Kelihos Spreads via USB Drives

By Ionut Arghire

Published: 2017-02-06 · Archived: 2026-04-05 20:06:08 UTC

Kelihos, the malware behind one of the longest standing botnets out there, was recently observed spreading via infected thumb drives, researchers have discovered.

The Kelihos botnet has been around for many years, and even survived takedown attempts over half a decade ago. Last year, the botnet's activity ramped up as tens of thousands of new bots were added to it. Kelihos was being used for the distribution of MarsJoke, Wildfire, and Troldesh ransomware and various Trojans, including Panda Zeus, Nymain and Kronos.

The botnet is being rented as part of the "spam as a service" business model and continues to be geo-targeting users. The latest campaign targeted users in Canada with links to web pages of Tangerine Bank phish websites, while distributing a link to the Ecstasy website to recipients with ".kz" email addresses, Arsh Arora, malware analyst and Ph.D. researcher at The University of Alabama at Birmingham, discovered.

The emails contain a webpage that attempts to trick the user into clicking a button with the subject line of "TANGERINE online account has been suspended" (where Tangerine is the Internet/telephone base bank formerly known as ING Direct). An HTML version of the page is displayed to the potential victims, encouraging them to click on a "Learn More" button, which would take them to a phishing site, in an attempt to steal their credentials by requesting them to verify their information.

The geo-tagging of addresses ending with ".kz" is something new for the Kelihos botnet, the security researcher notes. The spam message, which featured a subject line in Russian, was directing users to an adult site (*www[dot]almatinki[dot]com*).

The most interesting part of the attack, however, is the fact that the removable drives attached to the compromised machines would be infected with a copy of the original Kelihos binary. The security researcher says that the malware was written to a thumb drive connected to the virtual machine that was infected as part of the new campaign.

Saved on the thumb drive under the name of "*porn.exe*," the executable is hidden from the user, the same as a few shortcuts that were not present on the removable device before. The file, the security researcher says, is the Kelihos botnet.

The researcher also discovered that the Create File function was linked to the dropped executable. The malware attempts to open several files with CreateFile and, if it fails, it then reverts to creating the .exe file, after which it writes the malicious binary to this file. Next, the malware creates shortcuts for the hidden directories and executables.

"An Autorun.inf is not created to run this file, however, a shortcut to the file with the command C:WINDOWSsystem32cmd.exe F/c 'start %cd%porn.exe' can be found on the drive, as well as shortcut to several other hidden directories on the drive (not malicious)," the security researcher says.

When the executable runs, it behaves just like a normal Kelihos would, though the researcher says that they weren't yet able to infect a new drive with the botnet, meaning that further investigation is required to reveal the specific mechanism the malware uses for infection, especially with the executable seemingly identical to the original binary.

Related: Kelihos Botnet Triples in Size Overnight

Source: https://www.securityweek.com/kelihos-spreads-usb-drives