TamperedChef infostealer delivered through fraudulent PDF Editor - Again

Data: 2025-08-30 22:58:04

Autor: Inteligência Against Invaders

Threat actors have been using multiple websites promoted through Google ads to distribute a

convincing PDF editing app that delivers an info-stealing malware called TamperedChef.

The campaign is part of a larger operation with multiple apps that can download each other, some of them tricking users into enrolling their system into residential proxies.

More than 50 domains have been identified to host deceiving apps signed with fraudulent certificates issued by at least four different companies.

The campaign appears to be widespread and well-orchestrated as the operators waited for the ads to run their course before activating the malicious components in the applications, researchers say.

Full update delivers infostealer

A technical analysis from cybersecurity services company Truesec describes the process of TamperedChef infostealer being delivered to a user's system.

The researchers discovered that the malware was delivered through multiple websites that promoted a free tool called AppSuite PDF Editor.

Based on internet records, the investigators determined that the campaign started on June 26, when many of the websites involved were either registered or started to advertise AppSuite PDF Editor.

However, the researchers found that the malicious app had been verified through the VirusTotal malware scanning services on May 15th.

It appears that the program behaved normally until August 21st, when it received an update that activated malicious capabilities built to collect sensitive data like credentials and web cookies.

According to Truesec, TamperedChef infostealer is delivered with the "-fullupdate" argument for the PDF editor's executable.

The malware checks for various security agents on the host. It also queries the databases of installed web browsers using the DPAPI (Data Protection Application Programming Interface) – a component in Windows that encrypts sensitive data.

[IMAGEM REMOVIDA]

“Truesec has observed at least 5 different google campaign IDs which suggests a widespread campaign” – Truesec

The threat actor likely had a strategy to maximize the number of downloads before activating the malicious component in AppSuites PDF Editor, as they delivered the infostealer just four days before the typical expiration period of 60 days for a Google ad campaign.

Looking further into AppSuites PDF Editor, the researchers found that different versions of the program were signed by certificates “from at least four companies,” among them ECHO Infini SDN BHD, GLINT By J SDN. BHD, and SUMMIT NEXUS Holdings LLC, BHD.

Joining a residential proxy

Truesec found that the operator of this campaign has been active since at least August 2024 and promoted other tools, including OneStart and Epibrowser browsers.

It is worth noting that OneStart is usually flagged as a potentially unwanted program (PUP), which is typically the term for adware.

However, researchers at managed detection and response company Expel also investigated incidents involving AppSuites PDF Editor, ManualFinder, and OneStart, all “dropping highly suspicious files, executing unexpected commands, and turning hosts into residential proxies,” which is closer to malware-like behavior.

They found that OneStart can download AppSuite-PDF (signed by an ECHO INFINI SDN. BHD certificate), which can fetch PDF Editor.

“The initial downloads for OneStart, AppSuite-PDF, and PDF Editor are being distributed by a large ad campaign advertising PDFs and PDF editors. These ads direct users to one of many websites offering downloads of AppSuite-PDF, PDF Editor, and OneStart,” Expel.

The code-signing certificates used in this campaign have already been revoked, but the risk is still present for current installations.

In some instances of PDF Editor, the app would show users a message asking for permission to use their device as a residential proxy in return for using the tool for free.

The researchers note that the proxy network provider may be a legitimate entity not involved in the campaign and that the operatorof PDF Editor is capitalizing as affiliates.

It appears that whoever is behind PDF Editor is trying to maximize their profit at the expense of users worldwide.

Even if the programs in this campaign are considered PUPs, their capabilities are typical of malware and should be treated as such.

The researchers warn that the operation they uncovered involves more apps, some of them not yet

weaponized, capable of distributing malware or suspicious files, or executing commands surreptitiously on the system.

Both reports from Truesec and Expel [1, 2] include a large set of indicators of compromise (IoCs) that could help defenders protect users and assets from getting infected.

[IMAGEM REMOVIDA]