Author: Jack Fitzgerald

LetsDefend

Official Incident Report

Date: Mar, 22, 2021, 09:06 PM

Event ID: 85

Rule Name: SOC109 - Emotet Malware Detected

Table of Contents

Alert Details

Severity: Medium

Type: Malware

Source Address: 172.16.17.45

Source Hostname: RichardPRD

File Name: 1word.doc

File Hash: 349d13ca99ab03869548d75b99e5a1d0

File Size: 188.95 Kb

Device Action: Cleaned

Based on the information provided in the alert, it appears that a suspicious **word document** has been run on host **172.16.17.45**. The alert is triggered by rule SOC109 - Emotet Malware Detected.

Upon reviewing the alert, it is observed that a file named **1word.doc** with the file hash of **349d13ca99ab03869548d75b99e5a1d0** was executed on host **172.16.17.45**.

The device action is marked **cleaned**, indicating that the malware was successfully removed from the host machine.

Overall, it appears that the **alert** may be suspicious, and further investigation is needed to identify the extent of the alert and determine if any necessary actions are required to remediate the situation.

Detection

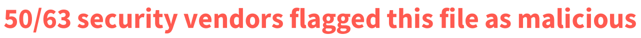
Verify

As a security analyst, one of the first steps we take to verify the alert and determine whether it is a **false positive** or a **true positive** incident is to analyse the logs collected from the host by our security products.

According to CISA, Emotet is an advanced Trojan primarily spread via phishing email attachments and links that, once clicked, launch the payload. The malware then attempts to proliferate within a network by brute forcing user credentials and writing to shared drives. Emotet is difficult to combat because of its “worm-like” features that enable network-wide infections. Additionally, Emotet uses modular Dynamic Link Libraries to continuously evolve and update its capabilities.

By investigating the word document **1word.doc**, with the MD5 hash of **349d13ca99ab03869548d75b99e5a1d0**, we can determine whether the executable along with the file is malicious or benign.

https://www.virustotal.com/gui/file/d34849e1c97f9e615b3a9b800ca1f11ed04a92b1014f55aa0158e3fffc22d78f



50/63 security vendors flagged this file as malicious

Based on the information provided by **VirusTotal**, it appears that **1word.doc** is not legit and has been flagged as malicious by many security vendors.

Analysis

The next step is to analyse the results of the **VirusTotal** file hash analysis. The macros extracted from the document exhibit several signs of malicious intent.

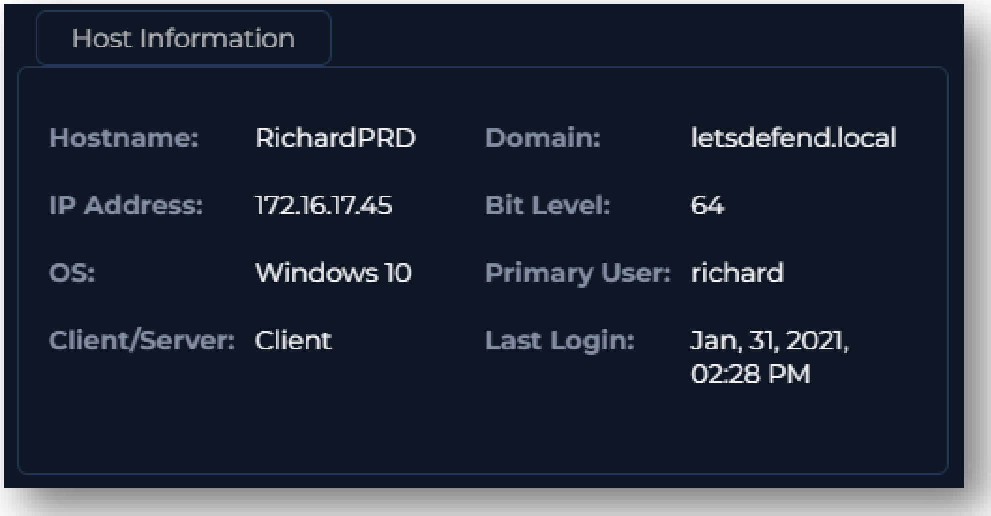
- Obfuscation
- Suspicious function calls
- Error handling
- Use of InlineShapes property
- Potential for persistence
- Use of alternative text

Analyzing the file hash using **Triage**, also identifies **1word.doc** as being malicious, via a sandbox environment.

https://tria.ge/251104-khb4ysbp8x

The next step is to investigate Endpoint Security, which can provide valuable insights into the commands executed by the user and help us understand the scope and intent of the suspicious activity.

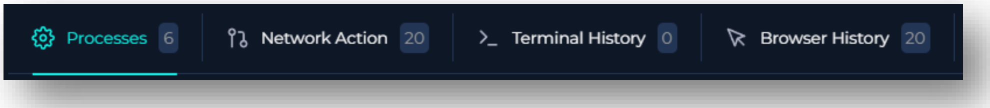
We determined some host information from here, such as Hostname, IP Address, OS, Client/Server, Domain, Bit Level, Primary User, and Last Login.



Host Information

Hostname:	RichardPRD	Domain:	letsdefend.local
IP Address:	172.16.17.45	Bit Level:	64
OS:	Windows 10	Primary User:	richard
Client/Server:	Client	Last Login:	Jan, 31, 2021, 02:28 PM

We can also investigate Processes, Network Action, Terminal History, and Browser History.



After investigating Endpoint Security, no suspicious activity was found relating to this alert.

There was also no suspicious activity related to this alert identified in Log Management.

Containment

Based on the information gathered during the investigation, it is highly unlikely that the system has been compromised. There is no need to isolate the system from the network.

Summary

The incident involves a non-compromised system named **RichardPRD** with an IP address of **172.16.17.45**. The alert was triggered by the detection of a suspicious **word document** being used, based on the rule SOC109 - Emotet Malware Detected.

Upon further analysis, it was discovered that **1word.doc** was a malicious file, containing enabled macros, acting as a Trojan, to attempt to proliferate within a network by brute forcing user credentials and writing to shared drives.

The analysis of **RichardPRD's** Endpoint Security and Log Management revealed no suspicious activity regarding this alert, due to the action of the SIEM, having **cleaned** the malware before it could be executed.

Based on the findings of the incident, no immediate action needs to be taken to isolate the compromised system, and the event was identified as a **True Positive**.

Lessons Learned

- Macros are disabled by default in Word because they can be a security risk; malicious actors use them to deliver malware, such as viruses, ransomware, or spyware

- Emotet is difficult to combat because of its “worm-like” features that enable network-wide infections. Additionally, Emotet uses modular Dynamic Link Libraries to continuously evolve and update its capabilities

Remediation Actions

- Only enable macros if you are sure, you know what they do and they come from a trusted source, as most security warnings are for files downloaded from the internet or received via email

- Apply protocols that block suspicious attachments, using antivirus software, and blocking suspicious IPs

- Adhere to the principle of least privilege

Appendix

MITRE ATT&CK

MITRE Tactics	MITRE Techniques
Defense Evasion	T1027 - Obfuscated Files or Information
Execution	T1059.005 - Command and Scripting Interpreter: Visual Basic

Artifacts

Value	Comment	Type
349d13ca99ab03869548d75b99e5a1d0	1word.doc	MD5 Hash

LetsDefend Playbook

LetsDefend Event ID: 85