NCA-43.091625 – NCERT Advisory – Trojanized AppSuite PDF Editor Malware (TamperedChef)

Introduction

A malicious software campaign has been identified involving a trojanized PDF editing tool distributed as AppSuite PDF Editor. The application, originally a legitimate PDF tool, began incorporating remote JavaScript-based update mechanisms from August 21, 2025, which were later associated with unintended or unauthorized functionality.

The malware, tracked as TamperedChef, establishes command-and-control (C2) communications, exfiltrates sensitive data, enumerates installed security tools, and can deliver secondary payloads such as ransomware or spyware.

Due to its combination of social engineering techniques and post-exploitation capabilities, this campaign poses a high risk to enterprise and government networks, potentially acting as an initial access vector for advanced persistent threats (APTs).

Impact

Successful infection can lead to:

- **Confidentiality Breach** – Theft of credentials, cookies, documents, and system information.
- **Integrity Loss** – Unauthorized modification of PDF files and registry persistence changes.
- **Availability Disruption** – Potential ransomware deployment resulting in lockouts or system downtime.
- **Organizational Risk** – Initial foothold for APTs, enabling large-scale intrusions and data exfiltration.

Threat Details

Malware Overview

Threat ID	Affected Product	Description
TamperedChef	AppSuite PDF Editor (Trojanized)	Malicious PDF editing tool masquerading as freeware. Establishes C2 communication, steals credentials, terminates browsers, modifies system files, and deliver

		secondary payloads (spyware/ransomware).

Attack Complexity & Vector

Attack Vector: Local — requires user download and execution of a trojanized installer delivered via phishing, malvertising, cracked software bundles, or infected USB drives.
Attack Complexity: Low (relies primarily on social engineering).
Privileges Required: Standard user (escalates via unpatched OS/PDF library flaws).
User Interaction: Required (download and execution).

Affected Systems

Windows OS (All Versions) – Particularly unpatched systems or those without active EDR/AV solutions.
Systems with weak endpoint protections or those permitting execution from **AppData** / **Temp** directories.
Users installing "free" or "cracked" PDF editors from non-official sources.

Exploit Conditions

Exploitation requires:

User downloading and executing the trojanized installer.
Lack of endpoint protections (AV/EDR disabled or absent).
Presence of unpatched OS vulnerabilities for privilege escalation.
Success of phishing or social engineering tactics.

This malware is already active in the wild and spreading via malvertising and phishing campaigns.

Indicators of Compromise (IOCs)

File Hashes

MD5: 9f3a5d6e92c1e44a3a48b0c27d56xxxx
SHA256: 3d7a56c49d9e0a9df6c0a2c71fcbxxxx

File Paths

C:\Users\<user>\AppData\Roaming\AppSuitePDFEditor\appsuite.exe

Registry Keys

HKCU\Software\Microsoft\Windows\CurrentVersion\Run\AppSuite

Network IOCs

Domains: editor-update[.]com, pdfsuite-sync[.]net
IPs: 185.92.223[.]14, 103.89.77[.]6

Dropped Files

C:\Temp\editor_update.dll
C:\Windows\System32\pdfsvc.exe

Indicators of Attack (IOAs)

Execution of unknown PDF editor binaries from AppData.
Outbound connections to suspicious domains/hosts shortly after installation.
Registry persistence under Run keys or scheduled tasks named like *"PDF Update"*.
Silent file modifications: PDFs edited without user input.
Periodic beaconing traffic (small encrypted packets over HTTP/HTTPS).

Recommendations & Mitigation Actions

Containment & Blocking

✓ Block IOCs at firewalls, IDS/IPS, and proxies.
✓ Prevent execution from AppData and Temp paths via Group Policy / AppLocker.

Detection & Monitoring

Hunt for IOAs using EDR, Sysmon, and SIEM logs.
Monitor for beaconing traffic to malicious C2 domains.
Deploy network anomaly detection for suspicious encrypted HTTP/HTTPS traffic.

User Awareness

Educate users on risks of downloading "free" PDF editors from ads or unverified sources.
Reinforce phishing awareness training.

Hardening Systems

Apply latest OS and library patches to reduce privilege escalation opportunities.
Enforce MFA for critical accounts.
Enable and update endpoint security tools.

Incident Response Actions

Isolate affected endpoints immediately.
Reset compromised credentials.
Review lateral movement across enterprise systems.
Perform full scans to remove TamperedChef and associated payloads.

Monitoring & Detection

Track execution of binaries from unusual directories.
Review browser crash reports (due to malware-forced termination).
Use IDS/IPS and SIEM to monitor outbound connections to editor-update[.]com or pdfsuite-sync[.]net.
Alert on new persistence entries with "PDF" or "AppSuite" in registry keys/scheduled tasks.

Incident Response & Readiness

Update playbooks to include TamperedChef infection scenarios.
Validate secure backups for recovery from potential ransomware payloads.
Share IOCs and IOAs with trusted threat intel networks.

References

Rewterz Threat Advisory: https://rewterz.com/threat-advisory/malvertising-campaign-delivers-tamperedchef-stealer-via-trojanized-pdf-tools-active-iocs
Cyber Security News: New TamperedChef Attack With Weaponized PDF Editor Steals Sensitive Data and Login Credentials
Bleeping Computer: TamperedChef infostealer delivered through fraudulent PDF Editor

Call to Action

The National CERT advises all organizations to:

Block IOCs at network and endpoint layers.
Immediately hunt for active infections using provided IOAs.
Restrict software installation to verified vendors and official stores.
Apply system hardening policies (AppLocker, MFA, EDR deployment).
Incorporate this risk into enterprise threat modeling and supply-chain defenses.

Early detection and containment are critical to prevent large-scale intrusions and ransomware deployment associated with TamperedChef.