Kaspersky Lab malware in May: Rogue antivirus programs attack Mac OS users

MOSCOW, RUSSIA: The experts at Kaspersky Lab present their monthly report about malicious activity on users' computers and on the Internet.

May in figures

The following statistics were compiled in May using data from computers running Kaspersky Lab products:

- 242,7 mln network attacks blocked;
- 71,3 mln attempted web-borne infections prevented;
- 213,7 mln malicious programs detected and neutralised on users' computers; 84,3 mln heuristic verdicts registered.

Rogue antivirus program for Mac OS X

In May, there were 109 218 attempts to infect users' computers with rogue antivirus programs via the Internet. This is twice as low as the peak activity seen in February-March 2010 - during this period, some 200 000 security incidents occurred each month. Nevertheless, rogue antivirus attacks came as a surprise to users of Apple computers. The first attacks were detected on 2 May when the web was a buzz with news about the death of Osama bin Laden. Some users searching Google for information about this event did not receive search results, but instead were presented with a notification in their browser windows that a Trojan had been detected on their machines and could be removed.

If a user agreed to try the suggested anti-malware software, the rogue antivirus (MAC defender in this case) would say that it had detected several malicious programs on the computer (which in fact were not there), and ask US$59-80 to remove them. If the victim paid for the fake program they received a registration key; when the user entered this key, the system stated it was now malware-free.

Interestingly, the purported number of "signatures' in MAC Defender's "antivirus database" is 184 230. For comparison, the

number of malicious programs created for Mac to date amounts to hundreds, but not tens of thousands.

Malware for Win64

The growth in the number of users who prefer the 64-bit OS did not go unnoticed. In May, Brazilian cybercriminals whose main "specialisation" over the last several years has been banking Trojans released the first banking rootkit for the Windows 64-bit OS (Rootkit.Win64.Banker). They targeted users' logins and passwords to online banking systems. During the attack the users were redirected to phishing pages which imitated the websites of respectable banks. May was also marked by ZeroAccess' comeback, but this time the Trojan was capable of functioning on x64 systems. Computers were infected using a drive-by download attack. After ZeroAccess penetrates a victim's computer it determines whether the victim's computer runs either a 32- or 64-bit operating system and downloads the appropriate version of the backdoor to it.

Sony targeted yet again

The hackers did not give Sony a chance to relax. After attacks on the Sony Playstation and Sony Online Entertainment Networks in late April - early May they compromised Sony's Thai site on 20 May. As a result, a phishing page targeting Italian credit card owners was hosted on hdworld.sony.co.th.

However this was not the end of it. On 22 May, the Greek site SonyMusic.gr was attacked, making user data available for public access, including users' nicknames, real names and email addresses. Two days later several vulnerabilities were detected on sony.co.jp. Nonetheless this time the stolen database did not contain users' personal data.

In our forecasts for 2011 we suggested that information of any type would become the target of many attacks. Unfortunately, the number of attacks on Sony reinforces the accuracy of this prediction. Currently, IT security issues are extremely important as services such as PSN and iTunes harvest as much information as possible. The legislation surrounding personal data security is not always clear and all users can really do is to stop using these services. There can be no doubt that the attacks on Sony were well planned and executed. We can confidently predict that in the future, services similar to PSN will become the targets of such attacks. Therefore users need to be very careful when using these services and with the companies that provide them.

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