Community Powered Threat Report released by AVG

In "AVG Community Powered Threat Report - Q4 2011", which was released recently by the provider of internet and mobile security, the risks of QR codes, stolen digital certificates bypassing security on mobile phones and the persistence of rootkits are highlighted.

Cybercrime has come a long way. Originally, it was mainly a digital form of vandalism, but has developed into a criminal business operated for financial gain. Cybercrime is now worth billions. The report provides insight, background and analysis on the trends and developments in the global online security threat landscape and focuses on some of the most notable cybercrime developments in the last quarter.

QR codes

QR codes are becoming a popular way for mobile users to insert text and URLs into the mobile device without typing. Unfortunately, they are also being discovered as an ideal way to distribute malware to unsuspecting victims. The user does not know what lurks behind the QR code until the malware is already installed and running. The report describes in detail this new technique already used by hackers, which is expected to gain momentum in 2012. Putting a malicious QR code sticker onto existing marketing material, or replacing a website's bona fide QR code with a malicious one, could be enough to trick many unsuspecting people.

"In Q4 we clearly saw that the convergence between computers and mobile phones applies to malware too. As phones become more like computers, so do the risks," said Yuval Ben-Itzhak, chief technology officer, AVG Technologies. "Many sophisticated computer tricks of the trade are now being repurposed for phones. However, as phones are often tied into billing systems, the gains can be far greater."

Malicious Android apps

2011 saw a surge in both Android users and Android malware samples. In December, Google removed 22 malicious apps from the Android Market, making the total for 2011 pass the 100 mark. Cyber criminals have clearly discovered phones as an interesting target. Another sign that mobile phones are becoming more like computers every day is in the use of stolen certificates now making their way on to mobile devices. Digital certificates are often used to certify the identity of the author of an application. If a criminal can get his hands on the certificate belonging to a major software developer, his malware can circumvent security provisions and give users a false sense of security.

Rootkits a serious threat

Rootkits have been one of the more serious threats to target operating systems in recent years. Rootkits evolved from commercial and financial use to cyber warfare with a very specific target (Stuxnet, Duqu2). In this report AVG points out that we are witnessing the first phase of the rootkit evolution on mobile devices (CarrierIQ3). Rootkits are ever-evolving, with more sophisticated samples showing up every few months.

The report focuses on one of the latest rootkits called ZeroAccess, a very sophisticated, very effective rootkit using advanced anti-forensic features. ZeroAccess is a kernel mode rootkit spying on users and is controlled from a remote server. Waiting for commands from the criminals behind it, the rootkit allows the criminals to use the infected machine when and how they wish.

Other key findings in the report:

- The Blackhole toolkit is currently the most active threat on the web with a share of nearly 50 percent of all detected instances and over 80% of all toolkits
- Around a million malicious mobile events have been detected during this quarter
- The US is still the largest source of spam, now followed by the UK. Compared to the previous quarter, the UK jumped from fourth to second place overtaking India and Brazil
- Brazil is not just a very active banking Trojan market; the report highlights Portuguese as the second-most-used language in spam messages.

JR Smith, CEO of AVG Technologies, said: "With threats such as ID theft, phishing attacks and Trojans, cyber criminals create an environment of increased risk that puts people off going online. At AVG we believe our role is to give people the tools and peace of mind to enjoy their online experience."