TamperedChef Malware Infection via Trojanised AppSuite PDF Editor Installer 2025-10-29

Title: TamperedChef Malware Infection via Trojanised AppSuite PDF Editor Installer
Date: 2025-10-29
Alert Type/Category: Malware Infection / Credential Theft (TamperedChef trojan)
Severity: High
Analyst Name:
Case #: INC-20251029-7001

DETECTION AND ANALYSIS

Alert Summary:

Microsoft Defender Endpoint and Defender AV, correlated with Sysmon and web proxy telemetry, detected execution of a trojanised “AppSuite PDF Editor” installer on host WIN10-SL-312 used by user karin.larsen@silverline.no. This activity is consistent with a malware / trojan infection delivering an infostealer (TamperedChef family) via a malvertising-driven software download. The malware establishes persistence on the endpoint, steals browser-stored credentials and communicates with external command-and-control (C2) endpoints for data exfiltration. Logs show that the user followed a Google ad to vault.appsuites[.]ai and downloaded AppSuite-PDF-1.0.28.exe / AppSuite-PDF-1.0.28.msi to `C:\Users\karin.larsen\Downloads\`, which were executed via `msiexec.exe` and unpacked `PDFEditor.exe` into `C:\Program Files\AppSuite PDF Editor\`. Shortly after installation, additional components such as `pdfeditor.js`, `UtilityAddon.node` and a helper binary `elevate.exe` were dropped, a Run key `HKCU\Software\Microsoft\Windows\CurrentVersion\Run\PDFEditorUpdater` was created, and a scheduled task was registered to ensure recurring execution of the PDF Editor binary with the `--cm=--fullupdate` parameter. Microsoft Defender Endpoint then recorded the infostealer dumping browser credential store contents to `%LOCALAPPDATA%\Temp\cred_dump_20251029.bin` (LOG1, SHA256 `aaf6e40848b904e664cdfbefa1e42870c3e42387471a03361e4fd0781943a032`), followed by outbound TLS connections from `PDFEditor.exe` to `product.update-appsuite[.]ai`, `vault.appsuites[.]ai` and `y2iax5[.]com`, with approximately 1.1 MB of data uploaded in multiple batches consistent with credential exfiltration. Defender AV subsequently detected the TamperedChef family on `PDFEditor.exe` (SHA256 `6fd6c053f8fcf345efaa04f16ac0bffe`), confirming a malware infection sourced from the trojanised installer hash `fde67ba523b2c1e517d679ad4eaf87925c6bbf2f171b9212462dc9a855faa34b` originally downloaded from vault.appsuites[.]ai. We assess that the host has been successfully infected and that browser credentials have likely been exfiltrated to attacker infrastructure, creating a high risk of account takeover for any services where the user had saved passwords; we recommend that you investigate this activity further, as the activity appears to represent successful credential theft and an ongoing compromise until the endpoint is fully remediated.

```
%USERPROFILE%\PDF Editor\PDF Editor.exe --cm=--fullupdate
```

This command is used in the HKCU Run key and scheduled task to automatically launch the trojanised PDF editor at user logon and on a daily schedule, maintaining persistence and enabling repeated C2 communication and data theft.

Key Details:

User: karin.larsen@silverline.no (Karin Larsen)
Host: WIN10-SL-312
Source IP: 85.162.45.9
Customer: Silverline Retail Corp
Department: Operations

Downloaded Installer: AppSuite-PDF-1.0.28.exe
Downloaded MSI: AppSuite-PDF-1.0.28.msi
Downloaded Installer SHA256:
fde67ba523b2c1e517d679ad4eaf87925c6bbf2f171b9212462dc9a855faa34b

Primary Malware Binary: C:\Program Files\AppSuite PDF Editor\PDFEditor.exe
PDFEditor.exe SHA256: 6fd6c053f8fcf345efaa04f16ac0bffe

Credential Dump File: %LOCALAPPDATA%\Temp\cred_dump_20251029.bin (LOG1)
Credential Dump SHA256: aaf6e40848b904e664cdfbefa1e42870c3e42387471a03361e4fd0781943a032

Supporting Components:
- %USERPROFILE%\AppData\Roaming\PDF Editor\pdfeditor.js
- C:\Program Files\AppSuite PDF Editor\resources\UtilityAddon.node
- elevate.exe (helper binary dropped alongside resource DLLs)

Domains:
- vault.appsuites[.]ai
- appsuites[.]ai
- product.update-appsuite[.]ai (C2 / update endpoint)
- y2iax5[.]com (additional C2 endpoint)

Persistence:
- HKCU\Software\Microsoft\Windows\CurrentVersion\Run\PDFEditorUpdater -> `%USERPROFILE%\PDF Editor\PDF Editor.exe --cm=--fullupdate`
- Scheduled task \Microsoft\Windows\PDFEditorScheduler -> `%USERPROFILE%\PDF Editor\PDF Editor.exe` (Trigger: Daily)

Command Executed:
- `msiexec.exe` installing AppSuite-PDF-1.0.28.msi with a quiet parameter (silent installation of the trojanised PDF editor)
- `C:\Program Files\AppSuite PDF Editor\PDFEditor.exe --cm=--fullupdate` (runtime with update/communication mode)

Process Chain:
- explorer.exe → BrowserDownload/Edge → msiexec.exe (AppSuite-PDF-1.0.28.msi) → AppSuite_PDF_Editor_v1.0.28.exe → PDFEditor.exe (`--cm=--fullupdate`)

Malware Signature: Trojan:Win32/TamperedChef.A (Microsoft Defender AV detection on PDFEditor.exe)

Network Activity:
- HTTP(S) download of AppSuite PDF installer from vault.appsuites[.]ai
- HTTP request from PDFEditor.exe to https://appsuites[.]ai/api/s3/new?fid=ip&version=1.0.28
- TLS connections from PDFEditor.exe to product.update-appsuite[.]ai and y2iax5[.]com
- Netflow summary: ~1.1 MB outbound to vault.appsuites[.]ai / product.update-appsuite[.]ai (credential exfiltration batches)

Notable Detection Events:
- EDR alert: Suspicious JavaScript module (`pdfeditor.js`) loaded by PDFEditor.exe
- EDR File.Write: Infostealer dumped browser credential store to cred_dump_20251029.bin
- AV detection: Microsoft Defender AV detected TamperedChef family on PDFEditor.exe
- Anomaly scoring: Newly installed unsigned PDF editor with persistence, credential dumping and early C2 flagged with high deviation score

Consequence:

The incident represents a confirmed malware infection with evidence of active credential theft on a user workstation in the Operations department. Browser-stored credentials have been written to a local dump file and are very likely exfiltrated to external C2 infrastructure, which can enable attackers to log in to corporate and third-party services as the affected user without needing to re-infect the endpoint. This exposes email, SaaS, VPN and other web-based accounts to potential takeover, opens a path for further lateral movement and privilege escalation, and may allow the adversary to deploy additional payloads or conduct fraud using the organisation’s retail and back-office systems. Until the endpoint is fully cleaned and all exposed credentials are reset, there is an ongoing risk of unauthorised access, data exposure and operational disruption.

CONTAINMENT

Executed Remediation Actions:

The following containment and eradication actions has been performed by our SOC:
- Isolated host WIN10-SL-312 from the network via the XDR platform to prevent further C2 communication and data exfiltration.
- Quarantined the primary malware binary (PDFEditor.exe) and associated dropped components (e.g. pdfeditor.js, UtilityAddon.node, elevate.exe) using Defender AV/XDR response actions.
- Blocked identified malicious domains (vault.appsuites[.]ai, product.update-appsuite[.]ai, y2iax5[.]com) and related file hashes in the XDR indicator blocklists for this customer tenant.
- Triggered a full Microsoft Defender AV and XDR malware scan on WIN10-SL-312 to detect and remove additional TamperedChef-related artifacts.
- Collected and preserved relevant proxy, Sysmon, EDR and AV telemetry for WIN10-SL-312 to support deeper incident investigation and potential forensic follow-up.

Recommended Remediation Actions:

Our SOC recommends that you do the following containment actions:

- Rebuild or reimage WIN10-SL-312 from a known-good, fully patched baseline image before returning it to production use.
- Remove the persistence mechanisms for the malicious PDF editor (Run key `PDFEditorUpdater` and any PDFEditor-related scheduled tasks) as part of the rebuild/clean-up process, if not automatically cleared by reimaging.
- Require an immediate password reset for user karin.larsen@silverline.no (and any other users who may have run the same installer) for all corporate and high-value external accounts, and invalidate existing browser-saved sessions where possible.
- Review authentication logs for cloud services, email and VPN for sign-ins using Karin Larsen's accounts from unusual locations, IP addresses or devices, and revoke any suspicious sessions.
- Search the environment for the known malicious file hashes (installer, PDFEditor.exe, credential dump file) and the persistence key `HKCU\Software\Microsoft\Windows\CurrentVersion\Run\PDFEditorUpdater`, and treat any additional hosts with matches as compromised and subject to the same containment and remediation steps.
- Block access to the known malvertising and distribution domains (appsuites[.]ai, vault.appsuites[.]ai, product.update-appsuite[.]ai) at web proxy and firewall level to prevent future downloads of the trojanised installer.