GlobalResearch
Center for Research on Globalization

Malware “Industrialises Spying”: The NSA has “Automated its Spying Operations”

By Jonathan Cook
Global Research, March 14, 2014
jonathan-cook.net

Region: USA
Theme: Intelligence, Police State & Civil Rights

The report from Glenn Greenwald and Ryan Gallagher, based on the Edward Snowden leaks reveals that the NSA – surprise, surprise – has automated its spying operations, so that malware once used to target the odd terror suspect can now be used routinely. The programme is called “Owning the net”. (Israel also gets a special shout-out in the report for its work with the NSA in developing malware.)So it’s no longer – and, of course, never was – only about tracking metadata from our phone calls and Google searches. This is industrialised spying, including on domestic populations, using our interactions with the net (which means most of our activities) to know what is going on in our minds.

Much of the evidence cited in the report is from 2009, so it is difficult to know how much further the NSA has gone in implementing its plans. My guess is things are far worse than even this report suggests: five years is a long time in software development.

> The automated system – codenamed TURBINE – is designed to “allow the current implant network to scale to large size (millions of implants) by creating a system that does automated control implants by groups instead of individually.” ...
>
> In 2004, according to secret internal records, the agency was managing a small network of only 100 to 150 implants. But over the next six to eight years, as an elite unit called Tailored Access Operations (TAO) recruited new hackers and developed new malware tools, the number of implants soared to tens of thousands. ...
>
> In many cases, firewalls and other security measures do not appear to pose much of an obstacle to the NSA. Indeed, the agency’s hackers appear confident in their ability to circumvent any security mechanism that stands between them and compromising a computer or network. “If we can get the target to visit us in some sort of web browser, we can probably own them,” an agency hacker boasts in one secret document.

As I have stated in these pages so often I’m starting to bore myself repeating it, we – the people who elect and supposedly control our governing bodies – are the ultimate targets of these surveillance operations. It is about developing the ability to identify early signs of dissent, so as to snuff out opposition before it can win large-scale support. I was intrigued by the brief reference in the piece to one programme called “Operation Socialist” – interesting to know who were included in that hacking operation.

These programmes are a backstop, designed to deal with the fall-out if our media fail in their struggle to persuade us – given the overwhelming evidence to the contrary – of our

leaders' benign intent and democratic accountability.

https://firstlook.org/theintercept/article/2014/03/12/nsa-plans-infect-millions-computers-malware/

– See more at: http://www.jonathan-cook.net/blog/2014-03-14/nsa-malware-industrialises-spying/#sthash.wl8v92kk.dpuf

---

Articles by: Jonathan Cook