INVESTIGATION OF A MALWARE INTRUSION

DONNA NAADU BOTCHWAY

APRIL 21, 2025

VIDEO LINK

Executive Summary

Date: 20 February 2025

Target: Windows 7 workstation (10.1.11.101) with outdated Internet Explorer 11 (Client Outreach Department).

Incident: Charlie reported pop-ups and system slowdown to Helpdesk (Lola) who suspected malware, marked it high alert & escalated.

Attack Type & Severity: Drive-by download via Exploit Kit (Rig/Sundown activity) exploiting CVE-2015-8651 (Flash). A medium to high severity.

Payloads: Smoke Loader trojan and Monero crypto miner.

Attack Duration: Approximately 7 minutes (3:36 - 3:43 AM); bypassed detection.

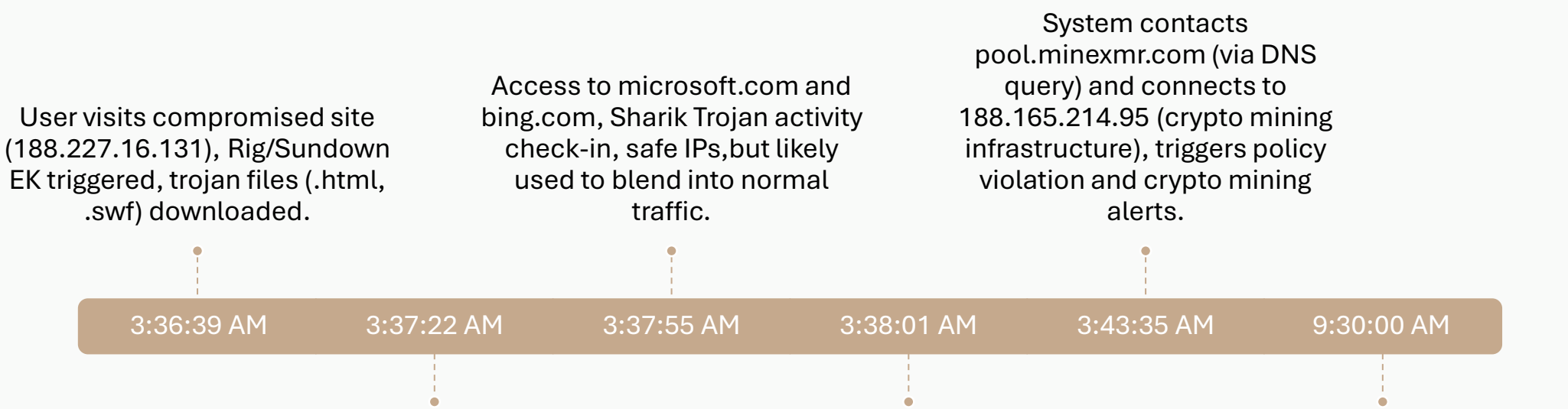
Tools Used: Security Onion Suite (Sguil, Network Miner, Kibana, Wireshark), VirusTotal.

Frameworks Mapped: Diamond Model, Cyber Kill Chain, MITRE ATT&CK (T1189:Drive-by Compromise, T1496:Resource Hijacking).

Identified Gaps: Outdated software and no automated alerting.

Recommendations: Patch management, Deploy Endpoint Detection and Response (EDR) , NIST CSF adoption.

Intrusion Timeline



Root Cause and Impact Analysis

Root Cause

- Exploit of unpatched Flash and IE11, enabling Sundown/Rig Exploit Kit to deliver trojan and crypto miner payloads.

Impact – Medium to High

- **Availability**: System slowdown due to Monero miner using CPU/GPU resources.
- **Integrity**: Potential tampering due to persistent mining, no direct evidence.
- **Confidentiality**: Malware presence risks unauthorized access, no direct data theft.

Patterns

- Repeated malicious IP connections and file downloads (MZ headers).
- Suspicious DNS queries to mining pool domains.

LESP Considerations

- **Ethical & Legal:** Adhered to ISO/IEC 27037, GDPR Art.25 (privacy-by-design), but malware pose privacy risk requiring assessment under GDPR breach notification (Art. 33)
- **Social**: Malware on a client-facing system risks reputational damage and loss of client trust, transparency and mitigation are needed.
- **Professional Responsibility**: Incident handled ethically, but reliance on user reporting highlighted the need for proactive monitoring.

Device Compromised & Indicators of Compromise (IOCs)

Compromised Device: Windows 7 workstation (IP: 10.1.11.101) using outdated Internet Explorer 11, used by Charlie (Client Outreach).

Indicators of Compromise (IOCs):

- 188.227.16.131 – Rig/Sundown Exploit Kit delivery
- 104.236.160.225 (saumottam.ru) – C2 server (Smoke Loader / Monero miner)
- 104.236.16.69 – bprocess.exe download (Monero miner)
- 188.165.214.95 – Crypto mining infrastructure (Minexmr pool)
- pool.minexmr.com – Known Monero crypto mining pool

File hashes:

- bprocess.exe – Malicious executable used for mining
- .html / .swf files – Dropped by exploit kit during initial compromise

See Evidence Portfolio 3.4, 3.5 for more detail.

Alerts Raised - Intrusion Detection

Security Onion (Sguil & Kibana) detected multiple alerts confirming malicious activity on Charlie's device (10.1.11.101) between 03:36 AM – 03:43 AM.
See Evidence Portfolio (Chapters 2 & 3) for full details.

- **Exploit Detected –** Visit to compromised site triggered Rig/Sundown Exploit Kit alerts known for exploiting browser and Flash vulnerabilities.
- **Malware Communication (C2) –** System connected to saumottam.ru, a known trojan C2 server (Smoke Loader).
- **Malicious Download –**bprocess.exe, an executable was downloaded from a malicious IP and likely executed to start crypto mining.
- **Cryptocurrency Mining Activity –** The system connected to a Monero mining server, triggering policy violation and mining alerts.

Packet captures from Wireshark and NetworkMiner, showing HTTP connections, DNS queries, and malicious file downloads supported alerts.

Methodology

A structured investigation using network traffic and malware analysis techniques:

1. **Data Collection:** Extracted artifacts from PCAPs, DNS logs, and downloaded files.
2. **Detection & Traffic Analysis:** Analysed Security Onion alerts and network.
3. **Reputation Checks:** Verified SHA1 hashes, IPs, and domains via VirusTotal.
4. **Technique Mapping:** Aligned attack with Diamond Model, Cyber Kill Chain, and MITRE ATT&CK.
5. **Impact & Remediation:** Assessed impact and suggest solutions.

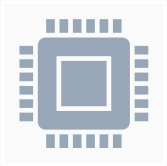
❖ **Evidence Sources:**

Security alerts (Exploit kit, Trojan and crypto miner indicators)

DNS logs, HTTP traffic, and dropped files

Threat intel (VirusTotal lookups for files/IPs)

Background of Malware and Exploit Kits



Sundown Exploit Kit

A web-based exploit kit that delivers malware via compromised sites or malvertising. It scans for outdated Flash/Silverlight plugins and uses standard file extensions like .swf or .xap. Known for simplicity over stealth (Biasini, 2016).

Rig Exploit Kit

An “exploit-as-a-service” platform active since 2014. Distributes malware through drive-by downloads, exploiting browser/Flash vulnerabilities. Frequently delivers trojans, stealers, and miners (BleepingComputer, 2023).

Smoke Loader (Sharik Trojan)

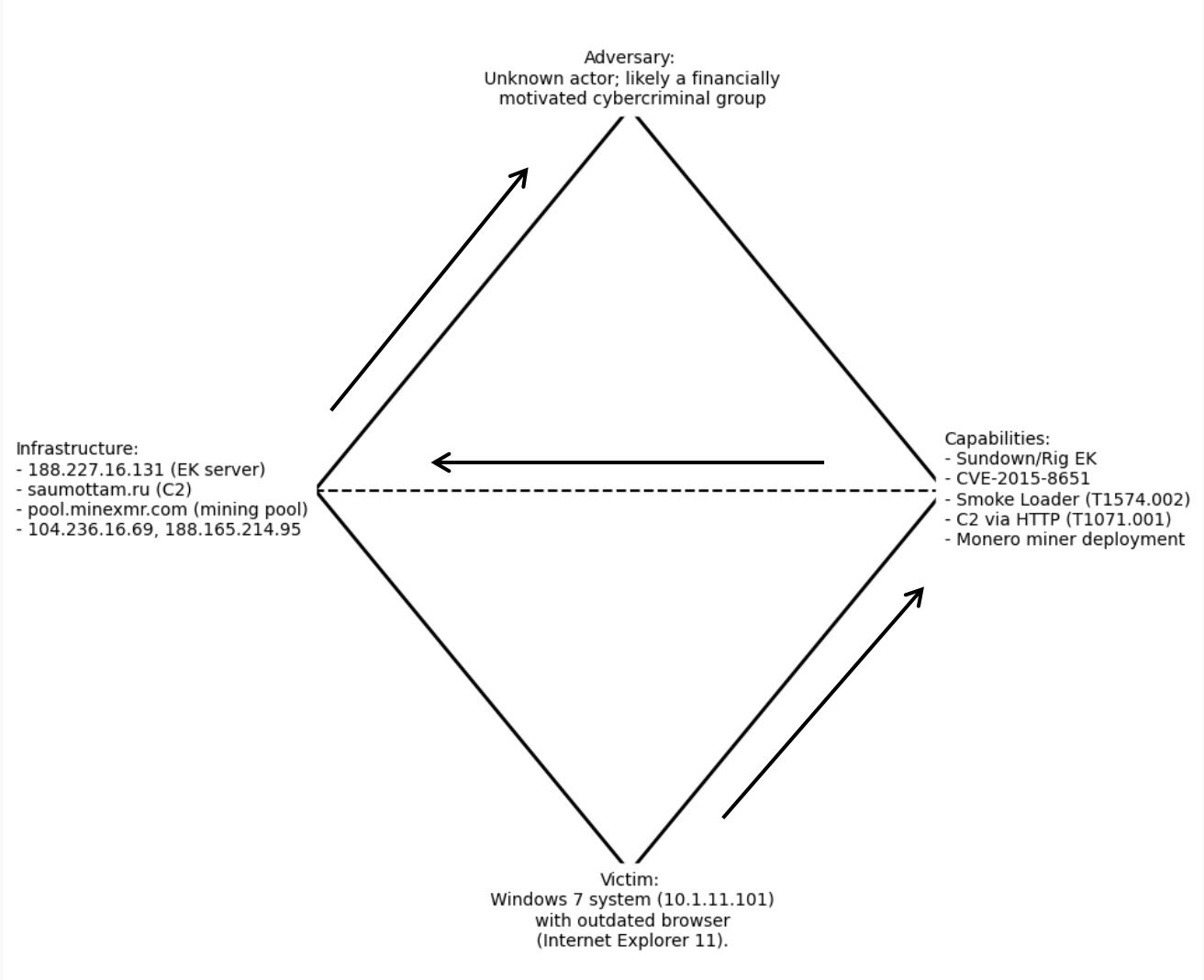
A modular trojan dropper used to install other malware such as info-stealers, ransomware, or miners. Known for using DLL side-loading and disguising traffic through common domains (MITRE, 2024).

Cryptocurrency Miners

Mining malware hijacks system resources (CPU/GPU) to generate cryptocurrency. Often stealthy, causing slowdowns without data theft. Common in post-compromise stages (Falco, 2022).

Diamond Model of Intrusion

The Diamond Model shows how the attacker, their tools, and the victim are connected (Tidmarsh, 2023). More in Evidence Portfolio 4.2.1.



Cyber Kill Chain

Reconnaissance

- Not directly observed but attacker likely scanned for vulnerable targets through web exploit.

Weaponization

- Prepares .html downloader and .swf Flash exploit.

Delivery

- Payloads delivered via HTTP from a compromised site after redirect.

Exploitation

- .html triggers .swf to exploit Flash (CVE-2015-8651).

Installation

- Smoke Loader installs bprocess.exe (Monero miner).

Command & Control

- Communication with malicious domains (saumottam.ru, 188.227.16.131).

Actions on Objectives

- System resources hijacked to mine Monero.

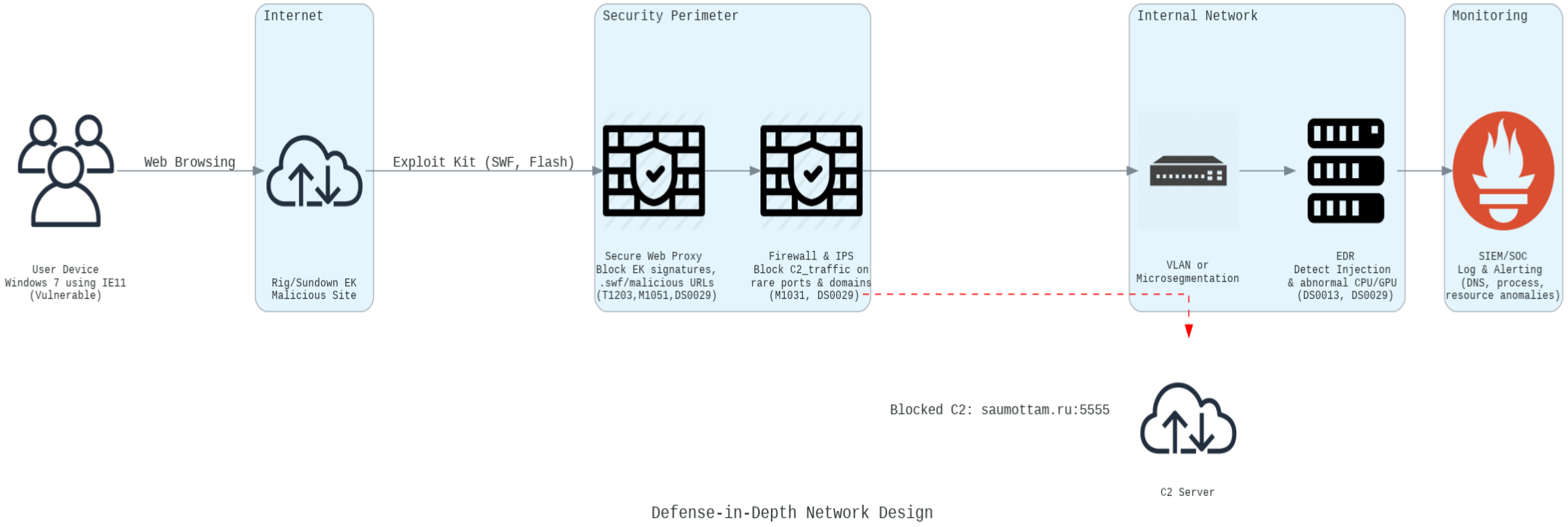
Defensive Recommendations (MITRE ATT&CK)

These MITRE ATT&CK-based recommendations defend against Sundown/Rig EK, Smoke Loader, and Monero mining, reducing future attack risks. See Evidence Portfolio 4.2.3 and 5.2.3 for more

Technique	Observed Behaviour	Defensive Measures
T1189 – Drive-by Compromise	User accessed Sundown EK site, redirected to Rig EK	Remove IE11 and use modern browsers to reduce exploit risk (M1051); monitor traffic for exploit kit patterns (DS0029)
T1203 – Exploitation for Client Execution	.swf exploited browser to run malware	Remove Flash and keep browsers patched (M1051); detect obfuscated script traffic (DS0029)
T1055 – Process Injection	Malware injected into legit processes	Detect injection via EDR tools and monitor for abnormal DLL/module loads (M1040, DS0011)
T1095 / T1071.001 – C2 Protocols	C2 over HTTP/DNS to saumottam.ru, port 5555	Block C2 domains/ports and detect persistent outbound traffic (M1031, DS0029)
T1496 – Resource Hijacking	Mining via bprocess.exe, high CPU/network use	Alert on abnormal resource usage and block traffic to mining pools (DS0013, DS0029)

Secure Network Design: Defence Against Malicious Web Traffic

This shows how the suggested network design defends against threats from malicious web traffic using layered security and MITRE-mapped controls.



Conclusion & Reflection

Identified Gaps

- The attack succeeded due to the use of deprecated software, specifically Flash and IE11.
- Windows 7's lack of security updates contributed to increased system vulnerability.
- The absence of automated defence measures and vulnerability assessments further enabled the success of the attack.

Immediate Actions

- Isolate system (10.1.11.101) to prevent further spread. (NIST CSF: Respond RS.MA-1)
- Delete malicious files (index.html, bprocess.exe) and run full malware scan. (Cyber Essentials: Protection from Malware)
- Update systems, patch vulnerabilities, and remove deprecated software (Flash) (NIST CSF: Protect PR.PS-02)

Long-Term Actions

- Update IDS/firewalls to detect and block malicious traffic and domains. (NIST CSF: Detect DE.CM-2, Cyber Essentials)
- Deploy EDR tools (e.g., Microsoft Defender) to monitor suspicious activities. (NIST CSF: Detect DE.CM-1, Respond RS.CO-2)
- Conduct employee training on safe browsing and software risks. (NIST CSF: Protect PR.AT-1)

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].

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].

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

References

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].

THANK YOU