Jaxx Liberty Wallet Users Targeted in Malware Campaign

flashpoint-intel.com/blog/malware-campaign-targets-jaxx-cryptocurrency-wallet-users/

September 12, 2018

Blogs

Blog

Malware Campaign Targeting Jaxx Cryptocurrency Wallet Users Shut Down

A website spoofing the official Jaxx cryptocurrency wallet site has been taken down after analysts at Flashpoint discovered a number of infections linked to the operation.

A website spoofing the official Jaxx cryptocurrency wallet site has been taken down after analysts at Flashpoint discovered a number of infections linked to the operation.

The phony site had a similar URL to the legitimate jaxx[.]io site and was serving a number of custom and commodity strains of malware with the end goal of emptying Jaxx users' wallets.

Jaxx is a popular cryptocurrency wallet that has been downloaded more than 1.2 million times on desktop and mobile platforms, according to a blog published on the Jaxx site in March. Jaxx Liberty, the latest version of the wallet, supports Bitcoin, Ethereum, and more than a dozen other cryptocurrencies.

Flashpoint analysts earlier this month notified Jaxx support teams as well as the Cloudflare content delivery network. Cloudflare took steps to suspend services to the spoofed site, which was a line-by-line copy of the actual Jaxx site that included modifications made to the download links, redirecting those to an attacker-controlled server.

It should be noted that this is primarily a social engineering attack and does not involve a vulnerability in the Jaxx application, website, or other domains owned by Decentral, a Canadian blockchain startup, that provides Jaxx.

It's unclear how the attackers were luring victims to the spoofed Jaxx site, whether they were relying on poisoned search engine results, phishing via email or chat applications, or other means to infect victims.

Focus on Windows, Mac Desktop Users

The start date for this campaign figures to be Aug. 19 when the fraudulent domain was created. The attackers were targeting Windows and Mac OS X users with a variety of malware developed for the desktop platforms. Anyone who clicked on the mobile downloads were redirected to the legitimate Jaxx website.

Visitors to the fraudulent website, below, would likely believe they were on the legitimate Jaxx page since the attackers went to the trouble of installing the legitimate wallet software onto victims' computers while malware silently installed in the background.

Image 1: The fraudulent Jaxx website.***Image 1:*** *The fraudulent Jaxx website.*
Visitors clicking on the fraudulent links for the Mac OS X software were presented with a custom-built malicious Java Archive (JAR) file. The fraudulent Windows software link downloaded a custom-written .NET application, which contained not only malicious behavior (such as exfiltrating all of the victim's desktop files to a command-and-control [C2] server), but also downloaded , KPOT Stealer and Clipper, both of which are marketed on underground Russian-language cybercrime sites.

The Mac OS JAR file is programmed in PHP and compiled using a Russian language IDE called DevelNext. The Jaxx branding throughout the code indicates the malware was developed solely for this campaign.

Victims executing the JAR see a message in Russian and English: "Temporarily due to technical problems on the server, you cannot create a new wallet." Victims are then routed to the "PAIR / RESTORE WALLET" screen which prompts them for their Jaxx wallet backup phrase — a password used to decrypt wallets in order for the attackers to exfiltrate the digital currency from the victim's account. The backup phrase is then exfiltrated to the attacker's web server while the victim receives another mixed Russian and English-language error message that states, "Server is not available. Try again in 4 hours," below.

 Image 2: Malicious JAR file containing error messages in English and Russian.***Image 2:*** *Malicious JAR file containing error messages in English and Russian.*

Victims on Windows who execute the malicious link download a Zip archive called LibertyBeta-setup-2.0.9.zip from a Google Docs URL. Like the Mac OS X JAR, the malicious .NET binary was likely created specifically for this campaign. The malware reaches out to the command-and-control server where all of the local .txt, .doc, and .xls files are uploaded. The phony application then downloads three executables from hardcoded URLs: the official Liberty Beta installer, and KPOT, which steals information from the local hard drive, as well as Clipper, which monitors the clipboard for digital wallet addresses; once an address is found, it is swapped out for a wallet address controlled by the attacker. By changing these addresses in the clipboard, victims may not notice the modified recipient after copying and pasting these long alphanumeric addresses while sending payments.

Assessment

This malware campaign indicates that cybercriminals may go to great lengths to socially engineer an organization's customers into installing malware to ultimately steal digital currency. It's likely cybercriminals will continue to leverage commodity malware kits offered for sale in underground hacking forums to steal credentials and/or digital currency from victims.

To download the IOCs for this Jaxx campaign, click here for CSV and click here for MISP JSON.

 avatar

Paul Burbage

Senior Malware Researcher

Paul is a Senior Malware Researcher at Flashpoint with over 15 years of experience in the threat intelligence and information security arena. He specializes in emerging threat research, botnet tracking, and reverse engineering malware. His passion lies in finding vulnerabilities in malware command and control infrastructure.