Cyber-security expert finds new flaw in smartphones

February 24 2012, By Ken Dilanian

Just as U.S. companies are coming to grips with threats to their computer networks emanating from cyber-spies based in China, a noted expert is highlighting what he says is an even more pernicious vulnerability in smartphones.

Dmitri Alperovitch, the former McAfee Inc. cyber security researcher best known for identifying a widespread China-based cyber-espionage operation dubbed Shady Rat, has used a previously unknown hole in smartphone browsers to plant China-based malware that can commandeer the device, record its calls, pinpoint its location and access user texts and emails. He conducted the experiment on a phone running Google Inc.'s Android operating system, although he says Apple Inc.'s iPhones are equally vulnerable.

"It's a much more powerful attack vector than just getting into someone's computer," said Alperovitch, who just formed a new security company called CrowdStrike with former McAfee Chief Technology Officer George Kutz.

Alperovitch, who has consulted with the U.S. intelligence community, is scheduled to demonstrate his findings Feb. 29 at the RSA conference in San Francisco, an annual cyber-security gathering. The Shady Rat attack he disclosed last year targeted 72 government and corporate entities for as long as five years, siphoning unknown volumes of confidential material to a server in China.

Alperovitch said he and his team commandeered an existing piece of malware called Nickispy, a remote access tool from China that was identified last year by anti-virus firms as a so-called Trojan horse. The malware was disguised as a Google+ app that users could download. But Google quickly removed it from its Android Market app store, which meant that few users were hit.

Alperovitch and his team reverse-engineered the malware, he said, and took control of it. He then conducted an experiment in which malware was delivered through a classic "spear phishing" attack - in this case, a text message from what looks like a mobile phone carrier, asking the user to click on a link. Alperovitch said he exploited what's known as a zero-day vulnerability in smartphone browsers to secretly install the malware. Zero-day vulnerabilities are ones that are not yet known by the manufacturers and anti-virus companies.

"The minute you go the site, it will download a real-life Chinese remote access tool to your phone," he said. "The user will not see anything. Once the app is installed, we'll be intercepting voice calls. The microphone activates the moment you start dialing."

The malware also intercepts texts and emails and tracks the phone's location, he said. In theory, it could be used to infiltrate a corporate network with which the phone connects.

There is no security software that would thwart it, he said.

As smartphone use has exploded, malware has not been as much of a problem as it has with laptops and desktops, Alperovitch said, because most people download applications through app stores that are regulated by Google and Apple. If cyber-thieves and spies figure out a way to get malware on the devices by bypassing the app store - as Alperovitch says he has demonstrated - it could cause huge problems.

"This really showcases that the current security model for smartphones is inadequate," he said.

Earlier this month, the top U.S. intelligence official, James Clapper, accused China and Russia of engaging in "wholesale plunder of our intellectual property" through cyber-attacks. Both countries deny a state-sponsored policy of cyber-espionage. The U.S. says it doesn't steal trade secrets or intellectual property. Western business executives who travel to China these days frequently take extraordinary computer security precautions, including ensuring that any device they bring to China is never again connected to their corporate networks.

Last year, anti-virus firm Trend Micro Inc. found a Chinese website that charged $300 to $540 to customers who wanted to spy on smartphones that ran Symbian or Windows Mobile operating systems. The website offered to send Nickispy as an attachment to a multimedia message.

Citation: Cyber-security expert finds new flaw in smartphones (2012, February 24) retrieved 27 April 2024 from https://phys.org/news/2012-02-cyber-security-expert-flaw-smartphones.html