EventID 93 SOC146 Phishing Mail

The SIEM created an alert of a Phishing Mail apparently triggered by Excel 4.0 Macros, let’s verify that.

The “Device Action” shows that the email was delivered to the user.

The incident is of type “Exchange”, indicating that the attack targeted Microsoft Exchange.

Microsoft Exchange is a mail server with calendar functionalities, developed by Microsoft, and used by businesses. Is possible that a Phishing Mail has been sent to this software, this is an Attack Vector.

The SIEM Rule responsible for creating this alert is called “SOC146 - Phishing Mail Detected - Excel 4.0 Macros”.

Incoming Email Information

- The email was sent the June 13th of 2021 at 14:11h
    - Sent on Sunday
- The SMTP Address is “24.213.228.54”
- The email of the sender is “trenton@tritowncomputers.com”
- The email of the recipient is “lars@letsdefend.io”
- The mail contains an attachment, its MD5 Hash is "11f44531fb088d31307d87b01e8eabff”
- The email content declares a brief and polite request to download and execute a file

Threat Intelligence Feed

I don’t find matches on VirusTotal or LetsDefend integrated Threat Intelligence Feed about the file MD5 Hash.

If it’s a malware, it could be polymorphic, so this alone doesn’t indicate the file is not malicious.

I’ve run “Get-FileHash -Algorithm SHA256 <file_name>” on PowerShell to obtain the SHA256 of the zip file, which is “38B01A12B8DCD39EBDCF9E97772E848237330EB227E1CCEE80125564B27377E5”.

I’ve pasted the SHA256 on VirusTotal, last analysis was 1 hour ago. After reanalyzing it, VirusTotal is not detecting malicious behavior on the file. There are a lot of user comments regarding this file as a malware.

As told in user comments, "https://tip.neiki.dev/” flags the SHA256 as malicious. Since the file is password protected, some security software is unable to analyze it.

I’ve dropped “iroto.dll” file on “filescan.io” and flags it as an IoC.

I’ve dropped “iroto1.dll” file on “filescan.io” and also flags it as an IoC.

VirusTotal flags “nws.visionconsulting.ro/N1G1KCXA/dot.html” address as malicious.

VirusTotal flags “royalpalm.sparkblue.lk/vCNhYrq3Yg8/dot.html” address as malicious.

Sandboxing

I’ve accessed a Windows Sandbox environment to download the attachment and analyze it.

I’ve choosen Windows in this case because the alert is targeted to Microsoft Exchange. It makes sense to me to guess that the hypotetical malware is targeted at Windows environments.

While downloading the file with Google Chrome, the browser flags the file as potential malware. After downloading it, the file explorer is unable to extract the .zip file, displaying “Error 0x80004005, Unespecified Error”.

Avoiding extraction could be intended if the malware detects the Sandbox environment. I’ve tried downloading the file again, to check the download was not corrupted, and the error persists.

I’ve also tried using Git Bash to unzip the file with “unzip” command, it failed because the command version was outdated for the version required.

Then, I’ve switched to a Linux Sandbox environment, and successfully unzipped the file with “7z” command. It was password protected, and compressed twice.

The uncompressed directory contains three files:

- iroto.dll
- iroto1.dll
- research-1646684671.xls

The presence of DDLs next to the apparently Excel document is a big red flag. I want to analyze this to get a definitive answer.

OLEVBA

OLEVBA is a Python-based tool from the oletools suite designed to detect, extract, and analyze macros in Microsoft Office files.

I've run "olevba" on the ".xls" file and the following was found:

- Presence of "EXEC" keyword which can run executable files or system commands using Excel 4 Macros
- Presence of "Hex Strings" which can be used to obfuscate strings
- Presence of "Base64 Strings" which can be used to obfuscate strings
- Presence of "XML Macro" which can execute code

The following URLs are present on the ".xls" file:

- nws.visionconsulting.ro/N1G1KCXA/dot.html
- royalpalm.sparkblue.lk/vCNhYrq3Yg8/dot.html

Logs

“explorer.exe” executed “excel.exe” at 14:20h and requested “https://nws.visionconsulting.ro/N1G1KCXA/dot.html” resource, which is an Indicator of Compromise.

Activity regarding “https://royalpalm.sparkblue.lk/vCNhYrq3Yg8/dot.html” resource has also been spotted. Excel contacted these two addresses.

There’s some serious C2 activity going on here, these logs prove it.

Excel 4.0 Macros

XLM Macros are an older, deprecated macro language from Microsoft Excel 4.0 released in 1992 that still works in modern Excel for backward compatibility.

A malicious actor can abuse from them because they:

- Evade detection because many security tools focus on VBA Macros
- Execute code silently without “Enable Content” warnings

The fact that the alert triggered for a legacy macro language doesn’t determine that it’s malware, but it’s highly suspicious that the attachment doesn’t use VBA Macros instead.

Living Of The Land Activity Detected

In Endpoint Security, I could look for the target computer system (owned by the recipient “lars@letsdefend.io”) and went to the terminal history to see if something was off.

Two executions of “regsvr32.exe” are spotted at 14:20h with “-s” flags which runs the command in silent mode.

These commands are silently registering two DDLs “iroto.dll” and “iroto1.dll” on the Windows system.

This proves that the payload reached the victim and it was executed, 9 minutes after the Phishing Email was sent (at 14:11pm).

Actions

The Endpoint has been contained first, then the Phishing Mail & downloaded attachments have been deleted.

Finally, I looked for indications of Lateral Movement in other Endpoints.

Conclusion

The attacker used social engineering, via Phishing Email, to persuade victim in order to execute an Excel file, with Excel 4 Macros embedded.

The Excel 4 Macros install DLLs leveraging LOTL tools (regsvr32.exe) to achieve persistence on the system. The macros also make contact with C2 servers, listening for instructions from the attacker.

With this information we can say this attack achieved at least Command and Control phase of Cyber Kill Chain.

Evidences point that the victim downloaded the Payload, Excel executed the Payload, and contact with C2 servers is detected.

Additionally, no more machines have made contact with the C2 servers, or contain iroto.dll/iroto1.dll files. This proves that Lateral Movement is not present.

I’ve double checked by looking for the MD5 Checksum of the original zip file on other Endpoints, no matches were found.

Attached Artifacts

- “24.213.228.54” SMTP Server Address
- “trenton@tritowncomputers.com” E-mail Sender of Payload
- “tritowncomputers.com” Domain Sender of Payload
- “nws.visionconsulting.ro/N1G1KCXA/dot.html” C2 Address
- “royalpalm.sparkblue.lk/vCNhYrq3Yg8/dot.html” C2 Address
- “11f44531fb088d31307d87b01e8eabff” Original ZIP MD5 Checksum
- “e03bde4862d4d93ac2ceed85abf50b18” (iroto.dll) MD5 Checksum
- “8e6fbefcbac2a1967941fa692c82c3ca” (iroto1.dll) MD5 Checksum
- “b775cd8be83696ca37b2fe00bcb40574” (research-1646684671.xls) MD5 Checksum