Amadey Trojan and Botnet

Author: Nicholas Sundvall

Overview

From 5 to 8 August, we observed a malicious email campaign distributing the Amadey trojan, which infects a computer and then incorporates it into the Amadey botnet. We observed a large number of emails related to this campaign. Amadey was first seen in late 2018 when the author put the botnet up for sale on Russian online forums.[1]

Customer Impact

Amadey infects a victim's computer and incorporates it into a botnet. The Amadey trojan can also download additional malware and exfiltrate user information to a command and control (C2) server. Moreover, it can engage the victim's system in distributed denial-of-service attacks[2] and have it send spam with additional malware. In July, Trend Micro reported that the threat actor TA505 used the Amadey botnet to deliver spam emails containing the FlawedAmmyy remote access trojan.[3]

Campaign Analysis

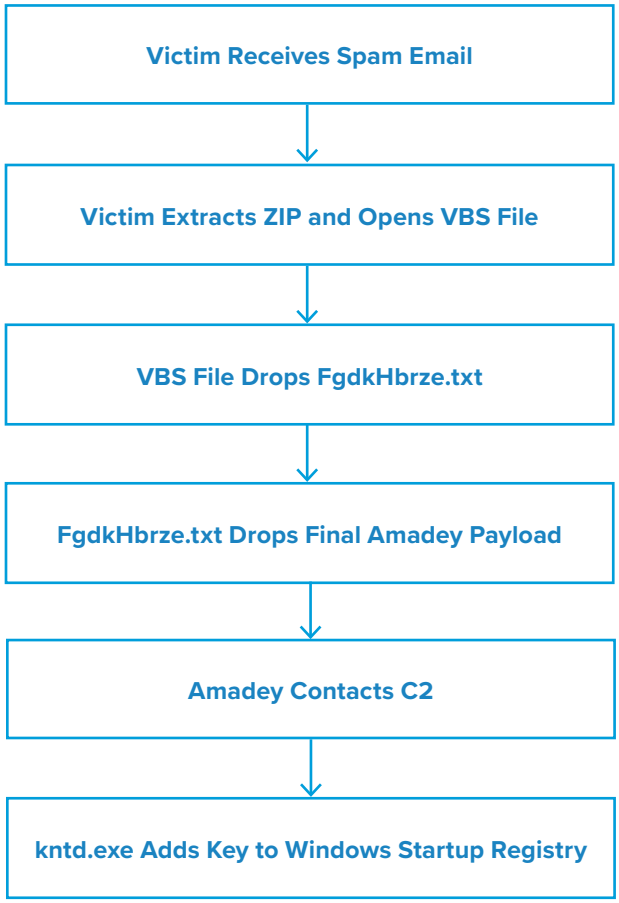
In the campaign we observed, the threat actor sent spam emails that reference a package or shipment. Many of the emails claim in the subject line that the package or shipment is from the shipping company DHL. For example, one subject line is "You have a package coming from DHL." The bodies of all of the emails we observed in this campaign are blank.

Each email has a ZIP attachment containing a Visual Basic Script (VBS) file. Each file name for the ZIP files is a series of numbers separated by an underscore, such as 410044450_64504154.zip. The VBS files have the same name as their ZIP file, except they have the VBS extension rather than the ZIP extension.

Attack Chain

The victim receives an email with an attached ZIP file. After extracting and opening the VBS file it contains, a window with the title "MS Word" appears. However, it is not a Microsoft Word document; it is a pop-up from the VBS file imitating an error that Word might throw. The window states that an unexpected error has occurred and to try again later.

In the background, the script extracts and executes the file FgdkHbrze.txt. Although it has the TXT extension, it is actually an executable file. FgdkHbrze.txt then extracts and executes the final Amadey payload, kntd.exe, which contacts its C2 and adds a key to the Windows Startup Registry to maintain persistence.



Vulnerabilities & Mitigation

Malicious email campaigns are a common tool threat actors use to distribute malware. Infoblox recommends the following precautions to reduce the possibility of infection.

- Always be suspicious of vague emails, especially if there is a prompt to open an attachment or click on a URL or clickable text.
- Be aware of any attachment's file type and never open files that could be a script (VBS, CMD, BAT) or another executable (EXE).
- Exercise caution if it is necessary to open emails with generic subject lines and/or typos, e.g., "You have a package on it's way."
- Verify important or potentially legitimate attachments with the sender via alternative means (e.g., by phone or in person) before opening them.

Endnotes

1. https://krabsonsecurity.com/2019/02/13/analyzing-amadey-a-simple-native-malware/
2. https://www.symantec.com/security-center/writeup/2019-062514-0848-99
3. https://blog.trendmicro.com/trendlabs-security-intelligence/latest-spam-campaigns-from-ta505-now-using-new- malware-tools-gelup-and-flowerpippi/

Corporate Headquarters | 3111 Coronado Dr. | Santa Clara, CA | 95054
+1.408.986.4000 | 1.866.463.6256 (toll-free, U.S. and Canada) | info@infoblox.com | www.infoblox.com