.update.microsoft.com/SLS/%7B522D76A4-93E1-47F8-B8CE-07C937AD1A1E%7D/x64/10.0.19045.4046/0?CH=686&L=en-US&P=&PT=0x30&WUA=10.0.19041.3996&MK=DELL&MD=DELL	unknown	–	–	–
–	–	POST	200	40.126.31.129:443	https://login.live.com/RST2.srf	unknown	xml	10.3 Kb	whitelisted
–	–	GET	200	13.107.246.45:443	https://xpaywalletcdn.azureedge.net/mswallet/ExpressCheckout/v2/GetEligibleSites?version=0&type=commonConfig&IsStable=false	unknown	binary	481 b	whitelisted
–	–	POST	403	23.35.229.160:443	https://go.microsoft.com/fwlink/?LinkID=2257403&clcid=0x409	unknown	html	384 b	whitelisted
–	–	POST	200	23.50.131.74:443	https://bzib.nelreports.net/api/report?cat=bingbusiness	unknown	–	–	whitelisted
–	–	GET	200	150.171.28.11:443	https://edge.microsoft.com/entityextractiontemplates/api/v1/assets/find-assets?name=edge_hub_apps_manifest_gz&version=4.10.*&channel=stable&key=d414dd4f9db345fa8003e32adc81b362	unknown	text	266 b	whitelisted
–	–	POST	200	23.50.131.78:443	https://bzib.nelreports.net/api/report?cat=bingbusiness	unknown	–	–	whitelisted
–	–	POST	403	23.35.229.160:443	https://go.microsoft.com/fwlink/?LinkID=2257403&clcid=0x409	unknown	html	384 b	whitelisted
–	–	POST	500	40.91.76.224:443	https://activation-v2.sls.microsoft.com/SLActivateProduct/SLActivateProduct.asmx?configextension=Retail	unknown	xml	512 b	whitelisted
–	–	GET	200	13.107.42.16:443	https://config.edge.skype.com/config/v1/Edge/122.0.2365.59?clientId=4286224394064939872&agents=Edge%2CEdgeConfig%2CEdgeServices%2CEdgeFirstRun%2CEdgeFirstRunConfig&osname=win&client=edge&channel=stable&scpfre=0&osarch=x86_64&osver=10.0.19045&wu=1&devicefamily=desktop&uma=0&sessionid=27&mngd=0&installdate=1662378849&edu=0&bphint=0&soobedate=1504771245&fg=1	unknown	binary	9.06 Kb	whitelisted

Figure 2A-F – AnyRun scans of IP linked from VirusTotal.

May 26, 2022	http://51.124.78.146:443/	51.124.78.146	Connection Er...	
Jul 27, 2021	https://51.124.78.146/settings/v2.0/wsd/muse?processorclockspeed=2712&flightids=rs:97a7,fx:11a8c293,fx:11a8c2fe,fx:11d898d7...	51.124.78.146	200	51.124.78.146
Jun 24, 2021	https://51.124.78.146/settings/v2.0/wsd/muse?processorclockspeed=3192&flightids=fx:119003Oe,fx:11e11e7a,fx:11e3e090,fx:11e5...	51.124.78.146	200	51.124.78.146
May 17, 2021	https://51.124.78.146/settings/v2.0/wsd/	51.124.78.146	404	51.124.78.146
May 17, 2021	https://51.124.78.146/settings/v2.0/wsd/muse?processorclockspeed=3000&flightids=fx:11a8c293,fx:11a8c2fe,fx:11d898d7,fx:11d...	51.124.78.146	200	51.124.78.146
Mar 26, 2021	https://51.124.78.146/settings/v2.0/wex/	51.124.78.146	404	51.124.78.146
Mar 26, 2021	https://51.124.78.146/settings/v2.0/wex/msphotos?conceptmodelver=12&deviceId=re7e3569a-934f-4094-96c5-8458c356...	51.124.78.146	200	51.124.78.146
Jan 6, 2021	http://51.124.78.146/	51.124.78.146	Connection Er...	
Jul 13, 2020	https://51.124.78.146	51.124.78.146	404	51.124.78.146
Mar 9, 2020	http://51.124.78.146	51.124.78.146	Connection Er...	

SHOWING 1 TO 12 OF 12 ENTRIES

Associated Files

Show 10 entries

DATE	HASH	AVAST	AVG	CLAMAV	MSDEFENDER
Aug 9, 2022	46a0d91ccf005ee0cad78ee01ce69a136c14f8c8d9b9f4e2ce0893e2f3c56815	Win32:PWSX-gen\ [Trj]		Win.Malware.Score-7096574-0	Trojan:Win32/Lunam
Aug 2, 2022	68a5165cbe365fe78ca251d1e030397090c5ed0948b4332ad9fc92c4d3cde268	Win32:PWSX-gen\ [Trj]		Win.Malware.Score-7096574-0	Trojan:Win32/Lunam
Aug 2, 2022	6a60de93995597427891a18ba267f396b100b4f20269d3ef20f4fef0c8e94f5d	Win32:PWSX-gen\ [Trj]		Win.Malware.Score-7096574-0	Trojan:Win32/Lunam
Oct 27, 2021	279d3cb2b8d39f664c211675b1e0666de92e5cb27f227f6cba5f28440fe0ed03	Win32:Mytob-PY\ [Wrm]			Backdoor:Win32/Mydoom.gen
Oct 27, 2021	0f93a008000b6e8e1241e800f9a1118232b0eeb2d93134e55bb44cacec13628f	Win32:Mytob-PY\ [Wrm]			Backdoor:Win32/Mydoom.gen
Oct 23, 2021	13372c8ba29125f51a7e76de51ba4851928eac62f3730a3717f42a36452f930a				
Apr 14, 2020	ad4e71d2db13a478148e12fff036e8f059c33cbf1ebc05ed911c34248e44ad7c	Win32:Trojan-gen			TrojanSpy:Win32/Ursnif.ARVIMTB
Mar 10, 2020	6b89c9f756e6155625d18913c0ae4f1885ca55723c66181a8fc5a7d268b1746b	Win32:BankerX-gen\ [Trj]			

SHOWING 1 TO 8 OF 8 ENTRIES

Associated Urls

Show 25 entries

Search:

DATE CHECKED	URL	HOSTNAME	SERVER RESPONSE	IP ADDRESS	GOOGLE SAFE BROWSING	ANTIVIRUS RESULTS
Apr 3, 2024	https://51.124.78.146/	51.124.78.146	404	51.124.78.146		
Oct 31, 2023	https://settings-prod-weu-1.westeurope.cloudapp.azure.com	settings-prod-weu-1.westeurope.cloudapp.azure.c...	404	51.124.78.146		
May 26, 2022	http://51.124.78.146:443/	51.124.78.146	Connection Er...			
Jul 27, 2021	https://51.124.78.146/settings/v2.0/wsd/muse?processorclockspeed=2712&flightids=rs:97a7,fx:11a8c293,fx:11a8c2fe,fx:11d898d7,...	51.124.78.146	200	51.124.78.146		
Jun 24, 2021	https://51.124.78.146/settings/v2.0/wsd/muse?processorclockspeed=3192&flightids=fx:119003Oe,fx:11e11e7a,fx:11e3e090,fx:11e5...	51.124.78.146	200	51.124.78.146		
May 17, 2021	https://51.124.78.146/settings/v2.0/wsd/	51.124.78.146	404	51.124.78.146		
May 17, 2021	https://51.124.78.146/settings/v2.0/wsd/muse?processorclockspeed=3000&flightids=fx:11a8c293,fx:11a8c2fe,fx:11d898d7,fx:11d...	51.124.78.146	200	51.124.78.146		
Mar 26, 2021	https://51.124.78.146/settings/v2.0/wex/	51.124.78.146	404	51.124.78.146		
Mar 26, 2021	https://51.124.78.146/settings/v2.0/wex/msphotos?conceptmodelver=12&deviceId=re7e3569a-934f-4094-96c5-8458c356...	51.124.78.146	200	51.124.78.146		
Jan 6, 2021	http://51.124.78.146/	51.124.78.146	Connection Er...			
Jul 13, 2020	https://51.124.78.146	51.124.78.146	404	51.124.78.146		
Mar 9, 2020	http://51.124.78.146	51.124.78.146	Connection Er...			

SHOWING 1 TO 12 OF 12 ENTRIES

Associated Files

Show 10 entries

DATE	HASH	AVAST	AVG	CLAMAV	MSDEFENDER
Aug 9, 2022	46a0d91ccf005ee0cad78ee01ce69a136c14f8c8d9b9f4e2ce0893e2f3c56815	Win32:PWSX-gen\ [Trj]		Win.Malware.Score-7096574-0	Trojan:Win32/Lunam
Aug 2, 2022	68a5165cbe365fe78ca251d1e030397090c5ed0948b4332ad9fc92c4d3cde268	Win32:PWSX-gen\ [Trj]		Win.Malware.Score-7096574-0	Trojan:Win32/Lunam
Aug 2, 2022	6a60de93995597427891a18ba267f396b100b4f20269d3ef20f4fef0c8e94f5d	Win32:PWSX-gen\ [Trj]		Win.Malware.Score-7096574-0	Trojan:Win32/Lunam

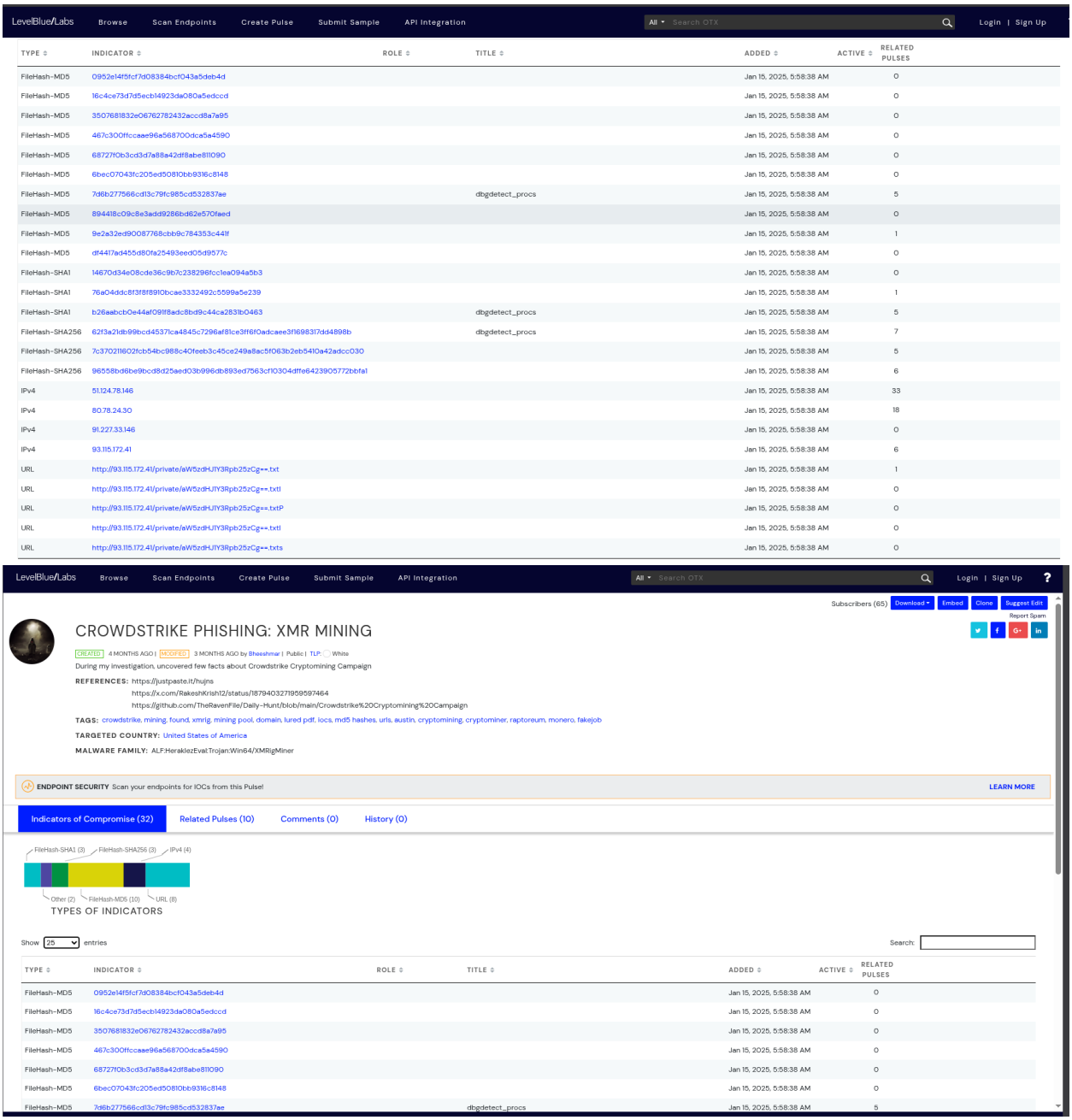
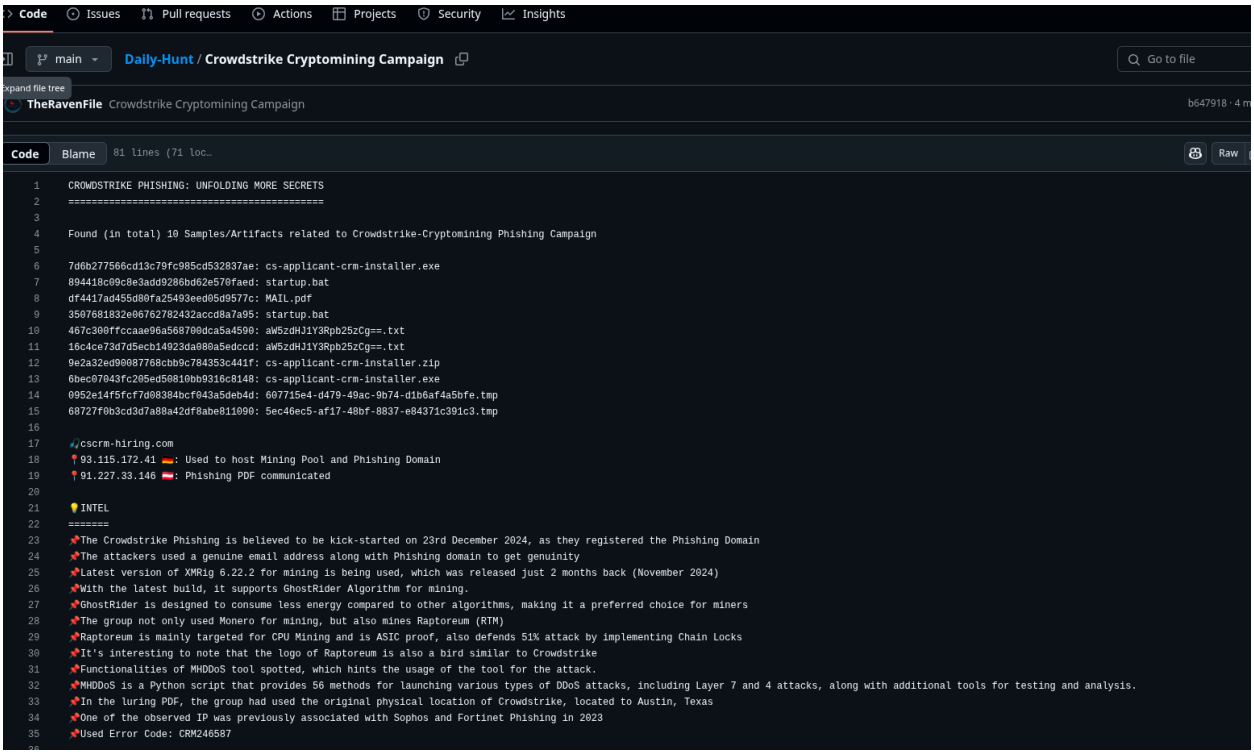


Figure 3A-D – OTX AlienVault scan of the IP displaying associated URLs, files and campaigns.


Code
Issues
Pull requests
Actions
Projects
Security
Insights
main
Daily-Hunt / Crowdstrike Cryptomining Campaign
Go to file
Expand file tree
TheRavenFile Crowdstrike Cryptomining Campaign
b647918 · 4 m
Code
Blame
81 lines (71 loc…
Raw
CROWDSTRIKE PHISHING: UNFOLDING MORE SECRETS
Found (in total) 10 Samples/Artifacts related to Crowdstrike-Cryptomining Phishing Campaign
7d6b277566cd13c79fc985cd532837ae: cs-applicant-crm-installer.exe
894418c09c8e3add9286bd62e570faed: startup.bat
df4417ad455d00fa25493eed05d9577c: MAIL.pdf
3507681832e06762782432accd8a7a95: startup.bat
467c300ffccaae96a568700dca5a4590: aW5zdHJ1Y3Rpb25zCg==.txt
16c4ce73d7d5ecb14923da080a5edccd: aW5zdHJ1Y3Rpb25zCg==.txt
9e2a32ed90087768cbb9c784353c441f: cs-applicant-crm-installer.zip
6bec07043fc205ed50810bb9316c8148: cs-applicant-crm-installer.exe
0952e14f5fcf7d08384bcf043a5deb4d: 607715e4-d479-49ac-9b74-d1b6af4a5bfe.tmp
68727f0b3cd3d7a88a42df8abe811090: 5ec46ec5-af17-48bf-8837-e84371c391c3.tmp
cscrm-hiring.com
93.115.172.41 : Used to host Mining Pool and Phishing Domain
91.227.33.146 : Phishing PDF communicated
INTEL
The Crowdstrike Phishing is believed to be kick-started on 23rd December 2024, as they registered the Phishing Domain
The attackers used a genuine email address along with Phishing domain to get genuinity
Latest version of XMRig 6.22.2 for mining is being used, which was released just 2 months back (November 2024)
With the latest build, it supports GhostRider Algorithm for mining.
GhostRider is designed to consume less energy compared to other algorithms, making it a preferred choice for miners
The group not only used Monero for mining, but also mines Raptoreum (RTM)
Raptoreum is mainly targeted for CPU Mining and is ASIC proof, also defends 51% attack by implementing Chain Locks
It's interesting to note that the logo of Raptoreum is also a bird similar to Crowdstrike
Functionalities of MHDDoS tool spotted, which hints the usage of the tool for the attack.
MHDDoS is a Python script that provides 56 methods for launching various types of DDoS attacks, including Layer 7 and 4 attacks, along with additional tools for testing and analysis.
In the luring PDF, the group had used the original physical location of Crowdstrike, located to Austin, Texas
One of the observed IP was previously associated with Sophos and Fortinet Phishing in 2023
Used Error Code: CRM246587

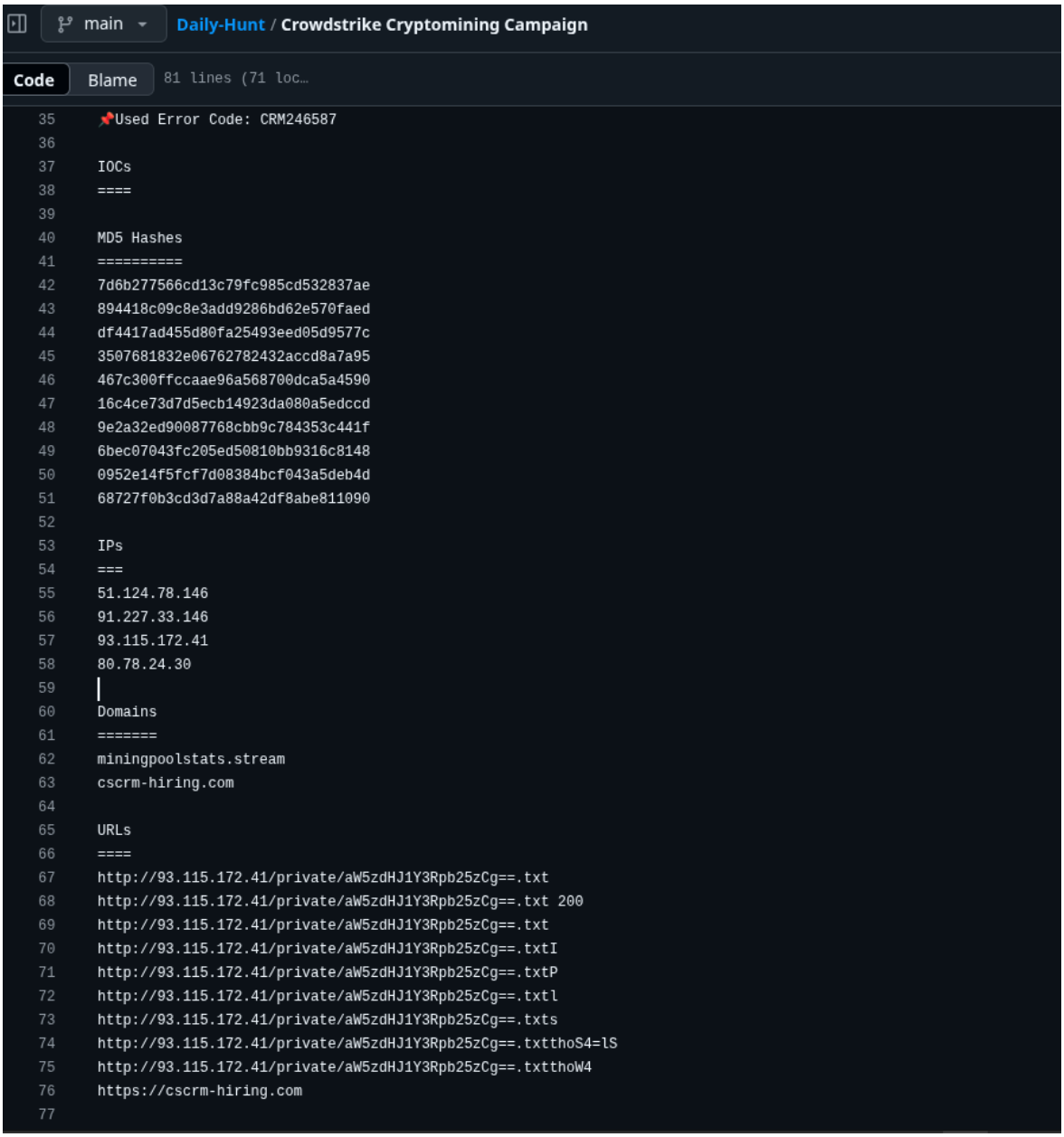
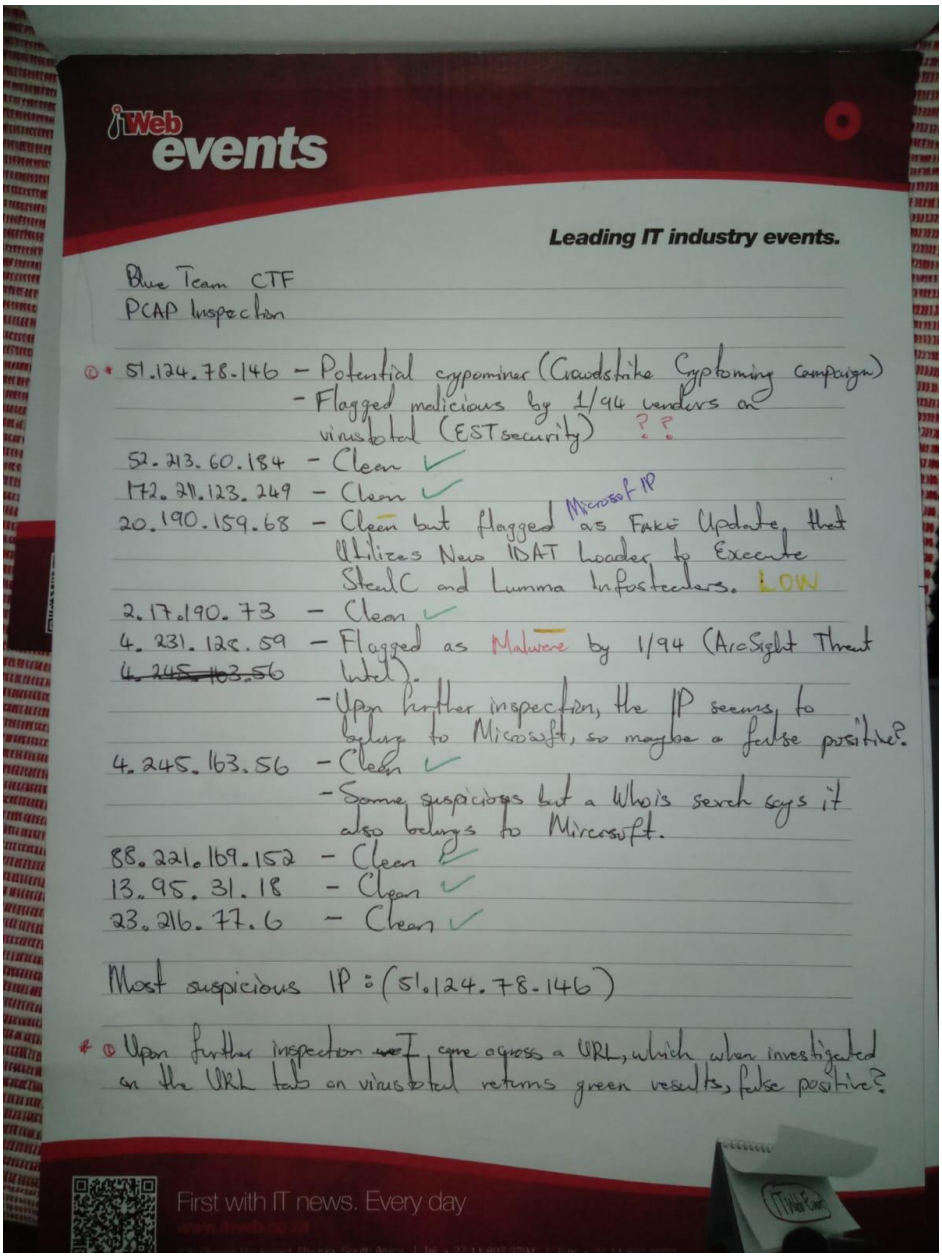


Figure 4A-B – GitHub report linking the IP to the CrowdStrike Crypto Mining and Phishing campaign.


iWeb events
Leading IT industry events.
Blue Team CTF
PCAP Inspection
① * 51.124.78.146 - Potential cypominer (Crowdstrike Cyptoming campaign)
- Flagged malicious by 1/94 vendors on virustotal (ESTsecurity) ??
52.213.60.184 - Clean
172.211.123.249 - Clean
Microsoft IP
20.190.159.68 - Clean but flagged as FAKE Update, that Utilizes New IDAT Loader to Execute StealC and Lumma Infostealers. LOW
2.17.190.73 - Clean
4.231.125.59 - Flagged as Malware by 1/94 (ArcSight Threat Intel).
4.245.163.56
- Upon further inspection, the IP seems to belong to Microsoft, so maybe a false positive?
4.245.163.56 - Clean
- Some suspicions but a Who is search says it also belongs to Microsoft.
88.221.169.152 - Clean
13.95.31.18 - Clean
23.216.77.6 - Clean
Most suspicious IP: (51.124.78.146)
* ① Upon further inspection ~~of~~ I came across a URL, which when investigated on the URL tab on virustotal returns green results, false positive?
First with IT news. Every day

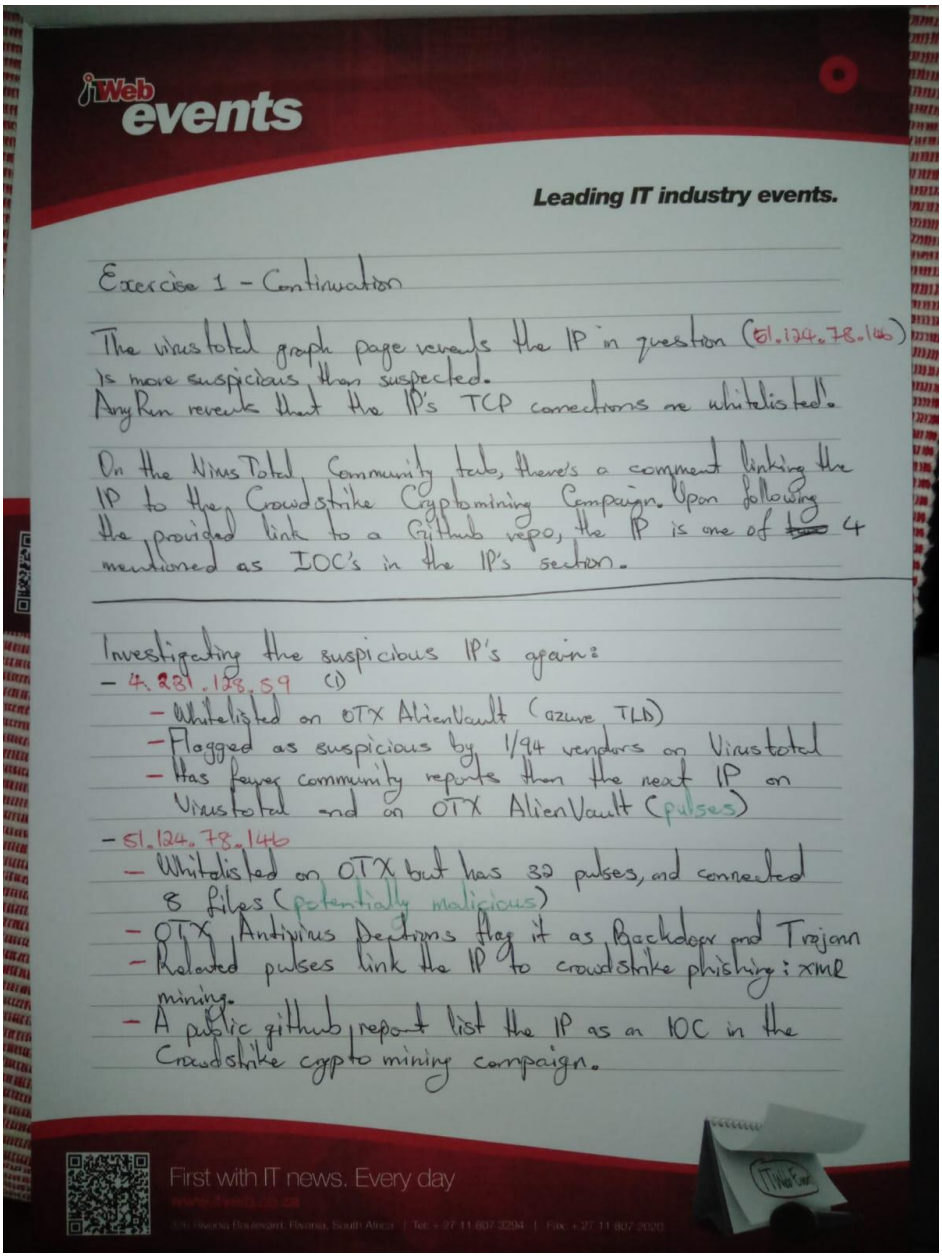


Figure 5A-B – Accompanying handwritten notes during the investigation

Blue Team CTF – IOC Correlation and Analysis Threat Report

Lutho Mboniswa 05 May 2025

Note:

I used ChatGPT to generate a template of this report, everything else was my own findings. Don't be surprised when you run *exiftool* on this document and you see a suspicious output on some of the fields.

1. Introduction

This report investigates an Indicator of Compromise (IOC) observed during the second exercise of the blue team CTF, courtesy of Snode Technologies during the Security Summit Ideathon. The objective is to identify the likely malware associated with the IOC, assess its potential impact, and provide recommendations for detection, prevention, and mitigation.

2. IOC Overview

IOC Provided:
453257c3494addafb39cb6815862403e827947a1e7737eb8168cd10522465deb
Type of Hash: SHA256 [*Figure 1.1*]
Initial Analysis Sources: VirusTotal, SOCRadar, TheHackerNews, Hybrid Analysis, AnyRun, OTX AlienVault, and Intezer.

3. Malware Identification

Based on threat intelligence reports and malware databases, the IOC is associated with the following malware:
- **Malware Name:** PlayCript, also known as Balloonfly and Fiddling Scorpius (by the Play Ransomware gang) [*Figure 1.2]*.
- **Malware Type**: Ransomware (double extortion, Ransomware-as-a-Service)
- **Hash Matches:**

* *Virustotal*: Flagged by 49/72 security vendors as malicious *[Figure 1.3].*

* *SOCRadar*: Flagged as critical IOC due to its association with potentially malicious files and network activity by both ***Cyber Threat Alliance*** and ***SOCRadar Threat Exchange*** *[Figure 1.4]*.

* *Any.run*: Found to be suspicious in 1/8 sandbox public submissions *[Figure 1.5].*

* *Hybrid Analysis*: Found in 2 sandbox submissions [November 26th, 2022 (UTC), December 19th, 2023, 16:38:00 (UTC)] *[Figure 1.6]*

* *OTX AlienVault*: Referenced in 38 pulses related to the Play Ransomware *[Figure 1.7]*.

* *Intezer*: Flagged as malicious and most likely coming across as packed malware, probably linked to the Medusah ransomware *[Figure 1.8].*

4. Risks and Potential Impact

- Data Loss – Critical data is encrypted and exfiltrated, making it unusable
- Spreading of ransomware infection to other hosts connected to the network
- Operational downtime and loss of business continuity – organizational operations grind to a halt as a result of the infection
- Financial losses and reputation damage – customers and external partners may lose trust in the organization, while the ransom and associated costs might be substantial for the organization.
- Legal consequences – organizations may incur heavy fines under privacy laws like POPIA, GDPR for not having adequate measures to protect personal data.

5. Malware Overview & Behavior

The Play ransomware group is a financially motivated threat actor that employs a double-extortion model, encrypting systems after exfiltrating data, and demands ransom payments from their victims. The threat actor is believed to have been active since at least June 2022 and has targeted a wide range of industries including Telecommunications, Healthcare, Communication and Media, and Technology in North America, Europe, and South America. According to intelligence shared by *CISA*, Mitre ATT&CK, and *The Hacker News*, *Playcript* has demonstrated highly sophisticated attack avenues, often leveraging both known vulnerabilities and social engineering tactics for initial access and a custom-built information stealer.

1. **Initial Access**:

Playcript usually gains initial access on victim systems and networks through one or more of the following vectors:

* Abuse of valid credentials and exploitation of public facing applications, specifically FortiOS (*CVE-2018-13379* and *CVE-2020-12812*) and Microsoft Exchange (ProxyNotShell [*CVE-2022-41040* and *CVE-2022-41082*]) vulnerabilities.

* Compromised Remote Desktop Protocol (*RDP*) and Virtual Private Networks (*VPN*) credentials.

2. **Discovery and Defense Evasion**:

The PlayCript threat actor use tools like:

* AdFind to run Active Directory queries

* GMER, IOBIT, PowerTool to disable antivirus software and clear event logs.

* Grixba, a custom-built information stealer tool which is also a network scanning tool used to enumerate all users and hosts in a domain. Also used to enumerate software and services, checks for existence of security and backup software, and remote administration tools.

3. **Execution and Lateral Movement:**

Once inside the target environment:

* The Play ransomware gang uses Command-and-Control (*108.61.142[.]190*) applications like Cobalt Strike and SystemBC, and tools like PsExec for lateral movement and file execution.

* The threat actors then utilize Mimikatz to dump credentials and obtain domain controller access on the victim networks.

* PlayCript threat actors have also been observed using Windows Privilege Escalation Awesome Scripts (*WinPEAS*) to enumerate further privilege escalation paths and then distribute their executables via Group Policy Objects.

4. **Double Extortion – Exfiltration and Encryption**:

Play ransomware group's ransomware payload exhibits the following behavior:

* Compromised victim's data is often split into smaller chunks to avoid triggering network data transfer and use tools like WinRAR for data compression.

* The threat actors utilize WinSCP, a Secure File Transfer Protocol (SFTP) and File Transfer Protocol client in Windows to exfiltrate the compromised data from victim systems to threat actor-controlled accounts and domains.

* After exfiltration, the files in the victim systems are encrypted with AES-RSA hybrid encryption, with each encrypted file having the ***.play*** file extension, though system files are ignored.

5. **Impact**:

* A ransom note (*ReadMe.txt*) is created and stored in the root (*C:*) directory. The ransom note does not specify any ransom amount demanded for a decryption but rather an email address through which they instruct the victims to contact them at.

* Threat actors provide wallet addresses to which the ransom should be paid. If a victim refuses to pay the ransom demand, the threat actors threaten to publish the exfiltrated data to their leak site on the dark web.

6. Recommendations

To protect against the identified threat, it is recommended to implement the following best practices:

1. Keep all operating systems, software and firmware updated to the latest versions to minimize exposure to cyber-security threats.

2. Require multi-factor authentication (MFA) for all services that access critical data, require all accounts with password logins to comply with NIST's standards for developing and managing password policies, and regularly audit user accounts with administrative privileges.

3. Filter network traffic by preventing unknown network sources from accessing internal network data and hosts.

4. Ensure backups are encrypted and maintain offline backups and regularly maintain back and restoration exercises.

5. Implement a solid recovery plan to maintain and retain multiple copies of sensitive data and servers in a physically separate and secure location.

7. Leveraging the IOC for Security Enhancements

The given IOC, which is a SHA256 hash, uniquely identifies a specific malicious file. It can be used in the following ways to improve threat detection and response:

1. Add the IOC hash to Antivirus software, Endpoint Detection and Response (allow/block list) to prevent the file from slipping through defenses and executing on any device within the internal network.

2. Set up an automated alert in the Security Information and Events Manager (SIEM) whenever a system tries to download or execute a file associated with that hash.

3. Include the hash in custom Yara, Sigma or Snort rules to continuously scan for matching files across systems and networks.

4. Collaborate with other security researchers by publishing reports on the IOC and sharing intel with reputable intel-sharing communities.

5. Add context to the hash by combining findings with additional context associated with the hash to paint the bigger picture.

8. Appendix: Threat Intel Links & Screenshots

The following section includes relevant screenshots and threat intel links used during the investigation:

- https://thehackernews.com/2025/03/the-new-ransomware-groups-shaking-up.html
- https://thehackernews.com/2023/11/play-ransomware-goes-commercial-now.html
- https://www.security.com/threat-intelligence/play-ransomware-volume-shadow-copy
- https://www.hookphish.com/blog/ransomware-play-group-hits-affordable-payroll-and-bookkeeping-services/
- https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-352a
- https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-play
- https://thehackernews.com/2023/12/double-extortion-play-ransomware.html
- https://thehackernews.com/2024/07/new-linux-variant-of-play-ransomware.html

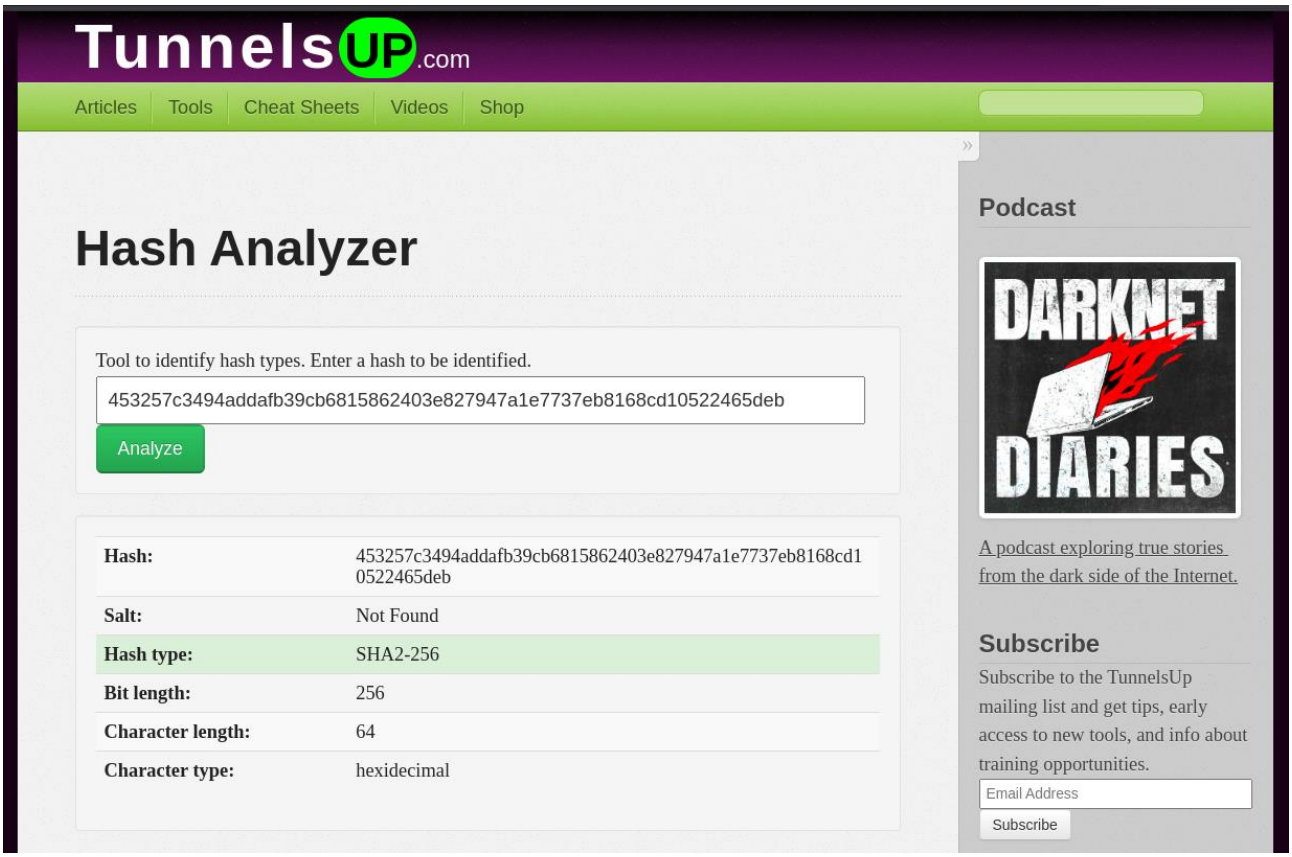


Figure 1.1 - Hash identifying software

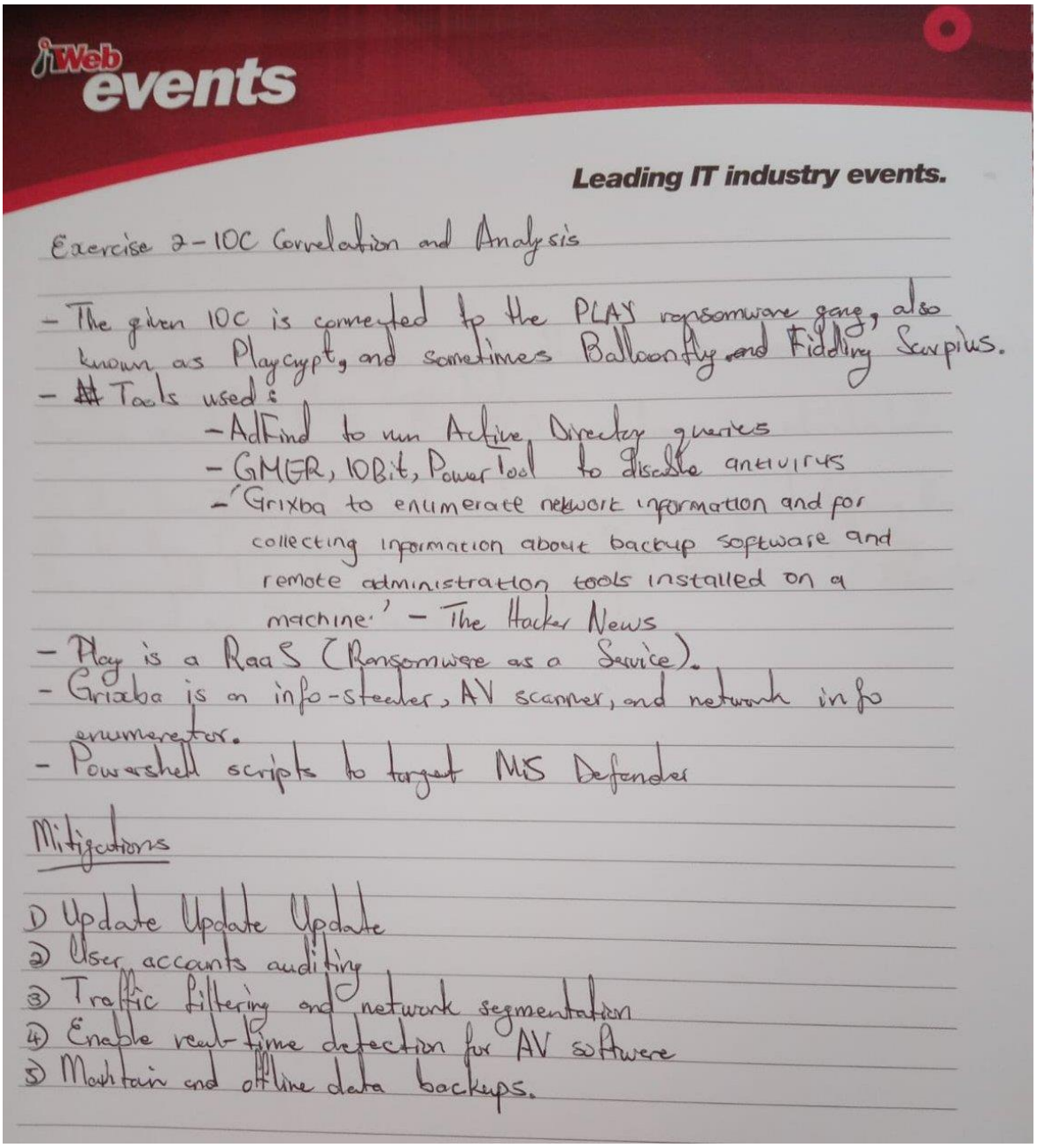


Figure 1.2 - Handwritten notes taken during the investigation.

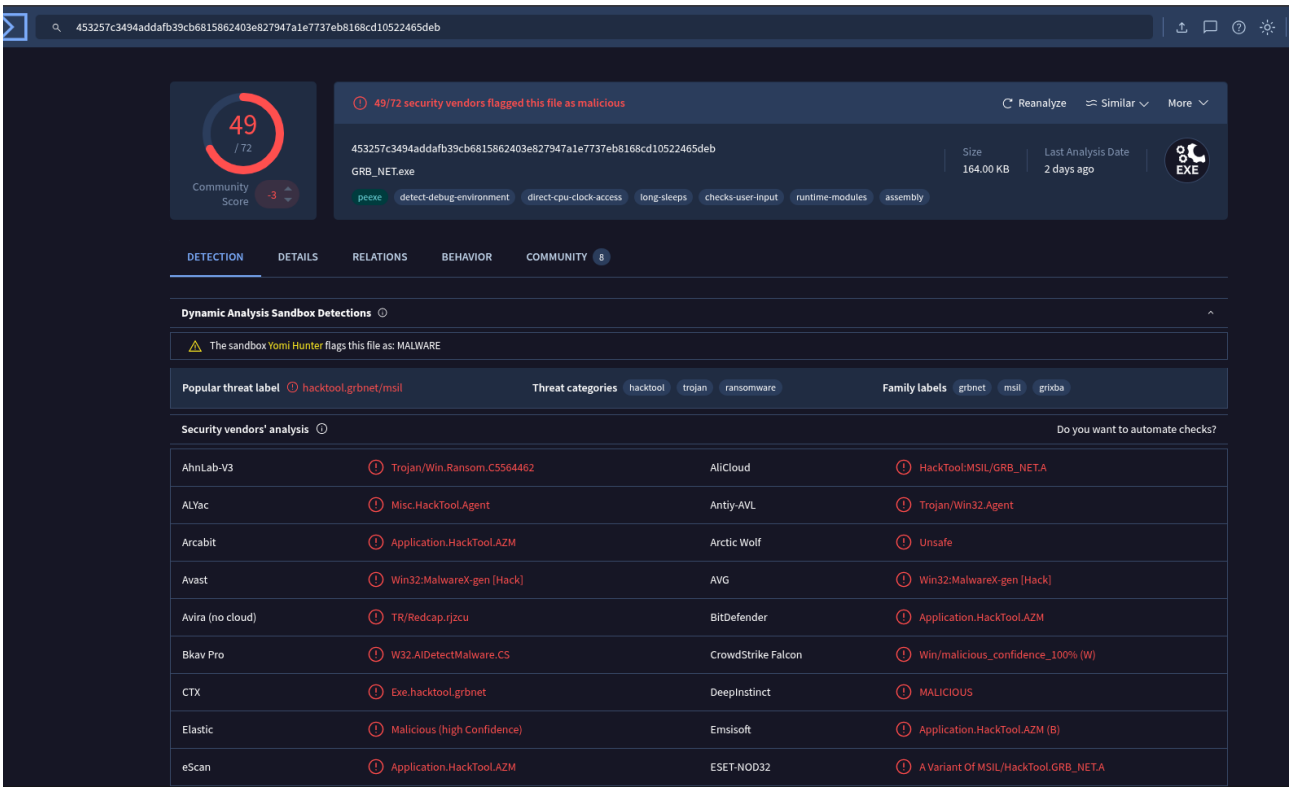


Figure 1.3 - Virustotal scan of the IOC summary

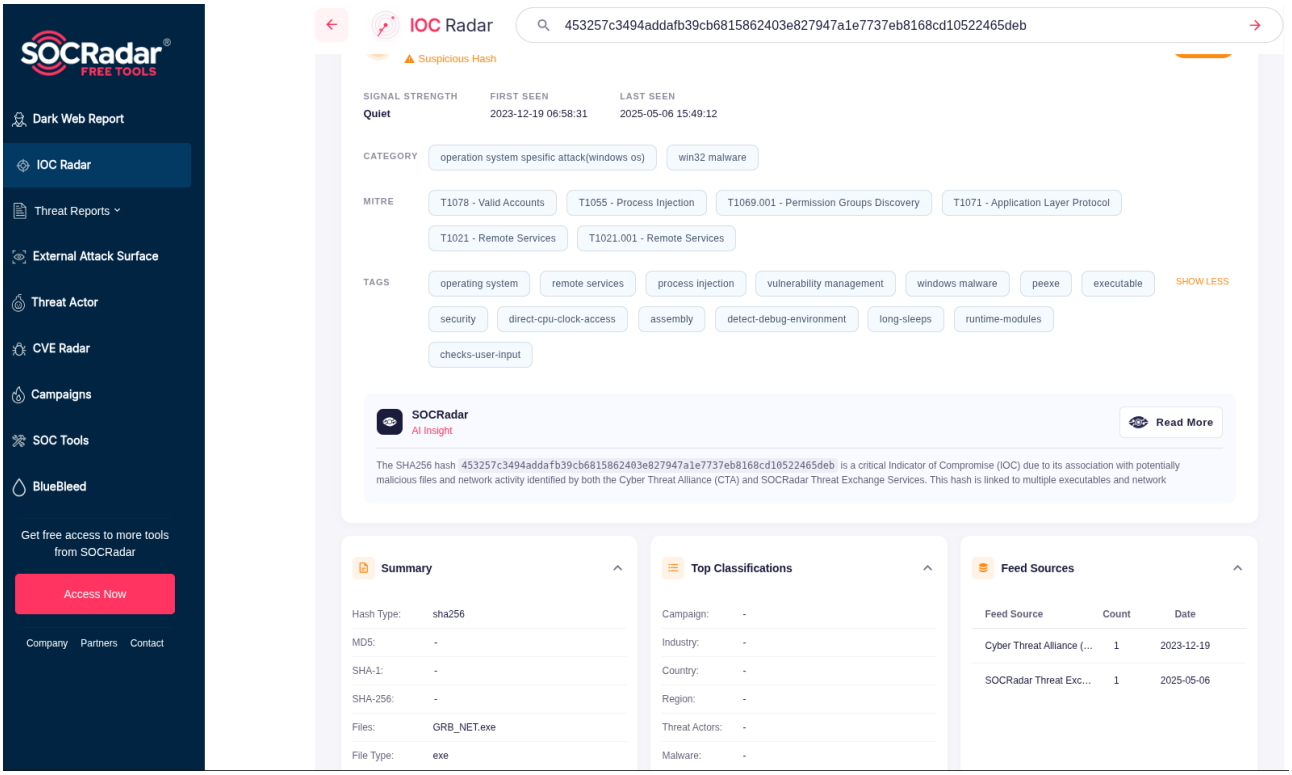
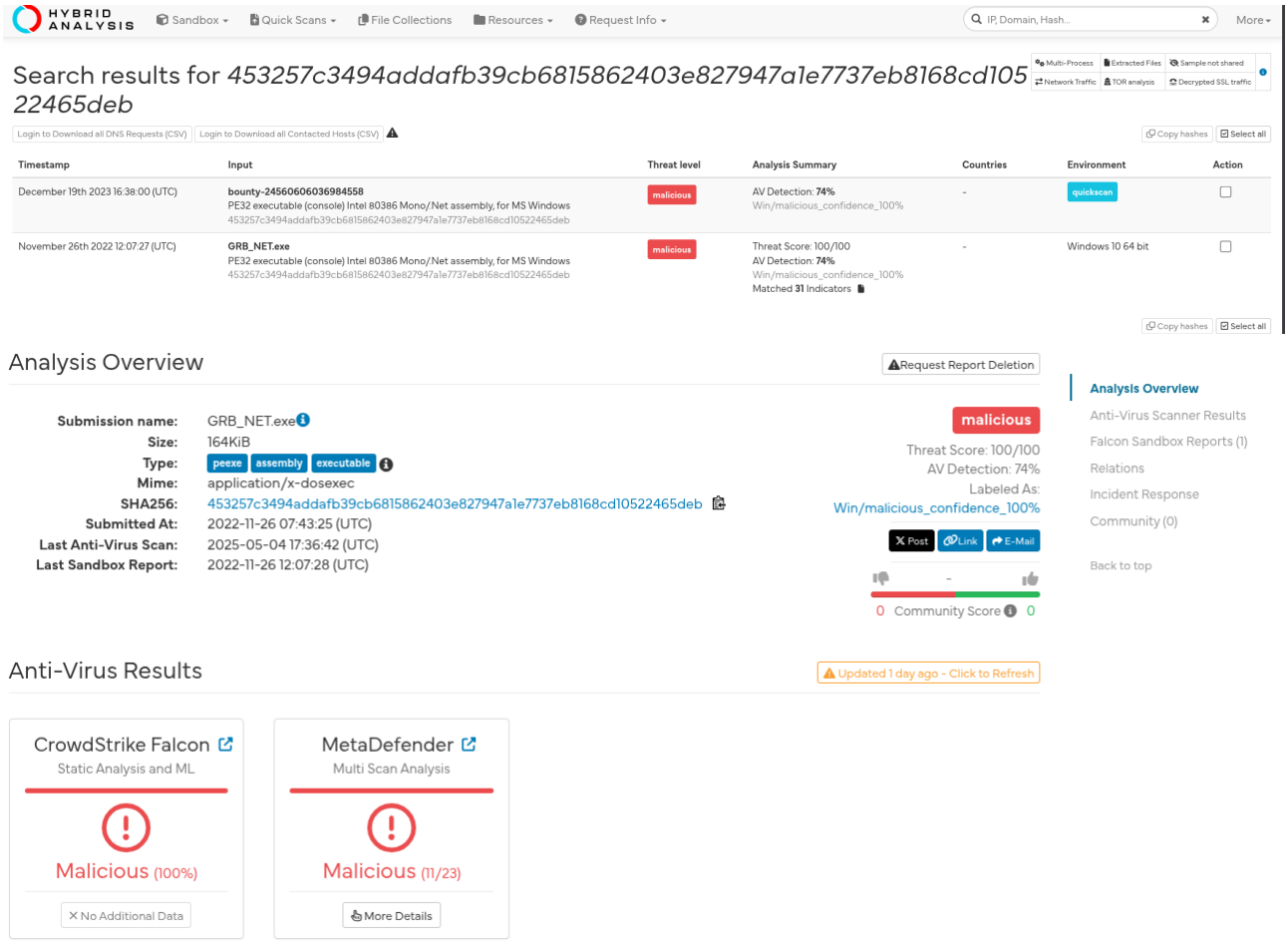


Figure 1.4 - SOCRadar scan of the IOC summary

Figure 1.5 - ANYRun scan of the IOC summary



Falcon Sandbox Reports (1)

Characteristics Legend | Show All As List | Submit

Windows 10 64 bit

GRB_NET.exe

November 26th 2022 12:07:28 (UTC)

Malicious

Threat Score: 100/100

Labeled As: Win/malicious_co...

Indicators: 3 20 8

Characteristics:

Falcon Sandbox Technology

Hybrid Analysis: Powered by Falcon Sandbox
Upgrade to a Falcon Sandbox license and gain full access to all features, IOCs and behavior analysis reportsData.

Easily Deploy and Scale
Process up to 25,000 files per month with Falcon Sandbox; because it is delivered on the cloud-native Falcon Platform, Falcon Sandbox is operational on Day One.

Extensive Coverage
Expanded support for file types and host operating systems.

Learn More!

GRB_NET.exe

malicious

This report is generated from a file or URL submitted to this webservice on November 26th 2022 12:07:28 (UTC)
Guest System: Windows 10 64 bit, Professional, 10.0 (build 16299),
Report generated by Falcon Sandbox © Hybrid Analysis

Threat Score: 100/100
AV Detection: 74%
Labeled as: Win/malicious_confidence_100%

Overview | Sample unavailable | Downloads | External Reports | Re-analyze | Hash Not Seen Before | Report False-Positive | Request Report Deletion

Post | Link | E-Mail

Incident Response

Risk Assessment

Spyware	Hooks API calls
Persistence	Installs hooks/patches the running process
Fingerprint	Queries process information Reads the active computer name Reads the cryptographic machine GUID Reads the windows installation language
Evasive	Contains ability to change service configuration Input file contains API references not part of its Import Address Table (IAT) Tries to sleep for a long time (more than two minutes)

MITRE ATT&CK™ Techniques Detection

This report has 19 indicators that were mapped to 11 attack techniques and 6 tactics. View all details

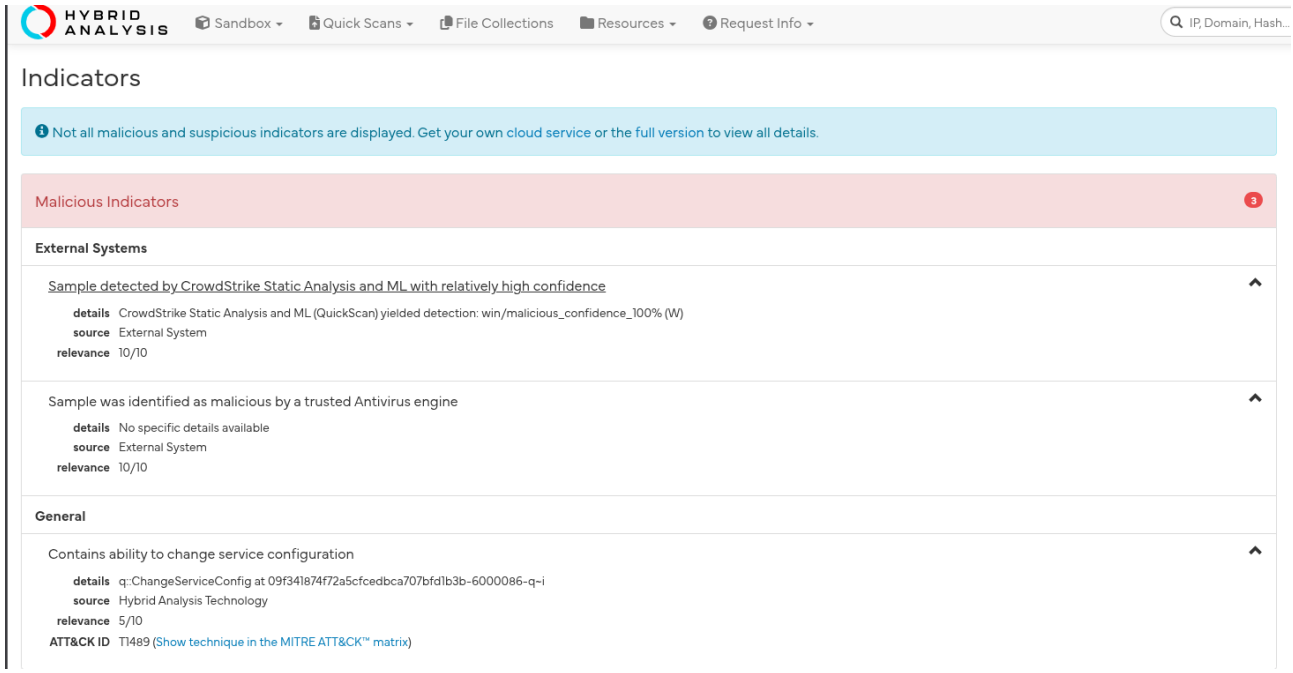


Figure 1.6A-E - Hybrid Analysis scans of the IOC summary

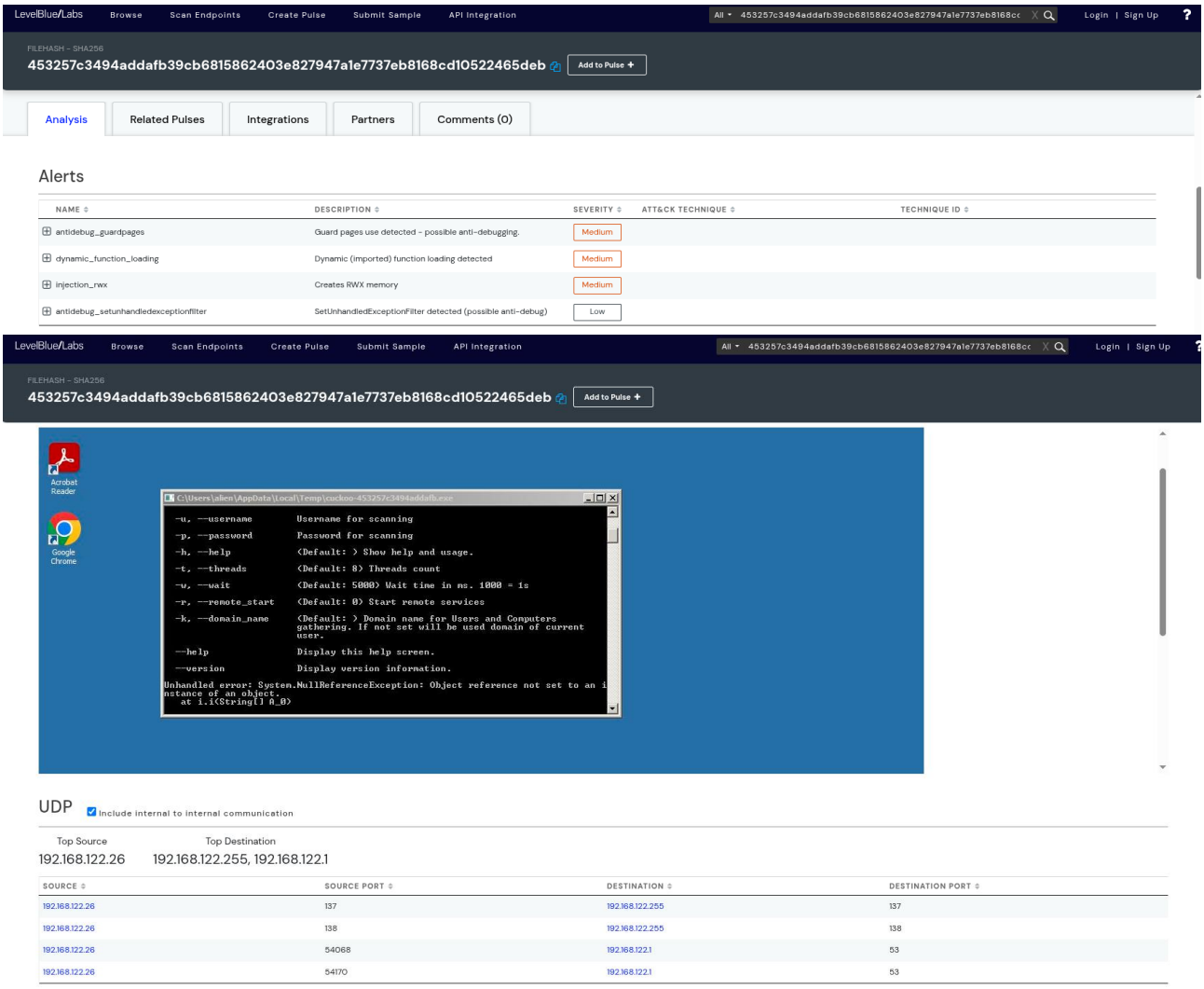


Figure 1.7A-B – OTX AlienVault scan of the IOC summary

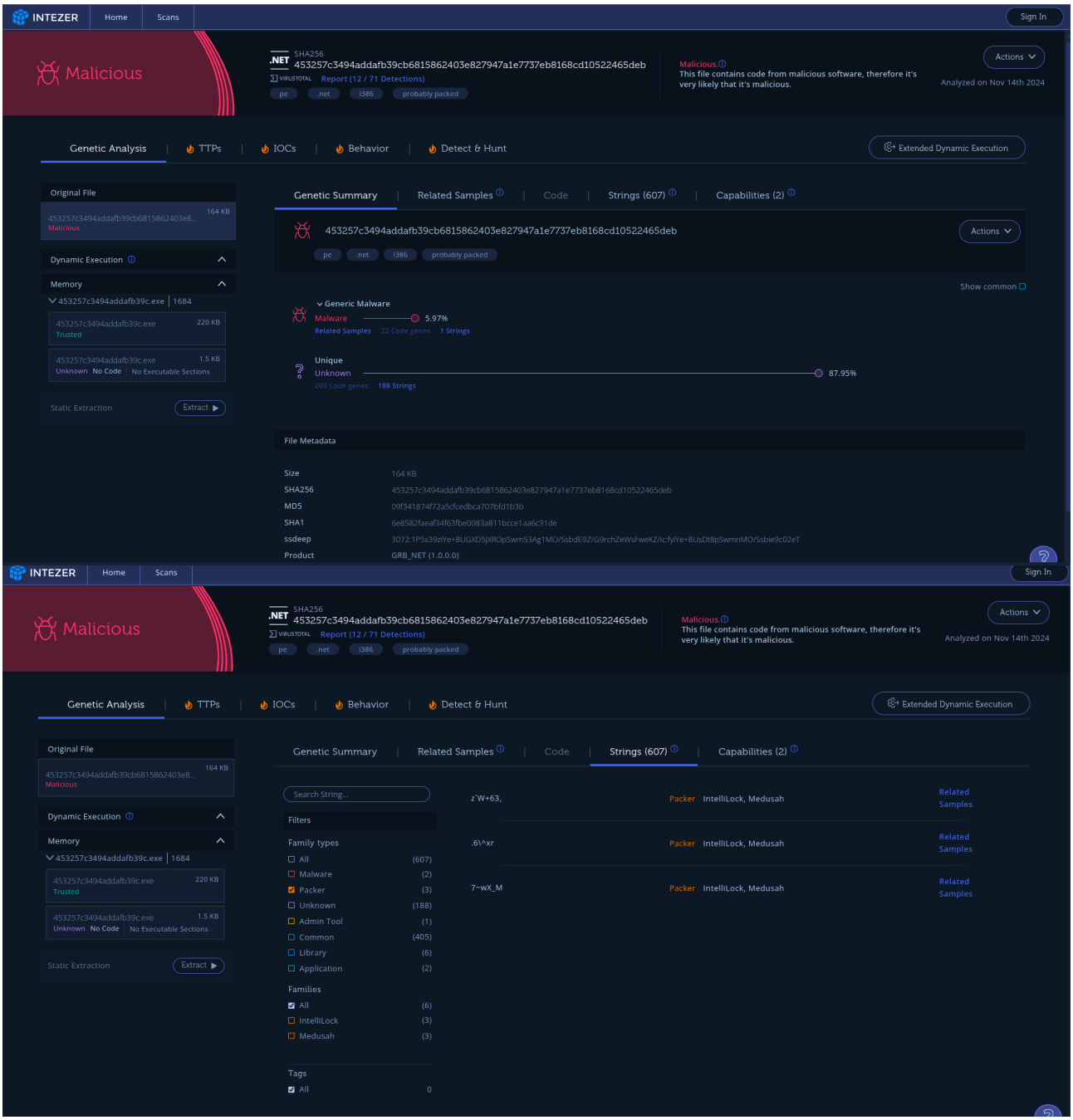


Figure 1.8A-B – Intezer scans of the IOC summary

Threat Actor TTP Mapping Report – Exercise 3

Lutho Mboniswa 06 May 2025

Objective: This report follows from the previous investigation in Exercise 2. In that phase, an Indicator of Compromise (IOC) was analyzed and associated with a ransomware strain, PlayCript, and attributed to a known threat actor, the Play ransomware gang (thanks for the hint). The current report focuses on mapping the tactics, techniques, and procedures (TTPs) used by that threat actor to the MITRE ATT&CK framework, ensuring continuity and depth in the threat analysis. Screenshots, references, and methodologies are attached where relevant.

MITRE ATT&CK Mapping Table

The table below outlines the most relevant TTPs associated with the Play ransomware group identified in Exercise 2. These entries are based on MITRE's official documentation and reflect the tactics this threat actor has been observed using across known campaigns.

MITRE ID	Tactic	Technique Name	Use by Threat Actor (Summary)
T1078	Initial Access	Valid Accounts	Play has used valid VPN accounts to achieve initial access.
T1078.002		Domain Accounts	Play has used valid domain accounts for access.
T1078.003		Local Accounts	Play has used valid local accounts to gain initial accounts.
T1133		External Remote Services	Play has used RDP and VPNs for initial access.
T1190		Exploit Public-Facing Application	Play has exploited known vulnerabilities [CVE-2018-13379 and CVE-202012812 in FortiOS and CVE-2022-41082 and CVE-2022-41040 (ProxyNotShell) in Microsoft Exchange] for initial access.
T1018	Discovery	Remote System Discovery	Play has used tools like AdFind, Nltest, and Bloodhound to

			enumerate shares and hostnames on compromised networks.
T1518.001		Software Discovery: Security Software Discovery	Play has used the Grixba info-stealer to scan for AntiVirus software.
T1082		System Information Discovery	Play has leveraged tools to enumerate system information.
T1016		System Network Configuration Discovery	Play has used the Grixba info-stealer to enumerate network information.
T1057		Process Discovery	Play has used the Grixba info-stealer to check for a list of security processes.
T1083		File and Directory Discovery	Play has used the Grixba info-stealer to list security files and processes.
T1588.002	Defense Evasion	Obtain Capabilities: Tool	Play has used multiple tools for discovery and defense evasion purposes on compromised hosts.
T1562.001		Impair Defenses: Disable or Modify Tools	Play has used tools like GMER, IOBit, and PowerTool to disable AV software.
T1070.001		Indicator Removal: Clear Windows Event Logs	Play has used tools to remove log files on targeted systems.
T1070.004		Indicator Removal: File Deletion	Play has used tools including Wevtutil to remove malicious files from compromised hosts.
T1027.010		Obfuscated Files or Information: Command Obfuscation	Play has used Base64-encoded PowerShell scripts for post exploit activities on compromised hosts.
T1003.001	Credential Access	OS Credential Dumping: LSASS Memory	Play has used Mimikatz and the Windows Task Manager to dump LSASS process memory.
T1059.001	Execution	Command and Scripting Interpreter: PowerShell	Play has used Base64-encoded PowerShell scripts to disable Microsoft Defender.
T1059.003		Command and Scripting Interpreter: Windows Command Shell	Play has used a batch script to remove indicators of its presence on compromised hosts.

T1587.001		Develop Capabilities: Malware	Play developed and employ PlayCript ransomware.
T1021.002	Lateral Movement	Remote Services: SMB/Windows Admin Shares	Play has used Cobalt Strike to move laterally via Server Message Block (SMB).
T1105	Command & Control	Ingress Tool Transfer	Play has used Cobalt Strike to download files to compromised machines.
T1560.001	Collection	Archive Collected Data: Archive via Utility	Play has used WinRAR to compress files prior to exfiltration
T1030		Data Transfer Size Limits	Play has split victims' files into chunks for exfiltration.
T1048	Exfiltration	Exfiltration Alternative Protocol	Play has used WinSCP to exfiltrate data to actor-controlled accounts.
T1657	Impact	Financial Theft	Play demands ransom payments from victims to decrypt filesystems and to not publish sensitive data exfiltrated from victim networks.

Methodology:

- Used the threat actor profile identified from Exercise 2.
- Referenced MITRE ATT&CK database directly for tactic and technique mapping.
- Ensured alignment with threat intelligence platforms utilized in Exercise 2 (VirusTotal, OTX AlienVault, SOCRadar, Hybrid Analysis, AnyRun).
- Captured screenshots of MITRE pages as supporting documentation.

Recommendations:

- Enforce Multifactor Authentication (MFA) and routinely audit domain account permission levels.
- Regularly audit local accounts and privileged access and regularly perform system scans to identify unauthorized archival utilities.
- Ensure super-user accounts have complex and unique passwords across all systems on the network and implement a Zero Trust Network architecture.
- Limit access to remote services, disable and block remotely available services that may be unnecessary. Disable or close unused ports.
- Patch! Ensure all systems stay updated and regularly scan externally facing systems for vulnerabilities.

Appendix:

Screenshots and evidence utilized to compile this report:

- https://attack.mitre.org/groups/G1040/
- https://attack.mitre.org/software/S1162
- https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-352a
- https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-play
- https://attack.mitre.org/techniques/T1560/001
- https://attack.mitre.org/techniques/T1190
- https://attack.mitre.org/techniques/T1133
- https://attack.mitre.org/techniques/T1003/001
- https://attack.mitre.org/techniques/T1078/002

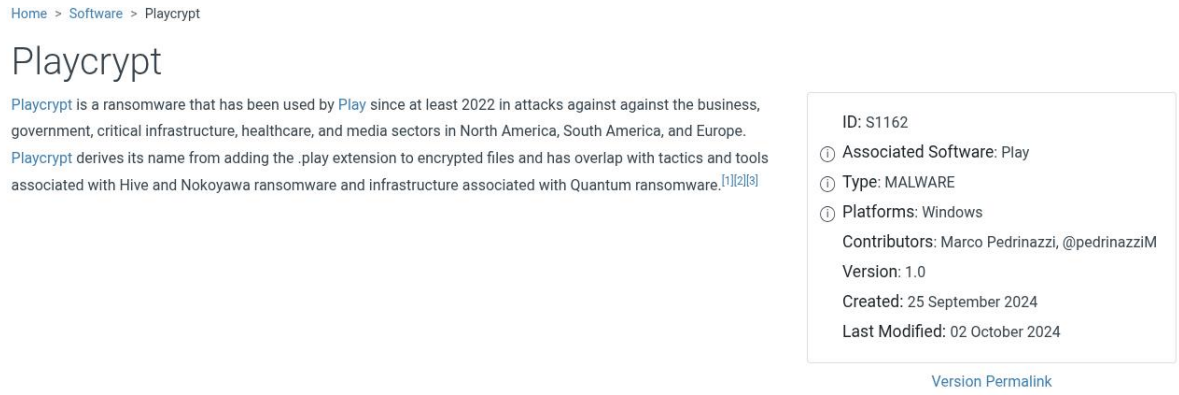


Figure 1.1 - Playcript description on the MITRE ATT&CK database

Play

Play is a ransomware group that has been active since at least 2022 deploying Playcrypt ransomware against the business, government, critical infrastructure, healthcare, and media sectors in North America, South America, and Europe. Play actors employ a double-extortion model, encrypting systems after exfiltrating data, and are presumed by security researchers to operate as a closed group.[1][2]

ID: G1040
Contributors: Marco Pedrinazzi, @pedrinazziM
Version: 1.0
Created: 24 September 2024
Last Modified: 02 October 2024

Version Permalink

Techniques Used

ATT&CK® Navigator Layers

Domain	ID		Name	Use
Enterprise	T1560	.001	Archive Collected Data: Archive via Utility	Play has used WinRAR to compress files prior to exfiltration.[1][2]
Enterprise	T1059	.001	Command and Scripting Interpreter: PowerShell	Play has used Base64-encoded PowerShell scripts to disable Microsoft Defender.[2]
		.003	Command and Scripting Interpreter: Windows Command Shell	Play has used a batch script to remove indicators of its presence on compromised hosts.[2]
Enterprise	T1030		Data Transfer Size Limits	Play has split victims' files into chunks for exfiltration.[1][2]
Enterprise	T1587	.001	Develop Capabilities: Malware	Play developed and employ Playcrypt ransomware.[2][1]
Enterprise	T1048		Exfiltration Over Alternative Protocol	Play has used WinSCP to exfiltrate data to actor-controlled accounts.[1][2]
Enterprise	T1190		Exploit Public-Facing Application	Play has exploited known vulnerabilities for initial access including CVE-2018-13379 and CVE-2020-12812 in FortiOS and CVE-2022-41082 and CVE-2022-41040 ("ProxyNotShell") in Microsoft Exchange.[1][2]

Figure 1.2A - Play ransomware group description and TTPs on the MITRE ATT&CK database

Enterprise	T1083		File and Directory Discovery	Play has used the Grixba information stealer to list security files and processes.[2]
Enterprise	T1657		Financial Theft	Play demands ransom payments from victims to unencrypt filesystems and to not publish sensitive data exfiltrated from victim networks.[1]
Enterprise	T1562	.001	Impair Defenses: Disable or Modify Tools	Play has used tools including GMER, IOBit, and PowerTool to disable antivirus software.[1][2]
Enterprise	T1070	.001	Indicator Removal: Clear Windows Event Logs	Play has used tools to remove log files on targeted systems.[1][2]
		.004	Indicator Removal: File Deletion	Play has used tools including Wevtutil to remove malicious files from compromised hosts.[2]
Enterprise	T1105		Ingress Tool Transfer	Play has used Cobalt Strike to download files to compromised machines.[2]
Enterprise	T1027	.010	Obfuscated Files or Information: Command Obfuscation	Play has used Base64-encoded PowerShell scripts for post exploit activities on compromised hosts.[2]
Enterprise	T1588	.002	Obtain Capabilities: Tool	Play has used multiple tools for discovery and defense evasion purposes on compromised hosts.[1]
Enterprise	T1003	.001	OS Credential Dumping: LSASS Memory	Play has used Mimikatz and the Windows Task Manager to dump LSASS process memory.[2]
Enterprise	T1057		Process Discovery	Play has used the information stealer Grixba to check for a list of security processes.[2]
Enterprise	T1021	.002	Remote Services: SMB/Windows Admin Shares	Play has used Cobalt Strike to move laterally via SMB.[2]
Enterprise	T1018		Remote System Discovery	Play has used tools such as AdFind, NItest, and BloodHound to enumerate shares and hostnames on compromised networks.[2]
Enterprise	T1518	.001	Software Discovery: Security Software Discovery	Play has used the information-stealing tool Grixba to scan for anti-virus software.[1]
Enterprise	T1082		System Information Discovery	Play has leveraged tools to enumerate system information.[2]
Enterprise	T1016		System Network Configuration Discovery	Play has used the information-stealing tool Grixba to enumerate network information.[1]

Figure 1.2B - More TTPs employed by the Play ransomware group

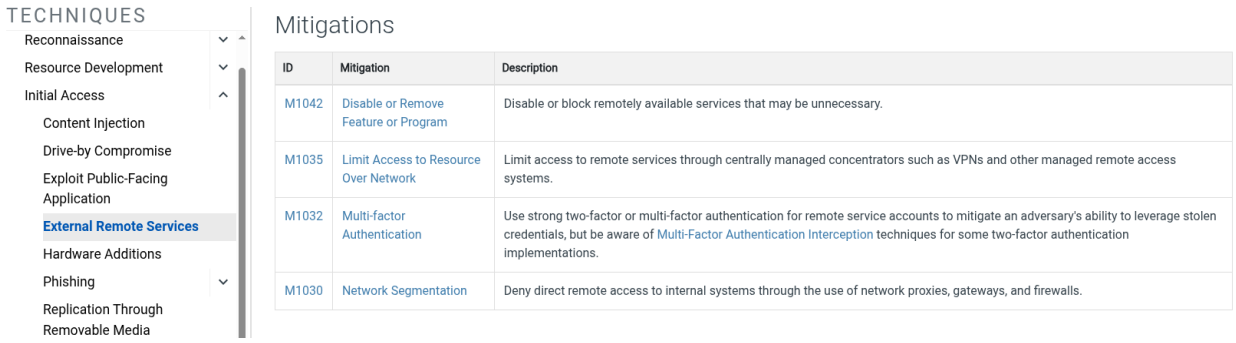


Figure 1.3 - Recommended mitigations against the exploitation of public facing remote services, per MITRE ATTA&CK database.

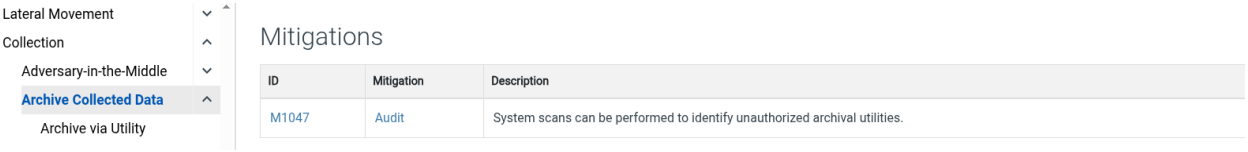


Figure 1.4 - Recommended mitigation against archiving of data, per MITRE ATT&CK database.

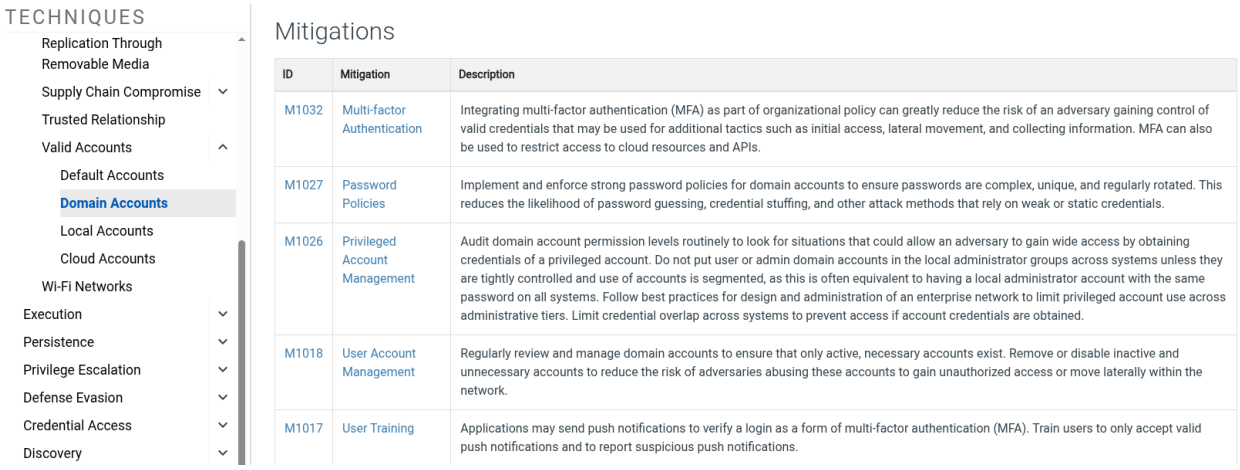
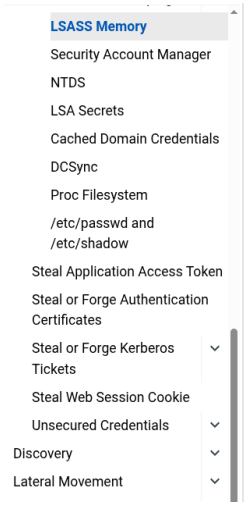


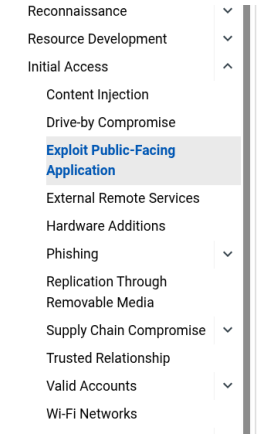
Figure 1.5 - Recommended mitigation against domain accounts unauthorized access, per MITRE ATT&CK database.



Mitigations

ID	Mitigation	Description
M1040	Behavior Prevention on Endpoint	On Windows 10, enable Attack Surface Reduction (ASR) rules to secure LSASS and prevent credential stealing. [108]
M1043	Credential Access Protection	With Windows 10, Microsoft implemented new protections called Credential Guard to protect the LSA secrets that can be used to obtain credentials through forms of credential dumping. It is not configured by default and has hardware and firmware system requirements. It also does not protect against all forms of credential dumping.[109][110]
M1028	Operating System Configuration	Consider disabling or restricting NTLM.[111] Consider disabling WDigest authentication.[112]
M1027	Password Policies	Ensure that local administrator accounts have complex, unique passwords across all systems on the network.
M1026	Privileged Account Management	Do not put user or admin domain accounts in the local administrator groups across systems unless they are tightly controlled, as this is often equivalent to having a local administrator account with the same password on all systems. Follow best practices for design and administration of an enterprise network to limit privileged account use across administrative tiers.
M1025	Privileged Process Integrity	On Windows 8.1 and Windows Server 2012 R2, enable Protected Process Light for LSA.[113]
M1017	User Training	Limit credential overlap across accounts and systems by training users and administrators not to use the same password for multiple accounts.

Figure 1.6 - Recommended mitigation against the exploitation of LSASS, per MITRE ATT&CK database.



Mitigations

ID	Mitigation	Description
M1048	Application Isolation and Sandboxing	Application isolation will limit what other processes and system features the exploited target can access.
M1050	Exploit Protection	Web Application Firewalls may be used to limit exposure of applications to prevent exploit traffic from reaching the application.
M1035	Limit Access to Resource Over Network	Ensure that all publicly exposed services are actually intended to be so, and restrict access to any that should only be available internally.
M1030	Network Segmentation	Segment externally facing servers and services from the rest of the network with a DMZ or on separate hosting infrastructure.
M1026	Privileged Account Management	Use least privilege for service accounts will limit what permissions the exploited process gets on the rest of the system.
M1051	Update Software	Update software regularly by employing patch management for externally exposed applications.
M1016	Vulnerability Scanning	Regularly scan externally facing systems for vulnerabilities and establish procedures to rapidly patch systems when critical vulnerabilities are discovered through scanning and through public disclosure.[10]

Figure 1.7 - Recommended mitigation strategies against the exploitation of public facing applications, per MITRE ATT&CK database