Author: Jack Fitzgerald

Official Incident Report

Date: Aug, 29, 2020, 11:05 PM

Event ID: 8

Rule Name: SOC101 - Phishing Mail Detected

Table of Contents

Alert Details

Severity: Low

Type: Exchange

SMTP Address: 63.35.133.186

Source Address: info@nexoiberica.com

Destination Address: mark@letsdefend.io

E-mail Subject: UPS Express

Device Action: Allowed

Based on the information provided in the alert, it appears that a suspicious **phishing email** sent to **mark@letsdefend.io** has been detected. The alert is triggered by rule SOC101 - Phishing Mail Detected.

Upon reviewing the alert, it is observed that an email with the subject **UPS Express** was sent from **info@nexoiberica.com** with an SMTP of **63.35.133.186**.

The device action is marked **allowed**, indicating that the email was successfully delivered to the **mark@letsdefend.io** inbox.

Overall, it appears that the email 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.

By searching for the SMTP of **63.35.133.186** in Log Management, we can find the log of the email and some further details.

The first step we take when investigating a potential phishing email is to parse the email information.

When was it sent?

Aug, 29, 2020, 11:00 PM

What is the email's SMTP address?

63.35.133.186

What is the sender's address?

info@nexoiberica.com

What is the recipient's address?

mark@letsdefend.io

Analysis

The next step is to determine whether there are any **Attachments** or **URLs** in the email. If the email is malicious, the recipient may be exposed to an attack. In this case, there is an attached zip file **21b3a9b03027779dc3070481a468b211.zip** identified.

We can upload this file to online analysis tools such as **VirusTotal** and **AnyRun**, to determine its behaviour and whether this file is malicious.

https://www.virustotal.com/gui/file/2abeaf4f1a0bea26a83fc03eeaabaf1c41c9e85115caaea0010ad07c363c2dc9

11/64 security vendors flagged this file as malicious

The zip file contains 1 file named **PTD-080120 ZGO-082920.doc**, and after examining the outputs, it becomes clear that this file is malicious.

https://app.any.run/tasks/f16207fe-0981-45c0-9fdb-47e71d65df7a

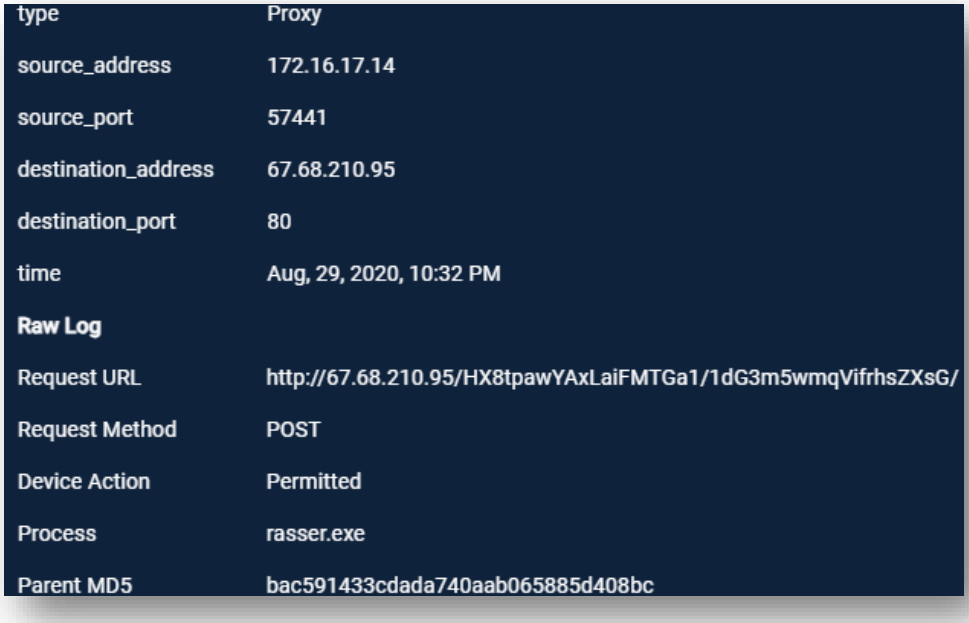
The macro-enabled word document first downloads a file from the unsecured URL **http://qstride.com/img/0/**, then requests another URL **67.68.210.95/sYRi1gXh/MT11zmUJJnEPL0yFBD/2eq2F/F9qzZD2wEYCCLpw/EJpn0u/**.

https://www.virustotal.com/gui/ip-address/67.68.210.95

9/95 security vendors flagged this IP address as malicious

We can further analyse the IP **67.68.210.95**, which happens to be the C2 address of the downloaded file.

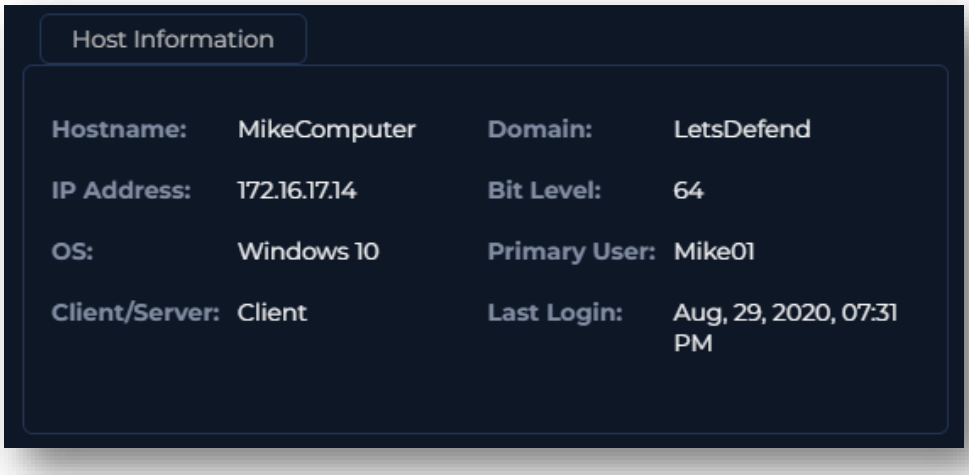
As part of the analysis, we can investigate deeper by searching for the IP of **67.68.210.95** in Log Management to determine whether the C2 address was accessed.



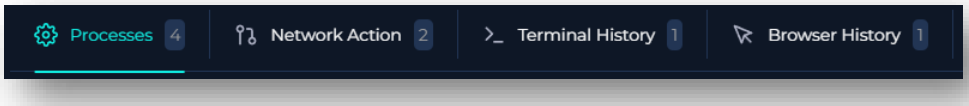
type	Proxy
source_address	172.16.17.14
source_port	57441
destination_address	67.68.210.95
destination_port	80
time	Aug, 29, 2020, 10:32 PM
Raw Log	
Request URL	http://67.68.210.95/HX8tpawYAxLaiFMTGa1/1dG3m5wmqVifrhsZXsG/
Request Method	POST
Device Action	Permitted
Process	rasser.exe
Parent MD5	bac591433cdada740aab065885d408bc

We can see here, that the C2 address was accessed at Aug, 29, 2020, 10:32 PM by device **172.16.17.14** via **http://67.68.210.95/HX8tpawYAxLaiFMTGa1/1dG3m5wmqVifrhsZXsG/**, running a process called **rasser.exe**. The device's action was permitted.

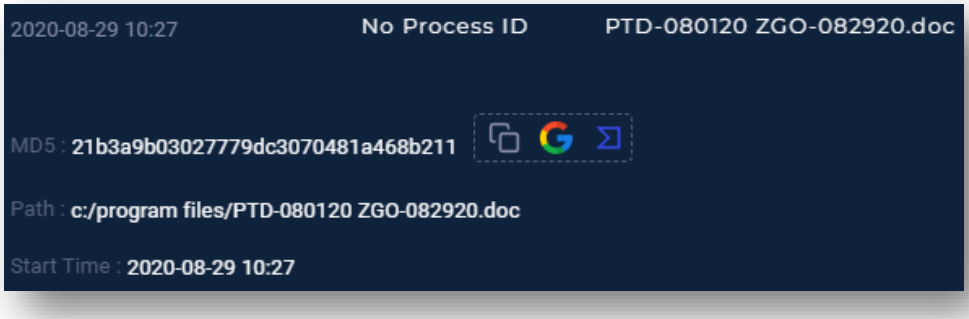
Further analysis requires us to dive into Endpoint Security, where we search for the device with the IP of **172.16.17.14**.



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



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



We have identified this process, which runs the macro-enabled word document that **mark@letsdefend.io** downloaded from their email. The process runs the malicious file **PTD-080120 ZGO-082920.doc**.

https://www.virustotal.com/gui/file/7dc9821a27cbc29bddb4bb3c708aad0b24a82d9beb1a2df9caeabf7ea6bd8e06

50/63 security vendors flagged this file as malicious

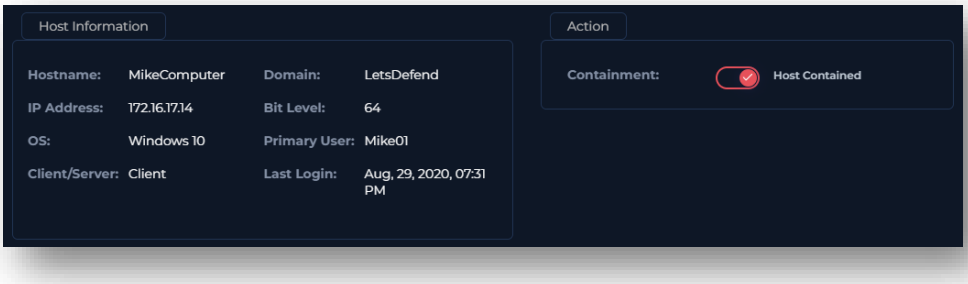
We have also identified this **powersheLL** command with **-e** being run, however, the command itself is quite obfuscated.

Containment

Based on the information gathered during the investigation, it is highly likely that the system has been compromised. To prevent further data loss or unauthorized access, it is recommended to isolate the system from the network immediately.

Isolation of the host can be made from the endpoint security tab.

Hostname	MikeComputer
IP Address	172.16.17.14



Summary

The incident involves a compromised system named **MikeComputer** with an IP address of **172.16.17.14**. The alert was triggered by the detection of a suspicious **phishing email**, sent to **mark@letsdefend.io**, based on the rule SOC101 - Phishing Mail Detected.

Upon further analysis, it was discovered that the suspicious email contained a malicious zip file containing **PTD-080120 ZGO-082920.doc**. The file was confirmed as malicious by various security vendors and online analysis tools.

The analysis of Log Management revealed that the C2 address **67.68.210.95** was accessed by **172.16.17.14**, indicating that the user of **MikeComputer** downloaded and executed the document.

The analysis of **MikeComputer's** processes revealed an instance of **PTD-080120 ZGO-082920.doc** matching the alert creation date, further substantiating the alert's authenticity. The Terminal history examination revealed a suspicious, yet obfuscated command executed by the user. This action included using **powersheLL -e**.

The findings indicate a successful phishing attempt on our LetsDefend user **mark@letsdefend.io**. The incident raises concerns about user awareness and security protocols.

Based on the findings of the incident, immediate action was taken to isolate the compromised system, named **MikeComputer** with the IP address **172.16.17.14**. Isolation is a critical step to prevent further unauthorized access and potential spread of the compromise to other systems within the network.

Lessons Learned

- Users may always be the weakest point of security within your organisation, therefore you should always allocate resources towards educating your users on security awareness and training modules

- Email security controls may be insufficient due to attackers referencing legitimate businesses, organizations, events, etc. in their subjects and message bodies

- Privilege and access management may be too permissive, as a single compromised account may grant excessive internal access

Remediation Actions

- Delete the identified email from the user's inbox and extend a block to the email sender and associated IPs and URLs

- Identify and remove any malicious files downloaded during the incident

- Isolate the compromised machine from the network to prevent the attacker from accessing other resources and systems within the domain

- Improve email filtering rules, and enable Attachment/URL scanning/sandboxing

- Conduct targeted security awareness training, focusing on social engineering recognition and reporting suspicious emails promptly

- Run simulated phishing campaigns to test and improve readiness

Appendix

MITRE ATT&CK

MITRE Tactics	MITRE Techniques
Reconnaissance	T1598.002 - Spearfishing Attachment
Initial Access	T1566.001 - Spearfishing Attachment
Execution	T1059.001 - Command and Scripting Interpreter: PowerShell
Execution	T1203 – Exploitation for Client Execution

Artifacts

Value	Comment	Type
http://qstride.com/img/0/	URL accessed	URL Address
info@nexoiberica.com		E-mail Sender
nexoiberica.com		E-mail Domain
63.35.133.186	SMTP address	IP Address
67.68.210.95	C2 address accessed	IP Address
4838f47bab3124fc72a3e89f91717b8a	21b3a9b03027779dc3070481a468b211.zip	MD5 Hash
21b3a9b03027779dc3070481a468b211	PTD-080120 ZGO-082920.doc	MD5 Hash

LetsDefend Playbook

LetsDefend Event ID: 8