2025

Evidence Portfolio: Exploit Kit and Cryptojacking Malware Incident

Robert Gordon University

Donna Naadu Botchway[redacted]

April 21, 2025

Table of Contents

1.0 Executive Summary. 1

2.0 Security Incident Report 2

2.1 Overview of Incident. 2

2.1.1 Reported Incident. 2

2.1.2 Severity of the Intrusion. 2

2.1.3 Tools Used for Investigation. 2

2.2 Intrusion Timeline. 2

2.3 Affected Devices and IPs 3

2.4. Intrusion Type and Severity. 4

2.5. Summary of Findings 4

3.0 Evidence and Analysis 5

3.1 IDS Alerts 5

3.2 Log Analysis 6

3.3 File Downloads & Hash Analysis. 7

3.4 Indicators of Compromise (IOCs) 7

3.4.1 IP Addresses 7

3.4.2 Domains 8

3.4.3 File Hashes (SHA-1) 8

3.5 IOC Evidence Snapshots (Visual Breakdown) 8

3.5.1 IOC 1 – IP: 188.227.16.131 (Sundown/Rig Exploit Kit Host) 8

3.5.2 IOC 2 – IP: 104.236.160.225 (saumottam.ru) 11

3.5.3 IOC 3 – IP: 104.236.16.69 (bprocess.exe) 14

3.5.4 IOC 4 – IP: 10.1.11.1 (DNS Activity) 19

3.5.5 IOC 5 – IP: 188.165.214.95 (pool.minexmr.com, Cryptocurrency Mining) 21

3.5.6 Suspicious Connections. 22

4.0 Cybersecurity Frameworks and Intrusion Methods 26

4.1 Background of Intrusion and Attack Methodology 26

4.1.1. Sundown and Rig Exploit Kits 26

4.1.2. Smoke Loader / Sharik Trojan 26

4.1.3. Cryptocurrency Miner 27

4.1.4 Attack Vector and Exploit 27

4.2 Relevant threat models 27
4.2.1 Diamond Model of Intrusion Analysis. 27
4.2.2 Cyber Kill Chain 28
4.2.3 MITRE ATT&CK Reference 28
4.3 Investigation Methodology 29
4.3.1 Approach 29
4.3.2 Evidence Collection 29
4.4 Analysis and Findings 30
4.4.1 Root Cause 30
4.4.2 Impact 30
4.4.3 Patterns 30
4.5 LESP Considerations 30
4.5.1 Legal and Ethical Implications 30
4.5.2. Social Considerations 31
4.5.3 Professional Responsibility in Breach Reporting 31
5.0 Recommendations 32
5.1 Immediate Fixes 32
5.2 Long-Term Strategies 32
5.3 Framework Alignment 32
5.3.1 Cyber Essentials (UK) 32
5.3.2 MITRE ATT&CK Aligned Preventive Controls 33
5.3.3 NIST Cybersecurity Framework (CSF) 34
6.0 Critical Reflection 35
6.1 What Went Well 35
6.2 What Didn't Work 35
7.0 References. 36

Table of Figures

Figure 1: Victim Host Details from NetworkMiner. 3
Figure 2: Table of IP Addresses Involved 4
Figure 3: Sguil Alert Overview 5
Figure 4: Kibana NIDS Alert Overview 5
Figure 5: Kibana showing DNS logs. 6
Figure 6: Kibana showing DNS Client and Server with a total of 12 DNS log. 6
Figure 7: Kibana showing HTTP-status-OK sites and the MIME type involved. 7
Figure 8: Sguil Alerts Triggered for 188.227.16.131 8
Figure 9: System overview for 188.227.16.131 during its connection to the victim host in NetworkMiner 9
Figure 10: Kibana showing connection overview for 188.227.16.131. 9
Figure 11: Kibana alerts for 188.227.16.131 show activity linked to Rig and Sundown Exploit Kits, likely delivered via redirect or malvertising. 9
Figure 12: Wireshark capture showing HTTP Traffic for 188.227.16.131 10
Figure 13: Confirmed Trojan Files Downloaded from 188.227.16.131 (Wireshark) 10
Figure 14:HTTP Traffic(x-msdownload) for 188.227.16.131 (Wireshark) 10
Figure 15: HTTP Stream (x-msdownload) for 188.227.16.131 (Wireshark) 10
Figure 16: File (x-msdownload) Downloaded from 188.227.16.131(Wireshark) 10
Figure 17: VirusTotal scan result for 188.227.16.131 showing its relations to malware (Smoke Loader, Rig EK, Monero miner). 11
Figure 18: Sguil alert (ET TROJAN Sharik/SmokeLoader) for 104.236.160.225 11
Figure 19: Kibana alerts for 104.236.160.225 show command-and-control (C2) activity with Smoke Loader infrastructure, indicating Sharik presence post-exploitation despite no binary capture. 11
Figure 20: : Host details for 104.236.160.225 12
Figure 21: Wireshark capture of HTTP Traffic and Files Downloaded from 104.236.160.225 linked to saumottam.ru 12
Figure 22: VirusTotal scan result for 104.236.160.225 linking it to saumottam.ru and a Rig EK and Smoke loader pcap file. 12
Figure 23: VirusTotal scan result for saumottam.ru confirming it as malicious and DNS replication to 104.236.160.225. 13
Figure 24: VirusTotal scan result for saumottam.ru showing relations to malware (Smoke Loader, Rig EK, Monero miner). 13
Figure 25: Sguil alerts for executable download from 104.236.16.69 14
Figure 26: Host details for 104.236.16.69 14
Figure 27: NetworkMiner showing parameters for the connection to 104.236.16.69 and the executable download. 14
Figure 28: HTTP GET Traffic for bprocess.exe from 104.236.16.69 (Wireshark) 15
Figure 29: File (bprocess.exe) downloaded from 104.236.16.69 (Wireshark) 15
Figure 30: Wireshark HTTP Stream for 104.236.16.69 showing GET bprocess.exe 15
Figure 31: Kibana showing connection overview for 104.236.16.69. 15
Figure 32: Kibana alerts for 104.236.16.69 showing an executable was downloaded from a dotted-quad IP, a known malware delivery tactic. 16

Figure 33: Kibana showing file (bprocess.exe) downloaded from 104.236.16.69 16
Figure 34:Kibana showing bprocess.exe downloaded from 104.236.16.69 17
Figure 35: VirusTotal scan result for 104.236.16.69, confirming it as malicious 17
Figure 36:VirusTotal scan result for 104.236.16.69 showing relations to malware (Smoke Loader, Rig EK, Monero miner). 17
Figure 37: VirusTotal scan result for bprocess.exe confirming it as malicious and connected to pool.minexmr.com (mining pool) 18
Figure 38: VirusTotal behaviour scan result for bprocess.exe showing DNS resolution to pool.minexmr.com (mining pool) 18
Figure 39: VirusTotal scan result for pool.minexmr.com, confirming it as malicious. 19
Figure 40: DNS-related alerts flagged in Sguil for 10.1.11.1 19
Figure 41: Kibana alert for 10.1.11.1 show a DNS request for Monero mining pool. 19
Figure 42: DNS Resolution logs for 10.1.11.1 from NetworkMiner 20
Figure 43: VirusTotal scan result for 10.1.11.1 showing its interaction with 4 known malicious files 20
Figure 44: : VirusTotal scan result (relations) for 10.1.11.1 20
Figure 45: Host details for 188.165.214.95 21
Figure 46: Sguil alert (ET POLICY Cryptocurrency Miner) triggered for 188.165.214.95 21
Figure 47: VirusTotal scan result for 188.165.214.95, confirming it as malicious. 21
Figure 48: VirusTotal scan result (relations) for 188.165.214.95 22
Figure 49: Host details for 23.34.134.22 showing Microsoft 22
Figure 50: Sguil Alert Triggered for 23.34.132.22_microsoft (likely false positive or malware behaviour) 23
Figure 51: NetworkMiner showing HTTP Cookies for 23.34.132.22 (Microsoft) 23
Figure 52: HTTP Traffic for 23.34.132.22_microsoft (Wireshark) 23
Figure 53: HTTP Transcript for 23.34.132.22 (Microsoft). 24
Figure 54: Kibana alert for 23.34.132.22 indicates a possible connectivity check via Microsoft by the Smoke Loader Trojan, a common tactic used by malware to blend into legitimate traffic. .. 24
Figure 55: VirusTotal scan result for 23.34.132.22 , confirming it as safe. 24
Figure 56: VirusTotal scan for 204.79.197.200 (Bing) – clean (0/94) but shows connections to 8 malicious files and Community score: -136. 25
Figure 57: VirusTotal scan result for 204.79.197.200_bing showing it communicates with several malicious files. 25
Figure 58: Security Recommendations Mapped to MITRE ATT&CK Framework 33
Figure 59: Secure Network Design 34

1.0 Executive Summary.

This evidence portfolio details a malware incident on 20 February 2025, affecting a Windows 7 workstation in the Client Outreach department. The investigation began after a staff member, Charlie, reported performance issues and pop-up messages. The helpdesk agent, Lola, escalated the issue upon signs of a malware infection.

The investigation confirmed the system was compromised via the Sundown Exploit Kit, which redirected to Rig Exploit Kit infrastructure exploiting unpatched software (CVE-2015-8651 in Adobe Flash) after a visit to a malicious website. This led to the installation of Smoke Loader trojans and a Monero cryptocurrency miner which hijacked system resources and communicated with malicious servers, including a mining pool. Despite lasting only seven minutes, the intrusion bypassed real-time detection, exposing weaknesses in endpoint protection and network visibility.

Analysis using Security Onion, VirusTotal, and threat intelligence frameworks identified several indicators of compromise, including suspicious IP addresses, file hashes, and domains. The attack was mapped to Cyber Kill Chain and MITRE ATT&CK techniques such as T1189 (Drive-by Compromise) and T1496 (Resource Hijacking).

The root cause was traced to outdated systems and inadequate monitoring. Although the helpdesk response was effective, delayed threat detection highlighted the need for improved automated alerting. Immediately, the infected system must be isolated and fully scanned.

To prevent recurrence, the organization must prioritize system patching, improve endpoint detection and response, implement network-based threat detection, and user awareness. Adopting industry frameworks like NIST CSF and MITRE ATT&CK will improve security posture and response capabilities. This incident shows the importance of having updated systems and layered defences against evolving threats like exploit kits, trojans, and crypto-mining malware.

2.0 Security Incident Report

2.1 Overview of Incident.

2.1.1 Reported Incident.

On 20th February 2025 at 09:30 AM, the first-line helpdesk received a report from Charlie, a staff member from the Client Outreach department, regarding unusual behaviour on their workstation. The user described the system as "acting funny" with symptoms running slowly, unresponsive applications, and the appearance of potential pop-up messages. These issues began shortly after browsing the internet. The helpdesk agent, Lola, carried out basic troubleshooting and recorded the incident under Ticket Number 12345.

2.1.2 Severity of the Intrusion.

Given the potential signs of malware infection like pop-ups, system lag, and suspicious behaviour, the incident was classified as high priority and escalated. Early indicators suggested a possible exploit-driven malware infection.

2.1.3 Tools Used for Investigation.

The following cybersecurity tools and platforms were used during the incident investigation:

- **Security Onion Suite specifically:**
    - **Network Miner** for passive network traffic analysis and evidence extraction.
    - **Wireshark** to inspect packet and protocols.
    - **Sguil** for reviewing and correlating alerts from Snort.
    - **Kibana** to visualize network activity logs.
- **VirusTotal** to analyse the reputation of files, IPs or domains found.

2.2 Intrusion Timeline.

Key Events:

- **03:36:39 AM** – Victim visits a Sundown Exploit Kit landing page at 188.227.16.131, which likely redirects to Rig Exploit Kit. (*Pg.8* - ET Alerts: Sundown EK RIP Landing, SIDs: 51306)
- **03:36:40 AM** – Multiple HTTP GET requests trigger the download of trojan-laced files (.html, .swf), confirmed malicious by VirusTotal and linked to Rig Exploit Kit and Monero coin miner. A .x-msdownload file was also downloaded but flagged safe. (*Pg.10* - ET Alerts: Sundown EK, Rig EK, SIDs: 5.1320, 5.1331, 5.1342)
- **03:36:43 AM** – Outdated Flash alert triggered (SID: 51343) as part of the ongoing Rig Exploit Kit activity, flagging the outdated Flash vulnerability as the entry point for the malware delivery.
- **03:37:22 AM** – Victim accessed saumottam.ru (104.236.160.225). From VirusTotal , the domain is flagged as malicious and known for malware delivery and Monero coin mining. (*Pg.11* - ET alerts: Trojan Sharik/Smoke — SIDs: 5.1347, 5.1349)

- **03:37:55 AM** - Visit to www.microsoft.com (23.34.132.22), including Visual Studio. It has "ET alert: Possible Sharik Trojan — SID: 5.1359" but was flagged safe by VirusTotal.
- **03:38:01 AM** – bprocess.exe downloaded from 104.236.16.69, confirmed by VirusTotal as malicious and communicates with pool.minexmr.com . The IP is also associated with malware delivery. (*Pg.14* - ET alerts: Executable Download, Info Suspicious, EXE Policy — SIDs: 5.1364, 5.1365, 5.1378)
- **03:43:35 AM** – DNS request made to internal IP 10.1.11.1, triggering a policy alert. pool.minexmr.com identified as a malicious mining pool communicating with several flagged IPs. (*Pg.19* - ET POLICY DNS request for monero mining pool— SID: 5.1395)
- **03:43:35 AM** - Connection established to 188.165.214.95. VirusTotal classified this IP as malicious and associated with cryptocurrency mining activity. The event (SID:5.1396) was flagged under ET POLICY Cryptocurrency Miner and policy violation alerts.
- **09:30 AM** – Helpdesk receives a call from Charlie reporting performance issues.

Duration:

The intrusion occurred in a short but intense window from 03:36 AM to 03:43 AM on February 20, 2025, and went undetected in real-time, raising concerns about endpoint monitoring and real-time alert response.

2.3 Affected Devices and IPs

Impacted Asset:

- **Victim Device**: IP:10.1.11.101, Windows 7 machine with Internet Explorer 11 browser (Figure 1)

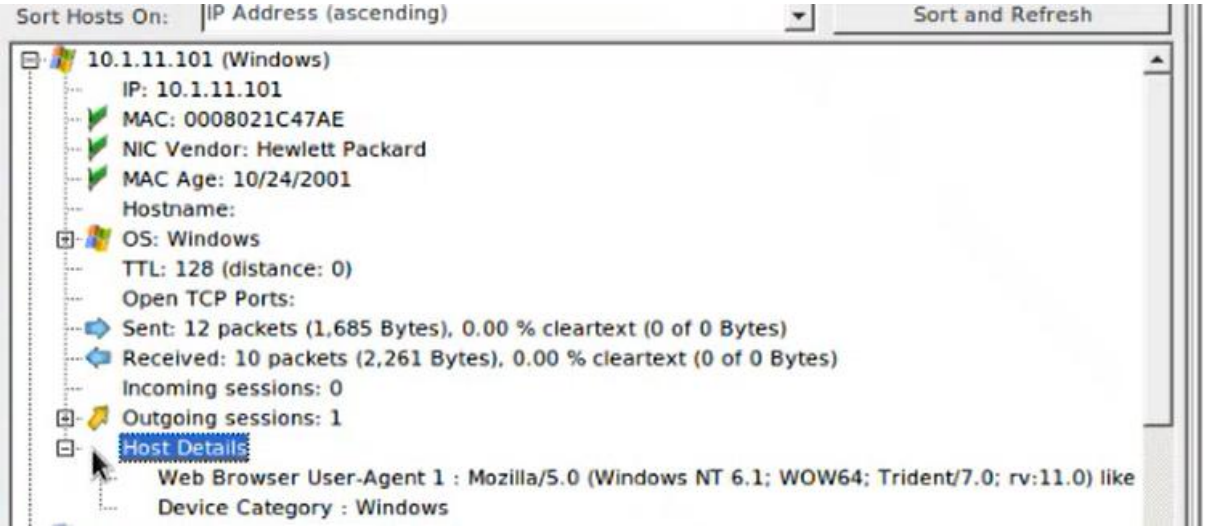


Figure 1: Victim Host Details from NetworkMiner.

IP Addresses Involved

IP Address	Domain/Port	VirusTotal Detection	Activity Summary
188.227.16.131	N/A (Russia) TCP 80	Malicious	Hosts Sundown/Rig Exploit Kit payloads (index.html, .swf) linked to trojan activity, *Smoke Loader* and *Monero* coin miner.
104.236.16.69	N/A (US) TCP 80	Malicious	Delivered bprocess.exe which is associated with Smoke Loader and pool.minexmr.com.
104.236.160.225	saumottam.ru TCP 80	Malicious	IP marked safe, but connects to a malicious domain linked to Rig Exploit Kit and Monero coin miner.
188.165.214.95	N/A (France) TCP 5555	Malicious	Cryptocurrency miner activity. Triggered policy violation and miner alerts
23.34.132.22	www.microsoft.com TCP 80	Safe	Normal traffic observed like Visual Studio visit and cookies exchange.
204.79.197.200	www.bing.com TCP 80	Suspicious	Communicates with malicious domains, flagged by VirusTotal
10.1.11.1	Internal TCP 55	Suspicious	Multiple DNS activity. VirusTotal shows communication with 4 malicious files.

Figure 2: Table of IP Addresses Involved

2.4. Intrusion Type and Severity.

Type: Exploit Kit (Sundown/Rig-EK), Trojan Activity, Executable Download from Dotted-Quad Hosts, Cryptocurrency Mining

Severity: Medium to High

- Known malware families (Smoke Loader, Monero Coin Miner) were successfully downloaded and executed on the system.
- Coin-mining activity detected (MITRE T1496 – Resource Hijacking)
- Communications with known C2 infrastructure and historical malware hosting servers

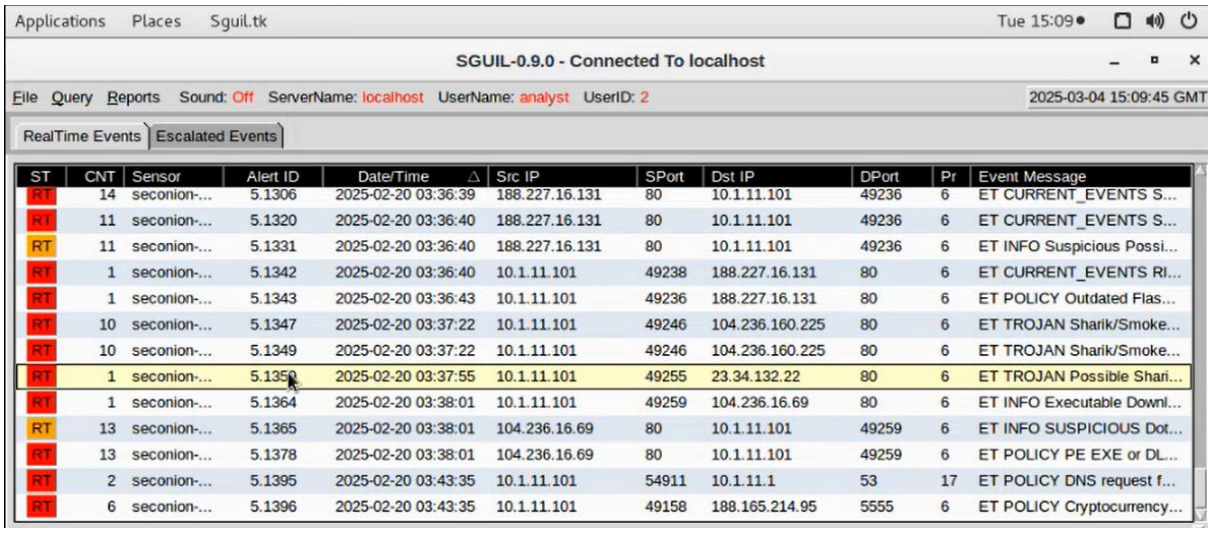
2.5. Summary of Findings

The investigation found that the Sundown EK initiated the attack and redirected to Rig Exploit Kit which delivered malware, leading to the download of a crypto miner and trojans. The infected system showed signs of resource hijacking for cryptomining and connected to malicious servers. The attack lasted about 7 minutes but was undetected in real-time, exposing weaknesses in monitoring and endpoint security. Immediate isolation and scanning of affected systems for persistence, along with improved detection rules, are required.

3.0 Evidence and Analysis

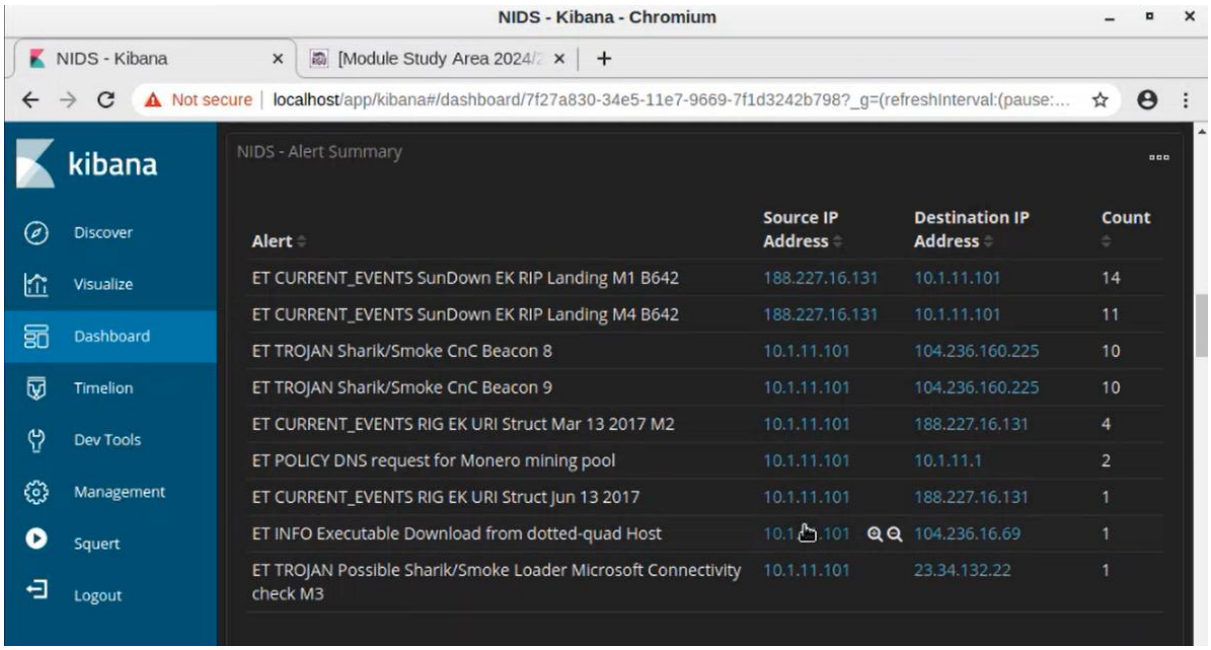
3.1 IDS Alerts

Multiple alerts were generated indicating suspicious and malicious activities on the 10.1.11.101 machine. The figures below show Sguil and Kibana alerts, triggered pointing to trojan activity and policy violations.



ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	14	seconion-...	5.1306	2025-02-20 03:36:39	188.227.16.131	80	10.1.11.101	49236	6	ET CURRENT_EVENTS S...
RT	11	seconion-...	5.1320	2025-02-20 03:36:40	188.227.16.131	80	10.1.11.101	49236	6	ET CURRENT_EVENTS S...
RT	11	seconion-...	5.1331	2025-02-20 03:36:40	188.227.16.131	80	10.1.11.101	49236	6	ET INFO Suspicious Possi...
RT	1	seconion-...	5.1342	2025-02-20 03:36:40	10.1.11.101	49238	188.227.16.131	80	6	ET CURRENT_EVENTS RI...
RT	1	seconion-...	5.1343	2025-02-20 03:36:43	10.1.11.101	49236	188.227.16.131	80	6	ET POLICY Outdated Flas...
RT	10	seconion-...	5.1347	2025-02-20 03:37:22	10.1.11.101	49246	104.236.160.225	80	6	ET TROJAN Sharik/Smoke...
RT	10	seconion-...	5.1349	2025-02-20 03:37:22	10.1.11.101	49246	104.236.160.225	80	6	ET TROJAN Sharik/Smoke...
RT	1	seconion-...	5.1350	2025-02-20 03:37:55	10.1.11.101	49255	23.34.132.22	80	6	ET TROJAN Possible Shari...
RT	1	seconion-...	5.1364	2025-02-20 03:38:01	10.1.11.101	49259	104.236.16.69	80	6	ET INFO Executable Downl...
RT	13	seconion-...	5.1365	2025-02-20 03:38:01	104.236.16.69	80	10.1.11.101	49259	6	ET INFO SUSPICIOUS Dot...
RT	13	seconion-...	5.1378	2025-02-20 03:38:01	104.236.16.69	80	10.1.11.101	49259	6	ET POLICY PE EXE or DL...
RT	2	seconion-...	5.1395	2025-02-20 03:43:35	10.1.11.101	54911	10.1.11.1	53	17	ET POLICY DNS request f...
RT	6	seconion-...	5.1396	2025-02-20 03:43:35	10.1.11.101	49158	188.165.214.95	5555	6	ET POLICY Cryptocurrency...

Figure 3: Sguil Alert Overview



Alert	Source IP Address	Destination IP Address	Count
ET CURRENT_EVENTS SunDown EK RIP Landing M1 B642	188.227.16.131	10.1.11.101	14
ET CURRENT_EVENTS SunDown EK RIP Landing M4 B642	188.227.16.131	10.1.11.101	11
ET TROJAN Sharik/Smoke CnC Beacon 8	10.1.11.101	104.236.160.225	10
ET TROJAN Sharik/Smoke CnC Beacon 9	10.1.11.101	104.236.160.225	10
ET CURRENT_EVENTS RIG EK URI Struct Mar 13 2017 M2	10.1.11.101	188.227.16.131	4
ET POLICY DNS request for Monero mining pool	10.1.11.101	10.1.11.1	2
ET CURRENT_EVENTS RIG EK URI Struct Jun 13 2017	10.1.11.101	188.227.16.131	1
ET INFO Executable Download from dotted-quad Host	10.1.11.101	104.236.16.69	1
ET TROJAN Possible Sharik/Smoke Loader Microsoft Connectivity check M3	10.1.11.101	23.34.132.22	1

Figure 4: Kibana NIDS Alert Overview

3.2 Log Analysis

Log reviews revealed DNS queries and HTTP communications with multiple malicious domains, key findings:

- DNS query logs show that the DNS server 10.1.11.1 resolved domains related to pool.minexmr.com and saumottam.ru (Figure 5, Figure 6).
- Filtering HTTP responses with status code 200 (OK), revealed successful connections to known malicious hosts such as 188.227.16.131 and 104.236.16.69, indicating file transfers (Figure 7).

DNS - Queries

Query	Count
saumottam.ru	3
pool.minexmr.com	2
www.bing.com	2
www.microsoft.com	2
go.microsoft.com	1
msdn.microsoft.com	1
www.visualstudio.com	1

DNS - Answers

Answer	Count
104.236.160.225	3
176.9.53.68	2
176.9.63.166	2
188.165.199.78	2
188.165.214.76	2
188.165.214.95	2
204.79.197.200	2
37.59.43.136	2
37.59.44.93	2
37.59.51.212	2

Figure 5: Kibana showing DNS logs.

DNS - Client

Client	Count
10.1.11.101	12

DNS - Server

Server	Count
10.1.11.1	12

Figure 6: Kibana showing DNS Client and Server with a total of 12 DNS log.

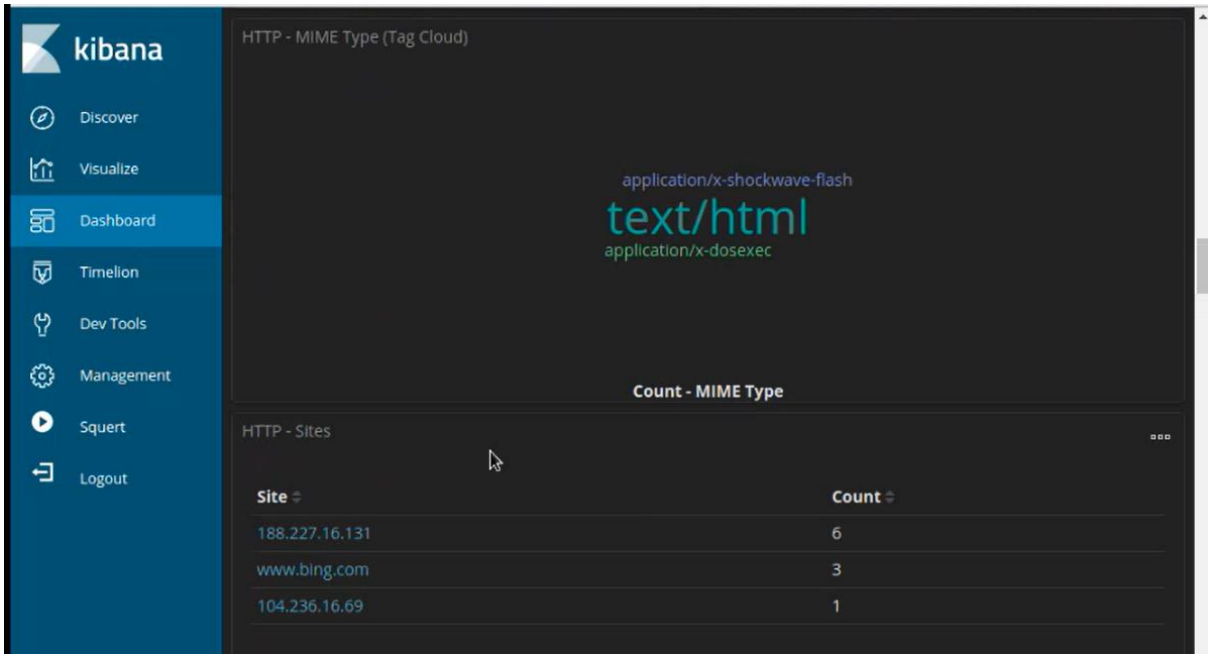


Figure 7: Kibana showing HTTP-status-OK sites and the MIME type involved.

3.3 File Downloads & Hash Analysis.

The table below shows downloaded files, extracted from NetworkMiner, Wireshark, and Kibana filter. VirusTotal was used to verify each file's classification.

Time	SHA1 Hash	Filename	Source IP	Size (Bytes)	VirusTotal Status
3:36 AM	8828de70aa6b650797a6e0a2af379890ecd0fe7d	index.html	188.227.16.131	97,378	Unsafe (Trojan)
3:36 AM	111df329c3be57e9fa7318f4f0345bbaec83ce46	index.html.swf	188.227.16.131	13,894	Unsafe
3:36 AM	1dfa7db2fa604fadbf2a294c9bf2ab954e52f091	index.html.x-msdownload	188.227.16.131	108,009	Safe
3:37 AM	ad14e9e88b59c52e35740b433c5468d48b029557	index[1].html	104.236.160.225	400	Safe
3:38 AM	e2efe60cb8bd67840f9a8bf92b57ade97e406a88	bprocess[1].exe	104.236.16.69	828,929	Unsafe (Miner)

3.4 Indicators of Compromise (IOCs)

The observed behaviours map to MITRE techniques such as T1189 (Drive-by Compromise), and T1496 (Resource Hijacking).

The main IOCs are as follows.

3.4.1 IP Addresses

- 188.227.16.131 – Sundown/Rig Exploit Kit host

- 104.236.160.225 – saumottam.ru related to Rig Exploit Kit, Smoke Loader and coin mining.
- 104.236.16.69 - Delivered malware
- 188.165.214.95 – Mining pool
- All IPs associated with pool.minexmr.com - Cryptocurrency mining infrastructure

3.4.2 Domains

- saumottam.ru – Related to malicious activity
- pool.minexmr.com – Cryptocurrency mining domain linked to cryptojacking campaigns

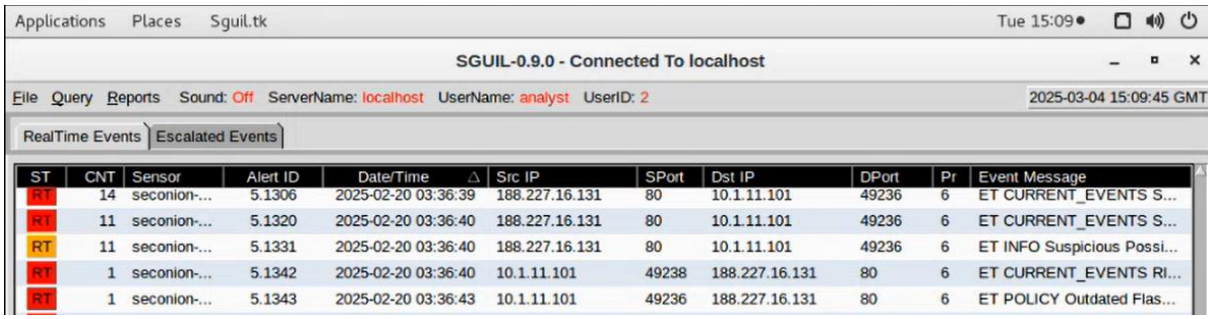
3.4.3 File Hashes (SHA-1)

- e2efe60cb8bd67840f9a8bf92b57ade97e406a88 (bprocess.exe) – Mining malware
- 8828de70aa6b650797a6e0a2af379890ecd0fe7d (index.html) - Trojan
- 111df329c3be57e9fa7318f4f0345bbaec83ce46 (.swf exploit) -Malicious Flash File

3.5 IOC Evidence Snapshots (Visual Breakdown)

This section provides visual evidence captured during the investigation, supporting the Indicators of Compromise (IOCs). The screenshots include IDS alerts, traffic analysis, file downloads, and VirusTotal reputation scans.

3.5.1 IOC 1 – IP: 188.227.16.131 (Sundown/Rig Exploit Kit Host)



ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	14	seconion-...	5.1306	2025-02-20 03:36:39	188.227.16.131	80	10.1.11.101	49236	6	ET CURRENT_EVENTS S...
RT	11	seconion-...	5.1320	2025-02-20 03:36:40	188.227.16.131	80	10.1.11.101	49236	6	ET CURRENT_EVENTS S...
RT	11	seconion-...	5.1331	2025-02-20 03:36:40	188.227.16.131	80	10.1.11.101	49236	6	ET INFO Suspicious Possi...
RT	1	seconion-...	5.1342	2025-02-20 03:36:40	10.1.11.101	49238	188.227.16.131	80	6	ET CURRENT_EVENTS RI...
RT	1	seconion-...	5.1343	2025-02-20 03:36:43	10.1.11.101	49236	188.227.16.131	80	6	ET POLICY Outdated Flas...

Figure 8: Sguil Alerts Triggered for 188.227.16.131

Alerts matched both Sundown and Rig Exploit Kit signatures involving 188.227.16.131, likely due to the attacker reusing or mimicking these infrastructures. However, the payload behaviour (Smoke Loader and cryptomining) aligns more closely with Rig Exploit Kit, commonly seen in 2017 to 2018.

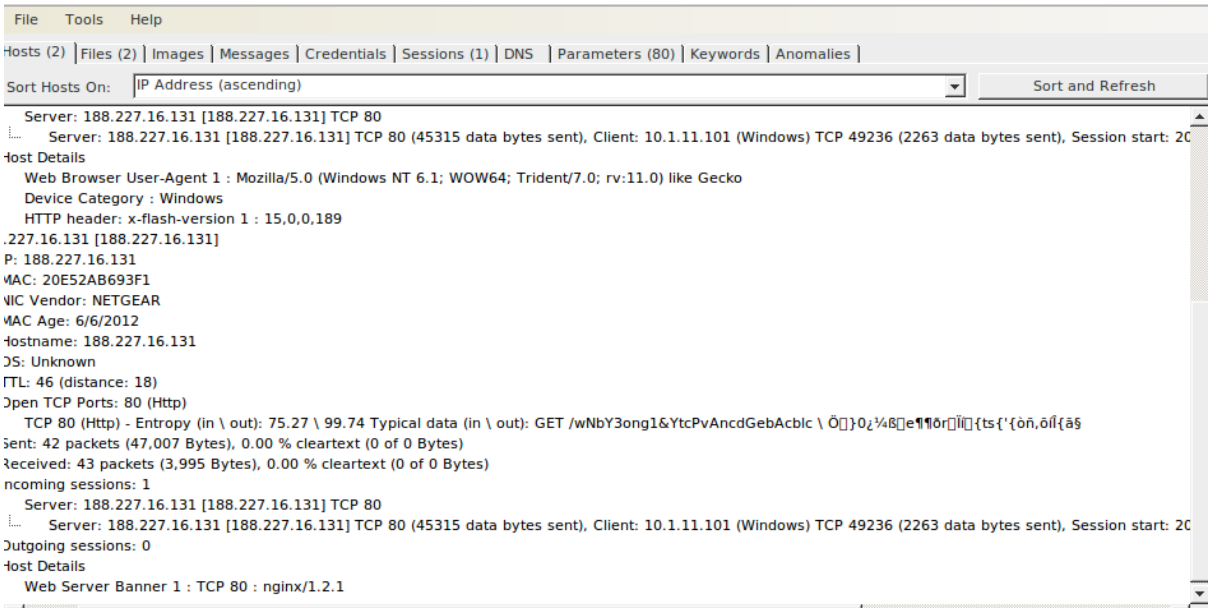


Figure 9: System overview for 188.227.16.131 during its connection to the victim host in NetworkMiner

The HTTP header reveals x-flash-version: 15,0,0,189, confirming that the client browser had Adobe Flash Player v15 installed—an outdated version often targeted by Rig Exploit Kit.

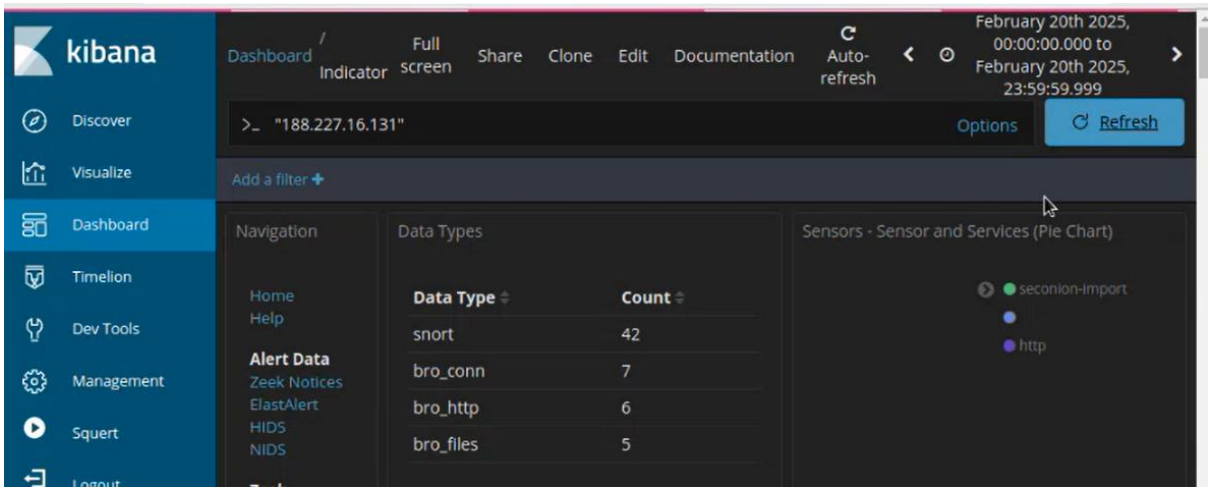


Figure 10: Kibana showing connection overview for 188.227.16.131.

This IP triggered 42 Snort alerts and was logged by Zeek with 7 connections, 5 file transfers, and 6 HTTP requests.

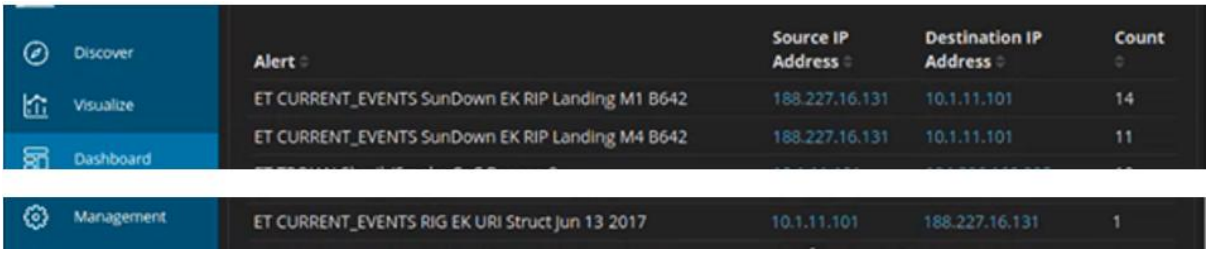
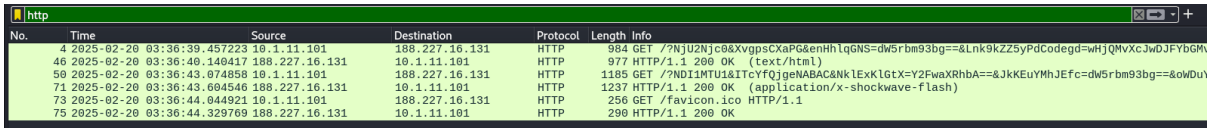
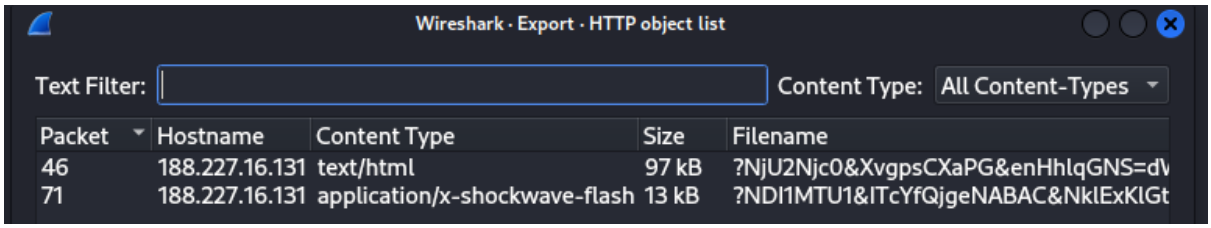


Figure 11: Kibana alerts for 188.227.16.131 show activity linked to Rig and Sundown Exploit Kits, likely delivered via redirect or malvertising.



No.	Time	Source	Destination	Protocol	Length	Info
4	2025-02-20 03:36:39.457223	10.1.11.101	188.227.16.131	HTTP	984	GET /?NjU2Njc0&XvgpsCXaPG&enHhlqGNS=dW5rbm93bg==&Lnk9kZZ5yPdCodegd=wHjQMvXcJwDJFYbGM
46	2025-02-20 03:36:40.140417	188.227.16.131	10.1.11.101	HTTP	977	HTTP/1.1 200 OK (text/html)
50	2025-02-20 03:36:43.074858	10.1.11.101	188.227.16.131	HTTP	1185	GET /?NDI1MTU1&ITcYfQjgeNABAC&NklExKlGtX=Y2FwaXRhbA==&JkKEuYMhJEfc=dW5rbm93bg==&oWDu
71	2025-02-20 03:36:43.604546	188.227.16.131	10.1.11.101	HTTP	1237	HTTP/1.1 200 OK (application/x-shockwave-flash)
73	2025-02-20 03:36:44.044921	10.1.11.101	188.227.16.131	HTTP	256	GET /favicon.ico HTTP/1.1
75	2025-02-20 03:36:44.329769	188.227.16.131	10.1.11.101	HTTP	290	HTTP/1.1 200 OK

Figure 12: Wireshark capture showing HTTP Traffic for 188.227.16.131

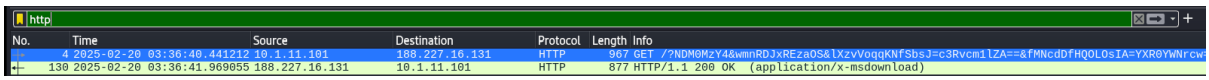


Wireshark · Export · HTTP object list

Text Filter: Content Type: All Content-Types

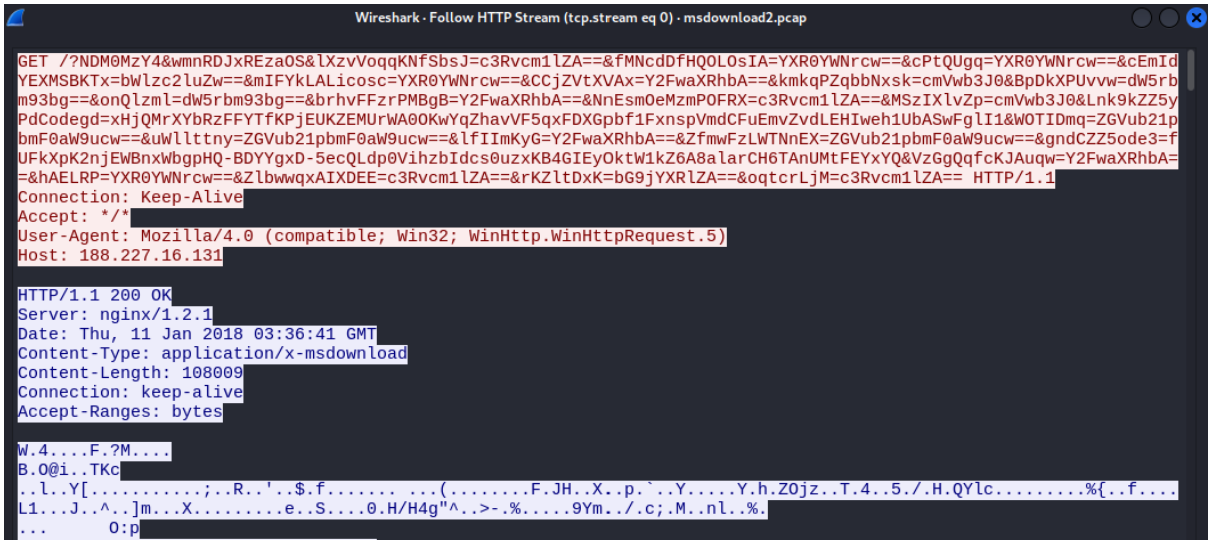
Packet	Hostname	Content Type	Size	Filename
46	188.227.16.131	text/html	97 kB	?NjU2Njc0&XvgpsCXaPG&enHhlqGNS=dV
71	188.227.16.131	application/x-shockwave-flash	13 kB	?NDI1MTU1&ITcYfQjgeNABAC&NklExKlGt

Figure 13: Confirmed Trojan Files Downloaded from 188.227.16.131 (Wireshark)



No.	Time	Source	Destination	Protocol	Length	Info
4	2025-02-20 03:36:40.441212	10.1.11.101	188.227.16.131	HTTP	967	GET /?NDM0MzY4&wmnRDJxREzaOS&lXzvVoqqKNfSbsJ=c3Rvcm1lZA==&fMNcdDfHQOLOsIA=YXR0YWNrcw
130	2025-02-20 03:36:41.969055	188.227.16.131	10.1.11.101	HTTP	877	HTTP/1.1 200 OK (application/x-msdownload)

Figure 14:HTTP Traffic(x-msdownload) for 188.227.16.131 (Wireshark)



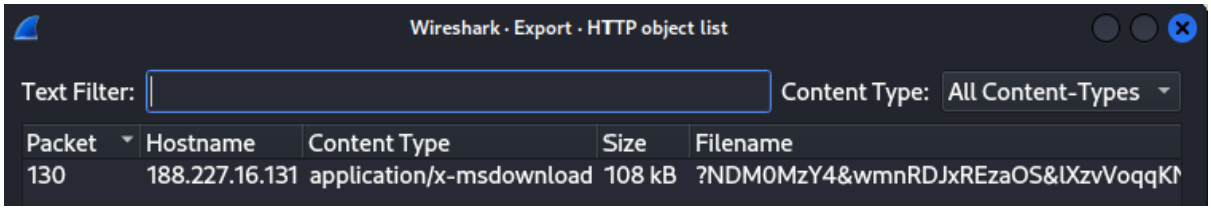
Wireshark · Follow HTTP Stream (tcp.stream eq 0) · msdownload2.pcap

```
GET /?NDM0MzY4&wmnRDJxREzaOS&lXzvVoqqKNfSbsJ=c3Rvcm1lZA==&fMNcdDfHQOLOsIA=YXR0YWNrcw==&cPtQUgq=YXR0YWNrcw==&cEmId
YEXMSBKTx=bWlzc2luZw==&mIFYkLALicosc=YXR0YWNrcw==&CCjZVtXVAx=Y2FwaXRhbA==&kmkqPZqbbNxsk=cmVwb3J0&BpDkXPUvvw=dW5rb
m93bg==&onQlzml=dW5rbm93bg==&brhvFFzrPMBgB=Y2FwaXRhbA==&NnEsmOeMzmPOFRX=c3Rvcm1lZA==&MSzIXlvZp=cmVwb3J0&Lnk9kZZ5y
PdCodegd=xHjQMrXYbRzFFYTfKPjEUKZEMUrWA0OKwYqZhavVF5qxFDXGpbf1FxnspVmdCFuEmvZvdLEHIweh1UbASwFglI1&WOTIDmq=ZGVub21p
bmF0aW9ucw==&uWllttny=ZGVub21pbmF0aW9ucw==&lfIImKyG=Y2FwaXRhbA==&ZfmwFzLWTNnEX=ZGVub21pbmF0aW9ucw==&gndCZZ5ode3=f
UFkXpK2njEWBnxWbgpHQ-BDYYgxD-5ecQLdp0VihzbIdcs0uzxKB4GIEyOktW1kZ6A8alarCH6TAnUMtFEYxYQ&VzGgQqfcKJAuqw=Y2FwaXRhbA=
=&hAELRP=YXR0YWNrcw==&ZlbwwqxAIXDEE=c3Rvcm1lZA==&rKZltDxK=bG9jYXRlZA==&oqtcrLjM=c3Rvcm1lZA== HTTP/1.1
Connection: Keep-Alive
Accept: */*
User-Agent: Mozilla/4.0 (compatible; Win32; WinHttp.WinHttpRequest.5)
Host: 188.227.16.131

HTTP/1.1 200 OK
Server: nginx/1.2.1
Date: Thu, 11 Jan 2018 03:36:41 GMT
Content-Type: application/x-msdownload
Content-Length: 108009
Connection: keep-alive
Accept-Ranges: bytes

W.4....F.?M....
B.O@i..TKc
..l..Y[..........;..R..'..$.f....... ...(........F.JH..X..p.`..Y.....Y.h.ZOjz..T.4..5./.H.QYlc.........%{..f....
L1...J..^..]m...X........e..S....0.H/H4g"^..>-.%.....9Ym../.c;.M..nl..%.
...      O:p
```

Figure 15: HTTP Stream (x-msdownload) for 188.227.16.131 (Wireshark)



Wireshark · Export · HTTP object list

Text Filter: Content Type: All Content-Types

Packet	Hostname	Content Type	Size	Filename
130	188.227.16.131	application/x-msdownload	108 kB	?NDM0MzY4&wmnRDJxREzaOS&lXzvVoqqKN

Figure 16: File (x-msdownload) Downloaded from 188.227.16.131(Wireshark)

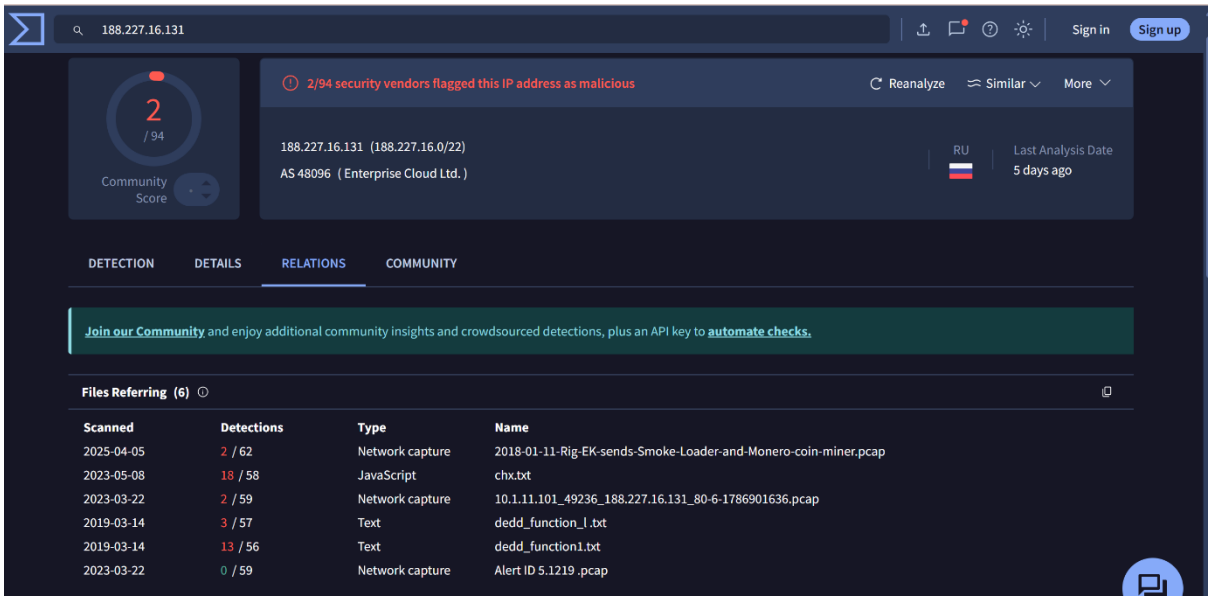


Figure 17: VirusTotal scan result for 188.227.16.131 showing its relations to malware (Smoke Loader, Rig EK, Monero miner).

3.5.2 IOC 2 – IP: 104.236.160.225 (saumottam.ru)

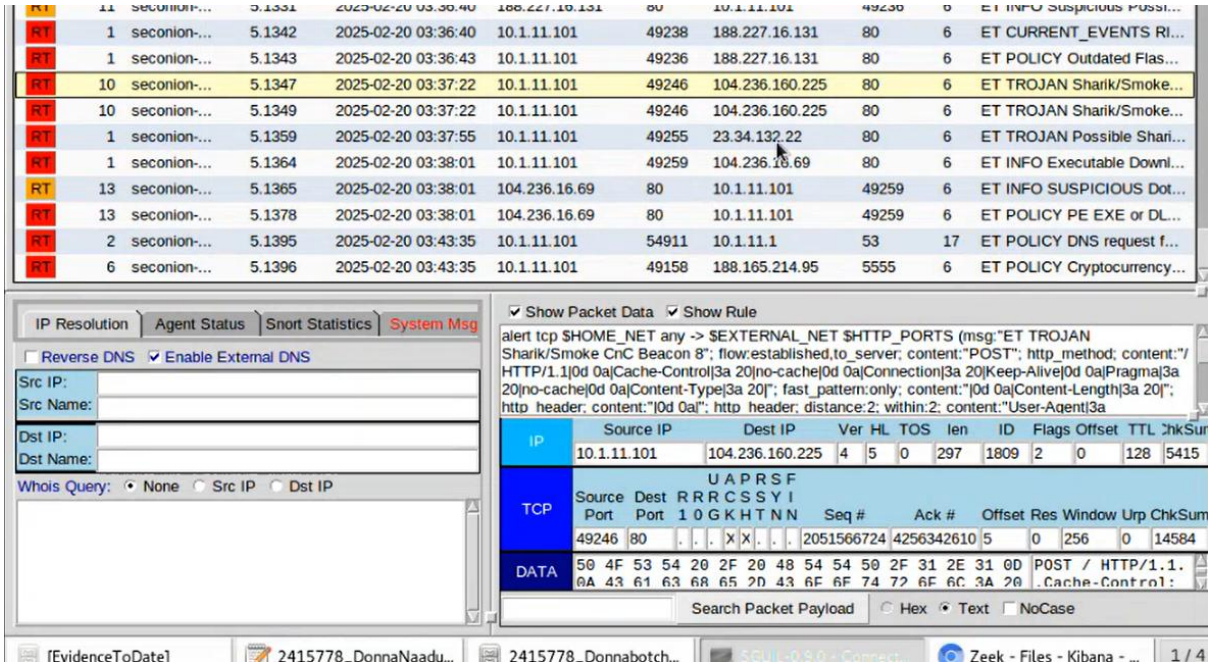


Figure 18: Sguil alert (ET TROJAN Sharik/SmokeLoader) for 104.236.160.225

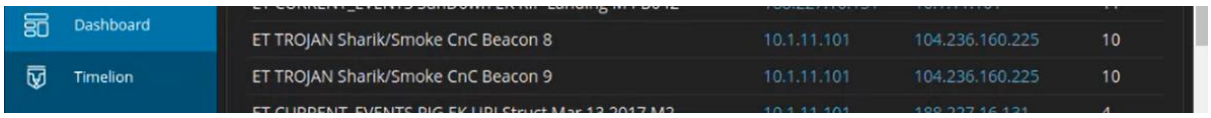


Figure 19: Kibana alerts for 104.236.160.225 show command-and-control (C2) activity with Smoke Loader infrastructure, indicating Sharik presence post-exploitation despite no binary capture.

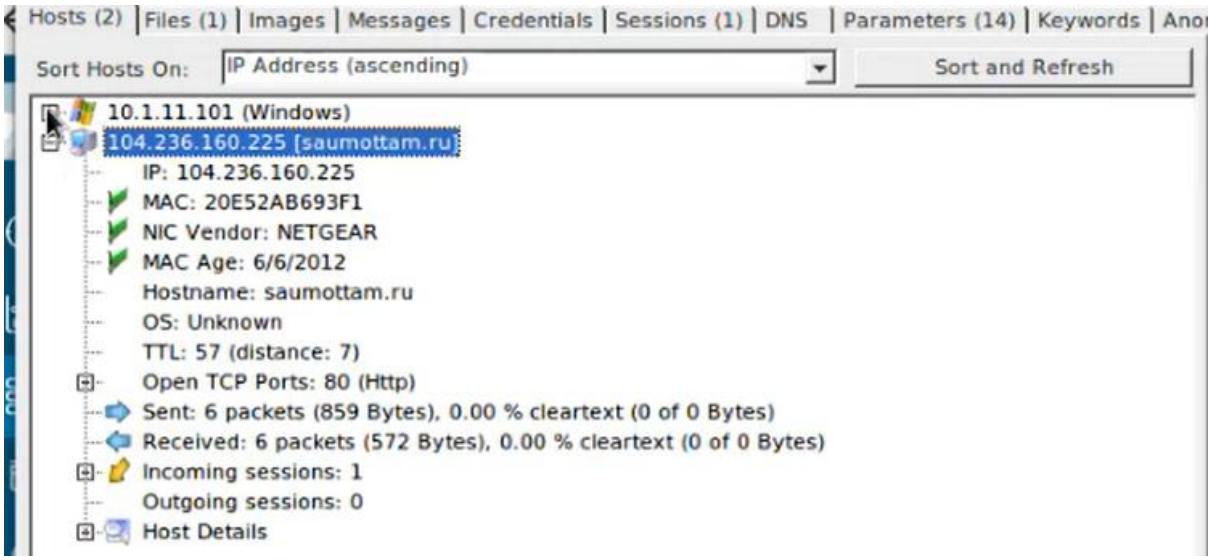


Figure 20: : Host details for 104.236.160.225

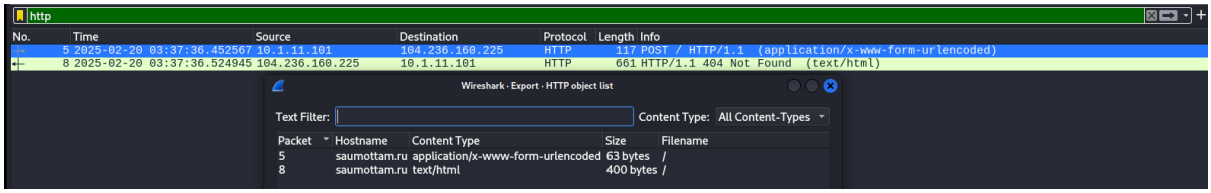


Figure 21: Wireshark capture of HTTP Traffic and Files Downloaded from 104.236.160.225 linked to saumottam.ru

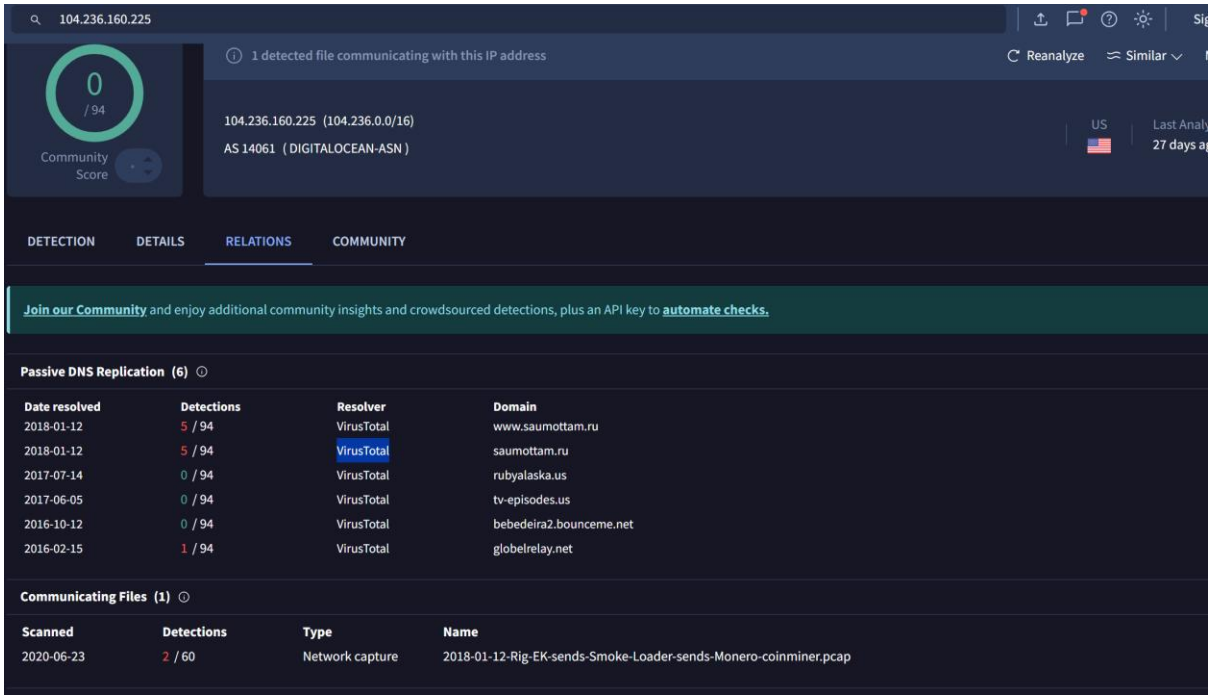


Figure 22: VirusTotal scan result for 104.236.160.225 linking it to saumottam.ru and a Rig EK and Smoke loader pcap file.

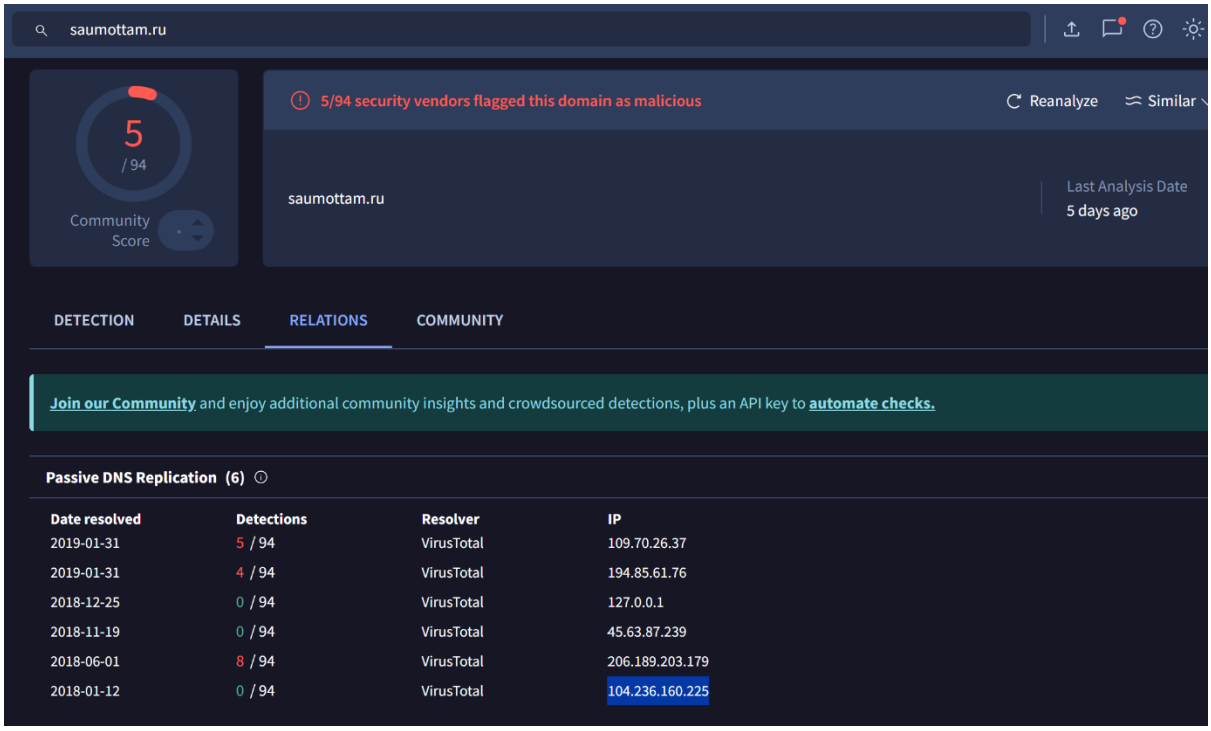


Figure 23: VirusTotal scan result for saumottam.ru confirming it as malicious and DNS replication to 104.236.160.225.

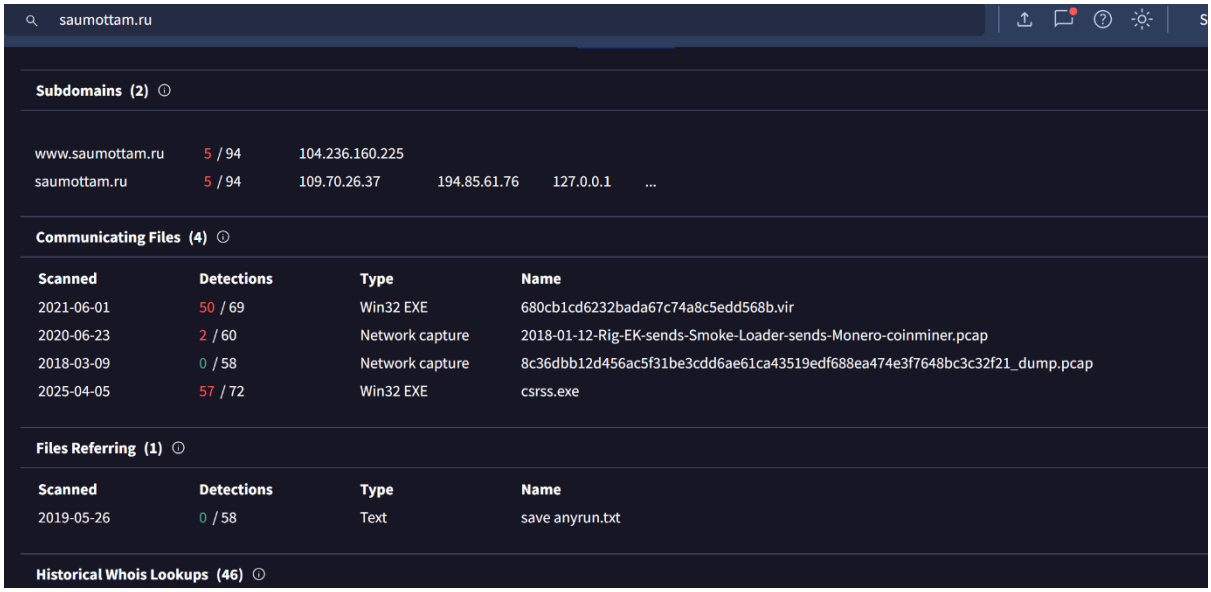


Figure 24: VirusTotal scan result for saumottam.ru showing relations to malware (Smoke Loader, Rig EK, Monero miner).

3.5.3 IOC 3 – IP: 104.236.16.69 (bprocess.exe)

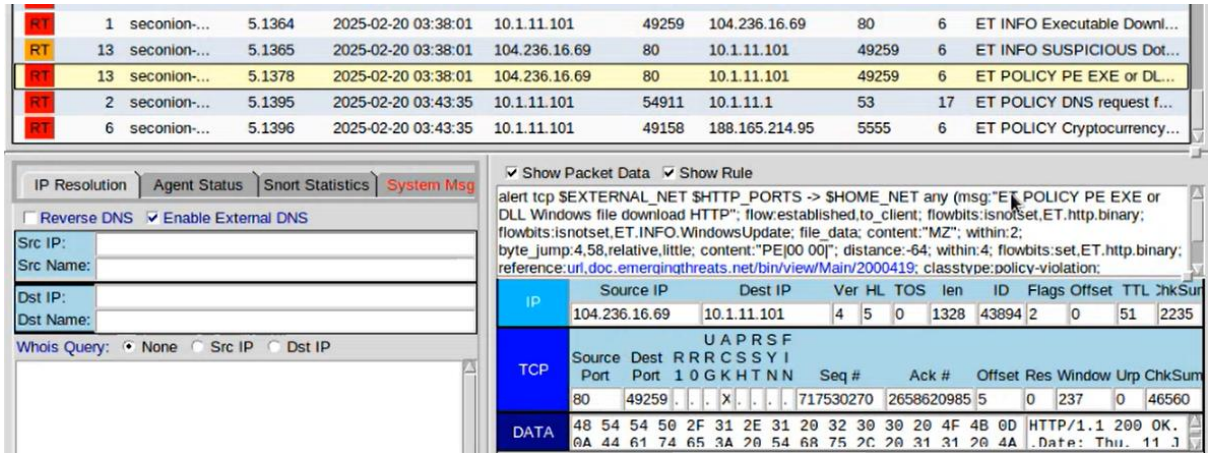


Figure 25: Sguil alerts for executable download from 104.236.16.69

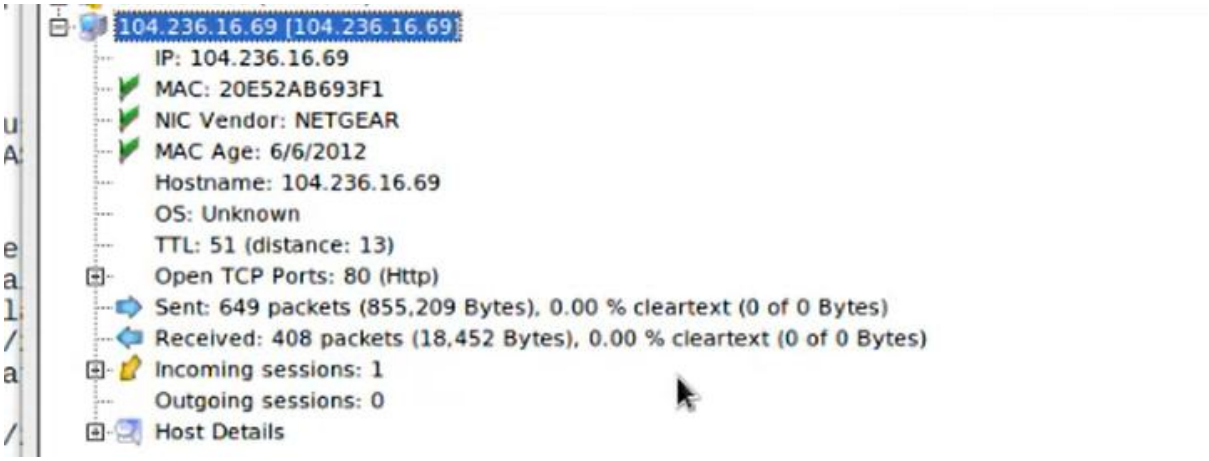


Figure 26: Host details for 104.236.16.69

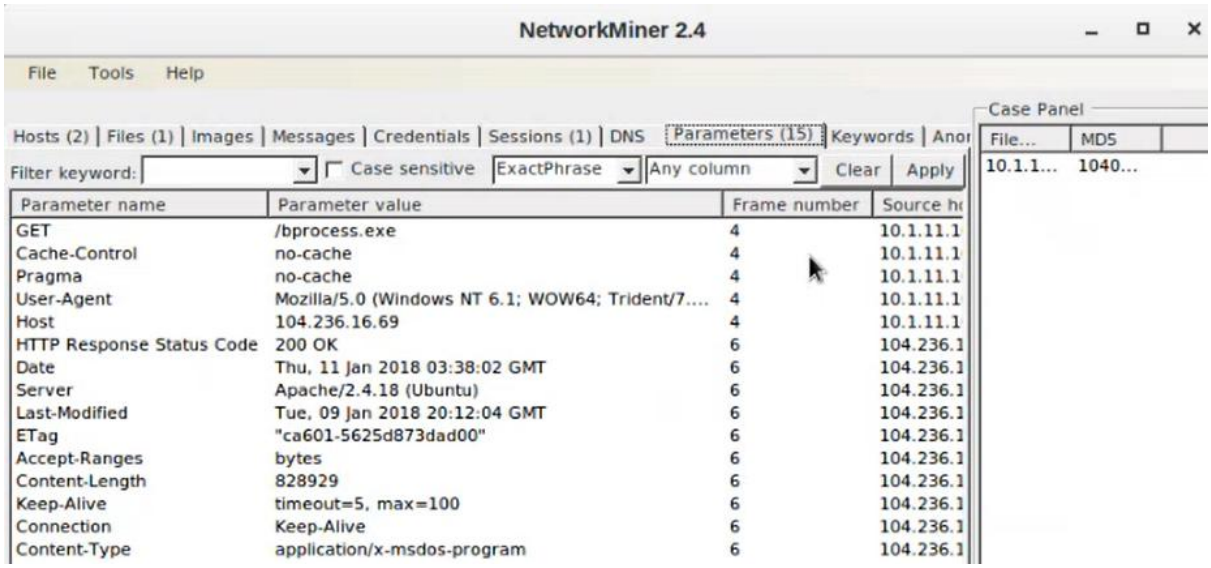
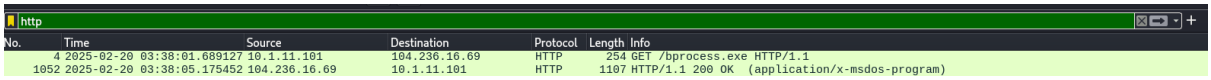


Figure 27: NetworkMiner showing parameters for the connection to 104.236.16.69 and the executable download.



No.	Time	Source	Destination	Protocol	Length	Info
4	2025-02-20 03:38:01.689127	10.1.11.101	104.236.16.69	HTTP	254	GET /bprocess.exe HTTP/1.1
1052	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)

Figure 28: HTTP GET Traffic for bprocess.exe from 104.236.16.69 (Wireshark)

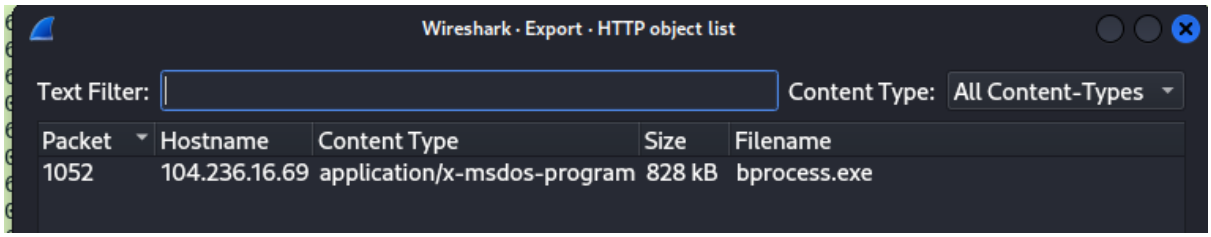
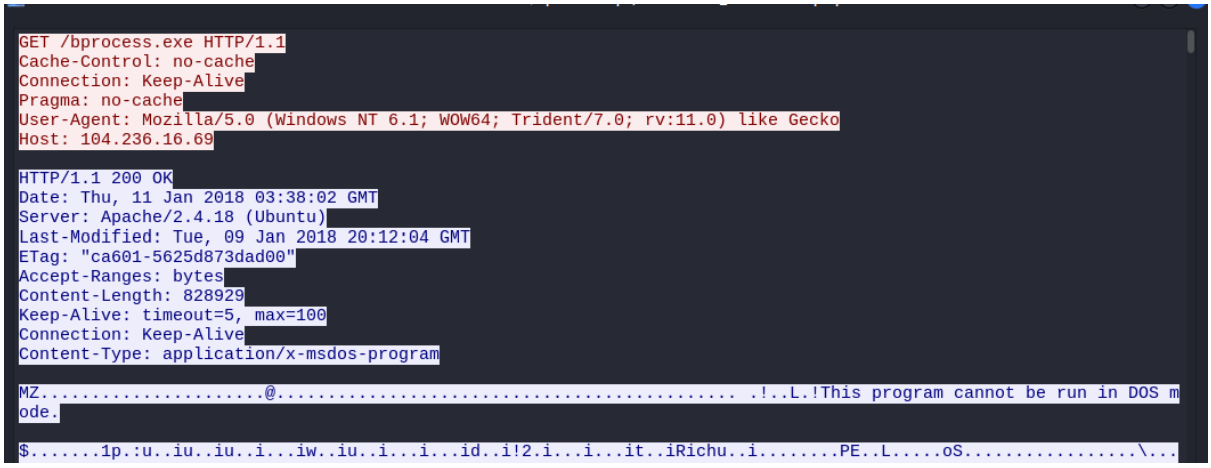


Figure 29: File (bprocess.exe) downloaded from 104.236.16.69 (Wireshark)

The application/x-msdos-program confirms bprocess.exe is a Windows executable. MZ Header indicates Windows PE EXE format.



```
GET /bprocess.exe HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Pragma: no-cache
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Host: 104.236.16.69

HTTP/1.1 200 OK
Date: Thu, 11 Jan 2018 03:38:02 GMT
Server: Apache/2.4.18 (Ubuntu)
Last-Modified: Tue, 09 Jan 2018 20:12:04 GMT
ETag: "ca601-5625d873dad00"
Accept-Ranges: bytes
Content-Length: 828929
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/x-msdos-program

MZ.....................@.......................................... .!..L.!This program cannot be run in DOS m
ode.

$.......1p.:u..iu..iu..i...iw..iu..i...i...id..i!2.i...i...it..iRichu..i........PE..L.....oS................\...
```

Figure 30: Wireshark HTTP Stream for 104.236.16.69 showing GET bprocess.exe

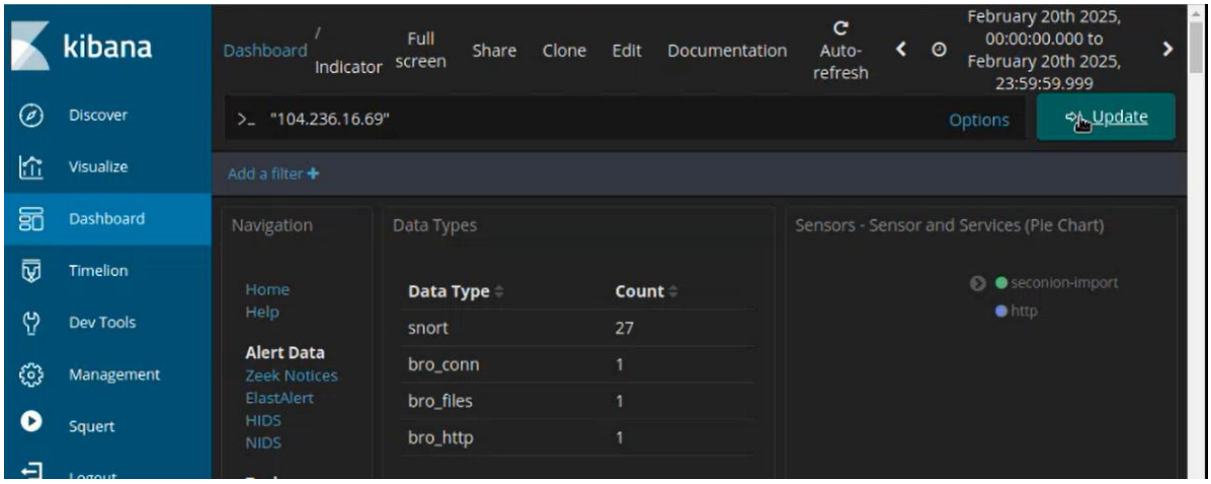


Figure 31: Kibana showing connection overview for 104.236.16.69.

This IP triggered 27 Snort alerts and was logged by Zeek with 1 connection, 1 file transfer, and 1 HTTP request.

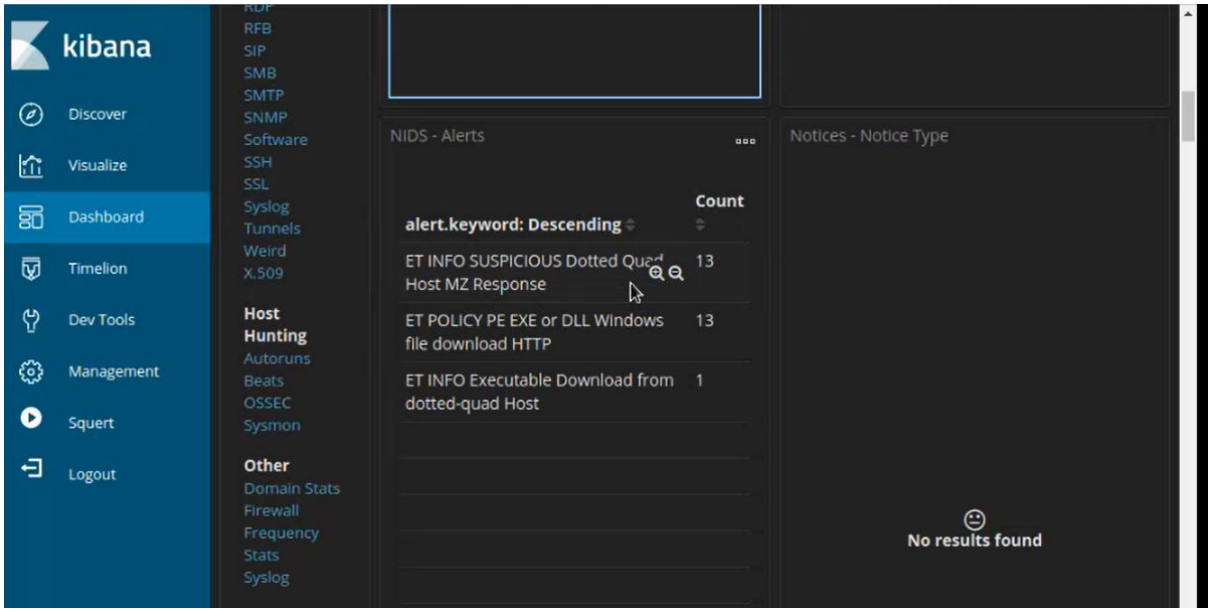


Figure 32: Kibana alerts for 104.236.16.69 showing an executable was downloaded from a dotted-quad IP, a known malware delivery tactic.

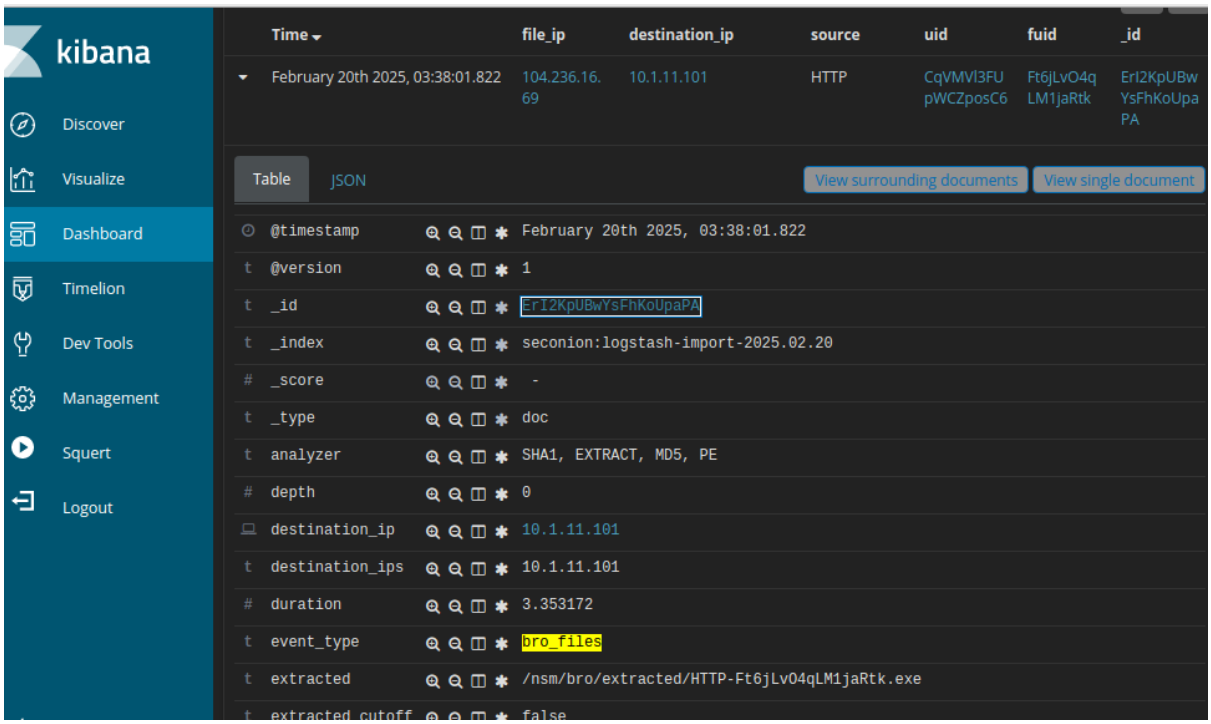


Figure 33: Kibana showing file (bprocess.exe) downloaded from 104.236.16.69

t	extracted	/nsm/bro/extracted/HTTP-Ft6jLvO4qLM1jaRtk.exe
t	extracted_cutoff	false
	file_ip	104.236.16.69
t	fuid	Ft6jLvO4qLM1jaRtk
t	host	7429cfa08569
t	ips	10.1.11.101,
t	is_orig	false
t	md5	7b3491e0028d443f11989efaeb0fbec2
t	message	{"ts":"2025-02-20T03:38:01.822280Z","fuid":"Ft6jLvO4qLM1jaRtk","tx_hosts":["104.236.16.69"],"rx_hosts":["10.1.11.101"],"conn_uids":["CqVMVl3FUpWCZposC6"],"source":"HTTP","depth":0,"analyzers":["SHA1","EXTRACT","MD5","PE"],"mime_type":"application/x-dosexec","duration":3.3531720638275146,"is_orig":false,"seen_bytes":828929,"total_bytes":828929,"missing_bytes":0,"overflow_bytes":0,"timedout":false,"md5":"7b3491e0028d443f11989efaeb0fbec2","sha1":"e2efe60cb8bd67840f9a8bf92b57ade97e406a88","extracted":"/nsm/bro/extracted/HTTP-Ft6jLvO4qLM1jaRtk.exe","extracted_cutoff":false}
t	mimetype	application/x-dosexec
#	missing_bytes	0B
#	overflow_bytes	0B
t	path	/nsm/import/bro/bro-yMSORTGb/files.log
#	seen_bytes	809.501KB
t	sha1	e2efe60cb8bd67840f9a8bf92b57ade97e406a88
t	source	HTTP

Figure 34:Kibana showing bprocess.exe downloaded from 104.236.16.69

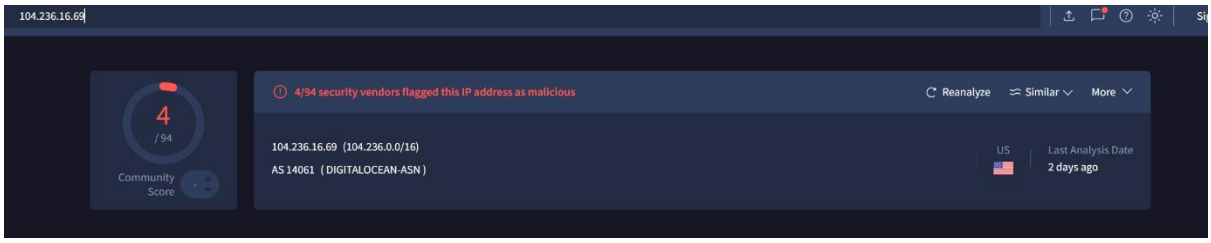


Figure 35: VirusTotal scan result for 104.236.16.69, confirming it as malicious

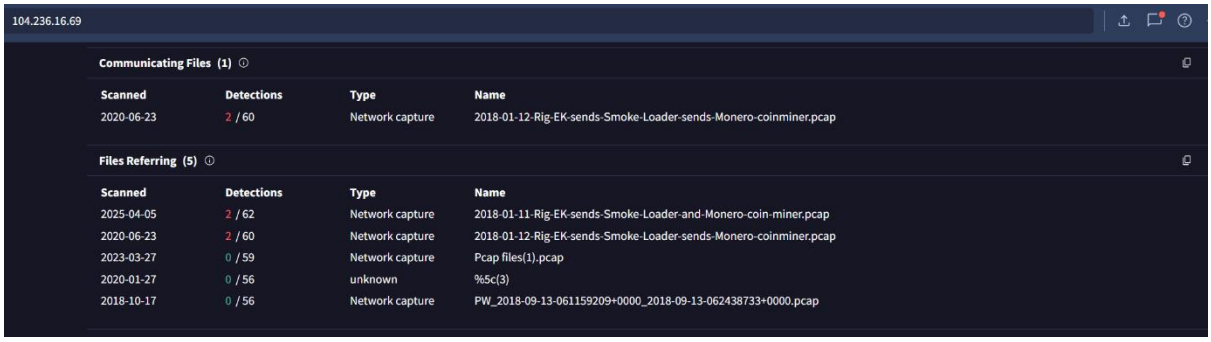


Figure 36:VirusTotal scan result for 104.236.16.69 showing relations to malware (Smoke Loader, Rig EK, Monero miner).

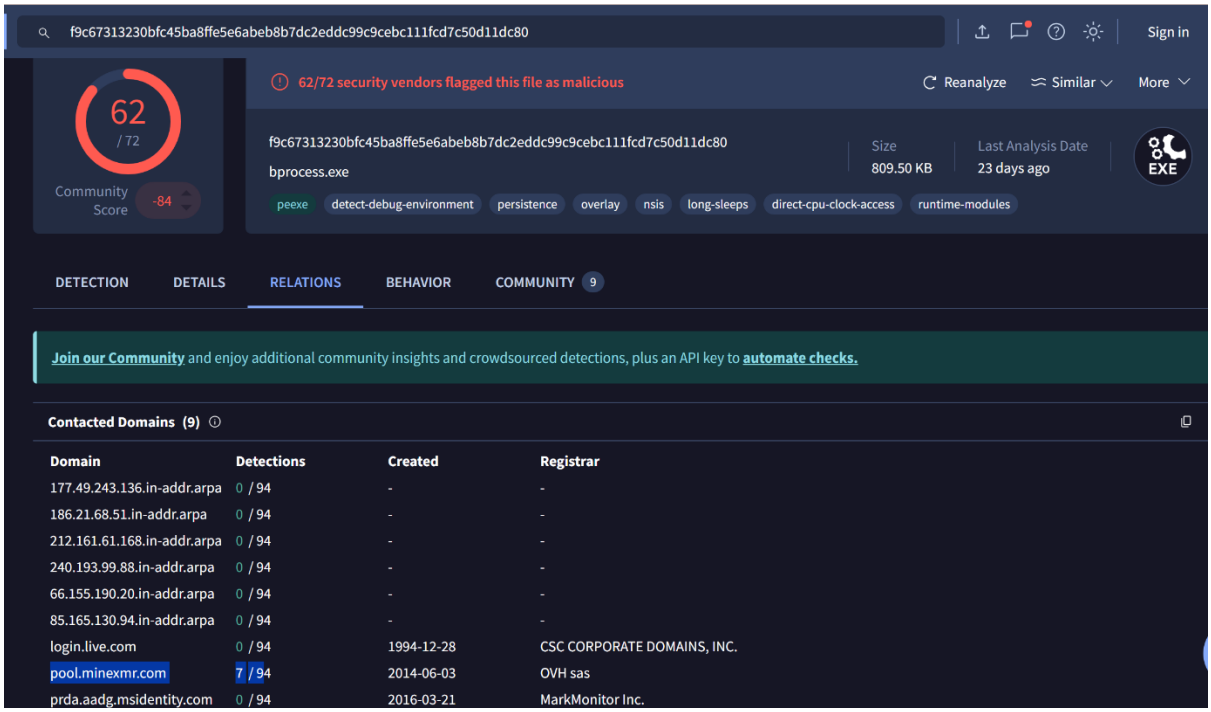


Figure 37: VirusTotal scan result for bprocess.exe confirming it as malicious and connected to pool.minexmr.com (mining pool)

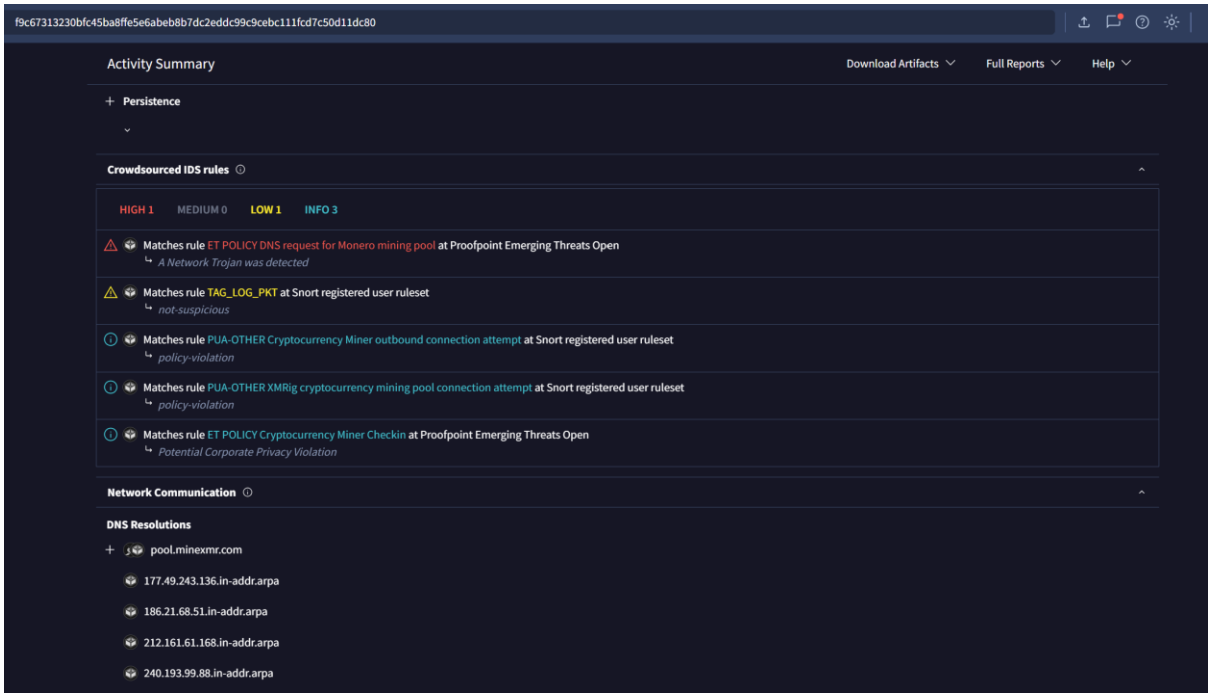


Figure 38: VirusTotal behaviour scan result for bprocess.exe showing DNS resolution to pool.minexmr.com (mining pool)

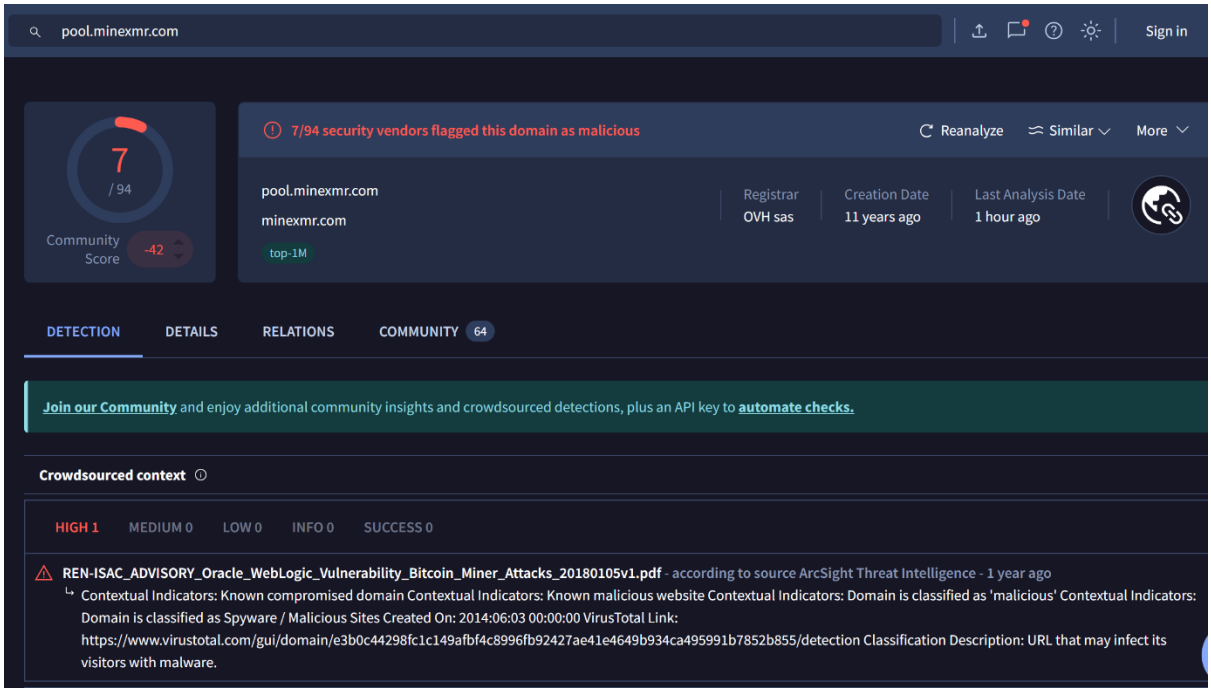


Figure 39: VirusTotal scan result for pool.minexmr.com, confirming it as malicious.

3.5.4 IOC 4 – IP: 10.1.11.1 (DNS Activity)

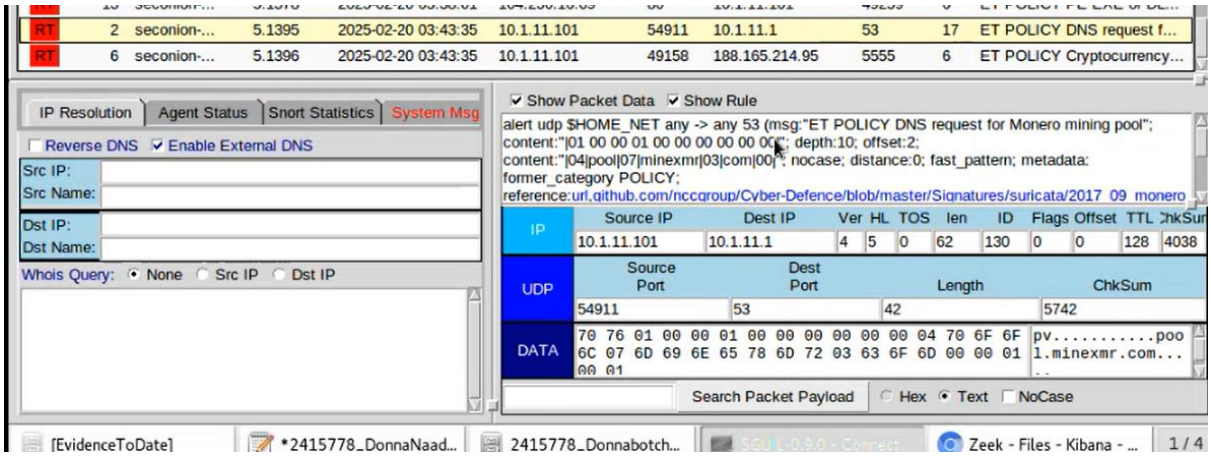


Figure 40: DNS-related alerts flagged in Sguil for 10.1.11.1

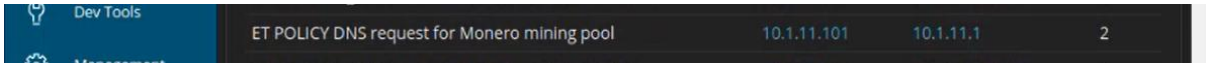


Figure 41: Kibana alert for 10.1.11.1 show a DNS request for Monero mining pool.

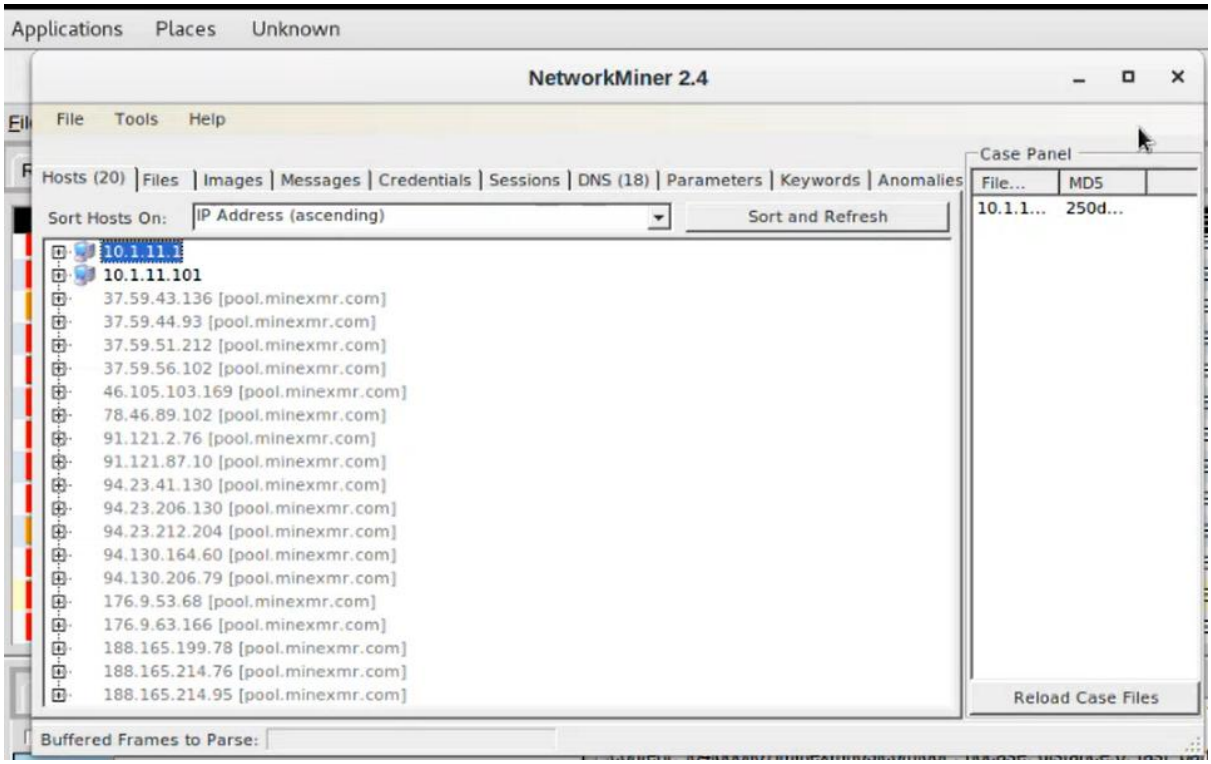


Figure 42: DNS Resolution logs for 10.1.11.1 from NetworkMiner

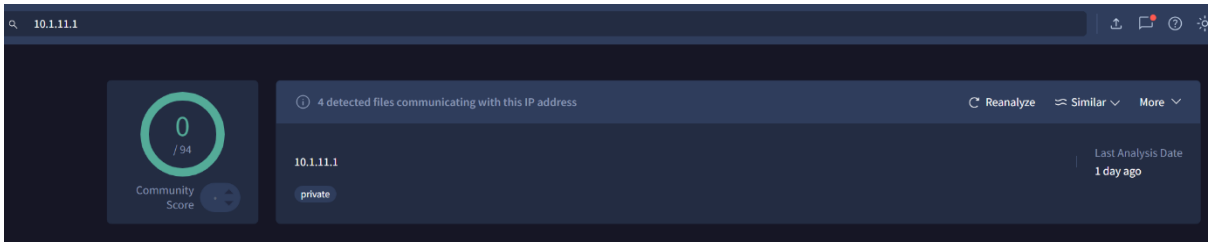


Figure 43: VirusTotal scan result for 10.1.11.1 showing its interaction with 4 known malicious files

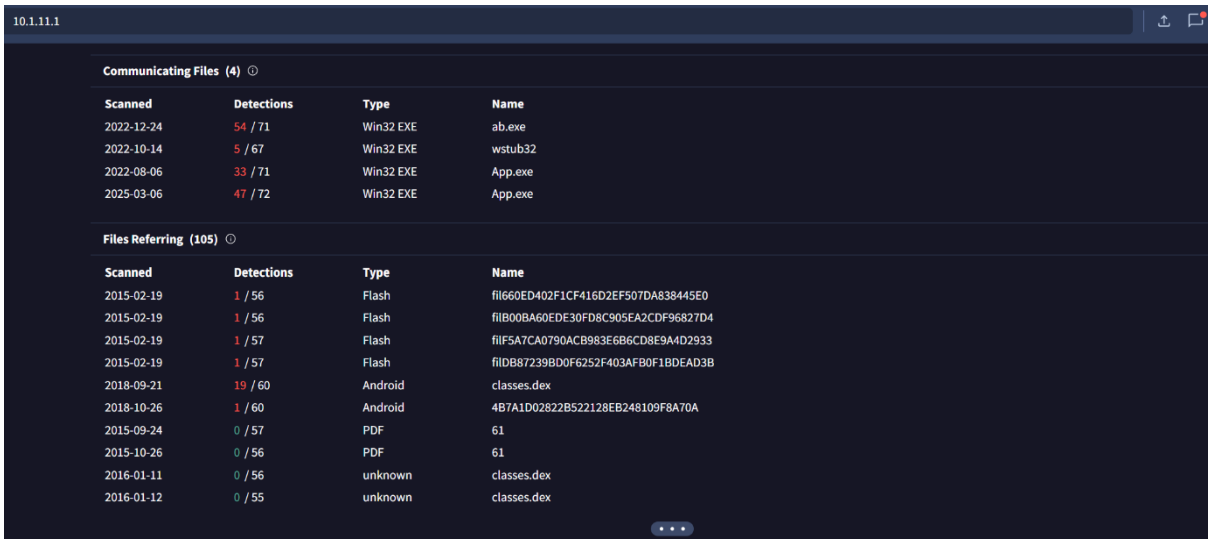


Figure 44: : VirusTotal scan result (relations) for 10.1.11.1

3.5.5 IOC 5 – IP: 188.165.214.95 (pool.minexmr.com, Cryptocurrency Mining)

Figure 45: Host details for 188.165.214.95

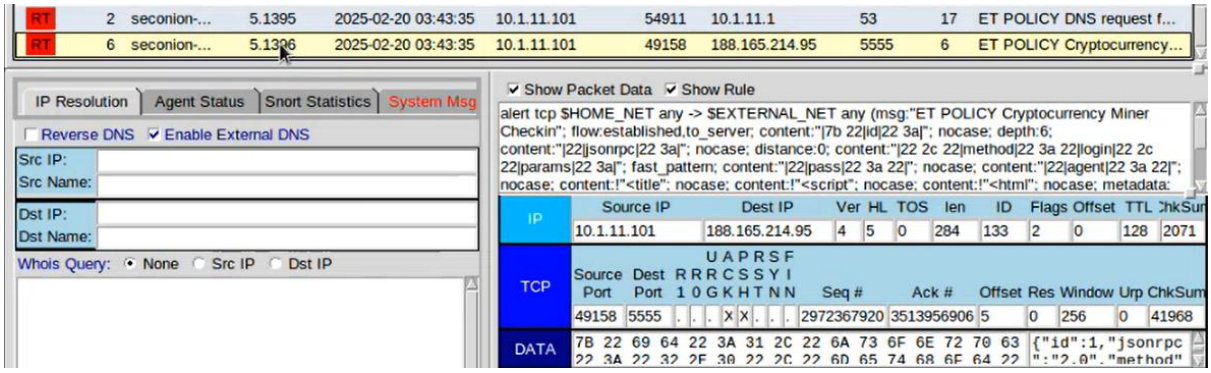


Figure 46: Sguil alert (ET POLICY Cryptocurrency Miner) triggered for 188.165.214.95

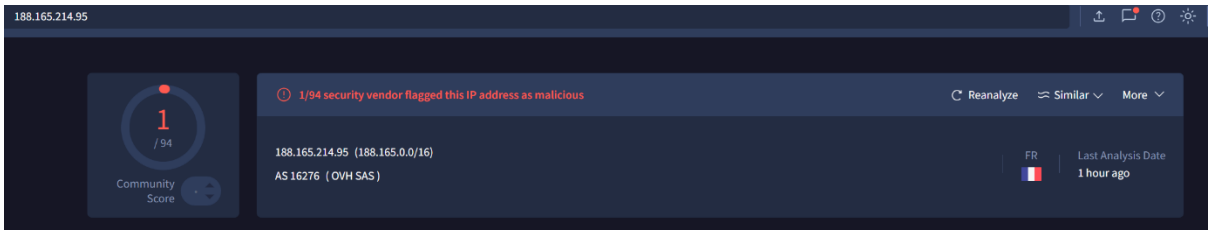


Figure 47: VirusTotal scan result for 188.165.214.95, confirming it as malicious.

188.165.214.95

Communicating Files (88)

Scanned	Detections	Type	Name
2019-02-14	46 / 66	Win32 EXE	5406e4d19aa3d3e50add6941dc81a4a3
2017-08-07	26 / 63	Win32 EXE	minnew.exe
2021-07-22	44 / 70	Win32 EXE	MSASCUI
2021-07-22	51 / 68	Win32 EXE	NINNDE.EXE
2017-12-19	61 / 67	Win32 EXE	1032-c6c5bf88723f46067d5f45e6654f32c78e47ad29
2020-11-27	47 / 71	Win32 EXE	virussign.com_22db06aa103ab6c7eefa49d758996880.vir
2021-10-21	33 / 59	Win32 EXE	Stellar.Phoenix.Windows.Data.Recovery.v7.0.0.3.exe
2021-03-05	58 / 71	Win32 EXE	cf5c39b02c8f38f92d9bbb672fd2f19f
2019-12-12	0 / 57	Network capture	Ross.pcap
2021-03-09	53 / 71	Win32 EXE	i4lthluu.exe

Files Referring (102)

Scanned	Detections	Type	Name
2025-04-10	43 / 63	GZIP	735da0b0d87f99a5b75a9e0af952ea09b87e9474a86d52843fbc261ef2be4303-1744119076768713934.gz
2025-04-10	48 / 71	Win32 EXE	303918553
2025-04-10	40 / 61	GZIP	650a4d645d08b330803a6c145b0c6b54b464782bc0eea0eb60ea322206647425-1744097434423787733.gz
2025-04-09	49 / 71	Win32 EXE	296933926
2025-04-09	45 / 71	Win32 EXE	685d47b6de92208130cbe59f932dca59.virus
2025-04-09	49 / 71	Win32 EXE	2024-06-18_7a52e0ced4361710595474adea6bf39b_magniber
2025-04-08	49 / 72	Win32 EXE	300243150

Figure 48: VirusTotal scan result (relations) for 188.165.214.95

3.5.6 Suspicious Connections.

Figure 49: Host details for 23.34.134.22 showing Microsoft

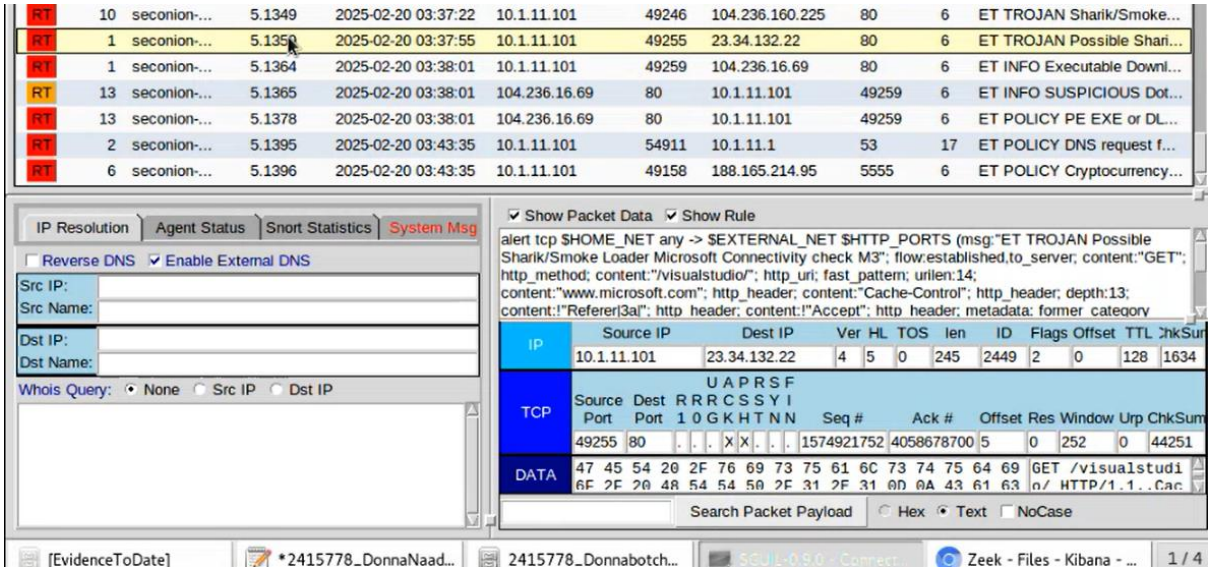


Figure 50: Sguil Alert Triggered for 23.34.132.22_microsoft (likely false positive or malware behaviour)

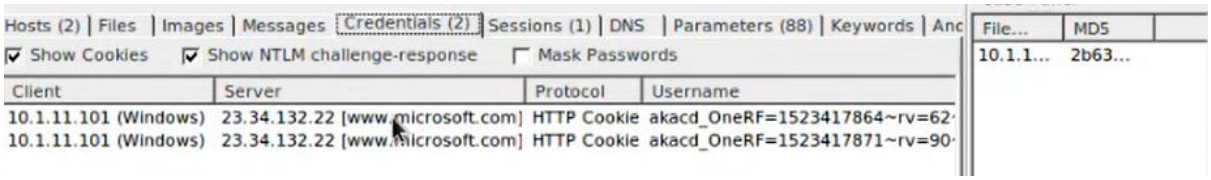


Figure 51: NetworkMiner showing HTTP Cookies for 23.34.132.22 (Microsoft)

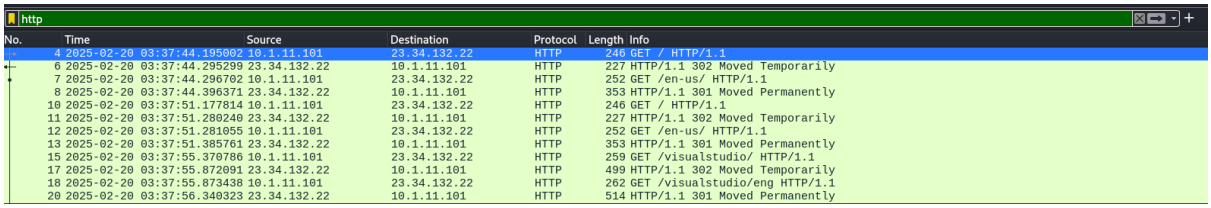


Figure 52: HTTP Traffic for 23.34.132.22_microsoft (Wireshark)

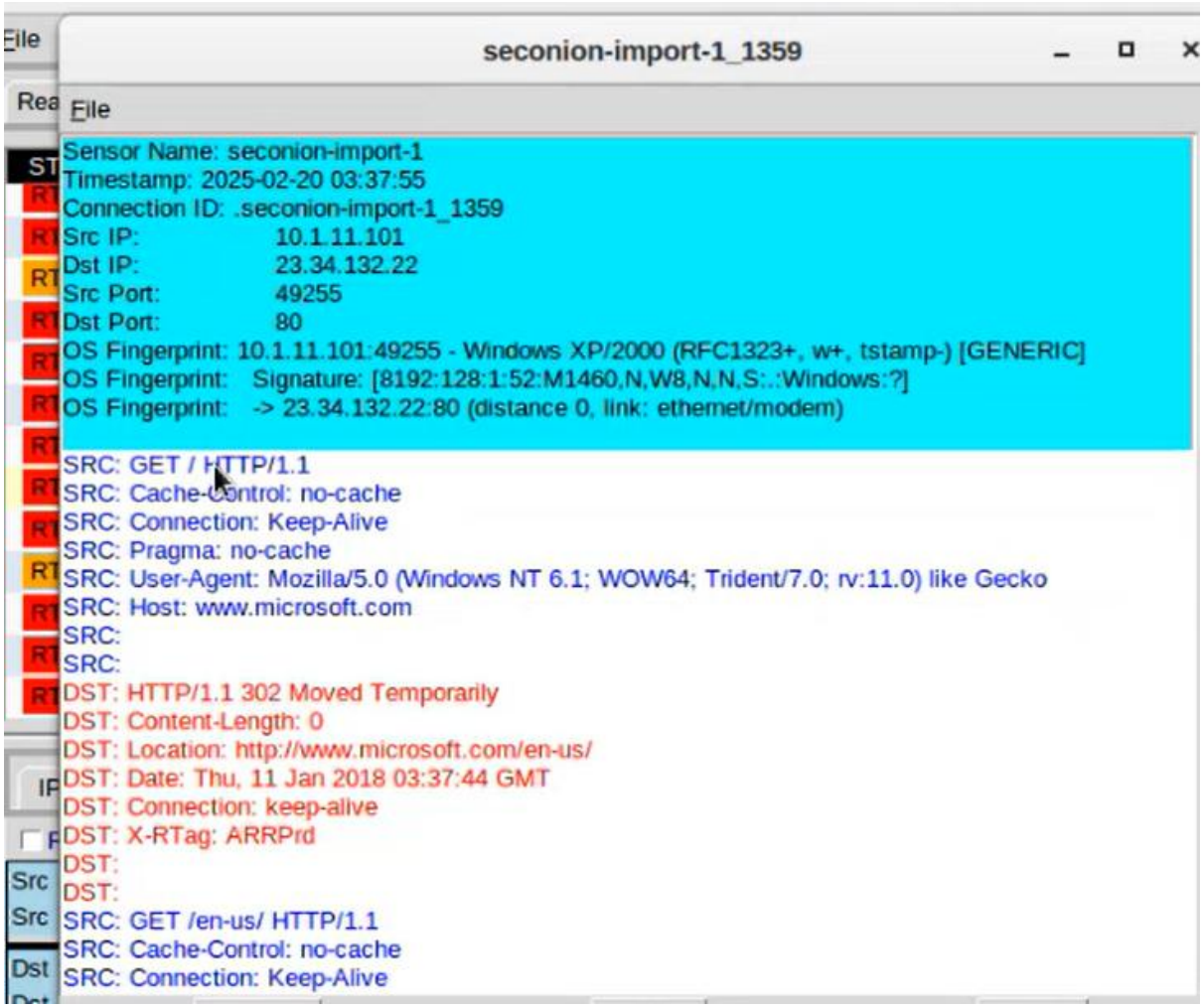


Figure 53: HTTP Transcript for 23.34.132.22 (Microsoft).

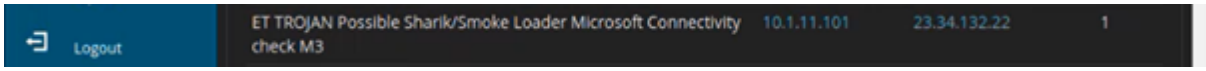


Figure 54: Kibana alert for 23.34.132.22 indicates a possible connectivity check via Microsoft by the Smoke Loader Trojan, a common tactic used by malware to blend into legitimate traffic.

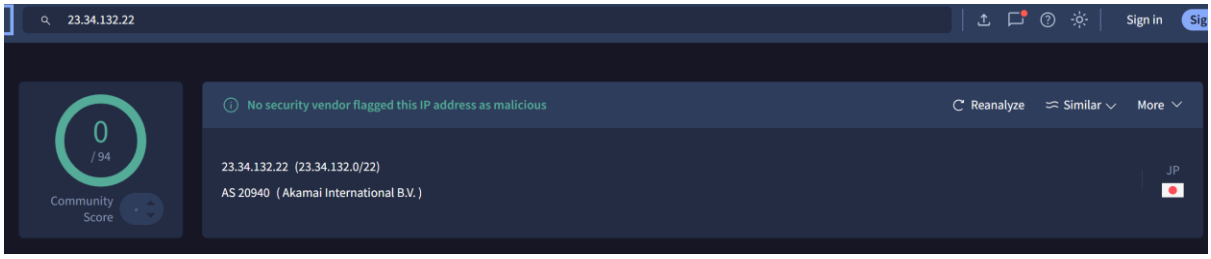


Figure 55: VirusTotal scan result for 23.34.132.22 , confirming it as safe.

Although Bing's IP (204.79.197.200) was not directly flagged as malicious, VirusTotal associates it with 8 malicious files and a notably negative community score as seen below. This result and the alerts regarding Microsoft's IP (Figure 50, Figure 54) point to possible abuse of legitimate infrastructure or redirection via compromised ads or links.

204.79.197.200

Sign in

0 / 94

Community Score -136

8 detected files communicating with this IP address

Reanalyze Similar More

204.79.197.200 (204.79.197.0/24)

AS 8068 (MICROSOFT-CORP-MSN-AS-BLOCK)

US

Last Analysis Date 5 hours ago

DETECTION DETAILS RELATIONS COMMUNITY 3.1 K

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

Passive DNS Replication (200)

Date resolved	Detections	Resolver	Domain
2025-04-04	0 / 94	VirusTotal	pi.msedgeservices.com
2025-04-01	0 / 94	VirusTotal R2DBox	m-ssl-bing-com.a-0001.a-msedge.net
2025-03-20	0 / 94	VirusTotal	tr253849097.mm.bing.net
2025-03-20	0 / 94	VirusTotal	tr406114826.mm.bing.net
2025-03-20	0 / 94	VirusTotal	tr861020775.mm.bing.net
2025-03-20	0 / 94	VirusTotal	tr408783310.mm.bing.net
2025-03-20	0 / 94	VirusTotal	en164142222.mm.bing.net

Figure 56: VirusTotal scan for 204.79.197.200 (Bing) – clean (0/94) but shows connections to 8 malicious files and Community score: -136.

204.79.197.200

Communicating Files (1 M)

Scanned	Detections	Type	Name
-	-	file	0000000000000000000000000000000100000000000000000000000000000000
2025-03-31	51 / 73	Win32 EXE	file-archive_FjMixC2ckw.exe
2025-04-03	67 / 72	Win32 EXE	IEDiagCmd.exe
2024-02-01	61 / 67	Win32 EXE	0000012ea6fe3418b78446902fdf6b2959bb6324671f7ccc000a9ca6b15da31a
2024-04-05	67 / 72	Win32 EXE	000002305f386d9f7223c3bbf47164ca6f09f947dcd83b54c657594c54c6a359.exe
2024-01-24	64 / 70	Win32 EXE	csrss.exe_
2025-04-02	67 / 72	Win32 EXE	000005427fbe8d0b914fc56eec86ca6ee480a3a44b5fb5cb19eaeec29c21240e
2024-11-02	0 / 71	Win32 EXE	GC_ServFact.exe
2024-12-23	1 / 71	Win32 EXE	CertificateDetectionService.exe
2024-07-17	70 / 74	Win32 EXE	HIBhbOID

Files Referring (200)

Scanned	Detections	Type	Name
2025-04-10	36 / 63	Win32 EXE	Win 10 Tweaker.exe
2025-04-10	6 / 72	Win32 EXE	Cut The Line
2025-04-06	33 / 72	Win32 EXE	fix10.exe
2025-04-09	10 / 71	Win32 EXE	tpvpyme
2025-04-09	39 / 72	Win32 EXE	Win 10 Tweaker.exe
2025-04-08	12 / 71	Win32 EXE	tpvpyme
2025-04-08	26 / 71	Win32 EXE	UnlockSoftwares.exe

Figure 57: VirusTotal scan result for 204.79.197.200_bing showing it communicates with several malicious files.

4.0 Cybersecurity Frameworks and Intrusion Methods

4.1 Background of Intrusion and Attack Methodology

4.1.1. Sundown and Rig Exploit Kits

Alert IDs: 5.1306, 5.1320, 5.1340
Sundown Exploit Kit (EK) was likely the intial point in this attack. Sundown EK directs users to a landing page that scans for vulnerabilities, redirecting them to an exploit page if one is found (Biasini, 2016). Sundown exploits Flash and Silverlight vulnerabilities using familiar extensions (.swf, .xap) without obfuscation. Recovered artifacts, including .swf files in PCAPs, confirms this. While less sophisticated than others like Angler, Sundown remains effective due to its simplicity (Biasini, 2016).

Shortly afterward, Rig Exploit Kit signatures followed suggesting possible reuse of infrastructure . First introduced in 2014, Rig Exploit Kit operates as an "exploit-as-a-service" platform used by cybercriminals to distribute malware through drive-by downloads and malvertising (BleepingComputer, 2023). It embeds malicious JavaScript into compromised websites, which silently exploits outdated browsers and plugins—most notably Internet Explorer and Adobe Flash (BleepingComputer, 2023). In this case, the exploit likely targeted CVE-2015-8651, a critical Flash Player vulnerability that enables remote code execution without user interaction (NIST, 2022).The delivered payloads such as index.html and index.html.swf are part of a drive-by attack and indicate the use of trojans.

Rig Exploit Kit is known to deliver a variety of malware including Smoke Loader, ransomware, and cryptocurrency miners once a vulnerable host is identified. This behaviour aligns with MITRE ATT&CK techniques T1189 (Drive-by Compromise) and T1203 (Exploitation for Client Execution). To mitigate such risks, organisations must update browsers, and remove deprecated software like Flash(NIST, 2022).

4.1.2. Smoke Loader / Sharik Trojan

Alert IDs: 5.1347, 5.1349

Smoke Loader (also known as Sharik or Dofoil) is a modular backdoor Trojan active since 2011 and catalogued under MITRE ID S0226. It often drops other malware such as stealers, miners, and ransomware. Its functionality depends on the specific plug-ins in use (MITRE, 2024). Commonly delivered via exploit kits like Rig Exploit Kit or Sundown Exploit Kit, Smoke Loader uses techniques such as DLL side-loading (T1574.002) and application-layer communication (T1071.001) to maintain stealth and persistence (MITRE, 2024). While the binary was not recovered, alerts triggered under the signature “ET TROJAN Sharik/SmokeLoader”, and connections to saumottam.ru, a domain linked to Rig Exploit Kit campaigns indicates its probable presence.

According to Malpedia, Smoke Loader disguises its command and control (C2) activity by making requests to legitimate domains like *microsoft.com* and *bing.com*, often returning HTTP 404 errors while still carrying data in the response body. Its widespread use and evolving

module-based architecture make it a common tool in cybercriminal campaigns (Fraunhofer FKIE, 2024).

4.1.3. Cryptocurrency Miner

Alert ID: 5.1396
The investigation revealed a Monero cryptocurrency miner based on network traffic to a known mining pool over port 5555 . This miner was likely dropped after the system was compromised, possibly by Smoke Loader. Miners don't steal data, but they consume CPU/GPU resources, and cause system slowdown and performance issues (Falco, 2022). They are usually stealthy and can go unnoticed unless performance is monitored. This activity maps to T1496 (Resource Hijacking) and possibly T1095 (Non-Application Layer Protocol) due to the observed C2 communication over custom ports.

4.1.4 Attack Vector and Exploit

The attack on the victim machine (10.1.11.101 running Windows 7 with Internet Explorer 11) started with a visit to a malicious website hosted at 188.227.16.131, which initially triggered the Sundown Exploit Kit landing page. This page then redirected the victim to Rig Exploit Kit infrastructure, which then exploited Flash vulnerabilities (likely CVE-2015-8651) to deliver trojan payloads such as index.html and index.html.swf. These files were confirmed in PCAP logs and recovered in NetworkMiner.

Then, communication with samottam.ru (104.236.160.225) suggests the presence of Smoke Loader, a known second-stage downloader. After receiving bprocess.exe, a Monero (XMR) miner from the server 104.236.16.69, it connected to the mining pool at 188.165.214.95 (pool.minexmr.com). The payloads included Trojan downloaders, Flash-based exploits, and a cryptominer. This chain of activity shows that Rig Exploit Kit deployed a trojan, which in turn dropped a cryptocurrency miner to mine monero with system resources. This is consistent with MITRE T1496: Resource Hijacking and T1203: Exploitation for Client Execution.

4.2 Relevant threat models

4.2.1 Diamond Model of Intrusion Analysis.

The Diamond Model breaks down a cyberattack into four key components: the adversary, victim, capabilities, and infrastructure. This structured view helps security analysts understand how each part contributes to the attack and how they connect (Tidmarsh, 2023).

- **Adversary:** The threat actor remains unidentified but is likely a cybercriminal group. Their use of the Sundown/Rig Exploit Kit, with Monero miners and malicious domains flagged by VirusTotal, suggests a financially motivated operation.
- **Infrastructure:** The group used malicious IPs and domains such as 188.227.16.131, 188.165.214.95, 104.236.160.225, saumottam.ru, and pool.minexmr.com, commonly associated with exploit kits and cryptocurrency mining.

- **Capabilities:** The group exploited CVE-2015-8651 (a Flash vulnerability) and deployed a Trojan (Smoke Loader) that delivers payloads like coin miners. Smoke Loader uses DLL side-loading (T1574.002) and command and control (C2) communications via application layer protocols (MITRE, 2024).
- **Victim**: Windows 7 system (10.1.11.101) with outdated browser (Internet Explorer 11).

4.2.2 Cyber Kill Chain

The Cyber Kill Chain shows the attacker's steps from planning to execution. It describes the movement through stages to exploit vulnerabilities, gain control, and achieve their goals (EC-Council, 2022).

1. **Reconnaissance**: While not directly observed, the attacker likely scanned for vulnerable targets using web-based exploit techniques.
2. **Weaponization**: The attacker prepared a .html Trojan downloader and a .swf Flash exploit file, intended to exploit a known Flash vulnerability (CVE-2015-8651).
3. **Delivery**: The attackers used a compromised site to deliver payloads over HTTP when the victim visited, using the Rig Exploit Kit after the Sundown Exploit Kit redirection.
4. **Exploitation**: The .html downloader loaded the .swf file, which exploited a Flash vulnerability in the outdated browser or plugin to execute malicious code on the victim's system.
5. **Installation**: Smoke Loader was deployed as a dropper, installing and executing bprocess.exe, the Monero cryptocurrency miner, after the .html downloader triggered the .swf Flash exploit.
6. **Command and Control (C2)**: The attackers used various malicious IPs and domains for C2 communication, with bprocess.exe maintaining control over the compromised system and directing the mining activity.
7. **Actions on Objectives**: The attackers hijack the CPU/GPU resources of the compromised system, running bprocess.exe to mine monero cryptocurrency.

4.2.3 MITRE ATT&CK Reference

The MITRE ATT&CK framework helps identify and understand attacker behaviour by mapping observed techniques to known tactics. Using it gives better insight into the attack chain and how to better defend, mitigating future threats.

- **Initial Access (T1189 - Drive-by Compromise):** The attacker used the Sundown/ Rig Exploit Kit to deliver a malicious index.html downloader and .swf Flash file via a compromised website, exploiting browser vulnerabilities when the victim visits.
- **Execution (T1203 - Exploitation for Client Execution):** The .html downloader loads the .swf Flash file, exploiting a Flash vulnerability to execute malicious code, which triggers

a PowerShell script. This pulls Smoke Loader and bprocess.exe from the C2 infrastructure (T1059 - Command and Scripting Interpreter).

- **Defence Evasion (T1055- Process Injection):** From VirusTotal, bprocess.exe may attempt to inject malicious code into legitimate processes, though these behaviours were not directly observed in the investigation.
- **Command and Control (T1071.001 - Application Layer Protocol):** bprocess.exe communicates with C2 servers over HTTP/DNS, with traffic directed to hosts including 188.165.214.95 on TCP port 5555, indicating the use of custom C2 tools (T1095 - Non-Application Layer Protocol).
- **Impact (T1496 - Resource Hijacking):** bprocess.exe hijacks the victim's CPU/GPU resources for Monero mining, with multiple connections to pool.minexmr.com (crypto mining pool) indicating cryptojacking activity.

See aligned prevention strategies in ***Chapter 5.3.2***.

4.3 Investigation Methodology

4.3.1 Approach

A structured investigation was conducted using network traffic and malware analysis techniques:

1. **Data Collection**: Extracted artifacts from PCAP files, DNS logs, and downloaded files.
2. **Initial Detection**: Reviewed alerts from Security Onion (Sguil, Kibana) that showed suspicious activity on the victim machine.
3. **Traffic Analysis**: Analysed network traffic using Wireshark and NetworkMiner to identify malicious HTTP requests and file downloads.
4. **Reputation Check**: Verified file and IP reputations via VirusTotal.
5. **Technique Mapping**: Mapped attacker behaviour to MITRE ATT&CK and Cyber Kill Chain**.**
6. **Impact & Remediation:** Assessed impact and suggest solutions.

4.3.2 Evidence Collection

Key evidence sources included:

- **Security Alerts**: Indicators of trojans and cryptocurrency miners.
- **Logs and Artifacts**: Analysed HTTP traffic, DNS queries/responses, and downloaded files.
- **Threat Intelligence**: Cross-checked SHA1 hashes and related IPs using VirusTotal.

4.4 Analysis and Findings

4.4.1 Root Cause

The attack exploited an unpatched browser and outdated Flash plugin that allowed the Sundown/Rig Exploit Kit to exploit the system through malicious files from 188.227.16.131. This triggered the download and execution of trojan payloads and crypto miner when the user visited a compromised website.

4.4.2 Impact

The attack impacted:

- **Availability:** The system's performance degraded due to high CPU and memory usage caused by the crypto mining of Monero miner.
- **Integrity:** The system may have been tampered with to allow persistent crypto mining, but no direct evidence was found.
- **Confidentiality :** No direct evidence observed, but the presence of malware poses a risk of unauthorized access.

The impact is rated medium, mainly due to system slowdown from mining activity. However, if left unchecked, it could escalate to high , due to the presence of Smoke Loader which can download more malicious files.

4.4.3 Patterns

Several patterns emerged that could be valuable for future detection:

- Repeated successful HTTP connections to known malicious IPs.
- Malicious file downloads including files with MZ headers.
- Suspicious DNS queries to mining pool domains.
- VirusTotal-flagged file hashes and C2 domains recurring in network logs.

4.5 LESP Considerations

4.5.1 Legal and Ethical Implications

The investigation focused only on network-based activity from 20th February 2025, analysing DNS, HTTP, and NIDS alerts via Sguil, Kibana, Wireshark, and NetworkMiner, to infer malicious activity. No host-based investigation or user data were accessed. File analysis relied solely on hash metadata, with all work conducted in isolated virtual environments.

All investigation steps were carried out ethically, and in line with ISO/IEC 27037 guidance for evidence handling showing responsible evidence handling. Legally, the investigation followed privacy-by-design principles (GDPR Article 25) and Security of Processing (GDPR Article 32),

emphasizing data minimization and secure handling to avoid accessing sensitive data or interacting with potentially malicious content.

Despite no direct evidence of data theft, the presence of malware particularly crypto-mining payloads poses a risk to system confidentiality and integrity of the client-facing system. The organization must assess whether sensitive data was exposed, its position under GDPR Article 33 (Breach Notification) and determine whether a breach notification is necessary. This incident may also fall under the Computer Misuse Act 1990 (UK) due to unauthorized access by malware. This event shows the need for secure configurations, regular patching, and active threat monitoring as part of data protection compliance.

4.5.2. Social Considerations

The incident shows possible impact on client trust especially given that the affected machine belonged to a staff member in a client facing role (Client Outreach). Although, there is no confirmed data loss, clients may perceive the company as vulnerable, damaging its reputation.

For SMEs, reputational damage due to a security incident can be really bad, affecting business continuity, client retention and future opportunities. To restore trust, the company must demonstrate improved security, be proactive in communication and transparent.

4.5.3 Professional Responsibility in Breach Reporting

The organization acted responsibly by investigating the incident in line with industry standards. However, the response exposed a gap in real-time detection and escalation. In this case, the issue was first noticed by the affected user and escalated through the help desk.

While it was correctly flagged as high risk and passed to the security team, the reliance on user reporting points to a gap in proactive threat detection. Ideally, the IDS identifies and alerts suspicious activity before the user experiences any impact. For SMEs, improving detection and response is vital, as they face greater risk from disruption, regulatory issues, and reputational damage, even with limited IT resources (dedicated security team).

5.0 Recommendations

5.1 Immediate Fixes

1. Immediately isolate the affected system (10.1.11.101) from the network to prevent further spread or communication with malicious hosts.
2. Delete malicious files, such as index.html , index.html.swf and bprocess.exe, to stop the mining activity.

   Run a full malware scan across all endpoints to detect and remove any additional threats.
3. Update and patch all systems, including browsers, operating system, plugins and software to fix known vulnerabilities.
4. Remove and fully uninstall outdated software, especially Flash Player (CVE-2015-8651), which is end-of-life from all systems.

5.2 Long-Term Strategies

To strengthen the organization's overall security posture and reduce the likelihood of future incidents:

1. Remove deprecated software and implement automated patch management for all systems, browsers, and plugins.
2. Regularly tune and update Intrusion Detection Systems or firewall to detect traffic to known malicious IPs and unusual file downloads.
3. Educate employees regularly on safe browsing, identifying malicious content and the risks of outdated software.
4. Enable web filtering to prevent access to known malicious and suspicious domains including those identified in this incident.
5. Deploy Endpoint Detection and Response (EDR) tools like Microsoft Defender for Endpoint or CrowdStrike Falcon to monitor and respond to suspicious activities such as DLL side-loading, or crypto mining based on unusual resource (CPU) usage.

5.3 Framework Alignment

5.3.1 Cyber Essentials (UK)

According to Cyber and Fraud Centre (2024), Cyber Essentials assist small organisations with practical guidance to improve their cyber posture regardless of their starting point.

Key recommendations include:

- **From Section 1.2 – Protection from Malware**
    - Keep systems and software regularly patched.
    - Use antivirus and anti-malware solutions.
- **From Section 2.2 – Firewalls**
    - Implement and monitor firewalls to manage and filter internet traffic in and out of the network.

These basic security hygiene measures must be regularly audited and enforced to reduce the risk of malware infections and network intrusions.

5.3.2 MITRE ATT&CK Aligned Preventive Controls

The following recommendations address the observed use of Sundown/Rig Exploit Kit, Smoke Loader, and Monero mining. Each control aligns with MITRE ATT&CK tactics and techniques previously detailed in Chapter 4.2.3, providing actionable prevention and detection guidance to reduce the likelihood of similar future attacks.

Technique	Detection / Mitigation ID	Observed Behavior	Defensive Action
T1189 – Drive-by Compromise (Initial Access)	M1051 – Update Software	User accessed Sundown EK landing page via compromised website, which redirected to Rig EK for exploitation	Remove Internet Explorer 11 and use modern browsers with auto-updates to patch known web-based exploit paths.
	DS0029 – Network Traffic		Monitor traffic for exploit kit patterns, redirects, and untrusted domains using IDS/SSL inspection
T1203 – Exploitation for Client Execution (Execution)	M1051 – Update Software	.swf Flash file exploited a vulnerability in browser to execute malware	Remove Flash; ensure browser is up-to-date and patched against known exploits
	DS0029 – Network Traffic		Detect exploit payloads and scripts by monitoring unusual or obfuscated traffic
T1055 – Process Injection (Evasion / Privilege Escalation)	M1040 – Behavior Prevention on Endpoint	Malware likely injected into legitimate processes to evade detection	Use endpoint protection tools like Microsoft Defender for Business or Sophos Intercept X to detect abnormal memory usage
	DS0011 – Module Load		Monitor DLL loads for unsigned or uncommon modules injected into trusted processes
T1095 / T1071.001 – C2 Protocols (Command & Control)	M1031 – Network Intrusion Prevention	C2 over HTTP/DNS to saumottam.ru, pool.minexmr.com, using port 5555	Block outbound traffic on uncommon ports like 5555 and known C2 domains/IPs
	DS0029 – Network Traffic		Monitor for persistent external communication or beaconing behavior
T1496 – Resource Hijacking (Impact)	DS0013 – Sensor Health Monitoring	bprocess.exe used CPU/GPU for Monero mining; high CPU/network usage seen	Alert on high resource usage by background or unauthorized processes
	DS0029 – Network Traffic		Detect and block outbound traffic to crypto mining pools and related domains/IPs with Deep Packet Inspection or firewall rules

Figure 58: Security Recommendations Mapped to MITRE ATT&CK Framework

To support the above controls, the diagram below illustrates the proposed security architecture. It shows how different layers of defence, such as secure web proxies, firewalls, and endpoint detection, work together to block exploit kits, control traffic, and prevent lateral movement within the network. The image highlights key mitigations, including blocking malicious communication attempts, ensuring the effectiveness of the security measures.

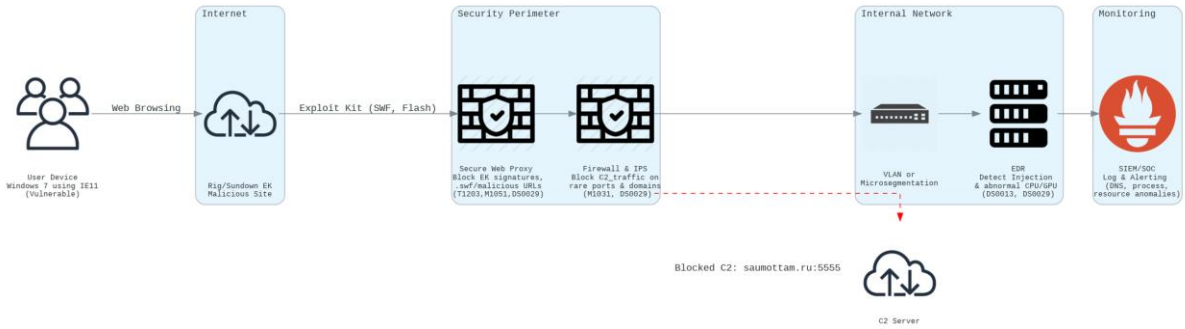


Figure 59: Secure Network Design

5.3.3 NIST Cybersecurity Framework (CSF)

The following outlines how to align the organization's cybersecurity framework with NIST Cybersecurity Framework (CSF) to improve risk management, threat detection, and incident response processes.

- **Identify (ID.RA-1)** – Conduct ongoing vulnerability assessment to detect at-risk assets.
- **Protect (PR.PS-02)** – Regularly patch all systems and remove end-of-life. This also aligns with ISO/IEC 27001 control A.12.2.1, which emphasizes up-to-date malware protection, timely patching, and user awareness beyond basic antivirus solutions (ISMS.online, 2024.
- **Detect (DE.CM-1, DE.AE-2)** – Improve network monitoring and anomaly detection by keeping up-to-date cyber threat intelligence in log analysis tools for better identification of threat actors, their methods, and indicators of compromise.
- **Respond (RS.MA-1, RS.CO-2)** – Have clear incident response (IR) playbooks and automated alerts to report confirmed incidents
- **Recover (RC.IM-1/ ID.IM-03)** – Lessons learned must be integrated into future planning.

6.0 Critical Reflection

6.1 What Went Well

- **Timely escalation:** The helpdesk quickly escalated the report once suspicious behaviour was noticed.
- **Comprehensive analysis:** The security team used key tools (Security Onion, VirusTotal, Kibana, Wireshark) to reconstruct the attack timeline and identify payloads.
- **Good logging and visibility:** Network logs and PCAPs enabled detailed investigation and evidence collection.

6.2 What Didn't Work

- **Delayed detection:** The attack began around 03:36 AM but wasn't reported until 09:30 AM, indicating a gap in real-time alerting or endpoint monitoring.
- **Legacy software exposure:** The use of Internet Explorer 11 on Windows 7 and Flash created exposure to known vulnerabilities.
- **Limited endpoint response:** No automatic action was taken, despite contacting known malicious domains.

7.0 References.

BleepingComputer (2023) RIG exploit kit still infects enterprise users via Internet Explorer. [Online] Available at: https://www.bleepingcomputer.com/news/security/rig-exploit-kit-still-infects-enterprise-users-via-internet-explorer/ [Accessed: 16 April 2025].

Biasini, N.(2016). Sundown EK: You Better Take Care. [online] Cisco Talos Blog. Available at: Sundown EK: You Better Take Care [Accessed 16 Apr. 2025].

Cyber and Fraud Centre (2024) Cyber Strategy for Small Organisations. [Online] Available at: https://www.flipsnack.com/57FD8577C6F/cyber-and-fraud-centre-cyber-strategy-forsmall-orgasniations/full-view.html [Accessed : 15 April,2025].

EC-Council (2022) The Cyber Kill Chain: The Seven Steps of a Cyberattack. [Online] Available at: https://www.eccouncil.org/cybersecurity-exchange/threat-intelligence/cyber-kill-chain-seven-steps-cyberattack/ [Accessed: 16 April 2025].

European Union. (n.d.) Article 25 GDPR – Data protection by design and by default. [Online] GDPR.eu. Intersoft Consulting. Available from: https://gdpr-info.eu/art-25-gdpr/ [Accessed 15 April 2025].

European Union. (n.d.) Article 32 GDPR – Security of processing. [Online] GDPR.eu. Intersoft Consulting. Available from: https://gdpr-info.eu/art-32-gdpr/ [Accessed 15 April 2025].

European Union. (n.d.) *Article 33 GDPR* – Notification of a personal data breach to the supervisory authority. [Online] Available from: https://gdpr-info.eu/art-33-gdpr/ [Accessed 15 April 2025].

Falco (2022). Falco detects cryptomining activity using syscall monitoring. [online] Falco. Available at: https://falco.org/blog/falco-detect-cryptomining/ [Accessed 16 Apr. 2025].

Fraunhofer FKIE. (no date) SmokeLoader – Malpedia. [Online] Available from: https://malpedia.caad.fkie.fraunhofer.de/details/win.smokeloader [Accessed 16 April 2025].

ISMS.online (2024) Annex A.12: Operations Security – ISO/IEC 27001. [Online] Available at: https://www.isms.online/iso-27001/annex-a-12-operations-security/#what-is-the-objective-of-annex-a126 [Accessed 16 Apr. 2025].

Lockheed Martin. (no date) Cyber Kill Chain. [Online] Available from: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html [Accessed 16 April 2025].

MBCProject. (2022) HTTP Communication – Micro Behaviors of Cybersecurity (mbc-markdown). [Online] GitHub. Available from: https://github.com/MBCProject/mbc-markdown/blob/main/micro-behaviors/communication/http-communication.md [Accessed 25 March 2025].

MITRE ATT&CK, 2024. Smoke Loader (S0226). [Online] Available at: https://attack.mitre.org/software/S0226/ [Accessed: 16 April 2025]

MITRE ATT&CK. (2023) DLL Search Order Hijacking (T1574.002). [Online] Available from: https://attack.mitre.org/techniques/T1574/002/ [Accessed 15 April 2025].

MITRE ATT&CK. (2023) Hijack Execution Flow (T1574). [Online] Available from: https://attack.mitre.org/techniques/T1574/ [Accessed 15 April 2025].

MITRE ATT&CK. (2023) Non-Application Layer Protocol (T1095). [Online] Available from: https://attack.mitre.org/techniques/T1095/ [Accessed 15 April 2025].

MITRE ATT&CK. (2023) Process Injection (T1055). [Online] Last modified: 30 March 2023. Available from: https://attack.mitre.org/techniques/T1055/ [Accessed 15 April 2025].

MITRE ATT&CK. (2024) Command and Scripting Interpreter (T1059). [Online] Last modified: 15 October 2024. Available from: https://attack.mitre.org/techniques/T1059/ [Accessed 15 April 2025].

MITRE ATT&CK. (2024) Drive-by Compromise (T1189). [Online] Last modified: 15 October 2024. Available from: https://attack.mitre.org/techniques/T1189/ [Accessed 15 April 2025].

MITRE ATT&CK. (2024) Exploitation for Client Execution (T1203). [Online] Last modified: 15 October 2024. Available from: https://attack.mitre.org/techniques/T1203/ [Accessed 15 April 2025].

MITRE ATT&CK. (2024) Resource Hijacking (T1496). [Online] Available from: https://attack.mitre.org/techniques/T1496/ [Accessed 15 April 2025].

MITRE ATT&CK. (2024) Web Protocols (T1071.001). [Online] Available from: https://attack.mitre.org/techniques/T1071/001/ [Accessed 15 April 2025].

NIST (2024) CSF 2.0 – Implementation Examples. [Online] Available at: https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fwww.nist.gov%2Fsystem%2Ffiles%2Fdocuments%2F2024%2F02%2F21%2FCSF%25202.0-Implementation_Examples.xlsx [Accessed: 16 April 2025].

NIST. (2022) CVE-2015-8651 Detail. [Online] Available from: https://nvd.nist.gov/vuln/detail/CVE-2015-8651 [Accessed 15 April 2025].

Tidmarsh, D. (2023) Diamond Model of Intrusion Analysis: What, Why, and How to Learn, Ethical Hacking, 7 November. [Online] Available at: https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/diamond-model-intrusion-analysis/ [Accessed: 16 April 2025].

VirusTotal. (no date) Detection – File: 535d02392f19fccc890133bc044fe17ef31500e17045c72458482e07b9aa37db. [Online] Available from: https://www.virustotal.com/gui/file/535d02392f19fccc890133bc044fe17ef31500e17045c72458482e07b9aa37db/detection [Accessed 25 March 2025].

VirusTotal. (no date) Domain: pool.minexmr.com – Detection. [Online] Available from: https://www.virustotal.com/gui/domain/pool.minexmr.com/detection [Accessed 25 March 2025].

VirusTotal. (no date) Domain: saumottam.ru – Relations. [Online] Available from: https://www.virustotal.com/gui/domain/saumottam.ru/relations [Accessed 25 March 2025].

VirusTotal. (no date) File: 535d02392f19fccc890133bc044fe17ef31500e17045c72458482e07b9aa37db. [Online] Available from: https://www.virustotal.com/gui/file/535d02392f19fccc890133bc044fe17ef31500e17045c72458482e07b9aa37db [Accessed 25 March 2025].

VirusTotal. (no date) File: 9deb6f277e2f657ff65c650c9f59a55e1fafa31e61928c49a2276fe2c4d7ec07. [Online] Available from: https://www.virustotal.com/gui/file/9deb6f277e2f657ff65c650c9f59a55e1fafa31e61928c49a2276fe2c4d7ec07 [Accessed 25 March 2025].

VirusTotal. (no date) File: e3d4ec3b6fdfe4cc100b4a3c9315041b5aa715f5715a4667e23d03fb3b4d8d2e. [Online] Available from: https://www.virustotal.com/gui/file/e3d4ec3b6fdfe4cc100b4a3c9315041b5aa715f5715a4667e23d03fb3b4d8d2e [Accessed 25 March 2025].

VirusTotal. (no date) IP Address: 10.1.11.1. [Online] Available from: https://www.virustotal.com/gui/ip-address/10.1.11.1 [Accessed 25 March 2025].

VirusTotal. (no date) IP Address: 104.236.16.69 – Relations. [Online] Available from: https://www.virustotal.com/gui/ip-address/104.236.16.69/relations [Accessed 25 March 2025].

VirusTotal. (no date) IP Address: 104.236.160.225 – Relations. [Online] Available from: https://www.virustotal.com/gui/ip-address/104.236.160.225/relations [Accessed 25 March 2025].

VirusTotal. (no date) IP Address: 104.92.3.176 – Relations. [Online] Available from: https://www.virustotal.com/gui/ip-address/104.92.3.176/relations [Accessed 25 March 2025].

VirusTotal. (no date) IP Address: 188.165.214.95. [Online] Available from: https://www.virustotal.com/gui/ip-address/188.165.214.95 [Accessed 25 March 2025].

VirusTotal. (no date) IP Address: 188.227.16.131. [Online] Available from: https://www.virustotal.com/gui/ip-address/188.227.16.131/details [Accessed 25 March 2025].

VirusTotal. (no date) IP Address: 204.79.197.200. [Online] Available from: https://www.virustotal.com/gui/ip-address/204.79.197.200 [Accessed 25 March 2025].

VirusTotal. (no date) IP Address: 23.34.132.22 – Details. [Online] Available from: https://www.virustotal.com/gui/ip-address/23.34.132.22/details [Accessed 25 March 2025].