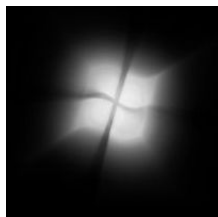


13 May 2009

By: Marius Oiaga, Technology News Editor



Trojan in pirated copies of Windows 7 RC builds botnet

[Pirated Trojan-Infested Windows 7 RC Builds Botnet](#)

According to security researchers

Malicious code piggyback riding the latest major Build of Windows 7 is estimated to have infected approximately 30,000 users. The malware was bundled into the code of the operating system, a scenario on which Microsoft had provided warnings to users in the past. Leaked builds of [Windows 7 Release Candidate \(RC\) Build 7100](#) available in the wild have become as common as the actual official interim milestones dogfooded (tested internally) by Microsoft. The Redmond company has not been shy of warning customers to [keep clear of Windows 7 leaked bits](#) from illegal third-party sources, especially BitTorrent trackers, and for good reason. Security researchers at Damballa have revealed that pirated, Trojan-infested copies of Windows 7 have been used by attackers to build a botnet, a network of compromised zombie computers under the control of the malware authors.

Tripp Cox, Damballa vice president of engineering, has indicated that the command and control server of the botnet built with the Windows 7 Trojans has been identified and shut down. "Since the pirated package was released on April 24th, my best guess is that this botnet probably had at least 27,000 successful installs prior to our takedown of its CnC command and control on May 10th," Cox explained, according to [eWeek](#).

On May 1st, 2009, [Alex Kochis](#), the director of Windows Genuine, pointed out that "leaked Windows 7 RC files that were obtained through bittorrent have been found to have been infected with a trojan. I say that I shouldn't be surprised because in research we supported a couple of years ago we discovered that the typical methods that someone would use to find and obtain unlicensed software (much of it over bittorrent) exposed users to significant risk from trojans and other malware."

The domain name "codecs.sytes.net" was used for the command-and-control server of the Windows 7 Trojan botnet, Damballa researchers informed. When the CnC was switched off, the rate of infections exploded to no less than 552 users per hour. The Damballa security experts explained that the Trojan built into Windows 7 was designed to download and install additional malware.

"The pirated software is the social enticement initially, and the second state is downloading additional packages of malware installed and distributed via the Trojan on a pay-per-install arrangement," Cox stated, as quoted by [DarkReading](#). Because it is deeply buried into the operating system, and due to yet immature security solutions for [Windows 7](#), end users have little chances of fighting the malicious code.

"We continue to see new installs happening at a rate of about 1,600 per day with broad geographic distribution. Since our takedown, any new installs of this pirated distribution of Windows 7 RC are inaccessible by the botmaster. The old installs are accessible. The countries with the largest percentage of installs are the U.S. (10%), Netherlands (7%) and Italy (7%)," Cox added.

On May 11th, security outfit Trend Micro confirmed TROJ_DROPPER.SPX and TROJ_AGENT.NICE as two pieces of malware associated with pirated copies of Windows 7. No official confirmation was provided on whether the Windows 7 Trojan detected by Damballa was the same as the one identified by Trend Micro.

"A file being hosted in popular torrent sites posing as a copy of the Windows 7 RC was found to be a Trojan by security researchers. The file which arrives with the file name setup.exe is detected as TROJ_DROPPER.SPX. TROJ_DROPPER.SPX drops TROJ_AGENT.NICE. Both files are detected by the Smart Protection Network. Windows 7 Release Candidate was leaked a couple of weeks prior to the official release, and was also hosted by and downloaded from popular torrent sites," explained [JM Hipolito](#), Technical Communications.

Windows 7 Release Candidate (RC) Build 7100 is at this point in time available for [download](#) via Microsoft's official and secure channels. Users will also be able to get [product keys](#) to activate the operating system, also from the Redmond company.