EventID 82 SOC140 Phishing Email Detected Suspicious Task Scheduler

The Task Scheduler is a Windows component that allows users to automate tasks by scheduling scripts, programs, or system operations to run at specific times or in response to certain events.

Tasks can be executed under the current user's account, any specified user account, or as SYSTEM (highest privileges).

Since Task Scheduler allows persistent execution of commands with high privileges, attackers commonly abuse it by:

- Creating tasks with payloads embedded in malicious attachments delivered in phishing emails
- Persisting malware, ensuring it runs after reboot
- Escalate privileges, by running tasks as SYSTEM

About the Incident

- Email was received: 2021, (Sunday) 21th of March at 12:26h
- Source SMTP Server address: 189.162.189.159
- Source email: aaronluo@cmail.carleton.ca
- Destination email: mark@letsdefend.io
- Device action: blocked
- Subject: “COVID19 Vaccine”

The SIEM detected suspicious activity related to the Task Scheduler in a phishing email, the device action is “blocked” indicating the email didn’t reach the user.

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

I find suspicious that the email was sent on Sunday, let’s analyze the email, and if attachments are found.

The email contains a file attached. Note that the sender is encouraging in the email to open the file attached, using Covid-19 as a pretext.

Threat Intelligence Feeds

I've uploaded the MD5 Hash of the zip file on both Karspersky and VirusTotal, to verify that the zip file itself is not dangerous.

I've also run "file" and "binwalk" commands on the zip file to double check it's safe to extract.

I've dropped the MD5 Hash of the PDF attached on the suspicious email at Karspersky threat intelligence portal and at VirusTotal.

Karspersky flags it as a Trojan disguised as a PDF, although the results are quite old.

On the other hand, VirusTotal has an analysis of 15 days ago, in which multiple security vendors flag the hash as a Trojan disguised as a PDF.

By looking for the source SMTP Server address "189.162.189.159" in Cisco Talos Intelligence, I've found the sender is located on Mexico, Leon De Los Aldama. And the IP reputation is considered poor.

By using MxToolbox SuperTool, I've checked that either "cmail.carleton.ca" or "carleton.ca" domains don't point to the source address "189.162.189.159". This means the email headers were spoofed to hide the real domain of the sender.

In fact, ".ca" TDL is located in Canada and "carleton.ca" domain belongs to Carleton University. This is definitely not located on Mexico.

Sandbox

I’m connecting to a Linux sandbox provided by LetsDefend to download the attachment and analyze it.

Since the alert detected presence of Task Scheduler instructions, I will actively look for any commands of that nature.

After running “file”, “binwalk”, “zipdetails”, and “unzip -lv” commands on the zip file, I verified it’s really a zip and the compression rate is around 1%, I’ve extracted it.

The zip file contains a PDF named “Material.pdf”.

After analyzing the PDF file with “pdfinfo” command, the output displays a suspicious author name, it was created using Foxit, and a syntax error of complex objects called “array<0a>” is displayed.

I’ve tried running other commands like “pdftotext” and “pdfdetach” with different flags on the PDF, but the output was either missing or corrupted.

Log Management

I've searched for the source email address "aaronluo@cmail.carleton.ca" and found a log entry that matches the time of the incident:

- Transmitted from 189.162.189.159:49371
  - Port 49371 is between the Ephemeral Range 49152–65535, assigned temporarily for outbound connections
  - May be obfuscated C2 traffic
- Transmitted to 172.16.20.3:25
  - Port 25 is primarily used for SMTP, unencrypted by default. Modern systems often use SMTPS on port 465 or STARTTLS on port 587
  - Spam bots often target open port 25 to relay spam

Looking in the EDR, I found the destination IP "172.16.20.3" to be an Exchange Server, and just to make sure, no commands have been executed by the time of the incident.

I've also looked for the presence of the zip attachment and PDF file on other endpoints, and no matches are found.

Artifacts

I've attached the following IoCs to this incident:

- "189.162.189.159" IP address of the sender
- "957774f297ae3c13d233bb0ba2dfc352" (MD5 Hash) zip attachment
- "72c812cf21909a48eb9cceb9e04b865d" (MD5 Hash) Material.pdf

Conclusion

The attacker sent a phishing email containing a Trojan disguised as a PDF. With the tactic DNS Spoofing, the attacker claimed to be from legitimate entity Carleton University located in Canada. This was proven because the source domain and source IP don't match.

In fact, the attacker sent the phishing email from Mexico, and the zip file attached contains a PDF that doesn't behave as expected, which suggests to be insecure.

The victim never received the phishing email because the Microsoft Exchange server blocked it, and no evidence of IoCs present on other endpoints was found.