

02 November 2009

Trojans Continue to Dominate BitDefender's Top Ten E-Threats for October

Trojan.Clicker.CM continues its hold as the number one e-threat

The top spot on [BitDefender's](#) Top Ten list of e-threats for October is once again **Trojan.Clicker.CM**, which is mostly present on websites hosting illegal applications such as cracks, keygens and serial numbers for popular commercial software applications. It is typically used to force advertisements inside the browser and comprises 9.47 percent of infected files this month.

Ranking second with 8.54 percent of the worldwide infections, **Trojan.AutorunInf.Gen** is a generic mechanism used to spread malware via removable devices such as flash drives, memory cards or external hard-disk drives. Win32.Worm.Downadup si Win32.TDSS are two of the most famous families of malware to use this approach to trigger newer infections.

Win32.Worm.Downadup takes third position with 5.29 percent of the total amount of infected machines. Also known as Conficker or Kido, the worm restricts access to the websites associated with IT security vendors. More than that, the latest variant of the worm installs rogue security software on the compromised machines.

Trojan.Wimad comes in fourth place with 4.90 percent of the global infections. It takes advantage of a less-known feature implemented by Microsoft in order to store coordinated digital media data. The Trojan affects ASF files, an extensible file format that supports data delivery over a wide variety of networks and is extremely easy to play back locally. A specially crafted ASF file abuses the feature which allows it to download the appropriate codec in order to install Trojans instead.

Exploit.PDF-JS.Gen, the fifth offender, is a generic detection for specially crafted PDF files that exploit different vulnerabilities found in Adobe PDF Reader's Javascript engine in order to execute malicious code on the user's computer. Upon opening an infected PDF file, a specially crafted Javascript code triggers the download of malicious binaries from remote locations. This threat makes up 4.84 percent of the worldwide infections.

Win32.Sality.OG takes the sixth position with 2.31 percent of the infections triggered globally. It is a polymorphic file infector that appends its encrypted code to executable files (.exe and .scr binaries). In order to hide its presence on the infected machine, it deploys a rootkit and attempts to kill antivirus applications installed locally.

The seventh place goes to **Trojan.Autorun.AET** at 2.20 percent of global infections, a malicious code spreading via the Windows shared folders, as well as through removable storage devices. The Trojan exploits the Autorun feature implemented in Windows for automatically launching applications when an infected storage device is plugged in.

Worm.Autorun.VHG is an Internet /network worm that exploits the Windows MS08-067 vulnerability in order to execute itself remotely using a specially crafted RPC (remote procedure call) package (an approach also used by **Win32.Worm.Downadup**). The worm ranks eight with 1.49 percent of the global infections.

Trojan.Swizzor.6 is yet another variant of the Swizzor family, "obfuscated" downloaders that would try to save and execute new threats on infected machines. The Trojan adds its key to the Windows Registry in order to execute a copy of itself each time Windows is started. This specific variant of Swizzor accounts for 1.22 percent of the global infections.

Ranking last in this month's Top Ten E-threats, **Gen:Adware.Heur.wq0@j4oukhei** scores 1.21 percent of the global infections. This generic routine detects a wide range of adware applications, especially the NaviPromo family.

BitDefender's October 2009 Top 10 E-Threat list includes:

1	Trojan.Clicker.CM	9.47%
2	Trojan.AutorunINF.Gen	8.54%
3	Win32.Worm.Downadup.Gen	5.29%
4	Trojan.Wimad.Gen.1	4.90%
5	Exploit.PDF-JS.Gen	4.84%
6	Win32.Sality.OG	2.31%
7	Trojan.Autorun.AET	2.20%
8	Worm.Autorun.VHG	1.49%
9	Trojan.Swizzor.6	1.22%
10	Gen:Adware.Heur.wq0@j4oukhei	1.21%
	OTHERS	58.53%

To stay up-to-date on the latest e-threats, sign-up for BitDefender's RSS feeds [here](#).

* * *

About BitDefender®

BitDefender is the creator of one of the industry's fastest and most effective lines of internationally certified [security software](#). Since its inception in 2001, BitDefender has continued to raise the bar and set new standards in proactive threat prevention. Every day, BitDefender protects tens of millions of home and corporate users across the globe - giving them the peace of mind of knowing that their digital experiences will be secure. BitDefender security solutions are distributed by a global network of value-added distribution and reseller partners in more than 100 countries worldwide. More information about BitDefender and its products are available at the company's [security solutions](#) press room. Additionally, BitDefender's [Malware City](#) provides background and the latest updates on security threats helping users stay informed in the everyday battle against malware.