Hackers hunt prey on smartphones, Facebook

April 5 2011, by Glenn Chapman

Hackers are following prey onto smartphones and social networking hotspots, according to reports released by a pair of computer security firms.

Hackers are following prey onto smartphones and social networking hotspots, according to reports released Tuesday by a pair of computer security firms.

Cyber criminals are also ramping up the sophistication and frequency of attacks on business and government networks, one of the companies, Symantec, said in the latest volume of its Internet Security Threat Report.

Symantec depicted a "massive" volume of more than 286 new computer threats on the Internet last year, continued growth in attacks at online social networks and "a notable shift in focus" by hackers to mobile devices.

"The major mobile platforms are finally becoming ubiquitous enough to garner the attention of attackers," Symantec said in its findings.

In March, smartphones running on Google-backed Android software were the target of the largest attack ever on the devices, noted a PandaLabs report focused on the first three months of this year.

"This assault was launched from malicious applications on Android Market, the official app store for the operating system," PandaLabs said.

Within a four-day span, seemingly legitimate Android smartphone applications rigged with malicious "Trojan" computer code were downloaded more than 50,000 times, according to PandaLabs.

"The Trojan steals personal information from cellphones, and downloads and installs other apps without the user's knowledge," the computer security firm said.

"Google managed to rid its store of all malicious apps, and several days later removed them from users' phones."

The Symantec report indicated that cyber crooks were also infiltrating news-feed capabilities at popular social networking services to "mass-distribute" attacks.

Such tactics typically involve getting into one person's account at a social network and then sending others links to websites booby-trapped with malicious computer code.

"Social network platforms continue to grow in popularity and this popularity has, not surprisingly, attracted a large volume of malware," Symantec said.

PandaLabs gave an example of a 23-year-old California man facing sentencing after pleading guilty to using information found on Facebook to hack email accounts to find compromising messages for blackmail.

Even Facebook founder Mark Zuckerberg saw his fan page at the social networking website hacked this year, the security firm noted.

PandaLabs researchers logged an average of 73,190 new snippets of malicious computer code daily during the first three months of this year in what was said to be a 26 percent jump from the same period in 2010.

Hackers showed a strong predeliction for a kind of malicious code used to mine bank account data and, ultimately, get into people's accounts, the computer security firm indicated.

China, Thailand and Taiwan had the highest rates of infection, with nearly 70 percent of the computers in those countries "riddled with malware," according to PandaLabs.

Many attacks on company or government computer networks involved hackers researching key employees and then duping them or colleagues into enabling access to protected networks, Symantec's report showed.

Researchers warned that onslaughts by "hacktivists" such as the group "Anonymous" and others with seeming political goals could signal a dangerous cyber arms race.

"Stuxnet and Hydraq, two of the most visible cyber-events of 2010, represented true incidents of cyberwarfare and have fundamentally changed the threat landscape," said Symantec Security Technology and Response senior vice president Stephen Trilling.

"The nature of the threats has expanded from targeting individual bank accounts to targeting the information and physical infrastructure of nation states."

Citation: Hackers hunt prey on smartphones, Facebook (2011, April 5) retrieved 23 April 2024 from https://phys.org/news/2011-04-hackers-prey-smartphones-facebook.html