Report on Malware Attack

Date: February 27, 2025

Prepared By: Ajibade Kabir

---

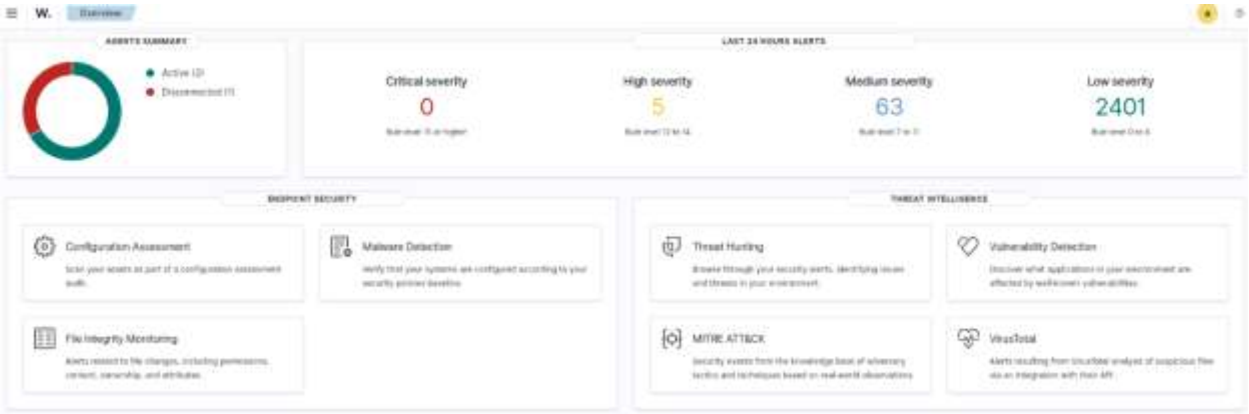
1. Summary of Incident

A malware attack was detected from one of the computers on our network, this attack which appeared to have originated from a word (.doc) document allowed the malware to infect the system. The malware is well known on many antimalware service providers such as virustotal and on malware bazaar.

2. Chronology of Events

- **Initial Notification and Response**

This activity was picked up through our SIEM and it raised five (5) critical level alerts on the computer that was infected on the dashboard.



Configuration Assessment: Scan your assets as part of a configuration assessment audit.

Malware Detection: Verify that your systems are configured according to your security policies baseline.

File Integrity Monitoring: Alerts related to file changes, including permissions, content, ownership, and attributes.

Threat Hunting: Browse through your security alerts, identifying issues and threats in your environment.

Vulnerability Detection: Discover what applications in your environment are affected by well-known vulnerabilities.

MITRE ATT&CK: Security events from the knowledge base of adversary tactics and techniques based on real-world observations.

VirusTotal: Alerts resulting from VirusTotal analysis of suspicious files via an integration with their API.

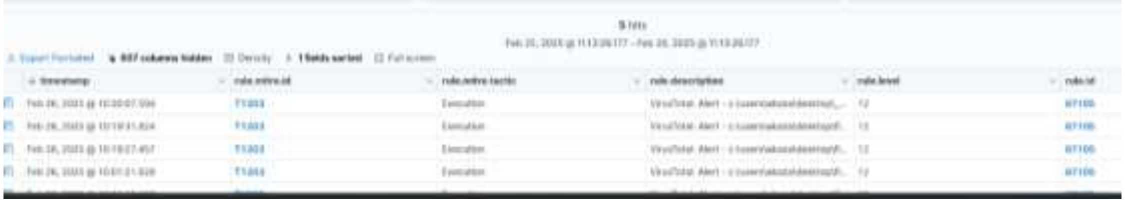
Fig1:SIEM alert on dashboard

- **Discovery and Follow-Up**

The source of this malware is a group of files which were downloaded by the unsuspecting user on the computer (agent 003) which is running a windows 10 operating system.

In order to investigate further I looked into the alert and found the files and their locations and found the following on SIEM.

- Agent (Endpoint Affected): DESKTOP-LCO16JU (192.168.43.161)
- File Path: c:\users\akaza\desktop\filez.doc
- VirusTotal Detection:
  - Malicious: Yes (1 engine detected it)
  - Positives: 34 antivirus engines flagged this file as malicious
  - Total Scans: 64 engines scanned the file
  - Threat Source: VirusTotal flagged the file based on its SHA1 hash
  - Scan Date: 2026-02-22 12:04:34
- Rule Level: 12 (Critical)
- File could be an exploit (MITRE ID T1203 - Exploitation for Client Execution).
- PCI DSS Violation: Affects security monitoring and intrusion detection compliance.
- GDPR Violation: Suggests possible data breach risks.



5 hits

Feb 25, 2025 @ 11:13:26.177 - Feb 26, 2025 @ 11:13:26.177

timestamp	rule.mitre.id	rule.mitre.tactic	rule.description	rule.level	rule.id
Feb 26, 2025 @ 10:30:07.556	T1203	Execution	VirusTotal: Alert - c:\users\akaza\desktop\...	12	87105
Feb 26, 2025 @ 10:19:31.824	T1203	Execution	VirusTotal: Alert - c:\users\akaza\desktop\f...	12	87105
Feb 26, 2025 @ 10:19:27.457	T1203	Execution	VirusTotal: Alert - c:\users\akaza\desktop\f...	12	87105
Feb 26, 2025 @ 10:01:21.828	T1203	Execution	VirusTotal: Alert - c:\users\akaza\desktop\f...	12	87105

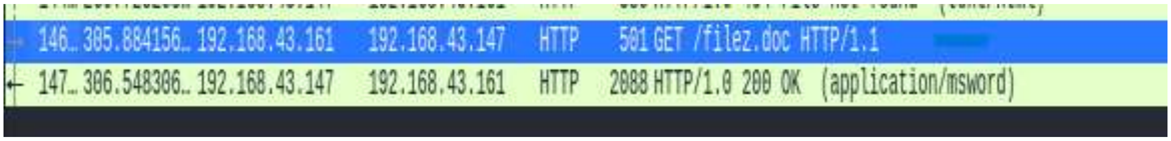
Social Engineering

This attack was later discovered to be executed through a phishing mail to the victim claiming to be from Google. The victim downloaded the file (word document) and the malware began through it.

3. Analysis

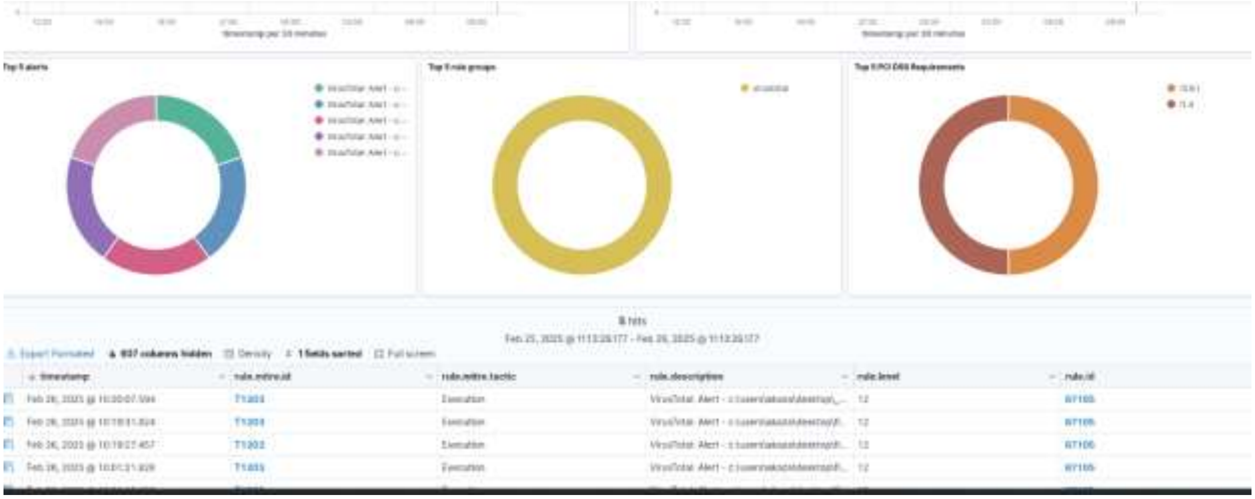
Social Engineering Attack: Phishing mail from (supposed) google scholarship grant.

I identified the source of the file by monitoring packets from the date of the attack through wireshark. Upon filtering the http requests, the source IP of the infected file was shown to be at 192.168.43.147. Looking at the requests to and from this IP address, I discovered other zip file from this origin and deleted it.



```
→ 146… 305.884156… 192.168.43.161   192.168.43.147   HTTP    501 GET /filez.doc HTTP/1.1
← 147… 306.548306… 192.168.43.147   192.168.43.161   HTTP   2088 HTTP/1.0 200 OK  (application/msword)
```

Fig 3: captured packet of infected file download



8 hits

Feb 25, 2025 @ 11:13:28.177 - Feb 26, 2025 @ 11:13:28.177

timestamp	rule.mitre.id	rule.mitre.tactic	rule.description	rule.level	rule.id
Feb 26, 2025 @ 10:30:07.594	T1203	Execution	VirusTotal Alert - c:\users\[illegible]	12	87105
Feb 26, 2025 @ 10:18:51.824	T1203	Execution	VirusTotal Alert - c:\users\[illegible]	12	87105
Feb 26, 2025 @ 10:19:27.457	T1203	Execution	VirusTotal Alert - c:\users\[illegible]	12	87105
Feb 26, 2025 @ 10:01:21.828	T1035	Execution	VirusTotal Alert - c:\users\[illegible]	12	87105

4. Actions Taken

1. I Isolated the Affected Device (DESKTOP-LCO16JU): Disconnect it from the network to prevent further spread.

2. Investigated the File (filez.doc): Check the file's VirusTotal report.

Manually updated the Windows Defender and scanned the file with Windows Defender. Once the file was confirmed to be malicious, I deleted it immediately.

3. I Performed a Full System Scan on the Affected Device using Windows Defender.

4. I updated Security Policies by blocking execution of .doc macros.

5. I blocked the IP address which was the origin of the malicious file.

5. Recommendations

1. Train employees to avoid opening unknown email attachments
2. Train employees to doublecheck on any email received requesting to follow a link or download a form

6. Conclusion:

The malware attack was carried out through social engineering techniques known as phishing mail, this is when a victim is sent an email from an attacker disguising as a legitimate corporation or firm in order to trick them into giving personal details or downloading infected files.

This attack was executed through a ms-word document and was flagged by SIEM and was confirmed on virustotal as a dangerous malware, this PC was disconnected from the network and the malware was eliminated and restored back to the network.