NSA pretended to be Facebook to infect millions of computers

March 12, 2014 By Andrew Couts Digital Trends

http://www.foxnews.com/tech/2014/03/12/nsa-pretended-to-be-facebook-in-its-effort-to-infect-millions-computers/?intcmp=latestnews

As part of its efforts to install malware on "millions" of computers worldwide, the National Security Agency impersonated Facebook to trick targets into downloading malicious code.

"In some cases the NSA has masqueraded as a fake Facebook server, using the social media site as a launching pad to infect a target's computer and exfiltrate files from a hard drive," reports The Intercept in its latest expose based on top-secret documents obtained by Edward Snowden.

"[The NSA] has sent out spam emails laced with the malware, which can be tailored to covertly record audio from a computer's microphone and take snapshots with its webcam. The hacking systems have also enabled the NSA to launch cyberattacks by corrupting and disrupting file downloads or denying access to websites."

The Facebook trick was called QUANTUMHAND by the NSA, and was initially tested on "about a dozen targets" before being launched on a larger scale in 2010, the documents show.

What began as a way to hit "hard-to-reach" targets – around 100 to 150 of them, as of 2004 – the NSA's malware-spreading efforts have since proliferated to potentially millions of computers around the globe using an automated system known internally as TURBINE. Using TURBINE, documents reveal, gave members of the NSA's Tailored Access Operations (TAO) unit the ability to tap into, or destroy, computers on a massive scale.

Here's how The Intercept's Ryan Gallagher and Glenn Greenwald describe some of the various tailored malware the NSA deploys into targeted machines:

One implant, codenamed UNITEDRAKE, can be used with a variety of "plug-ins" that enable the agency to gain total control of an infected computer.

An implant plug-in named CAPTIVATEDAUDIENCE, for example, is used to take over a targeted computer's microphone and record conversations taking place near the device. Another, GUMFISH, can covertly take over a computer's webcam and snap photographs. FOGGYBOTTOM records logs of Internet browsing histories and collects login details and passwords used to access websites and email accounts. GROK is used to log keystrokes. And SALVAGERABBIT exfiltrates data from removable flash drives that connect to an infected computer.

The documents also indicate that some of these viruses disable targets' ability to use encryption software to mask Internet activity or send emails privately. This and other malware efforts are part of what the NSA documents call its "Owning the Net" program.