Echelon Malware Found in Mobile Chats

safeguardcyber.com/blog/security/echelon-malware-crypto-wallet-stealer-malware

Recently, our Division Seven (D7) threat intelligence team detected a credential stealer piece of malware being posted in a cryptocurrency trading Telegram channel that we monitor as part of our work with financial service customers in the digital currency space. We analyzed and identified the malware sample as “Echelon” and reviewed the messages surrounding the post. The Echelon malware performs a variety of functions, targeting credentials, crypto wallets, and device details.

We believe that this particular incident was an isolated one-off attack meant to target new unsuspecting users of the channel. However, the incident points to the risk exposure financial institutions face as employees take to modern communication applications, including mobile chat like WhatsApp and Telegram, to conduct business. There are certainly compliance risks to business communications on these new application. However, the cybersecurity risks of employees communicating in these apps appear to be less well integrated to financial service institutions' overall security strategies.

This blog will present a summary of our analysis of Echelon, but we encourage you to download the full report for a more comprehensive analysis, including screenshot of the code.

SAFEGUARD CYBER

Malware Targeting Crypto Wallets Detected In Crypto Trading Forum

Malware Report

DIVISION SEVEN

Download Report

Threat Report: Malware Targeting Crypto Wallets Detected In Trading Forum

Malware Summary

This sample of Echelon was delivered in an .rar file titled “present).rar”. Inside it included 3 files:

- – pass - 123.txt: A Benign text document containing a password
- – DotNetZip.dll: A non-malicious - class library and toolset for manipulating zip files. (MD5 Hash: 60CAABBD43235889D64F230617C0E24E)
- – Present.exe: The malicious executable for the Echelon Credential Stealer/ Bitcoin Wallet Stealer (MD5 Hash: F407B3F68D5603C74C810BA16C08EC9D)

An analysis of the malicious executable shows that it contains several anti-analysis features. It has 2 anti-debugging functions, which immediately terminate the process if a debugger or other malware analysis tools are detected. Additionally, the sample is obfuscated using ConfuserEx v1.0.0.

After de-obfuscating the .NET code, we found that the sample performs several crypto wallet and credential stealing functions, as well as domain detection and computer fingerprinting. The malware will also attempt to take a screenshot of the victim machine.

The sample attempts to steal credentials from multiple different messaging, FTP, and VPN platforms, including:

- Discord
- Edge
- FileZilla
- NordVPN
- OpenVPN
- Outlook
- Pidgin
- ProtonVPN
- Psi(Jabber)
- Telegram
- TotalCommander

The sample attempts to steal the credentials/data for the following digital currency wallets:

- Armory
- AtomicWallet
- BitcoinCore
- ByteCoin
- DashCore
- Electrum
- Exodus
- Ethereum
- Jaxx
- LitecoinCore
- Monero
- Zcash

Fortunately, Windows Defender detects and deletes the Present.exe sample and alerts it as “#LowFI:HookwowLow”. RELEASE

Technical Details

Filename: Present).rar

Archived in Parent Archive:

- **pass - 123.txt**: Benign - Text document containing a password
- **DotNetZip.dll**: Not Malicious - class library and toolset for manipulating zip files. (MD5 Hash: 60CAABBD43235889D64F230617C0E24E)
- **Present.exe**: **Malicious** - Credential Stealer/ Bitcoin Wallet Stealer (MD5 Hash: F407B3F68D5603C74C810BA16C08EC9D)

Malware Original Name: Echelon.exe

Network traffic: Calls out to api.ipify.org

The following IP, which is most likely a proxy, was found in the sample .NET decompiled code and it appears to be where the sample may be attempting to POST the stolen data to:

168.235.103.57 Port:3128
Network Credentials = “echelon” , “002700z002700”

IOCs

- MD5 Hash: 60CAABBD43235889D64F230617C0E24E
- MD5 Hash: F407B3F68D5603C74C810BA16C08EC9D
- IP: 168.235.103.57

For more comprehensive code analysis, download the full report.

The Echelon infostealer malware targets not only Telegram login credentials but also information stored in popular collaboration and file-sharing applications. Because many users trust popular communication and file-sharing tools like Telegram, this makes them attractive prey for Echelon malware actors.

Bad actors continue to utilize various infiltration techniques to install and proliferate the Echelon malware within their target's IT network. These distribution methods include Trojans, cracking tools (illegal activation), fake updaters, spam campaigns, and dubious download websites. Once the Echelon malware is installed and activated, it triggers chain infections across the network, stealing and exfiltrating data from compromised devices.

What makes Echelon stealer malware so effective is the sophisticated construction and delivery of emails and messages that contain the malware. Messages are generally labeled as "urgent", "official", and "important", deceiving receivers into opening them and inadvertently installing the malware. In addition, the Echelon malware has advanced anti-analysis and anti-detection features, which complicates any discovery or research effort.

To learn more on how we can automate cybersecurity for your team’s digital communications, please get in touch with us.

If you are interested in learning more about the SafeGuard Cyber solution, you can take a quick 5-minute tour.

Explore Security Product

Mobile Messaging, Cybercrime, Featured, Malware, Threat Intelligence

Share: