Malware Traffic Detection and Analysis Report

Executive Summary

This report analyzes malware traffic where a system attempted to download a malicious KeePass (.kdb) file via HTTP from a flagged IP (192.241.205.137). The file had a high VirusTotal detection score (61/67), confirming its severity. Conversely, no DNS tunneling or beaconing was detected, further monitoring is recommended to identify potential delayed C2 activity. Finally, to mitigate risks, blocking IoCs, enhancing network security (TLS inspection, firewall rules), and enforcing endpoint protection are strongly advised.

Overview

This report details the analysis of malware traffic captured in a sandboxed environment using Wireshark. The goal of this investigation was to detect Indicators of Compromise (IoCs), analyze network traffic patterns, and assess potential security risks. A sample malware was executed in an isolated virtual machine, and its communication patterns were monitored. The analysis revealed that the malware attempted to download a malicious file from a suspicious IP address flagged by multiple security vendors.

1. Traffic Patterns Observed

1.1 Network Communication Details

- Source IP: `10.0.2.15` (Sandboxed VM)
- Source Port: `49912`
- Destination IP: `192.241.205.137` (Malicious server)
- Destination Port: `80` (HTTP)
- Protocol: `HTTP`
- Observed Malicious Request:
  - `GET /download00/eicar.com HTTP/1.1`
  - The malware attempted to download or drop a file from http://rb3.ftnt.io/download00/eicar.com
- Packet captures (PCAPs) were used for validation. Network traffic was captured and analyzed using Wireshark to verify the attempts to download or drop the file. The PCAP analysis confirmed the malicious request were observed.

🔹 Finding: The malware used unencrypted HTTP communication to retrieve a malicious payload. This indicates a lack of encryption, making the traffic easier to monitor but also vulnerable to interception.

1.2 VirusTotal Results (Destination IP)

- 3/94 security vendors flagged `192.241.205.137` as malicious
- Hosted by: DigitalOcean, LLC
- Location: San Francisco, California, USA

🔹 Finding: The IP is linked to a malicious server used to distribute malware payloads. The low detection rate (3/94) suggests it may be a new or low-profile threat.

2. Indicators of Compromise (IoCs)

2.1 Malicious File Downloaded or Dropped

- MD5 Hash: `69630e4574ec6798239b091cda43dca0`
- SHA256 Hash: `131f95c51cc819465fa1797f6ccacf9d494aaaff46fa3eac73ae63ffbdfd8267`
- File Size: `69 bytes`
- File Extension: `.Kdb` (KeePass database format)
- File Hex Signature: `58 35`
- VirusTotal Detection Score: 61/67 (Highly malicious)
- Behavior: Drops or downloads additional virus files

🔹 Finding: The malware file was downloaded from a known malicious source and has a high VirusTotal detection score, confirming it as a dangerous threat.

2.2 Malicious IP Address

- IP Address: `192.241.205.137`
- This IP has been active for 11.7 years, suggesting it may have been repurposed for malicious use.
- Registrar Name: `ARIN`
- ISP: `DigitalOcean, LLC`
- Organization: `AS14061 DigitalOcean, LLC`
- Contact Email: `abuse@digitalocean.com`

🔹 Finding: This IP is long-standing but may have been compromised or repurposed for malicious activity.

3. Malware Traffic Evasion Techniques

Real-world malware often uses evasion tactics to avoid detection by security tools. Some techniques that could be observed include:

3.1 Traffic Obfuscation

- Malware may encrypt or encode its communication to bypass security monitoring.

- In this case, the use of HTTP instead of HTTPS makes it easier to analyze, but future variants may use encryption. Future malware variants will likely use AES, RC4, XOR, or hybrid encryption techniques to obfuscate network traffic. However, TLS fingerprinting can help detect future encrypted malware variants, even if AES, XOR, or Base64 are used for payload encryption.
- Behavioral analysis & machine learning will enhance TLS fingerprinting to detect more advanced threats.

3.2 DNS Tunneling

- Malicious domains often use fast-flux DNS or dynamic domain generation to avoid blacklisting.
- The analyzed malware did not show DNS tunneling behavior but used an IP-based connection, reducing its dependency on DNS resolution.

3.3 Beaconing Activity

- Periodic communication with C2 servers is a hallmark of many malware strains.
- No periodic beaconing was detected within the monitored time window, but further long-term observation is recommended to detect delayed C2 activity.

4. Recommendations for Mitigation

4.1 Blocking Malicious IoCs

- Add the following to firewall and proxy blocklists:
  - Malicious IP: `192.241.205.137`
  - Domain: `rb3.ftnt.io`
- Implement firewall rules to block HTTP traffic from untrusted external sources, and enforce HTTPS inspection.

4.2 Network Security Enhancements

- Deploy Zeek (Bro) for network traffic analysis.
- Use TLS inspection to detect and analyze suspicious encrypted traffic.
- Also, recommended sandboxing solutions like Cuckoo Sandbox for deeper malware behavior analysis.

4.3 Endpoint Protection

- Enforce application whitelisting to prevent unauthorized downloads.
- Enable real-time antivirus scanning to block malware before execution.
- Additionally, suggested to use behavioral-based detection (EDR solutions) like CrowdStrike, SentinelOne, or Microsoft Defender ATP.

4.4 User Awareness & Phishing Prevention

- Educate users about the risks of unknown downloads and links.
- Enforce email filtering to block phishing attempts.

5. Conclusion

This analysis confirms that the executed malware attempted to download or drop a malicious file from a known malicious IP. The file was flagged as malware by 61/67 security vendors, indicating a high threat level. To prevent further infections, immediate action should be taken to block the identified IoCs, strengthen security controls, and investigate whether additional malware artifacts exist on the network.