Kaspersky issues report: Duqu Trogan poses biggest threat

MOSCOW, RUSSIA: Kaspersky Lab has issued its malware report for October and finds that the Duqu Trogan is the most dangerous Mac OS malware to date.

Out of the box activity
Duqu

The star of the show in October was undoubtedly the Duqu Trojan. Its numerous similarities to the first major cyber weapon, the Stuxnet worm, heightened interest in this newly-discovered malware. The striking parallels between the two malicious programs suggest they were both written by the same group of people or the Stuxnet source code (which has not been made publicly available) was used.

There are, however, significant differences between the two programs. In particular, Duqu contains no functionality targeting industrial systems as was the case with Stuxnet. As well as the main module, the Duqu files include an additional Trojan-Spy module capable of intercepting data entered via the keyboard, capturing screenshots, gathering information about the system etc. All this suggests industrial espionage as the main objective, rather than industrial sabotage.

Further investigation by the experts at Kaspersky Lab managed to identify new Duqu victims, primarily in Iran, which once again echoes the parallels with Stuxnet. "Additionally, we found new and previously unknown Duqu files. This confirms our suspicions that the people behind Duqu are continuing their activity, and their attacks, unlike the mass infections by Stuxnet, target carefully selected victims," adds Alexander Gostev, chief security expert at Kaspersky Lab. "A unique set of files is used for every targeted attack. It is also possible that other modules are used, and not just a Trojan-Spy but modules with a range of other functions."

Attacks on individual users
Bundestrojan

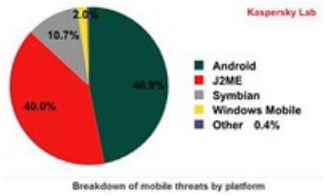
In Germany, five federal states admitted last month that they had used the Backdoor.Win32.R2D2 Trojan during their investigations - prompting an outcry. The country's federal laws only allow the police to intercept suspects' Skype traffic, but the malware was capable of spying on many other types of programs. An investigation by Chaos Computer Club, a German hacker community, which later involved experts from Kaspersky Lab's German office, revealed that apart from Skype the Trojan intercepted messages in all the most popular browsers, various instant messenger services and VoIP programs including the likes of ICQ, MSN Messenger, Low-Rate Voip, paltalk, SimpPro, sipgate X-Lite, VoipBuster and Yahoo! Messenger. It was also found that the backdoor was capable of working on 64-bit versions of Windows.

This case once again raises questions about the existence of so-called governmental Trojan programs and the legal issues associated with their use. It is worth stressing that Kaspersky Lab, like most other antivirus vendors, takes a firm stance on such questions highlighting that we detect, and will continue to detect, all malicious programs regardless of who developed them and why.

Android - top of the hit list

October was a turning point in the world of mobile threats, with Kaspersky Lab data showing that the total number of malicious programs for Android outstripped that for Java 2 Micro Edition for the first time. Malware for J2ME had been the most prevalent among mobile threats for over two years. "The fact that the growth in malware for Android has increased so dramatically indicates that for the time being the virus writers will most probably be concentrating on this operating system,"

warns Denis Maslennikov, senior malware analyst at Kaspersky Lab.



click to enlarge

The most dangerous Trojan for Mac OS X

October saw the emergence of Trojan-Downloader.OSX.Flashfake.d, a new version of the Flashfake Trojan for Mac OS X, which masquerades as an Adobe Flash Player installation file. Like its predecessors, its main function is to download files. However, new functionality has been added that disables Mac's built-in protection system XProtect, a simple signature scanner that is updated on a daily basis. Once disabled the protection system cannot receive updates from Apple, rendering it useless. The fact the developers failed to include a self-defence mechanism makes it possible to disable XProtect. After Trojan-Downloader.OSX.Flashfake.d launches on a computer, it not only protects itself from being deleted but also makes the system vulnerable to other malicious programs that would have been detected by the built-in protection system. As a result, this particular Trojan is much more dangerous than other OS X malware.

Attacks on state and corporate networks

When it came to attacks on corporate and state organisations - October was highlighted as a month of a number of such incidents. Organisations in the US and Japan were most frequently on the receiving end.

First of all, an attack was detected against members of Japan's lower house of parliament. As a result, it is highly likely that the hackers gained access to internal documents and the emails of affected parliamentarians. Malware was also detected on computers in several Japanese embassies around the world. The malicious programs contacted two servers located in China that have already been used in an attack on Google.

More information also emerged around the August attack on Mitsubishi Heavy Industries. The investigation conducted by the Tokyo police revealed that about 50 malicious programs were found on 83 computers targeted in the attack.

The infected system was accessed over 300 000 times by the hackers. The search for the source of the attack led to yet another infected computer that belonged to the Society of Japanese Aerospace Companies (SJAC). The hackers used this computer to send malicious emails to Mitsubishi Heavy and Kawasaki Heavy and covered their tracks by accessing the machine at SJAC from an anonymous proxy server in the US. Nevertheless, Japanese experts continue to advance the theory that the hackers hail from China.

The story of a virus found on the ground control systems of pilotless planes at a US air base may seem less dramatic, but it once again highlights the unacceptably lax levels of security at important installations. According to an anonymous source at the US Department of Defence, the Trojan was designed to steal user data for a number of online games. It most probably ended up on the air base's system by accident and was not part of an attack.

Top 10 threats on the Internet in October

1	Malicious URL	82.47%	=
2	Trojan.Script.Iframer	2.25%	+1
3	Trojan.Win32.Generic	1.41%	+4
4	Trojan.Script.Generic	1.18%	=
5	Exploit.Script.Generic	1.03%	+2
6	AdWare.Win32.Shopper.il	0.46%	New

7	Trojan-Downloader.Script.Generic	0.46%	+1
8	AdWare.Win32.Eorezo.heur	0.32%	-3
9	Trojan.JS.Popupper.aw	0.27%	New
10	AdWare.Win32.Shopper.jq	0.23%	New

More detailed information about the IT threats detected by Kaspersky Lab on the Internet and on users' computers in October 2011 is available at: www.securelist.com/en.

With the increase in a number of threats and malware as outlined above comes the announcement of the release of Kaspersky Endpoint Security 8 for Windows and Kaspersky Security Centre. The new endpoint protection solution and comprehensive management console are designed to keep businesses ahead of emerging threats by seamlessly harnessing new and improved features set, protecting companies from emerging threats and improving IT productivity. Kaspersky Endpoint Security 8 for Windows is a key addition to Kaspersky Lab's comprehensive security suite, which helps businesses prepare for the next challenge in IT security.

Infographic 1: Demonstrates the process of a typical targeted attack and indicates how Kaspersky Lab's product suite protects the customer at every step, even if the criminal has managed to bypass some protection methods.

click to enlarge

Infographic 2: Demonstrates the benefits of cloud-based security for businesses with facts and figures.

click to enlarge