CYBERSECURITY

NSA and the No Good, Very Bad Monday

By Nicholas Weaver Tuesday, August 16, 2016, 10:34 AM

DayZero: Cybersecurity Law and Policy

Monday was a tough day for those in the business of computer espionage. Russia, still using the alias Guccifer2.0, dumped even more DNC documents. And on Twitter, Mikko Hypponen noted an announcement on Github that had gone overlooked for two days, a group is hosting an auction for code from the "Equation Group," which is more commonly known as the NSA. The auctioneer's pitch is simple, brutal, and to the point:

> How much you pay for enemies cyber weapons? Not malware you find in networks. Both sides, RAT + LP, full state sponsor tool set? We find cyber weapons made by creators of stuxnet, duqu, flame. Kaspersky calls Equation Group. We follow Equation Group traffic. We find Equation Group source range. We hack Equation Group. We find many many Equation Group cyber weapons. You see pictures. We give you some Equation Group files free, you see. This is good proof no? You enjoy!!! You break many things. You find many intrusions. You write many words. But not all, we are auction the best files.

This release included two encrypted files, and the password to one was provided as proof while the other remains encrypted. The attackers claim that they will provide the password to the second file to the winner of a Bitcoin auction.

The public auction part is nonsense. Despite prevailing misconceptions on cryptocurrency, Bitcoin's innate traceability means that no one could really expect to launder even $1M out of a high profile Bitcoin wallet like this one without risking detection, let alone the $500M being requested for a full public release. The auction is the equivalent of a criminal asking to be paid in new, marked, sequential bills. Because the actors here are certainly not amateurs, the auction is presumably a bit of "Doctor Evil" theater—the only bids will be $20 investments from Twitter jokesters.

But the proof itself appears to be very real. The proof file is 134 MB of data compressed, expanding out to a 301 MB archive. This archive appears to contain a large fraction of the NSA's implant framework for firewalls, including what appears to be several versions of different implants, server side utility scripts, and eight apparent exploits for a variety of targets.

The exploits themselves appear to target Fortinet, Cisco, Shaanxi Networkcloud Information Technology (sxnc.com.cn) Firewalls, and similar network security systems. I will leave it to others to analyze the reliability, versions supported, and other details. But nothing I've found in

either the exploits or elsewhere is newer than 2013.

Because of the sheer volume and quality, it is overwhelmingly likely that this data is authentic. And it does not appear to be information taken from compromised targets. Instead, the exploits, binaries with help strings, server configuration scripts, 5 separate versions of one implant framework, and all sort of other features indicate that this is analyst-side code—the kind that probably never leaves the NSA.

It is also unlikely that this data is from the Snowden cache. Those documents focused on PowerPoint slides and shared data, not detailed exploits. Besides NSA, the only plausible candidate for ownership is GCHQ—and the implications of stealing Top Secret data from GCHQ and modifying it to frame the NSA would themselves be startling.

All this is to say that there is relatively high confidence that these files contain genuine NSA material.

From an operational standpoint, this is not a catastrophic leak. Nothing here reveals some special "NSA magic." Instead, this is evidence of good craftsmanship in a widely modular framework designed for ease of use. The immediate consequence is probably a lot of hours of work down the drain.

But the big picture is a far scarier one. Somebody managed to steal 301 MB of data from a TS//SCI system at some point between 2013 and today. Possibly, even probably, it occurred in 2013. But the theft also could have occurred yesterday with a simple utility run to scrub all newer documents. Relying on the file timestamps—which are easy to modify—the most likely date of acquisition was June 11, 2013 (**see Update, however**). That is two weeks after Snowden fled to Hong Kong and six days after the first *Guardian* publication. That would make sense, since in the immediate response to the leaks, as the NSA furiously ran down possible sources, it may have accidentally or deliberately eliminated this adversary's access.

As with other recent cyber conflicts, the espionage aspect is troubling but not entirely new. It's very, very bad that someone was able to go rummaging through a TS//SCI system—or even an unclassified Internet staging system where the NSA operator unwisely uploaded all this data—and to steal 300 MB of data. But whoever stole this data now wants the world to know—and that has much graver implications. The list of suspects is short: Russia or China. And in the context of the recent conflict between the US and Russia over election interference, safe money is on the former.

Right now, I'd imagine that the folks at NSA are having rather unpleasant conversations about what the other encrypted file might contain, and what other secrets this attacker may have gained access to. Even if they were aware of the attack that resulted in this leak, there's no way of knowing what is in the other archive. Is there evidence of another non-Snowden insider who went silent three years ago? Was a TS//SCI system remotely compromised? Was there some kind of massive screw-up at an agency which prides itself on world class OPSEC? Some combination of the three?

And—most chillingly—what else might be released before this war of leaks is over?

Update: Thanks to @botherder for pointing out that a couple files have a newer date: One file has a date of June 17th, 2013; another has a date of July 5th, 2013; three setup strips are dated September 4th, 2013; and two have dates of October 18th 2013. One of those files (which I'm currently investigating) is the database of allocated Ethernet MAC addresses, which may be able to identify a later minimum date of compromise. If the latter date of October 18th, 2013 is correct, this is even more worrysome, as this suggests that the compromise happened four months after the initial Snowden revelations—a period of time when the NSA's systems should have been the most secure.

Update 2: Looking at the dates again, it now does seem somewhat likely that this was data copied on June 11th, 2013 with a few updates with a compromise after October 18th. This does make it more likely that this was taken from a set of files deliberately moved onto a system on the Internet used for attacking others. To my mind, this is actually an even scarier possibility than the NSA internal system compromise: This scenario would have the NSA, *after the Snowden revelations*, practicing some incredibly awful operational security. Why should the NSA include five different versions of the same implant on a system used to attack other systems on the Internet? Let alone implants which still have all the debugging strings, internal function names, and absolutely no obfuscation?

Update 3: Kaspersky confirms that the particular use of RC6 matches the unique design present in other Equation Group malcode. XORcat apparently confirmed that the Cisco exploit works and, due to the versions it can attack, was a zero day at the time. This exploit would generally work to take over a firewall from the inside of a target network since it did require limited access that is almost always blocked from the outside.

Topics: Cybersecurity

Tags: National Security Agency (NSA)

Nicholas Weaver is a senior staff researcher focusing on computer security at the International Computer Science Institute in Berkeley, California. All opinions are his own.

@ncweaver

MORE ARTICLES ›

RELATED ARTICLES

What Sauron Tells Us About What NSA's Up To, and What It Should Do Next

Nicholas Weaver Mon, Aug 15, 2016, 2:52 PM

More on Securing the Election

Carrie Cordero Mon, Aug 15, 2016, 1:40 PM

More DNC Leaks

Paul Rosenzweig Sat, Aug 13, 2016, 10:47 AM

Hanging Internet Users Out to Dry

Marshall Erwin, Urmika Shah Fri, Aug 12, 2016, 1:45 PM

Apple at BlackHat: Reopening the "Going Dark" Debate

Matt Tait Fri, Aug 12, 2016, 9:42 AM