Worms dominate BitDefender’s Top Ten E-Threats

Submitted by: MJO Associates
Wednesday, 2 September 2009

Worms continue to dominate BitDefender's Top Ten E-Threats for August, with Trojan.Clicker.CM holding the number one spot. This Trojan is also becoming increasingly present on "warez" websites (download portals hosting cracks and keygens for commercial applications).

Ranking second on the list, Trojan.AutorunINF.Gen is accountable for 10 percent of the total number of infections globally. The Windows Autorun feature is used by multiple families of malware in order to propagate via removable media.

Trojan.Wimad.Gen.1 ranks third with 6 percent of the total number of worldwide infections. The Trojan affects ASF files with their ability to automatically download the appropriate video codec if it is missing from the system. Malware authors usually hijack the original specifications to force the file into downloading a malicious binary instead.

After more than 8 months since it first entered the BitDefender Top 10 E-Threats list, Win32.Worm.Downadup ranks fourth with 4 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.

Ranking fifth this month, Win32.Sality.OG 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.

Sixth place is taken by Win32.Induc.A, an unusual piece of malware infecting applications built with Borland (now Embarcadero) Delphi versions 4 through to 7. The virus does not infect binary file, but rather modifies the SYSCONST.PAS file, injects its malicious code and then compiles the file back. All the applications built with the compromised compiler would be infected with the virus. Win32.Induc.A has no malicious payload, but its abrupt escalation in the Top Ten list shows that only a few Delphi developers are aware of the widespread infection.

Trojan.Autorun.AET, in seventh position, is a piece of malware that spreads through the Windows shared folders, as well as via removable media (network attached storage devices or mapped drives). The Trojan exploits the Autorun feature implemented in Windows operating systems to automatically execute itself when an infected device is plugged in.

Ranking eighth in this month's Top Ten E-threats, Trojan. JS.PYV is a malicious script affecting users who are browsing malicious websites or legitimate websites which were compromised by attackers.

In ninth place is Win32.Virtob.Gen which is a file infector written in assembly language. The piece of malware hides its presence by injecting hooks into other Windows processes, but avoids compromising system files. It also opens a backdoor that can be exploited by a remote attacker to seize control over the infected machine. This is a high-risk infection; for more details on how to remove this threat, please visit http://www.bitdefender.co.uk/VIRUS-1000070-en--Win32.Virtob.Gen.html

In tenth, 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 increasing presence of the worm in BitDefender's Top Ten E-Threats list reveals that users are still ignoring Microsoft's security advisories and avoid deploying security patches.

BitDefender's August 2009 Top 10 E-Threats list includes:

Pos - name - %
1. Trojan.Clicker.CM - 14
2. Trojan.AutorunINF.Gen - 10
3. Trojan.Wimad.Gen.1 - 6
4. Win32.Worm.Downadup.Gen - 4
5. Win32.Sality.OG - 3
6. Win32.Induc.A - 2
7. Trojan.Autorun.AET - 2
8. Trojan.JS.PYV - 2
9. Win32.Virtob.Gen.12 - 2
10. Worm.Autorun.VHG - 2

To stay up-to-date on the latest e-threats, sign-up for BitDefender's RSS feeds here (http://www.bitdefender.co.uk/site/Using-Rss-Feeds.html)

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 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 www.malwarecity.com provides background and the latest updates on security threats helping users stay informed in the everyday battle against malware.

For more information see www.bitdefender.co.uk

ENDS

Contact:

Nick Billington
BitDefender Country Manager (UK and Ireland)
Tel: 0845 130 5096
E-mail: nbillington@bitdefender.co.uk

Issued by:

Mike Ottewell
MJO PR for BitDefender UK
Tel: 0845 883 3435
E-mail: mottewell@bitdefender.co.uk