Separ Malware Plucks Hundreds of Companies' Credentials in Ongoing Phish

By Lindsey O'Donnell

Published: 2019-02-20 · Archived: 2026-04-05 22:40:40 UTC

An ongoing phishing campaign is targeting hundreds of businesses to steal their email and browser credentials using a simply – but effective – malware.

An ongoing phishing campaign is using malicious PDF documents to spread Separ malware and ultimately steal victims' browser and email credentials.

Since the attack started at the end of January, it has affected around 200 companies and over 1,000 individuals, located mainly in Southeast Asia, the Middle East, and North America – and the bad actors behind the attack continue to upload stolen data daily, researchers with Deep Instinct told Threatpost.

The campaign's effectiveness stems from a simple but dangerous tactic used by the Separ credential-stealer for evading detection: Using a combination of legitimate executable files and short scripts.

"Although the attack mechanism used by this malware is very simple, and no attempt has been made by the attacker to evade analysis, the growth in the number of victims claimed by this malware shows that simple attacks can be very effective," said Guy Propper with Deep Instinct in a Tuesday post.

Earlier variants of Separ have existed since November 2017, with related info-stealers being active in the wild as far back as 2013, researchers said.

What sets this stealer apart is its use of a simply but tricky technique dubbed "living off the land." Hackers have used this popular tactic in the past to launch attacks based on legitimate files which are either common within the organization attacked, or are widely-used administrative tools. The legit files can be abused to perform malicious functions.

For Separ, that means using very short script and batch files, as well as legitimate executables, to carry out all of its malicious business logic.

These legitimate executables, explained in more depth below, include a browser-password and email-password dump tools by SecurityXploded, as well as software from NcFTP.

Attack Process

The attack starts with a phishing email that contains a malicious attachment – in this case, a decoy PDF document that purports to be a self-extracting executable. According to researchers, the fake documents relate to quotations, shipments and equipment specifications, and appear to target businesses.

Once the victim clicks on the attached "PDF document," the self-extractor calls wscript.exe to run a Visual Basic Script (VB Script) called adobel.vbs.

After the VB Script begins running, it executes an array of short batch scripts which have various malicious functions. The scripts masquerade as fake Adobe-related programs, with the malicious scripts and executable files named to resemble Adobe related programs, researchers said.

"The self-extractor contains within itself all files used in the attack – a VB Script, two batch scripts and four executable files, with the following names: adobel.vbs, adob01.bat, adob02.bat, adobepdf.exe, adobepdf2.exe, ancp.exe and Areada.exe," researchers said. "Many of the files are named to resemble files related to Adobe."

These scripts carry out a slew of malicious functions, which include changing the system's firewall settings and stealing all of its email and browser credentials. Meanwhile, the malware also opens up an empty decoy .jpg image to hide its activities from the victim.

In order to steal credentials, Separ uses password-dumping tools provided by SecurityXploded. SecurityXploded, which exists in the initial self-extractor, collects various user credentials and uploads them to the hosting service.

Interestingly, the malware uses an File Transfer Protocol (FTP) client to upload its stolen data to a legitimate service called freehostia[.]com. Both this executable and the service are legitimate, researchers said: The source of ancp.exe is a real FTP software provider (NcFTP), and FreeHostia is a well-known and widely-used hosting service.

"We were able to access the FTP server several times, and the growth in the number of victims was clearly visible, meaning the attack is ongoing and successfully infecting many victims," researchers said.

Ongoing Attack

Access to the hosting service used by Separ in this recent attack shows that its activity continues, and data stolen from many additional victims is being uploaded daily, researchers said.

"The attack has affected hundreds of companies, located mainly in Southeast Asia and the Middle East, with some targets located in North America," said Propper. "Based on the names of the fake documents which initiate the attack, it appears the attacker is targeting business organizations, as most fake documents appear to be concerned with quotations, shipments and equipment specifications."

Researchers urged potential victims to restrict the use of scripts and scripting tools in their firms and avoid clicking on unknown or untrusted links: "Infection through social engineering is the most common method of infection," said Propper.

Source: https://threatpost.com/separ-malware-credentials-phishing/142009/