New Snowden document reveals NSA's international malware operation

Kevin Reed
28 November 2013

A presentation slide provided by Edward Snowden and published by the Dutch media outlet NRC on November 23 shows that the NSA has infected more than 50,000 computer networks worldwide with malicious software designed to steal sensitive and private information.

The 2012 NSA management slide shows a world map that illustrates Computer Network Exploitation (CNE) points all over the globe with the label ">50,000 World-wide implants."

According to the Dutch *NRC Handelsblad* newspaper, the malware is distributed by the NSA's Office of Tailored Access Operations (TAO) unit and, after being implanted inside a private, government or business network, can be controlled remotely "with a single push of button" like a digital sleeper cell.

This latest Snowden revelation highlights further the blatant criminality of the top-secret US intelligence agency and its anti-democratic activity. To the NSA's maniacal quest to spy and gather data on all cell phone and Internet activity is now added the cyber crime of hacking into all local area networks and so-called "off-net operations" to steal private information and communications. *NRC Handelsblad* reported that the malware implants often remain active for years without being detected and that such operations were carried out with particular focus on China, Russia, Venezuela and Brazil. According to the NSA's website, CNE "includes enabling actions and intelligence collection via computer networks that exploit data gathered from target or enemy information systems or networks."

In a report by Matthew M. Aid—a US intelligence and NSA expert—published in *Foreign Policy* last June, more than 1,000 military and civilian professional computer hackers staff the TAO unit and work around the clock in an ultramodern facility called the Remote Operations Center (ROC) at NSA headquarters in Fort Meade, Maryland. The elite TAO unit specializes in hacking into closed networks and, in some cases, use malicious software to destroy or damage computers and data via cyberattacks.

Aid reported that, according to NSA officials that were interviewed, TAO's mission is to "collect intelligence information on foreign targets by surreptitiously hacking into their computers and telecommunications systems, cracking passwords, compromising the computer security systems protecting the targeted computer, stealing the data stored on computer hard drives, and then copying all the messages and data traffic passing within the targeted email and text messaging systems. … TAO is also responsible for developing the information that would allow the United States to destroy or damage foreign computer and telecommunications systems with a cyberattack if so directed by the president."

As has been established in relation to all other illegal spying operations of the NSA, references to "foreign targets" as the sole subject of TAO hacking are a lie. The illegal methods of surveillance used by TAO to attack private networks are no doubt taking place both inside and outside the United States.

Founded in 1997, TAO has emerged as one of the most important operations within the NSA because it has software engineers and computer scientists belonging to the Data Network Technologies Branch. These experts develop the sophisticated malware that enable the TAO unit to collect intelligence that cannot be obtained in any other way. The super-secret TAO unit has grown in size and importance under the Obama administration. In addition to the operations at Fort Meade, there are mini-TAO units operating at the NSA centers at Wahiawa, HI, Fort Gordon, GA, San

Antonio, TX and Buckley Air Force Base outside Denver.

The *Washington Post* speculated that TAO was involved in the deployment of Stuxnet and Flame, malware programs jointly developed by the United States and Israel in 2010 for the purpose of attacking Iran's nuclear program. Stuxnet infected systems via a USB stick and proceeded to penetrate all computers on the network running Microsoft Windows. Its primary purpose was to destroy Iran's nuclear centrifuges. In this particular instance, the malicious software made its way into the "digital wild" and had an uncontrollable blowback impact on government and business computers within the US.

The *Washington Post* also reported in August, based on Snowden's revelations, that the US had conducted 231 offensive cyber-operations in 2011 that exploited the penetration of foreign computer networks with malware. Under a campaign code named GENIE, the NSA has plans to infect over 80,000 networks worldwide by placing millions of software implants into the routers, switches and firewalls of well-known technology providers. These backdoor operations allow the NSA to harvest communications and store them at the Utah Data Center for future analysis as part of its overall illegal cyber surveillance activities. *Der Spiegel* reported on November 10 details of how the British intelligence service GCHQ, operating as part of the "Five Eyes" nations, infected with malware the computer network at a Belgium telecom company. Based upon documents provided by Snowden, GCHQ hackers used a technique called "Quantum Insert" to place spying code into the computers of Belgacom network engineers by luring them onto replica web sites of LinkedIn and Slashdot.org.

The methods of malware distribution employed by the NSA are more commonly referred to as "phishing" and "pharming." Cyber criminals have used these techniques for the purpose of online identity theft since public Internet commerce was born in the 1990s. Utilizing psychological manipulation or confidence tricks, hackers lure individuals into a trap and fraudulently obtain sensitive information such as usernames and passwords, or credit card and social security numbers.

Phishing is a process whereby hackers send fake email or text messages that look like authentic communications from popular social web sites or financial institutions. These messages often contain links to bogus web pages that also have the "look and feel" of the real site and request that unsuspecting users update their personal information there. In some cases, the fake web pages are infected with malware that is then transmitted to the user's computer.

Pharming is a method of redirecting a legitimate website's traffic to a fake site masquerading as the real thing. Since pharming is a cyber attack on a website and exploits weaknesses in the Internet's Domain Name System (DNS), it cannot be combated with antivirus or spyware removal software. Pharming malware typically attacks an individual computer's "hosts file" or compromises a local network router. Users are thus completely unaware of the fact that the hacker site has replaced the legitimate web site and proceed to share sensitive information and download harmful data to their local hard drive.

In some instances, pharming can attack the firmware (software embedded at the hardware level) of a computer or network device and completely reconfigure settings without the knowledge of individual users or network administrators. Also, as has been previously reported, the manufacturers of computer and information technologies have built back door access into their systems, making them vulnerable to hacking.

Based upon the latest information supplied by Edward Snowden, it is now clear that the US government and its global spying partners are the primary distributors of malware and purveyors of cyber crime in the world.