Leaked NSA documents expose agency's sophisticated malware arsenal

Thomas Gaist
14 March 2014

In an article published Wednesday by the *Intercept*, "How the NSA Plans to Infect 'Millions' of Computers with Malware," Glenn Greenwald and Ryan Gallagher made public yet more revelations—based on documents provided to them by Edward Snowden—about US National Security Agency surveillance operations.

The latest documents show that the NSA has escalated its "active" surveillance operations exponentially during the past decade. In contrast to passive surveillance, active surveillance methods involve intervening directly against targeted machines using a sophisticated arsenal of malware for a range of surveillance-related purposes. According to the *Intercept*, the NSA's malware efforts have already infected at least 85,000 to 100,000 computers.

The leaked documents detail various aspects of a worldwide surveillance machine that is increasingly automated.

The growth of spying operations has encouraged the agency to automate aspects of its work. The NSA presentation states, "One of the greatest challenges for active SIGINT/attack is scale," and adds, "Human 'drivers' limit ability for large-scale exploitation (humans tend to operate within their own environment, not taking into account the bigger picture.)"

A program codenamed TURBINE, which has been operating since at least the summer of 2010, automated aspects of the process of malware deployment by NSA hackers. The *Intercept* described the program as "a major tactical shift within the NSA that was expected to have a profound impact—allowing the agency to push forward into a new frontier of surveillance operations." One NSA document leaked to the *Intercept* conceived TURBINE as a means to "increase the current capability to deploy and manage hundreds of Computer Network Exploitation (CNE) and Computer Network Attack (CNA) implants to potentially millions of implants."

The intelligence "Black Budget" leaked by Snowden listed TURBINE as a main component of the NSA project "Owning the Net."

The NSA leaks characterize TURBINE as: "A new intelligent command and control capability designed to manage a very large number of covert implants for active SIGINT and active Attack that reside on the GENIE covert infrastructure (for endpoint data extraction). It will increase the current capability to deploy and manage hundreds of Computer Network Exploitation (CNE) and Computer Network Attack (CNA) implants to potentially millions of implants."

Malware tools deployed by the NSA and operating increasingly on an automated basis under TURBINE, include:

UNITEDRAKE—takes control over computers through plug-ins

CAPTIVATEDAUDIENCE—takes control of computer microphones and records users' conversations

GUMFISH—accesses computer webcams to take photos of those nearby

FOGGYBOTTOM—records users' browsing histories and collects login information including passwords for email accounts

SALVAGERABBIT—extracts data from removable flash drives once they are linked to a targeted machine

HAMMERCHANT and HAMMERSTEIN—carries out "exploitation attacks" against Virtual Private Network (VPN) systems, track phone calls sent via Skype

QUANTUMSKY—blocks targeted computers from accessing web sites

QUANTUMCOPPER - corrupts files downloaded by targeted computers

WILLOWVIXEN—sends spam messages with malicious links containing “back-door implants”

QUANTUMHAND—uses fake Facebook server to “shoot” malware packets at target

SECONDDATE—modifies content of communications between servers and clients in real time, redirects browsers to NSA servers codenamed FOXACID, said by NSA docs to have “mass exploitation potential for clients passing through network choke points”

VALIDATOR—downloads and uploads data to and from targeted computers

The NSA also launches malware attacks against systems administrators of telecommunications providers. This practice enables the NSA to spy on all communications being handled by a given provider.

“Sys admins are a means to an end” wrote an NSA operative in an internal message titled, “I hunt sys admins,” the documents show.

TURBINE operations are coordinated with a global network of surveillance “sensors,” codenamed TURMOIL, set up by the NSA around the world. This network finds targets by identifying data “selectors” including email and IP addresses, usernames, etc.

The documents leaked to the *Intercept* show that the other major powers which make up the “Five Eyes” global surveillance alliance—the UK, Canada, New Zealand, and Australia—have been involved in the use of malware implants. As part of its TURMOIL network, the NSA runs a joint eavesdropping base with the Government Communications Headquarters (GCHQ) in Britain, called the Menwith Hill satellite eavesdropping base.

The latest documents also revealed that GCHQ has been targeting systems administrators at Belgacom, known as “Operation Socialist,” since at least 2010.

In the wake of Snowden’s exposure of the mass surveillance, a propaganda offensive was initiated by the ruling elite, claiming that the spying was “narrowly targeted” against highly specific, imminent terrorist threats. These arguments have been thoroughly discredited. As the most recent leaks show, the US and its allies are carrying out aggressive surveillance and cyberwarfare operations against their own populations and targets around the world.

The implementation of “active” surveillance practices reflects the drive of the state to accumulate as much information on as many people as possible, in preparation for state repression against the mass struggles now developing in the international working class. This political agenda is propelling the continuous expansion and automation of the spying machinery.