Kaspersky Lab analyses new version of Kido (Conficker)

kaspersky.com/about/press-releases/2009_kaspersky-lab-analyses-new-version-of-kido--conficker

May 26, 2021

Kaspersky Lab, a leading developer of secure content management solutions, announces that a new version of the malicious program Kido (aka Conficker and Downadup) has been detected. During the night of 8th/9th April, computers infected with *Trojan-Downloader.Win32.Kido* (aka Conficker.c) contacted each other over P2P, telling infected machines to download new malicious files, thus activating the Kido botnet.

This latest Kido variant differs significantly from previous variants: the malware is now once again a worm. Initial analyses suggest it has date-limited functionality until 3rd May 2009.

In addition to downloading updates for itself, Kido also downloads two new files to infected machines. One is a rogue antivirus application (detected as *FraudTool.Win32.SpywareProtect2009.s*) that is being spread from sites located in Ukraine. When it's run, the program offers to delete "detected viruses" for a charge of $49.95.

The second file which Kido downloads to infected systems is *Email-Worm.Win32.Iksmas.atz*. This email worm is also known as Waledac, and is able to steal data and send spam. When this malicious program was first detected in January 2009, a lot of IT experts noted the similarity between Kido and Iksmas. The Kido epidemic was mirrored by an email epidemic of a similar scale caused by Iksmas.

“Over a 12-hour period, Iksmas connected to its control centers around the globe a number of times and received commands to send out spam mailings. In just 12 hours, one bot alone sent out 42,298 spam messages,” Aleks Gostev, head of Kaspersky Lab’s Global Research and Analysis Team, said in comments about the current situation. “Virtually every email contained a unique domain. This was obviously done to prevent anti-spam filters from detecting the mass mailings using methods that analyze the frequency with which a specific domain is used. Overall, we detected the use of 40,542 third-level domains and 33 second-level domains. Virtually all of these sites are located in China and are registered in the names of various people, most probably invented.

“A simple calculation shows that one Iksmas bot sends out around 80,000 emails in 24 hours. Assuming that there are 5 million infected machines out there, the botnet could send out about 400 billion spam messages over a 24-hour period!”

Kaspersky Lab is currently carrying out a detailed analysis of the new Kido variant. The company’s experts are working on a new version of the KKiller utility, taking into account the specific functionality of the latest version of the worm.

Users of Kaspersky Lab products have no cause for concern – the new version of the Kido worm (*Net-Worm.Win32.Kido.js*) has been detected heuristically from the outset (as *HEUR:Worm.Win32.Generic*), as has the variant of Iksmas that it downloads.

Kaspersky
A new version of the malicious program Kido (aka Conficker and Downadup) has been detected by Kaspersky Lab; computers infected with Trojan-Downloader.Win32.Kido (aka Conficker.c) have now contacted each other over P2P, telling infected machines to download new malicious files, thus activating the Kido botnet.

Related Articles Virus News

- ## Russian-speaking APTs Turla and Sofacy share malware delivery scheme, and overlap some targets in Asia

  Kaspersky Lab researchers monitoring the various clusters of the long standing, Russian-speaking threat actor, Turla (also known as Snake or Uroburos) have discovered that the most recent evolution of its KopiLuwak malware is delivered to victims using code nearly identical to that used just a month earlier by the Zebrocy operation

  Read More >

- **New variant of SynAck ransomware uses sophisticated Doppelgänging technique to evade security**

  Kaspersky Lab researchers have discovered a new variant of the SynAck ransomware Trojan using the Doppelgänging technique to bypass anti-virus security by hiding in legitimate processes.

  Read More >