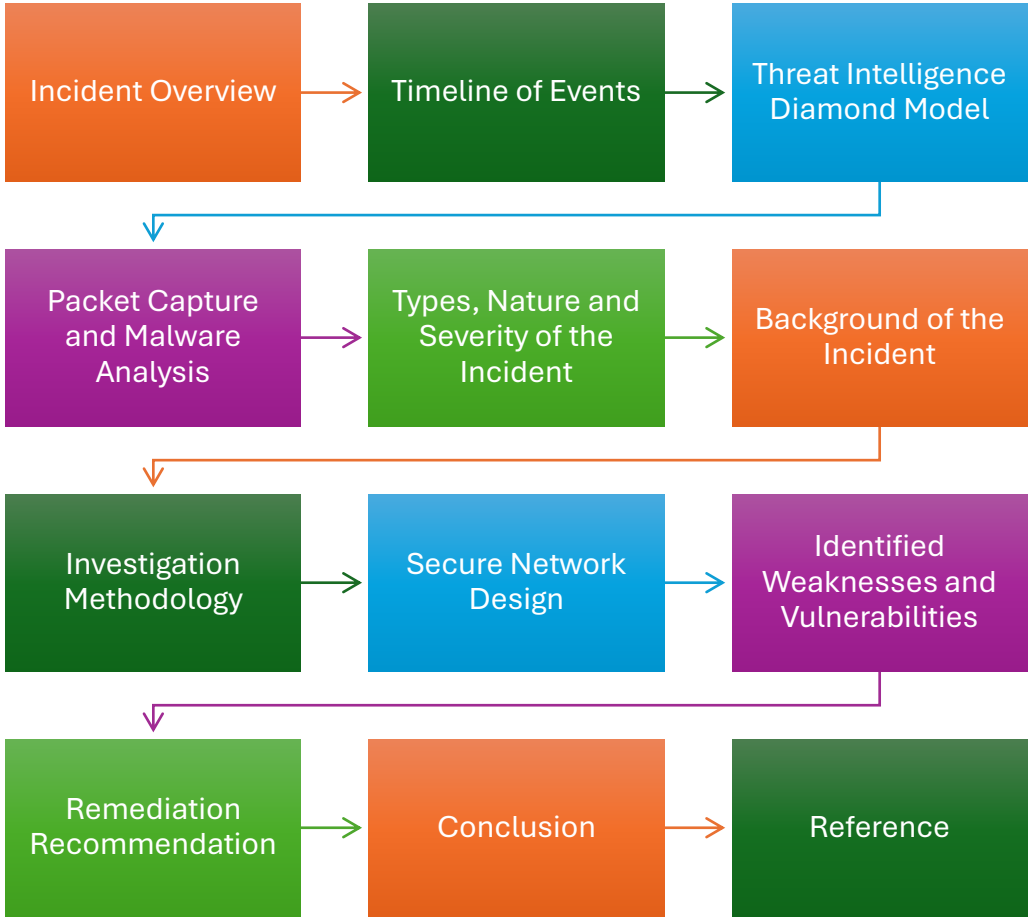
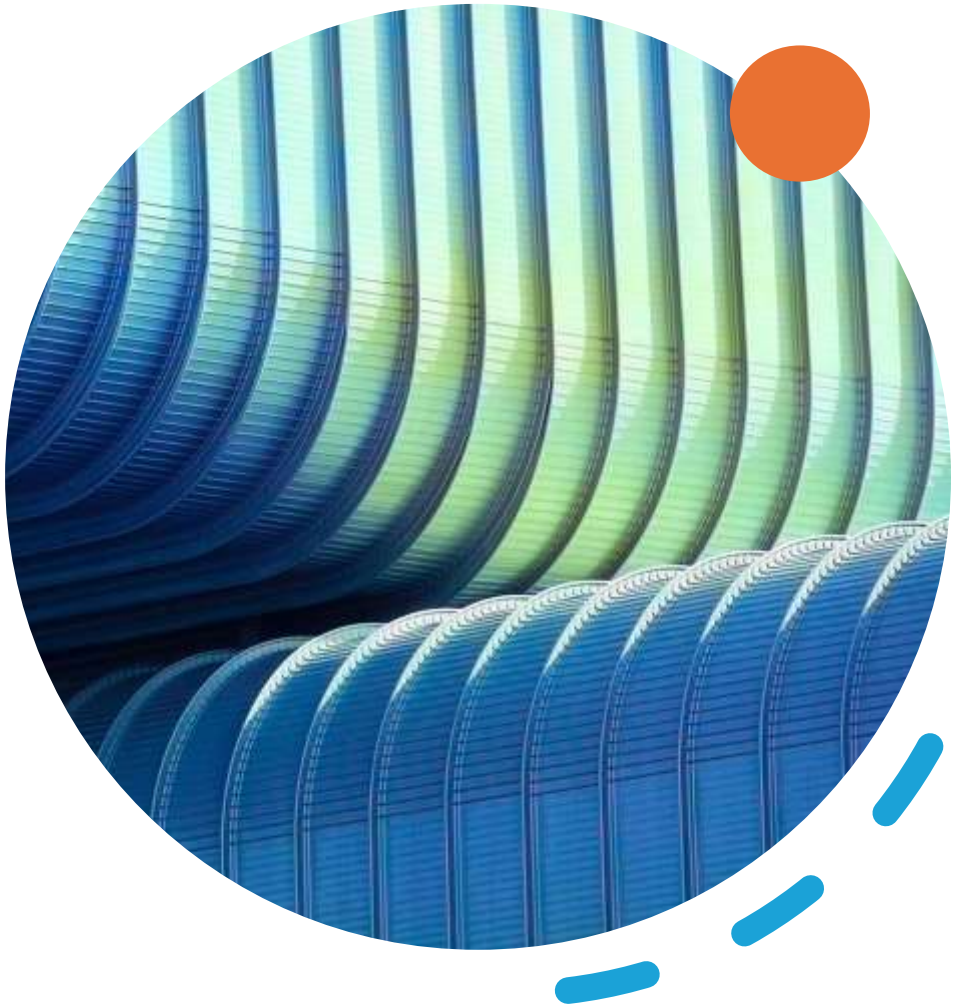
Network Intrusion Event Presentation

By

Usiwoghene Ekebor

Roadmap


Incident Overview
Timeline of Events
Threat Intelligence Diamond Model
Packet Capture and Malware Analysis
Types, Nature and Severity of the Incident
Background of the Incident
Investigation Methodology
Secure Network Design
Identified Weaknesses and Vulnerabilities
Remediation Recommendation
Conclusion
Reference



Incident Overview

Incident Date: February 20, 2025

Incident Type: Trojan-based malware infection and cryptocurrency mining exploitation

Target Device: Windows XP Machine with IP address 10.1.11.101

Attacker IP: Multiple Malicious IPs

Key Findings:

- Malware downloaded (HTML, SWF, EXE files)
- Connection to crypto-mining domain pool.minexmr.com
- System resources used for cryptocurrency mining

Timeline

2025-02-20 03:36:39 - Initial trojan files downloaded with a GET request: HTML & SWF

2025-02-20 03:38:01 - Download of .exe file "bprocess.exe" (MZ signature)

2025-02-20 03:43:35 - A DNS query was sent to 10.1.11.1 which seem to be the IP of pool.minexmr.com domain.

2025-02-20 03:43:35 - TCP connection to crypto-mining pool (188.165.214.95:5555)

Incident duration: 7 minutes

Threat Intelligence Diamond Model

Adversary: Unidentified attacker exploiting malware for cryptocurrency mining

Capability: Malware delivery through malicious GET requests, execution of "bprocess.exe" for mining

Infrastructure: Malicious domains (188.227.16.131, 104.236.16.69, 10.1.11.1 pool.minexmr.com)

Victim: Device at IP 10.1.11.101 (compromised and used for mining)

Packet Capture and Malware Analysis

Packet Capture Evidence:

- Malicious GET requests to download trojan files
- Execution of "bprocess.exe" leading to communication with a crypto-mining domain
- DNS query sent to to 10.1.11.1
- TCP Connection Initiated to 188.165.214.95 for mining related activities

Malware Analysis:

- .HTML file downloaded from **188.227.16.131**
- .SWF flash file downloaded from **188.227.16.131**
- Executable file “bprocess.exe” with MZ signature downloaded from **104.236.16.69**

Types, Nature, and Severity of the Incident

- **Type**: Cyberattack involving trojan malware and cryptocurrency mining
- **Attack Nature**: External exploitation for resource hijacking (cryptocurrency mining)
- **Severity**:
  - Affected system performance (slowness)
  - Potential data breach (exploitation of resources for illicit purposes)
  - High risk of further infections or lateral movement in the network

Background of the Incident

Threat Landscape:

- Rising trends in malware attacks targeting devices for cryptocurrency mining
- Use of trojan-based malware to bypass traditional defences

Previous Incidents:

- Similar attacks observed in 2024 where systems were hijacked for mining purposes
- The use of malicious executable files as a common attack vector

Investigation Methodology and Detailed Findings

- **Methodology**:
  - **MITRE ATT&CK Framework**
  - Identified the attack techniques and mapped it out to understand the attacker's behaviour.
    - Squill and Kibana logs used to track the sequence of events
    - Packet captures analysed to identify malicious payloads and network connections
    - Hash analysis of downloaded files to confirm malware
- **Cyber Kill Chain**
  - **Reconnaissance**: The attacker identifies vulnerable system (IP 10.1.11.101).
  - **Weaponization**: Malicious files (.html, .swf, .exe) are prepared for delivery.
  - **Delivery**: The trojan files are delivered through GET requests:
    - .html and .swf files from **188.227.16.131**.
    - bprocess.exe from **104.236.16.69**.
  - **Exploitation**: The files are executed, and the system is compromised (bprocess.exe executed).
  - **Installation**: Crypto-mining software is installed, initiating unauthorized mining.
  - **Command & Control (C2)**: Communication with pool.minexmr.com to mine cryptocurrency.
  - **Actions on Objectives**: The system experiences slow performance due to mining activities.

Secure Network Design

Network Segmentation:

- Isolate critical systems and devices to limit lateral movement

Firewall Protection:

- Implement stricter firewall rules to block access to known malicious IPs

Intrusion Detection System (IDS):

- Continuous monitoring for unusual traffic patterns and suspicious file downloads

Endpoint Protection:

- Deploy advanced endpoint protection softwares with malware detection

Secure Communications:

- Encrypt sensitive data and network traffic to protect from interception

Identified Weaknesses and Vulnerabilities

Lack of Endpoint Security: Failure to detect trojans and malicious downloads

Unfiltered HTTP Traffic: Insecure GET requests led to malware downloads

Cryptocurrency Mining Exposure: Inability to detect or block connections to mining pools

Outdated OS: Windows XP no longer get security support and patches from Microsoft

Remediation Recommendation

Malware Detection: Implement stronger malware detection solutions and file integrity monitoring

Network Monitoring: Enable deep packet inspection to detect malicious traffic

System Hardening: Update and patch vulnerable systems, especially legacy ones like Windows XP

Access Control: Limit unnecessary external network communications and restrict administrative access

Conclusion

- **Key Findings**: The system was compromised through trojan malware, with its resources hijacked for cryptocurrency mining. Logs indicated a well-coordinated attack with targeted malicious file downloads.
- **Recommendation**: Stronger security measures, continuous monitoring, and patch management are critical to prevent future incidents.
- **Impact**: The attack severely affected the device’s performance and put the organization at risk of further exploitation.

References

- 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.