GlobalResearch
Center for Research on Globalization

The US Government Might Be the Biggest Hacker in the World

By RT
Global Research, May 17, 2013
RT 12 May 2013

Region: USA
Theme: US NATO War Agenda

Cyber crime is big business in the US. It's used to spy, steal, harass competition, political opponents, or to stage an attack and blamed it on a foreign enemy.

Is the government in on this crime industry? Yes, and in bigger ways than you can imagine...

This trend is enabled domestically by an institutionally corrupt US legal system and a police state which are fast working to shut and jail security consultants and white hat hackers who help to expose security flaws and government hegemony over cyber space. The reason for this is because the state wants to be able to operate in secret – as the world's biggest and most prolific hacking machine. In other words, the US government want hackers to exist, but only hackers who are on their payroll.

Still not convinced? According to McAfee, the United States is home to the largest number of botnets or "zombie armies – a hive of computers that are used to generate spam, relay viruses and flood networks and servers with excessive requests to cause it to fail – in the world, and even control remote overseas servers used to hack other computers worldwide.

Want more? Data from Germany's Deutsche Telekom shows that more attacks against its networks come from the US.

Obama will tell his people that the Chinese are responsible for this hack, or that one. Still think that the US is not the number one cyber threat to the planet in 2013?

Read this shocking report...

The United States government is investing tens of millions of dollars each year on offensive hacking operations in order to exploit vulnerabilities in the computers of its adversaries, Reuters reports.

 According to an in-depth article published Friday by journalist Joseph Menn, the US and its Department of Defense contractors are increasingly pursuing efforts to hack the computers of foreign competitors, in turn exposing a rarely discussed aspect of the nation's clandestine cyber operations.

In a time when the government continues to prosecute alleged domestic computer criminals — so much so that demands for technology law reform have been rampant as of late — Menn says the US is guilty of spending millions on discovering, identifying and exploiting previously unknown security flaws, often gaining unfettered access to the systems and networks of international targets.

As a result, the US has become one of the world's top players in regards to wreaking havoc over the Internet — even as calls to investigate foreign hackers increase in Congress.

On Tuesday, a bipartisan supported proposal was introduced in Congress specifically to protect US commercial data from being compromised by foreign hackers. According to Menn, however, the American government is just as guilty of cybercrimes as the countries it warns against in introducing the "Deter Cyber Theft Act."

"*Even as the US government confronts rival powers over widespread Internet espionage, it has become the biggest buyer in a burgeoning gray market where hackers and security firms sell tools for breaking into computers*," Menn wrote.

In his report, Menn explained that a large chunk of the country's current cyber endeavors does not rely on defensive strategy as one might imagine, but instead involves offensive operations launched with the intent of causing harm on the computers of adversaries.

Menn wrote defense contractors "*spend at least tens of millions of dollars a year*" on simply researching exploits that, if pursued, could put the eyes and ears of the American intelligence company essentially anywhere in the world.

And although the US has not officially gone on the record to acknowledge these shadowy operations, Menn wrote that the nation's most well-known cyber endeavor — the Stuxnet worm that targeted Iranian nuclear plants — is just one example of the budding attempts to attack foreign entities.

"*Computer researchers in the public and private sectors say the US government, acting mainly through defense contractors, has become the dominant player in fostering the shadowy but large-scale commercial market for tools known as exploits, which burrow into hidden computer vulnerabilities*," he wrote.

"*In their most common use, exploits are critical but interchangeable components inside bigger programs. Those programs can steal financial account passwords, turn an iPhone into a listening device or, in the case of Stuxnet, sabotage a nuclear facility*."

Menn cited several defense contractors and government officials — many speaking on condition of anonymity — who admitted the increasingly dominant role the US government has in pursuing research on these exploits and using them to attack rival networks.

According to the report, "*Reuters reviewed a product catalogue from one large contractor, which was made available on condition the vendor not be named. Scores of programs were listed. Among them was a means to turn any iPhone into a room-wide eavesdropping device. Another was a system for installing spyware on a printer or other device and moving that malware to a nearby computer via radio waves, even when the machines aren't connected to anything*."

These contractors, he wrote, spend upwards of $100,000 on licensing single operations to governments, including the US. The result has been the development of a thriving industry, largely underground, where exploits are bought and sold before patches are developed to protect against intrusions. These "zero-day exploits"— labeled as such because developers are unaware of the flaw until it's announced — fetch big bucks from contractors, governments and hackers.

And as the demand for these exploits increases, so do the players in the game. One example cited by Menn is Atlanta-based Endgame Inc., which recently brought in $23 million in funding courtesy of Silicon Valley venture capital firm Kleiner Perkins Caufield & Byers. But as early as 2011, Endgame and similar entities have been on the radar of hacktivists hell-bent on exposing the largely unknown doings of defense contractors.

When the loose-knit hacking collective Anonymous investigated security consultants HBGary in 2011, they uncovered only the tip of an intricate iceberg made up of former federal employees and other intelligence workers being paid boatloads to give governments exploits that could be used to their advantage. Project PM, the open-source online think tank started by former Anonymous collaborator Barrett Brown, discussed Endgame and its associates in great detail.

From a Business Week article cited by Brown:

> "*Endgame executives will bring up maps of airports, parliament buildings and corporate offices. The executives then create a list of the computers running inside the facilities, including what software the computers run, and a menu of attacks that could work against those particular systems. Endgame weaponry comes customized by region — the Middle East, Russia, Latin America and China — with manuals, testing software and 'demo instructions.' There are even target packs for democratic countries in Europe and other US allies*."

Last year Brown was arrested on unrelated counts and remains in custody six months later with an eventual trial still a ways before him. The US government has since subpoenaed Internet host Cloudflare for records pertaining to Project PM, and has equated the website as a criminal enterprise.

"*Project PM served as a forum through which defendant Brown and other individuals sought*

to discuss their joint and separate activities and engage in, encourage, or facilitate the commission of criminal conduct online," the government alleged when it fought back attempts from the current Project PM administrator to quash that subpoena.

Brown fired back from prison: "*It makes it much more obvious that this investigation and the charges against me has to do with our successful research into what may be criminal activities by firms close to the government*."

If convicted on all counts — more than one dozen including threatening a federal agent andsharing a hyperlink — Brown could be sentenced to 100 years in prison.

> "*It is virtually impossible to conclude that the obscenely excessive prosecution he now faces is unrelated to that journalism and his related activism*," Glenn Greenwald wrote earlier this year for The Guardian.

Meanwhile, Menn admitted that other investigative computer work — specifically discovering exploits like the one Endgame thrives off of — is an endeavor that discourages people outside of the government and defense industry from entertaining.

> "*Most companies, including Microsoft, Apple Inc. and Adobe Systems Inc, on principle won't pay researchers who report flaws, saying they don't want to encourage hackers*," he wrote. "*Those that do offer 'bounties,' including Google Inc. and Facebook Inc., say they are hard-pressed to compete financially with defense-industry spending*."

Andrew Auernheimer, a 26-year-old independent security researcher, was recently sentenced to 41 months in prison for identifying and disclosing a harmless exploit on the servers of AT&T that allowed anyone with the know-how to collect the email addresses of thousands of Apple iPadusers. After he was convicted, Auernheimer wrote for Wired that the selective prosecution of some security researchers will deter future hackers from ever disclosing exploits, even critical ones that effect national security.

> "*In an age of rampant cyber espionage and crackdowns on dissidents, the only ethical place to take your zero-day is to someone who will use it in the interests of social justice. And that's not the vendor, the governments, or the corporations — it's the individuals*," he wrote. "*In a few cases, that individual might be a journalist who can facilitate the public shaming of a web application operator. However, in many cases the harm of disclosure to the un-patched masses (and the loss of the exploit's potential as a tool against oppressive governments) greatly outweighs any benefit that comes from shaming vendors. In these cases, the antisec philosophy shines as morally superior and you shouldn't disclose to anyone*."

Articles by: RT