NSA's TURBINE server pumps 'malware into MILLIONS of PCs'

by Iain Thomson via tone - The Register *Thursday, Mar 13 2014, 3:36am*
international / prose / post

> This piece is for specialists so I'm very sorry lamers, u'll jus have to go watch American idol and other digital effluent on your idiot boxes! *HOWEVER, IT SHOULD BE NOTED THAT THE ACTIVITIES DESCRIBED IN THE ARTICLE BELOW ARE IN FLAGRANT VIOLATION OF NUMEROUS COMMUNICATION LAWS IN AUSTRALIA AND MANY OTHER WESTERN NATIONS. THE QUESTION ARISES WHAT ARE THE GOVERNMENTS OF THESE NATIONS DOING ABOUT GROSSLY ILLEGAL ACTIVITIES, INCLUDING PAN SURVEILLANCE, CONDUCTED BY THE AMERICAN NSA IN THEIR COUNTRIES?* ***THAT IS THE REAL ISSUE!*** *DEMOCRATIC GOVERNMENTS ARE SUPPOSED TO REPRESENT YOUR INTERESTS AND WISHES, MORONS -- or should we let this one pass like all the other criminal activities (extra-judicial killing, etc) the USA engages in on a DAILY BASIS?*

Ed Snowden, ex military special ops, CIA and NSA

Elite crews notice immediately that this report covers decades old hacks and ploits -- thanks Ed for revealing NOTHING NEW as usual!

Notice how fifth-rate NSA hackers are simply using very old code and tools with the not so very glamorous (non) innovation of brute force, with dedicated servers.

How 'creative and innovative,' NSA, excuse my sarcasm!

Government agencies by nature are criminal organisations and NEVER attract the core ELITE from the underground. We hoped that somewhere in Israel or the USA highly paid fifth-rater (no-hopers) would at least produce something useful and NEW, however, lamers remain uncreative lamers.

What is new, CREATIVE or INNOVATIVE in the digital world delivers HUGE advantage if knowledge is contained in small groups, which is a cardinal rule of the underground Uber elite. Innovations become awesome power tools for the few and with permission I am now able to release knowledge of only one such recent innovation to the public -- the ability to communicate in new unknown channels or corridors in existing protocols -- its all in the numbers!

It became necessary to develop new means of private communication so the elite simply worked and found various -- NOT just one -- avenues of approach and are now able to communicate in complete privacy by simply running tiny packages that exploit existing code.

What is that degree of privacy worth in todays world? But I'm sorry to say that the usefulness of the

package depends entirely on its small and secret user base -- in other words lamers, the most powerful social force in the world (YOU) remains divided, subjugated, cowardly sheep and the elite remain the elite -- it's just the natural order of things! Why have you not yet remedied the NSA problem by simply uniting and demanding an end to these nefarious practices? Humans utilise the solutions immediately available to them and the obvious solution to all the problems the masses face today is not genius or high skill levels, it's simply the sheer force of NUMBERS -- you (potentially) control the social reality but cower in fear because a few evil groups intimidate you with false or exaggerated information -- you tragic slaves -- LOL!

N'way, to return to the topic tho I never miss an opportunity to spell it out for the morons.

There is nothing new in the tools the NSA are employing, the NSA have simply boosted performance with dedicated servers - doh! Not very difficult when you have unlimited time and funds supplied by the moronic masses.

The following story from 'The Register' (unintentionally we hope) portrays the NSA as some truly powerful group when in reality they can barely find their dicks to take a piss! Also, a few words for Ed Snowden government agent, please Mr Agent tell us something we don't already know or that has not been freely available in the public domain for decades!

It all simply demonstrates how easily duped deeply flawed personalities like Assange and Greenwald are! Ask yourselves what type of mentality enlists in the armed forces and undertakes training in special ops then works for the CIA then NSA and then mysteriously becomes a highly PUBLICISED whistleblower that reveals nothing new -- you fuckin' dunderheads, LMAO? I have never met a real hacker in my life that has a background like that -- you can't see the nose on your stupid narcissistic faces:

> **NSA's TURBINE robot pumps 'malware into MILLIONS of PCs'**
>
> (Sysadmins, routers, criminals' IRC botnets, and maybe terrorists, all for the pwning)
>
> The latest batch of top-secret intelligence documents from the hoard collected by NSA whistleblower Edward Snowden detail the massive increase in the agency's use of its Tailored Access Operations (TAO) hacking unit – including a system dubbed TURBINE that can spam out millions of pieces of sophisticated malware at a time.
>
> The presentation slides, published by The Intercept, show that 10 years ago the NSA had infiltrated and tapped a modest number of computers, but has since hugely bolstered its toolkit and increased its target list. Within eight years, the number of active pieces of implanted spyware was in the tens of thousands, and slides show an extensive arms catalog of malware for the TAO team to choose from.
>
> "One of the greatest challenges for active SIGINT/attack is scale," explained one presentation from 2009, marked top secret. "Human 'drivers' limit ability for large-scale exploitation (humans tend to operate within their own environment, not taking into account the bigger picture)."
>
> The solution was to build TURBINE, which can carry out "automated implants by groups instead of individually," and scale to operate millions of implants at a time. This command-and-control server includes an "expert system" that automatically picks the right malware for a victim and installs it on their computer, thus "relieve the [TURBINE]

user from needing to know/care about the details."

TURBINE was active from at least July 2010, the documents state, and has infected up to 100,000 devices and machines, with more planned. According to the agency's 2013 budget files, some of the $67.6m of taxpayer dollars allocated to the NSA's TAO team went to maintaining and developing the system.

TURMOIL hunts the sysadmin

TURBINE also links into a NSA sensor system dubbed TURMOIL, which taps into computer networks around the world to monitor data traffic and identify potential targets. It can track down a mark from their email address or IP address, which device he or she is using, or by web cookies from Google, Microsoft, Twitter, Yahoo! and others.

While terrorist targets are mentioned, it's clear from the documents that system administrators are also high on the todo list for the TAO team. One comment on an internal NSA message board system was titled simply: "I hunt sys admins."

"Sys admins are a means to an end," it states. "Once you have control of the IT manager's computer then it's easy to monitor any "government official that happens to be using the network some admin takes care of."

Pwning the sysadmin is useful for malware attacks against large commercial routers and to defeat VPNs. The documents detail two pieces of NSA-developed malware, HAMMERCHANT and HAMMERSTEIN, which are designed to sit on routers and eavesdrop on VoIP traffic, and grab encryption keys to decrypt supposedly secure VPN connections, all in real time.

Other malware includes code called QUANTUMSKY, developed in 2004, which can block access to websites, and a 2008 creation dubbed QUANTUMCOPPER which automatically corrupts any data downloaded by a user.

TURBINE is run though stations at the NSA's headquarters in Maryland, along with ancillary offices in the British Menwith Hill facility and from Misawa, Japan. Documents show the UK's GCHQ has been active in developing exploits for TURBINE and that it uses information gleans from the system, as do the other "Five Eyes" nations of Canada, Australia, and New Zealand.

"All of GCHQ's work is carried out in accordance with a strict legal and policy framework which ensures that our activities are authorized, necessary and proportionate, and that there is rigorous oversight," the British intelligence agency said in a statement.

The Snowden documents show that the TAO team now has access to a very sophisticated toolkit for implanting trackers on systems, and how the methods of spreading the code have evolved to match consumer behavior.

A 2012 presentation complains that the traditional method of infection, spamming out infected attachments, was only achieving a one per cent success rate because people are getting smarter about avoiding potentially malicious downloads. To get around this, the agency switched to browser attacks, which it said upped success rates to 80 per cent in some cases.

Targets visiting certain websites were redirected to an NSA WILLOWVIXEN server, allowing software called FOXACID to find a browser vulnerability and exploit this to compromise the PC or handheld. The documents claim that a fake Facebook server was set up for this purpose and used to distribute malware dubbed QUANTUMHAND, which went live in October 2010.

"If we can get the target to visit us in some sort of web browser, we can probably own them," a TAO team member reports in one document. "The only limitation is the 'how.'"

Other code, called SECONDDATE uses a man-in-the-middle attack to allow "mass exploitation potential for clients passing through network choke points, but is configurable to allow surgical target selection as well."

A 2010 presentation also gives details about the QUANTUM family of malware developed by the government for attacking systems. This includes code for the redirection of web traffic, controlling crooks' IRC botnets, hijacking DNS, and corrupting downloads.

Another malware system, called UNITEDRAKE, comes with a selection of plugins for different purposes, each with its own classification. The CAPTIVATEDAUDIENCE plugin will take over a system's microphone to record conversations, FOGGYBOTTOM will record internet history and login details, and SALVAGERABBIT copies the contents of any flash drives plugged into the machine.

The agency is well aware that antivirus companies are on the lookout for new and interesting malware samples, particularly after the Flame debacle. A NSA trojan dubbed VALIDATOR can be set with an automatic self-destruct sequence and delete itself from a target's system after a set period.

The madness is spreading

Despite efforts to limit the exposure of its systems to outside interest, the documents show that the NSA is aware that other governments are copying their techniques.

"Hacking routers has been good business for us and our 5-eyes partners for some time," notes one NSA analyst in a top-secret document dated December 2012. "But it is becoming more apparent that other nation states are honing their skillz [sic] and joining the scene."

This is already worrying security analysts, and was top of the agenda at last month's TrustyCon conference. F-Secure's malware research chief Mikko Hyppönen told the summit that so far government-developed malware was coming from Germany, Russia, China, and even Sweden, and there was a thriving trade by ethically challenged companies willing to develop malware for repressive regimes.

Similar concerns were echoed at the RSA 2014 conference, with the company's chairman Art Coviello calling for an international moratorium on attack code before the situation gets out of control. If government cyberattacks are normalized then the effects on the general public could be catastrophic, he noted, but there's no sign of a change of policy from the NSA.

> "As the [US] President made clear on 17 January," the agency said in a statement, "signals intelligence shall be collected exclusively where there is a foreign intelligence or counterintelligence purpose to support national and departmental missions, and not for any other purposes."
>
> Copyright applies to external text.

Follow link for additional embedded material.

)

Failed Oz communications minister, Malcolm Turnbull

http://tinyurl.com/qf696ka
