Incident Report 2025-11-11

Title:
Date:
Alert Type/Category:
Severity: Low / Medium / High / Critical
Analyst Name:
Case #:

DETECTION AND ANALYSIS

Alert Summary:

The user karin.larsen@silverline.no was observed downloading the potentially malicious file "AppSuite-PDF-1.0.28.exe" on the host WIN10-SL-312. This file is flagged as malicious by 21/47 vendors on VirusTotal and it can be observed that the file's signature has been revoked [1].

After the download we see that the user executes the installer file AppSuite-PDF-1.0.28.msi from the downloads folder. Following this several files are installed and the executable PDFEditor.exe is executed with the –instalol flag. Several files are created including:
- %USERPROFILE%\AppData\Roaming\PDF Editor\pdfeditor.js
- C:\Program Files\AppSuite PDF Editor\resources\UtilityAddon.node

We also observe the creation of the following registry key:
HKCU\Software\Microsoft\Windows\CurrentVersion\Run\PDFEditorUpdater = ""%USERPROFILE%\PDF Editor\PDF Editor.exe –cm=–fullupdate\

This key will execute "PDF Editor.exe" every time the user logs on to the system [2]. We also observe the creation of a scheduled task with a daily trigger that also executes this program.

Further alerts indicate that the program was used to dump credentials stored in the browser and initiated communications with the potential C2 addresses product.update-appsuite[.]com and y2iax5[.]com.

References:

[1]
https://www.virustotal.com/gui/file/cb15e1ec1a472631c53378d54f2043ba57586e3a28329c9dbf40cb69d7c10d2c
[2] https://learn.microsoft.com/en-us/windows/win32/setupapi/run-and-runonce-registry-keys

Key Details:

User account: karin.larsen@silverline.no
SHA256:
- cb15e1ec1a472631c53378d54f2043ba57586e3a28329c9dbf40cb69d7c10d2c (PDF Editor.exe)
- da3c6ec20a006ec4b289a90488f824f0f72098a2f5c2d3f37d7a2d4a83b344a0 (pdfeditor.js)
- 6022fd372dca7d6d366d9df894e8313b7f0bd821035dd9fa7c860b14e8c414f2 (chrome_killer.exe)

C2 address:
- product.update-appsuite[.]com
- y2iax5[.]com

Consequence:

This indicates that the host is infected with potentially malicious software that has obtained persistence on the system through scheduled tasks and the Run registry key. The activity suggests that the passwords in the browser was dumped and potentially exfiltrated, as such these credentials should be considered compromised.

CONTAINMENT

Executed Remediation Actions:

- Initiated quarantine of the identified files
- Isolated the endpoint
- Reset password, and revoked all sessions

Recommended Remediation Actions:

- Re-image the host to ensure the malware is properly evicted from the system
- Ask user to rotate all password, since browser credentials were dumped.