EventID 45 SOC114 Malicious Attachment Detected

- The email was sent on: 2021, (Sunday) 31th of January at 15:48h
- Source IP address: 49.234.43.39
- Source email address: accounting@cmail.carleton.ca
- Destination IP address: 172.16.17.45
  - Hostname: “RichardPRD”
- Destination email address: richard@letsdefend.io
- Subject: “Invoice”

This incident is of type “Exchange”, indicating that it’s related to Microsoft Exchange.

The device action is “Allowed”, so the email was not blocked, and reached the recipient.

About the Email

After looking for the recipient (richard@letsdefend.io) on Email Security section of LetsDefend, I've found the email related to this case:

- Contains a zip file attached to it
- The email body claims to provide an invoice for shopping that the recipient has done
    - If this was a phishing email, this could be a social engineering attack, tempting the recipient to look for an alleged invoice of shopping that actually never happened

Sandbox

I have prepared an Ubuntu VM with VirtualBox on my Windows host, in which I can download the suspicious attachment for further analysis.

Before extracting the contents of the zip attachment, I've run "zipinfo", "file" and "binwalk" commands on it to verify it's actually a zip file and that the compression rate is not unsafe to extract.

After extracting the zip file, I've run "file" command on it, which displayed the file is "CDFV2 Encrypted".

The target file is a ".xlsx", specifically an Excel Open XML Spreadsheet file. These kind of files are essentially ZIP archives containing XML and other supporting files.

The Excel file is using an older Compound File Binary (CFB) format. “CDFV2” stands for Compound Document File Version 2, which refers to the binary format used by older Microsoft Office files.

This is unusual for a “.xlsx” file, which should be a ZIP archive with XML files inside, not a CFB. This suggests:

- The file extension is misleading, it may not actually be a valid “.xlsx” file, but instead an older binary format with encryption
- Or it could be a malicious file disguised with a “.xlsx” extension, using encryption to hide its contents

I’ve tried to spot OLE objects, running “olevba” and “oleobj” commands on the “.xlsx” file, and the commands didn’t display any OLE objects.

Threat Intelligence

I’ve dropped the MD5 Hash of the Excel file on VirusTotal, in which 36/61 security vendors flag the file as malicious, mainly a Trojan.

The last analysis was recent (4 days ago).

Recent anti-virus reports on Hybrid Analysis, when searching for the MD5 Hash of the Excel file, identify it as malicious and label it as “CVE-2017-11882”.

By directly uploading the Excel file on Hybrid Analysis, the following is displayed under risk assessment:

- That the file downloads executable files on the internet
- Finds pressence of exploitation of the Equation Editor
- Finds that the Microsoft Equation Editor is executed

Additionally, by applying DNS Lookup on the source domain (cmail.carleton.ca), the resolved IP address doesn't match the source address (49.234.43.39) of the suspicious email.

What is CVE-2017-11882

Common Vulnerabilities and Exposures is a standardized naming system to identify known cybersecurity vulnerabilities. I've searched more information about this specific vulnerability on "https://www.cve.org".

Long story short, this is a vulnerability of Microsoft Office published on 2017, that allows an attacker to run arbitrary code in the context of the current user.

This vulnerability affects the Equation Editor (EQNEDT32.EXE) in Microsoft Office.

EDR

Under Endpoint Security section of LetsDefend, I've looked for the victim which is "richard@letsdefend.io" whose hostname is "RichardPRD".

The suspicious email was received at 15:48h, and the processes of the endpoint display that user Richard executed "EQNEDT32.EXE" process at 16:15h. This is Microsoft Equation Editor, which proves that the victim executed the Excel file.

If the result of Hybrid Analysis was on the right track, the Excel file will download an executable from the internet. By looking under browser history of the endpoint in Endpoint Security, I can see that Richard requested "http://andaluciabeach.net/image/network.exe" resource:

- The time of this request is 16:15h, and matches with the execution time of the Microsoft Equation Editor process
- The requested resource is an executable
- VirusTotal flags the URL as malware, last analysis being 14h ago, at the time of writting this documentation
- The resource is requested through unencrypted HTTP

Just after the execution of "EQNEDT32.EXE", another process called "JuicyPotato.EXE" was executed at 16:20h.

JuicyPotato is a privilege escalation tool that exploits a vulnerability in Windows COM server. This tool escalates privileges from a regular user to SYSTEM, the highest privileged user on a Windows system.

JuicyPotato is a descendant of the older RottenPotato exploit, and the design flaw exploited with it is classified under "CVE-2018-0833".

I've looked for "JuicyPotato.EXE", "http://andaluciabeach.net/image/network.exe", and "andaluciabeach.net" presence on other endpoints.

Only the victim system matches with the searches, proving no signs of lateral movement.

Actions

The suspicious email has been proved to be malicious, and therefore has been deleted from the victim's mailbox.

Evidence points that the malicious file was executed, so Richard's endpoint has been contained.

Conclusion

The attacker delivered a phishing email to the victim, claiming to contain a shopping invoice attached to it. The attacker achieved delivery and exploitation through a social engineering attack.

The alleged shopping invoice was a Trojan disguised as an Excel Open XML Spreadsheet that exploited a vulnerability of Microsoft Office's Equation Editor.

Through successful exploitation of this vulnerability, the attacker executed arbitrary code on the victim's system, requesting an executable from a C2 Server.

Once the executable was downloaded, it was executed on the victim's system, with the objective of escalating privileges on the victim's system by executing JuicyPotato tool.

Once the attacker had SYSTEM privileges on the Windows machine, it could achieve persistence through the use of backdoors, or moving laterally.

Traces of lateral movement were not found in other endpoints, and the threat was contained.

Artifacts

I’ve attached the following artifacts to this case:

- “6fdf4a6ddd6f564589dd060bdc4da2c3” (MD5 Hash) zip attachment
- “c9ad9506bcccfaa987ff9fc11b91698d” (MD5 Hash) excel file
- “808502752ca0492aca995e9b620d507b” (MD5 Hash) JuicyPotato.exe
- “http://andaluciabeach.net/image/network.exe” C2 Server
- “49.234.43.39" IP address of the malware provider
- “andaluciabeach.net” domain of the malware provider