BIZCOMMUNITY

Kaspersky Lab Malware in June scammers turn to BitCoins

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

June 2011 in figures

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

- 249 345 057 network attacks blocked;
- 68 894 639 attempted web-borne infections prevented;
- 216 177 223 malicious programs detected and neutralised on users' computers;
- 83 601 457 heuristic verdicts registered

Difficult times for cybercriminals

June brought some notable successes for various law enforcement agencies in the war on cybercrime. In the US, the activities of two international cybercriminal groups that made money from fake antivirus programs were terminated. According to preliminary estimates, the damage caused by the groups amounted to US$74 million*. In addition to US agencies, the operation to shut down these groups involved law enforcement agencies from another 11 countries. About 600 people suspected of implementing fraudulent online schemes were arrested in several South East Asian countries. Another major event in June was the arrest of Pavel Vrublevsky, owner of Russia's biggest payment processing centre ChronoPay, on charges of organising a DDoS attack on a competing service.

Crime in the clouds

In June, cybercriminals used Amazon's cloud to host and distribute malware that targeted Brazilian users and was designed to steal data from customers of nine Brazilian banks. To improve its chances of success, the malware blocked the normal operation of AV programs and special plug-ins that are supposed to make online banking secure. The malware also stole digital certificates and Microsoft Live Messenger credentials.

Money from thin air

Russian scammers tried their luck at making money for nothing in June using the BitCoins virtual money system. With the help of a new malicious program they launched a legitimate BitCoins file on the victim computer in an attempt to generate the cyber currency in their own accounts. The BitCoins site administration reacted quickly to block the attacker's account, as such the cybercriminals appear to have made very little money.

Mac OS X still very much in the cybercriminals' sights

June saw cybercriminals distributing a new backdoor - Backdoor.OSX.Olyx.a - designed to provide attackers with remote control over victim's machines. This enabled them to use infected computers to download more malware, launch programs and send commands to an interpreter for execution.

New malicious specimens

The Top 20 malicious programs on the Internet in June included a large number of new entries. Once again it was dominated by malware that makes use of drive-by attacks - redirectors, script downloaders and exploits. These made up 14 of the 20 places in this rating. One of the more notable new entries this month was Exploit.HTML.CVE-2010-4452.bc which uses a straightforward vulnerability in Java Runtime Environment to download and launch a Java exploit. This in turn allowed other malicious programs to be installed on the victim computer.

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

**Exchange rate at time of posting: US$1=R6.85*