Network Security: Network Intrusion Investigation portfolio

By

Usiwoghene Ekebor

Table of Content Page Number

Executive Summary

This portfolio was prepared for the CEO of an SME to give a detailed breakdown of the network intrusion attack that took place on the 20-02-2025 with the aim of identifying what led to system slowdown. By using SecurityOnion VM which is integrated with tools like Squil and Kibana, the network activities and system logs was thoroughly analysed. The analysis reveals that the system slowdown issues was caused because the compromised device with IP 10.1.11.101 got infected by a trojan malware. Subsequently, this trojan malware instigated a cryptocurrency mining operations which resulted in the system degradation. To further illustrate, this analysis identified key indicators of compromise (IoCs), which include malicious IP addresses, hashes of downloaded files which was generated from Squil and domain name system which pointed to the involvement crypto mining operation in the affected system. This portfolio provides detailed analysis of the network intrusion, the timeline of events and tools that was used which offered a clear insight in what led to the security breach that impacted the company's system.

1.0 Introduction

The past two decade has saw the rise in the adoption crypto currency and to get hold of this asset requires individuals to either buy some or mine with a powerful computer resource. The concerns of an SME were drawn to the reason why there was a significant slowdown in its system performance, to address this an investigation was conducted to determine the cause of the slowdown affecting the computer of the business. To conduct This investigation which is aimed at identifying the security threats and unauthorised access to system resources, a SecurityOnion vm equipped with tools like Squil shows real-time intrusion alerts and Kiban which provide visual representation of network activities and security events was deployed. These tools assisted in pinpointing the root cause of the system slowdown by providing a complete review of the potential indicators of compromise.

This analysis concentrated on analysing the intrusion detection alert and event logs to uncover any security breaches. Initial findings suggest that the slow system performance may have been caused by unauthorised system access and execution of malicious software which required further analysis. By using the Security Onion vm, this portfolio highlights the detailed examination of the incident by providing detailed insight into the security threats encountered and suggesting recommendations to mitigate future risks.

2.0 Methodology

This intrusion analysis followed a structured approach to identify the root cause of the system's performance issues. By following the MITRE ATT&CK framework, the process began with data collection using SecurityOnion, specifically leveraging Squil for real-time intrusion detection alerts and Kibana for visualizing network and security logs. Extracted PCAP files from Squil were analysed to examine the network traffic patterns, while system logs from Kibana were reviewed for unusual activity.

Furthermore, the collected data was scrutinized for indicators of compromise (IoCs), including suspicious IP addresses, unusual connections, and abnormal system processes. Comparing the alerts in Squil with log data in Kibana provided deeper insights into the attack timeline and tactics used. Findings were documented to establish correlations between network events and the system slowdown. Finally, all evidence was compiled into a portfolio detailing the potential security threats, their impact, and recommendations to prevent future incidents.

3.0 Timeline of Evidence and Affected Device Details

3.1 Timeline of Evidence

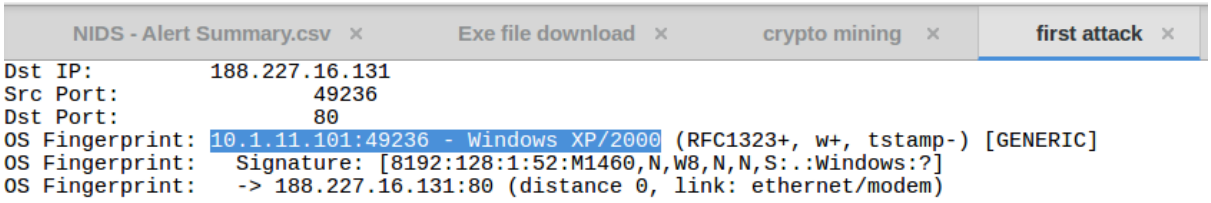
- 2025-02-20 03:36:39: The attack began with a GET request from IP 10.1.11.101 to 188.227.16.131, downloading two trojan malware files: a HTML file and an Adobe Flash (.swf) file. Both files were flagged as malicious but had fictitious hash values.
- 2025-02-20 03:38:01: A GET request was sent from 10.1.11.101 to 104.236.16.69, downloading an executable file, "bprocess.exe," with an MZ signature, indicating a potentially harmful file.
- 2025-02-20 03:43:35: A DNS query was sent from 10.1.11.101 to 10.1.11.1 which seem to be the IP of pool.minexmr.com domain.

- 2025-02-20 03:43:35: A TCP connection was initiated from 10.1.11.101 to 188.165.214.95 on port 5555, suggesting the device was being used for cryptocurrency mining.

3.2 Affected Device Details

The affected device, identified by IP 10.1.11.101, is a Windows XP/2000 machine that downloaded and executed malicious files, leading to the device's involvement in mining cryptocurrency, causing performance issues Figure 1.

Figure 1 Affected device information



Source Alert transcript from Squil analysis

4.0 Finding from the Alert/Logs Evidence

The Squill and Kibana analysis provided evidence of malicious activity on a device. The Squill alerts revealed the download of trojan files (.html,.swf, .exe) and a connection to a cryptocurrency mining domain. Moreover, the extracted PCAP files disclosed detailed information about the compromised device behaviour, showing the execution of mining operations. The Kibana provided more information about the destination server location and timestamp.

4.1 Squill Analysis

Squill alerts captured multiple malicious events, starting with a GET request from the victim device whose IP address is 10.1.11.101 to 188.227.16.131 at 2025-02-20 03:36:39. This initiated the download of a .html file at 2025-02-20 03:36:40. Furthermore, another GET request from the victims device was sent to the same destination IP which downloaded a .swf file, which is an Adobe Flash file that contain video based animation, graphics and text Figure 2.

Figure 2 Packet capture of the downloaded .html and .swf files

Source Extracted PCAP of the Trojan download from the Squil analysis

Both files had fictitious hash values, raising suspicions about their authenticity. Following this, series of processes ran on the victims device, and another GET request was logged at 03:38:01 to IP 104.236.16.69, resulting in the download of the "bprocess.exe" file, which is indicative of malware with an MZ (Mark Zbikowski) signature which is a signature for an MS-DOS Portable Executable file Figures 3.

Figure 3 Packet capture of the downloaded .exe file

Time	Source	Destination	Protocol	Length	Info
2025-02-20 03:38:01.689127	10.1.11.101	104.236.16.69	HTTP	254	GET /bprocess.exe HTTP/1.1
2025-02-20 03:38:05.175452	104.236.16.69	10.1.11.101	HTTP	1107	HTTP/1.1 200 OK (application/x-msdos-program)

Source Extracted PCAP of the Trojan download from the Squil analysis

Figure 4 .EXE file download transcript from Squil

```
Sensor Name:    seconion-import-1
Timestamp:      2025-02-20 03:38:01
Connection ID:  .seconion-import-1_1364
Src IP:         10.1.11.101
Dst IP:         104.236.16.69
Src Port:               49259
Dst Port:               80
OS Fingerprint: 10.1.11.101:49259 - Windows XP/2000 (RFC1323+, w+, tstamp-) [GENERIC]
OS Fingerprint:   Signature: [8192:128:1:52:M1460,N,W8,N,N,S:.:Windows:?]
OS Fingerprint:   -> 104.236.16.69:80 (distance 0, link: ethernet/modem)

SRC: GET /bprocess.exe HTTP/1.1
SRC: Cache-Control: no-cache
SRC: Connection: Keep-Alive
SRC: Pragma: no-cache
SRC: User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
SRC: Host: 104.236.16.69
SRC:
SRC:
DST: HTTP/1.1 200 OK
DST: Date: Thu, 11 Jan 2018 03:38:02 GMT
DST: Server: Apache/2.4.18 (Ubuntu)
DST: Last-Modified: Tue, 09 Jan 2018 20:12:04 GMT
DST: ETag: "ca601-5625d873dad00"
DST: Accept-Ranges: bytes
DST: Content-Length: 828929
DST: Keep-Alive: timeout=5, max=100
DST: Connection: Keep-Alive
DST: Content-Type: application/x-msdos-program
DST:
DST: MZ.....................@.....................................................!..L.!This program cannot be run in DOS mode.
```

Source Alert transcript from the Squil analysis

Subsequently, the execution of this file likely led to the device connection to a crypto-mining domain at pool.minexmr.com. The alert also supports the reason for the slow-down of the device, consistent with the suspected mining activity, evidenced by the TCP connection to 188.165.214.95 on port 5555 Figures 5, 6, 7.

Figure 5 Packet capture of DNS query to the Crypto mining domain

Time	Source	Destination	Protocol	Length	Info
2025-02-20 03:43:35.650878	10.1.11.101	10.1.11.1	DNS	76	Standard query 0x7076 A pool.minexmr.com
2025-02-20 03:43:35.675716	10.1.11.1	10.1.11.101	DNS	364	Standard query response 0x7076 A pool.minexmr.com A 188.165.214.76 A 188.165.199.78 A

Source Extracted PCAP from the Squill alert

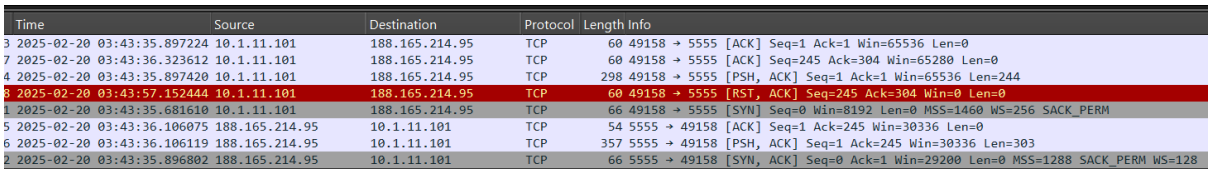
Figure 6 Cryptocurrency mining alert transcript from Squil

```
Sensor Name:    seconion-import-1
Timestamp:      2025-02-20 03:43:35
Connection ID:  .seconion-import-1_1396
Src IP:         10.1.11.101
Dst IP:         188.165.214.95
Src Port:               49158
Dst Port:               5555
OS Fingerprint: 10.1.11.101:49158 - Windows XP/2000 (RFC1323+, w+, tstamp-) [GENERIC]
OS Fingerprint:   Signature: [8192:128:1:52:M1460,N,W8,N,N,S:.:Windows:?]
OS Fingerprint:   -> 188.165.214.95:5555 (distance 0, link: ethernet/modem)

SRC: {"id":1,"jsonrpc":"2.0","method":"login","params":
{"login":"49CYQrmrqP2LyHQdMY26JGiq3M9cxFkiSU9PyfSEiXAPVR3kSWwj8Jdh2pJRPHV1ZTCQGwivo1a6494wNk7iasLpD2VrGrx","pass":"x","agent":"XMRig/2.4.2 (Windows NT 6.1;
Win64; x64) libuv/1.14.1 gcc/7.2.0"}}
SRC:
DST: {"id":1,"jsonrpc":"2.0","error":null,"result":{"id":"420086065750467","job":
{"blob":"0606c1badbd20500c87701067decf8faa567ae9e7f9577b3b2565a56900caefe52fe404a6626f300000000a694711710d37eb6b5e842505c82104eda75f8ab23079feaf185a20470917b640
DST:
```

Source Alert transcript from Squil analysis

Figure 7 Cryptocurrency mining TCP connection



	Time	Source	Destination	Protocol	Length	Info
3	2025-02-20 03:43:35.897224	10.1.11.101	188.165.214.95	TCP	60	49158 → 5555 [ACK] Seq=1 Ack=1 Win=65536 Len=0
7	2025-02-20 03:43:36.323612	10.1.11.101	188.165.214.95	TCP	60	49158 → 5555 [ACK] Seq=245 Ack=304 Win=65280 Len=0
4	2025-02-20 03:43:35.897420	10.1.11.101	188.165.214.95	TCP	298	49158 → 5555 [PSH, ACK] Seq=1 Ack=1 Win=65536 Len=244
8	2025-02-20 03:43:57.152444	10.1.11.101	188.165.214.95	TCP	60	49158 → 5555 [RST, ACK] Seq=245 Ack=304 Win=0 Len=0
1	2025-02-20 03:43:35.681610	10.1.11.101	188.165.214.95	TCP	66	49158 → 5555 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
5	2025-02-20 03:43:36.106075	188.165.214.95	10.1.11.101	TCP	54	5555 → 49158 [ACK] Seq=1 Ack=245 Win=30336 Len=0
6	2025-02-20 03:43:36.106119	188.165.214.95	10.1.11.101	TCP	357	5555 → 49158 [PSH, ACK] Seq=1 Ack=245 Win=30336 Len=303
2	2025-02-20 03:43:35.896802	188.165.214.95	10.1.11.101	TCP	66	5555 → 49158 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1288 SACK_PERM WS=128

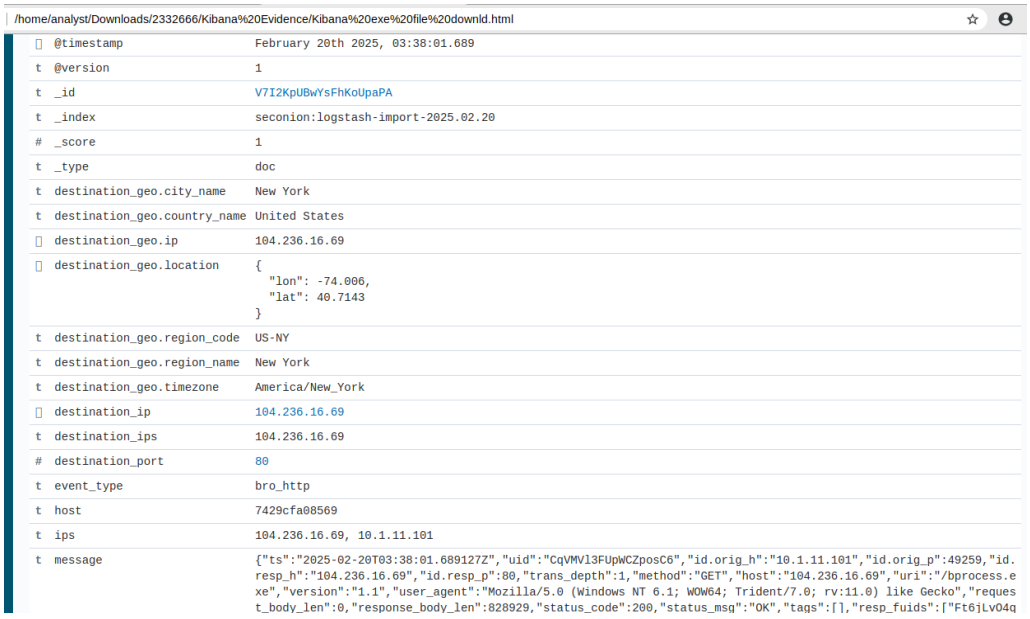
Source Extracted PCAP from the Squill alert

These Squill findings are crucial in understanding the timeline of the attack, with the screenshots of the alert events reinforcing the analysis.

4.2 Kibana Analysis

The Kibana logs provided a more detailed insight into the attack's timeline, showing a GET request for the "bprocess.exe" file from the victim's device with IP 10.1.11.101 to 104.236.16.69 at 03:38:01. The logs also confirmed that the request status was "200 OK," meaning the file was successfully downloaded. The Kibana logs also revealed the user's agent as "Mozilla/5.0," and the MIME type as "application/x-dosexec," which confirms the executable file's malicious nature. The logs also contained geo-location data, pinpointing the destination IP to New York, USA, providing valuable contextual information. Figure below.

Figure 8 bprocess.exe download information



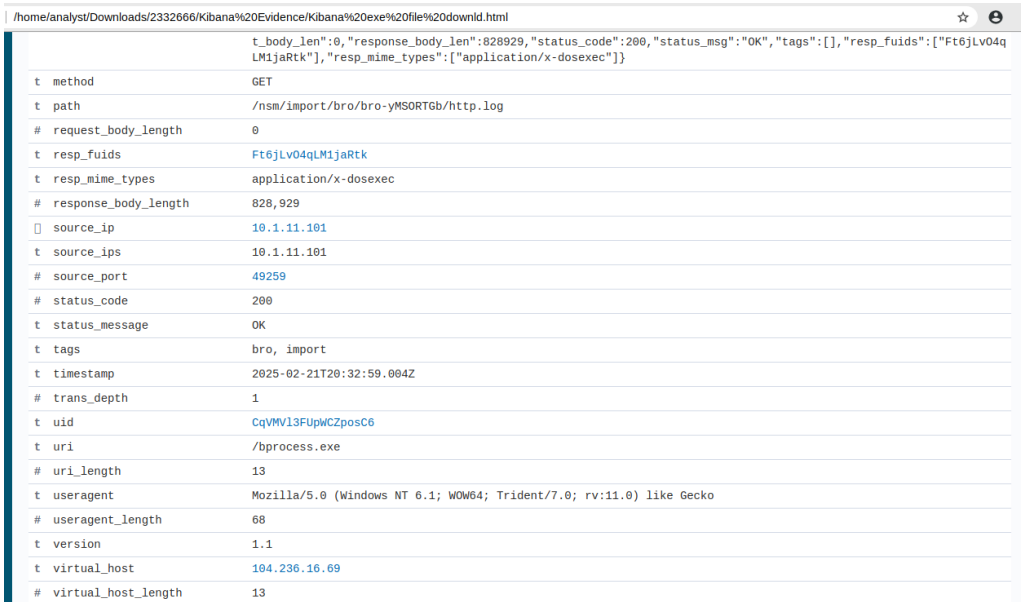
/home/analyst/Downloads/2332666/Kibana%20Evidence/Kibana%20exe%20file%20downld.html

□	@timestamp	February 20th 2025, 03:38:01.689
t	@version	1
t	_id	V7I2KpUBwYsFhKoUpaPA
t	_index	seconion:logstash-import-2025.02.20
#	_score	1
t	_type	doc
t	destination_geo.city_name	New York
t	destination_geo.country_name	United States
□	destination_geo.ip	104.236.16.69
□	destination_geo.location	{ "lon": -74.006, "lat": 40.7143 }
t	destination_geo.region_code	US-NY
t	destination_geo.region_name	New York
t	destination_geo.timezone	America/New_York
□	destination_ip	104.236.16.69
t	destination_ips	104.236.16.69
#	destination_port	80
t	event_type	bro_http
t	host	7429cfa08569
t	ips	104.236.16.69, 10.1.11.101
t	message	{"ts":"2025-02-20T03:38:01.689127Z","uid":"CqVMVl3FUpWCZposC6","id.orig_h":"10.1.11.101","id.orig_p":49259,"id.resp_h":"104.236.16.69","id.resp_p":80,"trans_depth":1,"method":"GET","host":"104.236.16.69","uri":"/bprocess.exe","version":"1.1","user_agent":"Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko","request_body_len":0,"response_body_len":828929,"status_code":200,"status_msg":"OK","tags":[],"resp_fuids":["Ft6jLvO4q

Source Kibana Logs

Thus, confirming that the GET request was sent to a server with a different time zone from the source device. The Kibana log shows the timestamp as 2025-02-21 20:32:59. Figure below

Figure 9 bprocess.exe download log information



Source Kibana Logs

These Kibana data aided in confirming the device's involvement in crypto mining, which supports the conclusions drawn from the Squill alerts.

5.0 Indicators of System Compromise

The investigation into the compromised system revealed several key indicators of compromise (IOCs) that point to a malware infection and unauthorized activity. These indicators include malicious IP addresses and domains, which provide strong evidence of the attack.

5.1 IP Addresses

188.227.16.131: This IP address was involved in the initial download of trojan files, specifically the .html and .swf files. It appears to be the source of the malicious payload.

104.236.16.69: This IP was used to deliver the "bprocess.exe" file, which was identified as a malicious executable. Following the download, this IP resolved to a crypto-mining domain, indicating that the compromised system was used for cryptocurrency mining.

10.1.11.1: This IP address seem to be the IP of pool.minexmr.com domain which is linked to cryptocurrency mining.

188.165.214.95: This IP address was involved in the final connection attempt to the device on port 5555, potentially used to mine cryptocurrency, contributing to the system’s slow performance.

5.2 File Hashes

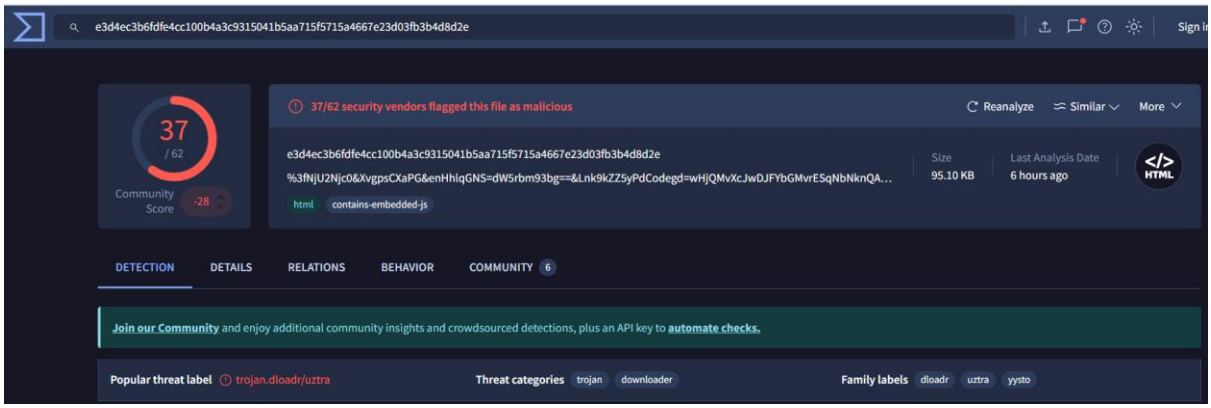
Below is the file hashes generated from the squil alerts investigation, these hashes are associated with trojan files that were downloaded and executed on the compromised machine.

.html file hash: 8828de70aa6b650797a6e0a2af379890ecd0fe7d

.swf file hash: 111df329c3be57e9fa7318f4f0345bbaec83ce46

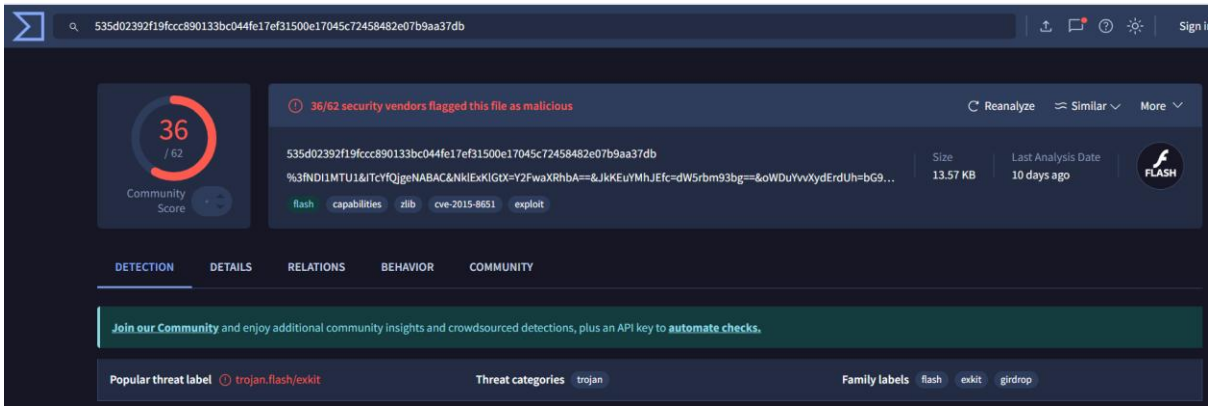
.exe file hash: e2efe60cb8bd67840f9a8bf92b57ade97e406a88

Figure 10 .html file hash against public virus domain



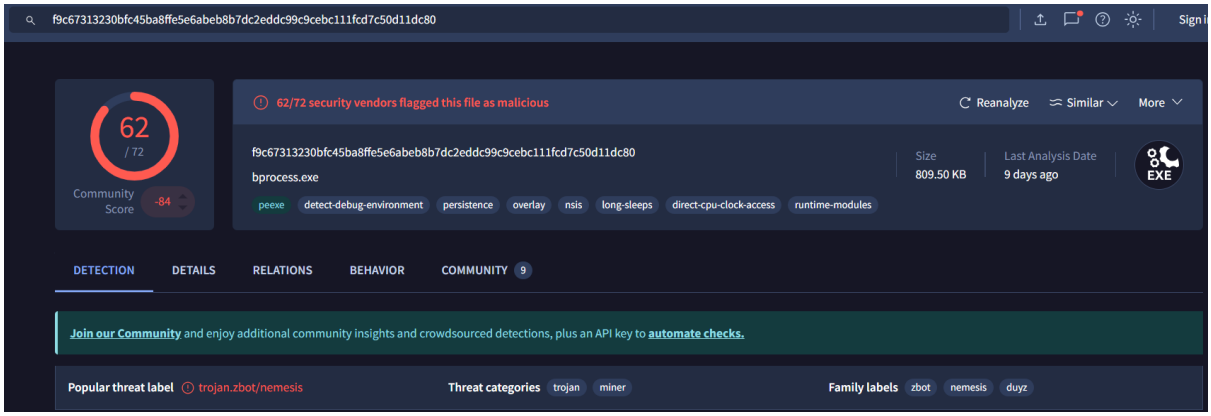
Source Virustotal.com

Figure 11 .swf file hash against public virus domain



Source Virustotal.com

Figure 12 .exe file hash against public virus domain



Source Virustotal.com

5.3 Domains

pool.minexmr.com: This domain is linked to cryptocurrency mining, as confirmed by the communication from the compromised device. This domain was used for crypto-mining activities, further solidifying the nature of the compromise.

6.0 Conclusion:

The investigation into the compromised system revealed a clear and coordinated attack involving multiple stages of exploitation. The initial signs of compromise came from a series of alerts captured by Squill, which identified suspicious GET requests from the target system. The first alerts indicated the download of trojan files, including a .html and a .swf file, which were initially deemed fictitious after their hash codes were checked against malware databases. However, the presence of these files marked the beginning of the attack.

Furthermore, the downloaded .exe file, bprocess.exe seemingly got executed which triggered further malicious activities. The execution led a connection to a cryptocurrency mining pool, which suggests that the attackers had taken control of the systems resources for the purpose of mining crypto currency. To understand the full extent of the attack, key indication of compromise like IP addresses, file hashes and domain connections were critically analysed. The existence of crypto mining related activities and the degradation of the device performance reinforced the confirmation that the system had been hijacked for unauthorised crypto mining operations

To sum up, the analysis uncovers a complex attack that involves the download of malware and the exploitation of system resources for cryptocurrency mining which prompted the need for investigation.

7.0 Recommendations

To mitigate future risks and prevent similar incidents, multiple key recommendations are proposed. First, endpoint security should be enhanced through the implementation of advanced malware protection, this will ensure stronger malware detection and file integrity monitoring. Also, a deep packet inspection to detect malicious traffic like a firewall should be enabled, that way only clean and reliable traffic goes through the system. Regular system and network scans should be scheduled to detect unusual activities before any system damage is dome. Additionally, all devices should be updated with the latest operating system version and patches to close any security vulnerabilities. Finally, the employees that uses these devices should also be trained to recognize malicious attachments that may lead to infections.

References

. *DOS MZ executable.*a [online]. Available from: https://en.wikipedia.org/wiki/DOS_MZ_executable#:~:text=Portable%20Executable,format%20and%20differs%20from%20it.

MITRE ATT&CK Framework.

ADOBE, *. What is an SWF file?* [online]. Available from: https://www.adobe.com/creativecloud/file-types/video/container/swf.html#:~:text=types%20to%20SWF-,What%20is%20an%20SWF%20file%3F,the%20format%20in%20late%202020.

KIM, S., PARK, K. and LU, C., 2022. A survey on network security for cyber–physical systems: From threats to resilient design. *IEEE Communications Surveys & Tutorials,* 24(3), pp. 1534–1573.

LOCKHEED MARTIN, *Cyber Kill Chain.*

SHINDE, O. et al. , 2024. A survey: Network attack detection and mitigation techniques. *International conference on smart computing and communication.* 2024. Springer, pp. 263–275.