Warezov Email Worm

Author: Nicholas Sundvall

Overview

During 9-12 July, we discovered a malicious spam campaign distributing the Warezov worm. Also known as Stration, Warezov is an email worm that was first seen in 2006. Warezov is known for frequently downloading new variants of its code from remote servers. Warezov was most prevalent between 2006 and 2008, and there has been little public reporting about it since then.

During this week we observed a high volume of emails related to this campaign, and we did not observe it dropping any additional malware.

Customer Impact

Warezov infects a victim's computer and incorporates it into a botnet. The computer then sends malicious emails to all of the found contacts to spread the Warezov malware and infect new victims. The worm may not drop a malware payload, but the attacker can use the victims - now bots - for other malicious purposes such as denial of service attacks.

Campaign Analysis

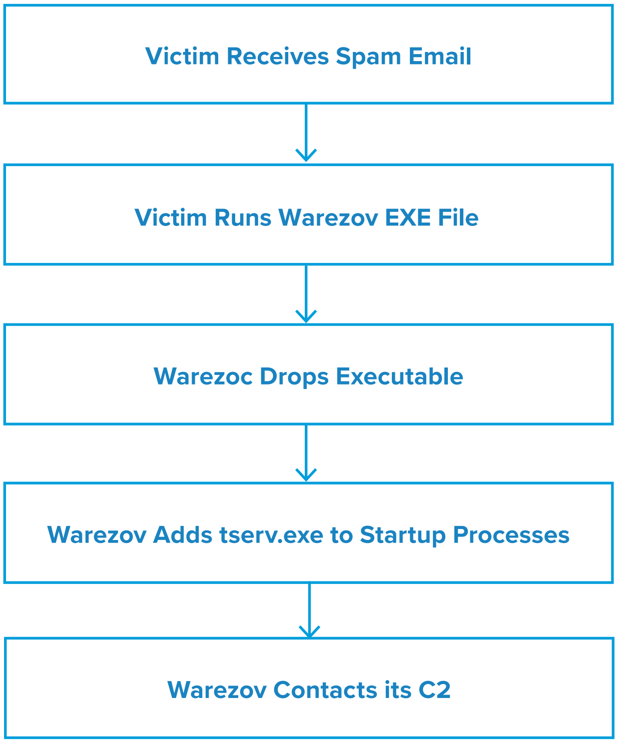
The threat actors deliver Warezov via email. The subject line of each message is "Mail server report." and ironically, the body warns the victim that their computer is being used to distribute a worm, and urges them to install an update to stop the worm from spreading.

Consistent with earlier campaigns, the emails carry a malicious EXE attachment, whose file name variants mimic Microsoft's Windows updates, for example Update-KB4082-x86.exe. We observed many different file hashes related to this campaign, likely due to Warezov's frequently changing code.

Attack Chain

Warezov tricks the victim into launching the EXE by telling them they need to install updates on their computer. After running the EXE, the victim sees a pop-up window that says "Update successfully installed."

The EXE then drops an executable file named tserv.exe and adds it to the list of startup processes. The EXE then attempts to contact a command and control (C2) server.



Victim Receives Spam Email

Victim Runs Warezov EXE File

Warezoc Drops Executable

Warezov Adds tserv.exe to Startup Processes

Warezov Contacts its C2

Vulnerabilities & Mitigation

Infoblox recommends the following precautions to reduce the possibility of infection by Warezov.

- Be cautious of emails from unfamiliar senders and inspect unexpected attachments before opening them.
- Always be suspicious of vague emails, especially if there is a prompt to open an attachment or click on a URL or clickable text.
- Filter attachments to reduce the likelihood of malicious content reaching a user's workstation.
- Be aware of any attachment's file type and never open files that could be a script (.vbs, .cmd, .bat) or another executable (.exe).

Endnotes

1. https://www.pcworld.com/article/127711/article.html

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