

Malware and AV Technology Trends in 2010

At the beginning of 2009 internet users have had to cope with approximately 2,000 new and mutated viruses per day, almost 50,000 phishing attempts per month and more than 1,000,000 hijacked computers that spread bots, rootkits, Trojans and other malware. The reason behind 95 percent of all these e-threats remains profit, both financial and technological.

Since almost 45 percent of the e-threats in the wild are distributed exclusively via or rely to some extent on e-mail, securing the e-mail communication should continue to be a priority in 2010.

Malware production holds an ascending trend, exploiting the same web-based capabilities of Trojans, spyware and rootkits. Early days of 2009 already saw a 460 percent increase in web-based infections and a 400 percent augmentation of e-mail spam distributing Trojans. It is certain that many of the existing e-threat families will suffer significant upgrades and mutations, in terms of stealth and automation of spreading mechanisms.

As the latest issue of BitDefender E-Threats Landscape Report shows, between January and June 2009, the most active countries in the realm of malware propagation were China (33%), France (24%) and the United States (14%), followed by Romania and Spain (6%), Australia and Germany (4%), India and Canada (3%), UK and Mexico (below 1.8%).

The top 10 most spread viruses in the United Kingdom between May and October 2009 include:

1	Trojan.Wimad.Gen.1	9.07
2	Iframe.Malware.1C15745E	5.94
3	Trojan.AutorunINF.Gen	4.25
4	Trojan.JS.PYV	2.12
5	Trojan.Generic.1609040	2.10
6	Trojan.Skintrim.HTML.A	1.32
7	Trojan.Script.14303	1.13
8	Win32.Virtob.Gen.12	1.12
9	Trojan.Autorun.AET	1.04
10	Trojan.Generic.IS.574696	1.03
	Other	70.88

During the first half of 2009, phishing messages reached an alarming threshold of 7 percent of the spam messages sent worldwide. As expected, the most receptive countries in terms of phishing are the United States, Canada and the United Kingdom – three English-speaking countries. However, Russia is another significant source of phishing messages, mostly because of its lax legislation regarding cyber-crime, as well as of the current unemployment rates.

Exploiting application vulnerabilities will continue to hold the focus in the upcoming period, as pointed out by one of the password stealing applications that BitDefender's researchers identified. Disguised as a Mozilla® Firefox® additional component, Trojan.PWS.ChromeInject.A steals data sent to over 100 online banking web sites.

Particular attention should be paid to the major growth of Web 2.0 sites and their ongoing development. The most targeted Web 2.0 applications will remain the social networks. The

last few months brought into the spotlight Win32.Worm.KoobFace.A, which now also affects Twitter™, as well as Facebook® and MySpace™ users, but also the dissemination of rogue antivirus, such as Personal Antivirus or Antivirus 2009, via poisonous shortened URLs.

In 2010, we also expect to see a rise of e-threats and attacks targeting “in-the-cloud” based services and applications. To address these menaces, BitDefender has developed a very light-weight malware scanner, *BitDefender Quick Scan* (<http://quickscan.bitdefender.com>), which is able to run as a plug-in for all major Web browsers (Firefox, IE, Opera, Chrome and Safari).

Quick Scan combines intelligent local scanning and in-the-cloud scanning to create an advanced online tool which detects e-threats in memory quickly. Unlike other online virus scanners, Quick Scan’s engines do not need to be downloaded, installed in the system or even updated. The thorough examination of all the running processes (including the hidden ones) is performed completely remotely, using the BitDefender Antivirus technologies.

For disinfection purposes and advanced proactive protection, BitDefender offers both on-line solutions, such as *BitDefender On-line Scanner*, and state of the art antimalware suites, namely the *BitDefender 2010 Suites*.

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