Incident Report 2025-11-11

Title:
TamperedChef malware via trojanized AppSuite PDF installer (malvertising)

Date:
2025-10-29

Alert Type/Category:
Malware Infection

Severity:
Medium

Analyst Name:

Case #:
INC-20251029-7001

DETECTION AND ANALYSIS

Alert Summary:

Microsoft Defender detected a suspicious file download and subsequent malware execution on host WIN10-SL-312 used by Karin Larsen. This activity aligns with a malvertising-driven trojanized installer that deployed the TamperedChef infostealer, aiming to establish persistence, harvest browser credentials, and communicate with command-and-control (C2) infrastructure. The user followed a Google ad to vault.appsuites[.]ai and downloaded AppSuite-PDF-1.0.28 (hash fde67ba523b2c1e517d679ad4eaf87925c6bbf2f171b9212462dc9a855faa34b; 39/VT vendors flag malicious [1]); the installer invoked msiexec, unpacked PDFEditor.exe (sha256 6fd6c053f8fcf345efaa04f16ac0bffe), created persistence via HKCU Run key PDFEditorUpdater and a scheduled task, and loaded an obfuscated module pdfeditor.js. Execution of PDFEditor.exe with the update switch triggered browser-killer behavior (UtilityAddon.node/elevate.exe), dumped browser credential stores to %LOCALAPPDATA%\Temp\cred_dump_20251029.bin, and initiated TLS egress to product.update-appsuite[.]ai (earlier resolving via vault.appsuites[.]ai) and y2iax5[.]com; outbound volume was observed around 1.1 MB. Defender AV then identified the sample as TamperedChef, confirming a credential-stealing compromise with C2 communication and persistence present. We recommend that you investigate this activity further, as the activity appears to have resulted in credential exfiltration.

```
msiexec.exe /i C:\Users\karin.larsen\Downloads\AppSuite-PDF-1.0.28.msi /quiet
```
Executes the MSI installer silently.

```
"C:\Program Files\AppSuite PDF Editor\PDFEditor.exe" --cm=--fullupdate
```
Runs the trojanized PDFEditor with its update switch that loads the infostealer module and attempts C2.

References:

[1]
https://www.virustotal.com/gui/file/fde67ba523b2c1e517d679ad4eaf87925c6bbf2f171b9212462dc9a855faa34b

Key Details:

User: karin.larsen@silverline.no (Karin Larsen)
Host: WIN10-SL-312
Source IP: 85.162.45.9
First Event Time: 2025-10-29 09:59:12+0000
Last Event Time: 2025-10-29 10:06:05+0000
Downloaded File: AppSuite-PDF-1.0.28.msi
Downloaded File Hash (sha256): fde67ba523b2c1e517d679ad4eaf87925c6bbf2f171b9212462dc9a855faa34b
Installed Binary: C:\Program Files\AppSuite PDF Editor\PDFEditor.exe
Installed Binary Hash (sha256): 6fd6c053f8fcf345efaa04f16ac0bffe
Related Files:
- %USERPROFILE%\AppData\Roaming\PDF Editor\pdfeditor.js (sha256: b3ef2e11c855f4812e64230632f125db5e7da1df3e9e34fdb2f088ebe5e16603)
- C:\Program Files\AppSuite PDF Editor\resources\UtilityAddon.node (sha256: 6022fd372dca7d6d366d9df894e8313b7f0bd821035dd9fa7c860b14e8c414f2)
Persistence (Registry Run): HKCU\Software\Microsoft\Windows\CurrentVersion\Run\PDFEditorUpdater = "%USERPROFILE%\PDF Editor\PDF Editor.exe –cm=–fullupdate"
Persistence (Scheduled Task): \Microsoft\Windows\PDFEditorScheduledTask (daily)
Credential Dump Artifact: %LOCALAPPDATA%\Temp\cred_dump_20251029.bin
Commands Executed: msiexec.exe /i C:\Users\karin.larsen\Downloads\AppSuite-PDF-1.0.28.msi /quiet
Commands Executed: "C:\Program Files\AppSuite PDF Editor\PDFEditor.exe" –cm=–fullupdate
Process Chain: explorer.exe -> msiexec.exe -> PDFEditor.exe -> "PDF Editor.exe" -> UtilityAddon.node (browser-kill)
Domains:
- vault.appsuites[.]ai
- product.update-appsuite[.]ai
- appsuites[.]ai
- y2iax5[.]com
Observed Egress: TLS SNI=product.update-appsuite[.]ai (~1.1 MB outbound)
AV Detection: Trojan:Win32/TamperedChef.A on PDFEditor.exe
Persistence Indicator: Deviation score 94/100 (autostart, browser-kill, early C2)

Consequence:

This incident indicates confirmed host compromise with credential theft. Browser credential stores were accessed and dumped, and outbound communications to suspected C2 were established, suggesting potential exfiltration of saved credentials and session data. Persistence was installed via registry Run key and a scheduled task, increasing the likelihood of reinfection after reboot. Stolen credentials may enable unauthorized access to internal and external services, potential lateral movement, and account takeover.

CONTAINMENT

Executed Remediation Actions:

The following containment and eradication actions has been performed by our SOC:
- Isolated host WIN10-SL-312 from the network (wired and wireless) due to confirmed TamperedChef activity and observed credential exfiltration.

- Quarantined suspicious files on the endpoint: PDFEditor.exe, pdfeditor.js, UtilityAddon.node, elevate/helper binaries, and installer artifacts.
- Triggered a full AV/EDR scan on WIN10-SL-312 and initiated an enterprise-wide IOC sweep for the listed domains, file names, and hashes.
- Force immediate password resets for the affected user and any accounts with stored browser credentials; revoke refresh tokens and re-enroll MFA where applicable.

Recommended Remediation Actions:

Our SOC recommends that you do the following containment actions:
- Reimage WIN10-SL-312 from a known-good baseline or restore from a verified clean backup, then apply latest patches.
- Review authentication logs for signs of credential misuse and block any suspicious sessions originating after the compromise window.
- Keep network/domain blocks for the listed IOCs in place until eradication is verified; monitor for any attempts to reach these destinations.
- Run targeted scans on endpoints where AppSuite PDF Editor may have been installed; remove the application if found and check for the same persistence keys.
- Blocked known malicious file hashes across EDR and mail/web gateways:
fde67ba523b2c1e517d679ad4eaf87925c6bbf2f171b9212462dc9a855faa34b;
6fd6c053f8fcf345efaa04f16ac0bffe;
b3ef2e11c855f4812e64230632f125db5e7da1df3e9e34fdb2f088ebe5e16603;
6022fd372dca7d6d366d9df894e8313b7f0bd821035dd9fa7c860b14e8c414f2.
- Collected volatile forensics from the host: memory snapshot, running processes, network connections, autoruns, registry hives, and the cred_dump_20251029.bin file.
- Implemented temporary blocks for domains and URLs: vault.appsuites[.]ai, product.update-appsuite[.]ai, appsuites[.]ai, y2iax5[.]com at firewall, proxy, and DNS.
- Removed persistence after evidence collection: deleted HKCU Run key PDFEditorUpdater and disabled the PDFEditorScheduledTask.
- Disabled SMB/mapped shares on WIN10-SL-312 to reduce propagation risk while isolated.