Schneier on Security

Blog >

Who Are the Shadow Brokers?

In 2013, a mysterious group of hackers that calls itself the Shadow Brokers stole a few disks full of NSA secrets. Since last summer, they've been dumping these secrets on the Internet. They have publicly embarrassed the NSA and damaged its intelligence-gathering capabilities, while at the same time have put sophisticated cyberweapons in the hands of anyone who wants them. They have exposed major vulnerabilities in Cisco routers, Microsoft Windows, and Linux mail servers, forcing those companies and their customers to scramble. And they gave the authors of the WannaCry ransomware the exploit they needed to infect hundreds of thousands of computer worldwide this month.

After the WannaCry outbreak, the Shadow Brokers threatened to release more NSA secrets every month, giving cybercriminals and other governments worldwide even more exploits and hacking tools.

Who are these guys? And how did they steal this information? The short answer is: we don't know. But we can make some educated guesses based on the material they've published.

The Shadow Brokers suddenly appeared last August, when they published a series of hacking tools and computer exploits -- vulnerabilities in common software -- from the NSA. The material was from autumn 2013, and seems to have been collected from an external NSA staging server, a machine that is owned, leased, or otherwise controlled by the US, but with no connection to the agency. NSA hackers find obscure corners of the Internet to hide the tools they need as they go about their work, and it seems the Shadow Brokers successfully hacked one of those caches.

In total, the group has published four sets of NSA material: a set of exploits and hacking tools against routers, the devices that direct data throughout computer networks; a similar collection against mail servers; another collection against Microsoft Windows; and a working directory of an NSA analyst breaking into the SWIFT banking network. Looking at the time stamps on the files and other material, they all come from around 2013. The Windows attack tools, published last month, might be a year or so older, based on which versions of Windows the tools support.

The releases are so different that they're almost certainly from multiple sources at the NSA. The SWIFT files seem to come from an internal NSA computer, albeit one connected to the Internet. The Microsoft files seem different, too; they don't have the same identifying information that the router and mail server files do. The Shadow Brokers have released all the material unredacted, without the care journalists took with the Snowden documents or even the care WikiLeaks has taken with the CIA secrets it's publishing. They also posted anonymous messages in bad English but with American cultural references.

Given all of this, I don't think the agent responsible is a whistleblower. While possible, it seems like a whistleblower wouldn't sit on attack tools for three years before publishing. They would act more like Edward Snowden or Chelsea Manning, collecting for a time and then publishing immediately -- and publishing documents that discuss what the US is doing to whom. That's not what we're seeing here; it's simply a bunch of exploit code, which doesn't have the political or ethical implications that a whistleblower would want to highlight. The SWIFT documents are records of an NSA operation, and the other posted files demonstrate that the NSA is hoarding vulnerabilities for attack rather than helping fix them and improve all of our security.

I also don't think that it's random hackers who stumbled on these tools and are just trying to harm the NSA or the US. Again, the three-year wait makes no sense. These documents and tools are cyber-Kryptonite; anyone who is secretly hoarding them is in danger from half the intelligence agencies in the world. Additionally, the publication schedule doesn't make sense for the leakers to be cybercriminals. Criminals would use the hacking tools for themselves, incorporating the exploits into worms and viruses, and generally profiting from the theft.

That leaves a nation state. Whoever got this information years before and is leaking it now has to be both capable of hacking the NSA and willing to publish it all. Countries like Israel and France are capable, but would never publish, because they wouldn't want to incur the wrath of the US. Country like North Korea or Iran probably aren't capable. (Additionally, North Korea is suspected of being behind WannaCry, which was written after the Shadow Brokers released that vulnerability to the public.) As I've written previously, the obvious list of countries who fit my two criteria is small: Russia, China, and -- I'm out of ideas. And China is currently trying to make nice with the US.

It was generally believed last August, when the first documents were released and before it became politically controversial to say so, that the Russians were behind the leak, and that it was a warning message to President Barack Obama not to retaliate for the Democratic National Committee hacks. Edward Snowden guessed Russia, too. But the problem with the Russia theory is, why? These leaked tools are much more valuable if kept secret. Russia could use the knowledge to detect NSA hacking in its own country and to attack other countries. By publishing the tools, the Shadow Brokers are signaling that they don't care if the US knows the tools were stolen.

Sure, there's a chance the attackers knew that the US knew that the attackers knew -- and round and round we go. But the "we don't give a damn" nature of the releases points to an attacker who isn't thinking strategically: a lone hacker or hacking group, which clashes with the nation-state theory.

This is all speculation on my part, based on discussion with others who don't have access to the classified forensic and intelligence analysis. Inside the NSA, they have a lot more information. Many of the files published include operational notes and identifying information. NSA researchers know exactly which servers were compromised, and through that know what other information the attackers would have access to. As with the Snowden documents, though, they only know what the attackers could have taken and not what they did take. But they did alert Microsoft about the Windows vulnerability the Shadow Brokers released months in advance. Did they have eavesdropping capability inside whoever stole the files, as they claimed to when the Russians attacked the State Department? We have no idea.

So, how did the Shadow Brokers do it? Did someone inside the NSA accidentally mount the wrong server on some external network? That's possible, but seems very unlikely for the organization to make that kind of rookie mistake. Did someone hack the NSA itself? Could there be a mole inside the NSA?

If it is a mole, my guess is that the person was arrested before the Shadow Brokers released anything. No country would burn a mole working for it by publishing what that person delivered while he or she was still in danger. Intelligence agencies know that if they betray a source this severely, they'll never get another one.

That points to two possibilities. The first is that the files came from Hal Martin. He's the NSA contractor who was arrested in August for hoarding agency secrets in his house for two years. He can't be the publisher, because the Shadow Brokers are in business even though he is in prison. But maybe the leaker got the documents from his stash, either because Martin gave the documents to them or because he himself was hacked. The dates line up, so it's theoretically possible. There's nothing in the public indictment against Martin that speaks to his selling secrets to a foreign power, but that's just the sort of thing that would be left out. It's not needed for a conviction.

If the source of the documents *is* Hal Martin, then we can speculate that a random hacker did in fact stumble on it -- no need for nation-state cyberattack skills.

The other option is a mysterious second NSA leaker of cyberattack tools. Could this be the person who stole the NSA documents and passed them on to someone else? The only time I have ever heard about this was from a *Washington Post* story about Martin:

> There was a second, previously undisclosed breach of cybertools, discovered in the summer of 2015, which was also carried out by a TAO employee [a worker in the Office of Tailored Access Operations], one official said. That individual also has been arrested, but his case has not been made public. The individual is not thought to have shared the material with another country, the official said.

Of course, "not thought to have" is not the same as not having done so.

It is interesting that there have been no public arrests of anyone in connection with these hacks. If the NSA knows where the files came from, it knows who had access to them -- and it's long since questioned everyone involved and should know if someone deliberately or accidentally lost control of them. I know that many people, both inside the government and out, think there is some sort of domestic involvement; things may be more complicated than I realize.

It's also not over. Last week, the Shadow Brokers were back, with a rambling and taunting message announcing a "Data Dump of the Month" service. They're offering to sell unreleased NSA attack tools -- something they also tried last August -- with the threat to publish them if no one pays. The group has made good on their previous boasts: In the coming months, we might see new exploits against web browsers, networking equipment, smartphones, and operating systems -- Windows in particular. Even scarier, they're threatening to release raw NSA intercepts: data from the SWIFT network and banks, and "compromised data from Russian, Chinese, Iranian, or North Korean nukes and missile programs."

Whoever the Shadow Brokers are, however they stole these disks full of NSA secrets, and for whatever reason they're releasing them, it's going to be a long summer inside of Fort Meade -- as it will be for the rest of us.

This essay previously appeared in the *Atlantic*, and is an update of this essay from *Lawfare*.

Tags: cybersecurity, cyberweapons, hacking, leaks, NSA, vulnerabilities, whistleblowers

Posted on May 30, 2017 at 6:08 AM • 26 Comments

Comments

Anders Reed-Mohn (@itinsecurity) • May 30, 2017 6:46 AM

One thing that strikes me is the consistency in the "bad english" language of some of the ShadowBrokers' messages.

I get the sense that whoever is writing is very much on command of their words, just masking just how good their english is, and is really a native English speaker.

Steven C. Buttgereit • May 30, 2017 7:03 AM

More in jest, but perhaps not completely so, I'll put forward: a small group of skilled, but unscrupulous security consultants or security company; including perhaps former members of the intelligence community.

All of the motivations and payoffs that seem to conflict in the blog post, ultimately seem to benefit computer security professionals the most. The releases forces companies to act and act on an emergency basis, the slow staging of releases ensures that there has to be multiple calls for service, and the flow of cash is tied to a legitimate business activity since the nefarious bit isn't tied to a financial transaction directly.

Of course, the flaw in the argument is while any number of good security teams are well paid, I suppose it wouldn't be the most profitable use of the data... but.... just maybe :-)

Matt G. • May 30, 2017 7:27 AM

If their mission is simply to render the leaked code useless to the NSA by convincing people to patch their software, then it would seem to be working to some extent.

Puppet Master • May 30, 2017 7:33 AM

Assuming that NSA knows which server the files have come from, they would also be aware what will be in the next dumps. One would assume that if NSA knows that one or more exploits will be public in the coming months, then they would want to warn the manufacturer in advance.

However there has been no stream of suspicious additional updates to Windows, Linux, etc. in the last few months. So perhaps this is it. Maybe the hackers are bluffing?

Wilhelm • May 30, 2017 7:34 AM

From the Shadow Brokers latest message *"TheShadowBrokers was very very sad! Story is now sounding like silly children's' book. TheShadowBrokers is writing to audience reading level, thepeoples is having average reading level of 8th grade."*

Sounds very American and intentionally broken.

Wilhelm • May 30, 2017 7:37 AM

This too, sounds very American - *"TheShadowBrokers is launching new monthly subscription model. Is being like wine of month club. Each month peoples can be paying membership fee, then getting members only data dump each month. What members doing with data after is up to members."*

Their English is broken, but their references are accurate. Very strange.

---

mostly harmful • May 30, 2017 8:13 AM

> In the coming months, we might see new exploits against web browsers, networking equipment, smartphones, and operating systems -- Windows in particular. Even *scarier*, […]

Wait. Why should anyone be "afraid" of something so utterly predictable?

Exploits are publicised, and then patches are made and released. That's how it works, is it not? Known-to-be clusterfscked machines are thereby incrementally improved, though very possibly inadequately so (depending on your purposes).

What is remotely *scary* about that process?

If one seeks something unsettling to contemplate, merely consider that all these Rube Goldberg machines are routinely represented as fit for serious purpose.

But frankly I'm far more concerned about the black hole that seems to have swallowed the unnamed TAO employee refered to in Ellen Nakashima's November 19, 2016 Washington Post article:

> But there was a second, previously undisclosed breach of cybertools, discovered in the summer of 2015, which was also carried out by a TAO employee, one official said. *That individual also has been arrested, but his case has not been made public.* The individual is not thought to have shared the material with another country, the official said.

Is this Washington Post article the only public information available regarding this individual and their present welfare?

Clive Robinson • May 30, 2017 8:42 AM

@ Bruce,

> the Shadow Brokers **stole** a few disks full of NSA secrets

That is very much an assumption currently. Which when you consider the number of leaks that have been happening may actually be a disgruntaled insider "arranging" for who ever now has the dump to have it or be given it.

It is after all not unknown for inter-agency turf wars to spill out into a more public arena.

I guess time will tell but untile then I'm going to stick with "aquired" rather than "Stolen".

Terry • May 30, 2017 8:52 AM

You keep searching a motive.
Sometimes they just want to watch things burn.

Much Success for Make Benefit Glorious America • May 30, 2017 9:02 AM

This is a silly article, but then it's for the Atlantic, so it has to be. There's nothing perplexing about this leak. It's standard counter-sabotage applied to shared infrastructure.

https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol7no2/html/v07i2a06p_0001.htm

It effectively promotes all counter-sabotage objectives (except where corporations collude with NSA tampering, and that works out too, because in that case treacherous US suppliers cede markets to trusted foreign producers.)

It doesn't have to be RUSSIA RUSSIA RUSSIA. It could be civil society, which takes many transnational forms. But the Atlantic propaganda line is that there is no civil society, only enemy nations. Everyone on earth outside the beltway has a stake in stopping NSA and CIA sabotage. Everybody's rights are under threat from the US Stasi.

---

ab praeceptis • May 30, 2017 9:21 AM

If I may ...

- the entity acting in a publicly visible way (and calling itself Shadow Brokers) may - or may not - be the same entity that got the material.

- the entity - or entities - having taken the data from nsa may - or may not - be the entity that had and passed on, with whatever intention, access to the data.

- the year 2013 might have different reasons. One of which is what Bruce Schneier assumes. Another one might be that they put their material in two baskets, namely a "current high value" one and a "older, lower value" one mainly for marketing purposes. Yet other reasons are conceivable.

- the motives for providing access to and/or taking the data can be entirely different from the motives for publishing/playing the Shadow Brokers games. Any deduction from the latter to the former is highly doubtful.

- *Obviously*, us america isn't a halfway consistent entity anymore; this can be easily seen when looking at how (forgive my lose classification) obamistas, clintonistas and trumpistas fight each other. But it can also be seen from the eu reaction to trump; the eu seems much more linked to obama (albeit an ex-president) than to trump whom they seem to consider more of an enemy than a friend.

It would be surprising if that fractioning and infighting within washington wouldn't be found with intelligence circles, too.

- It seems rather superficial to me to see China as "making friendly" and Russia as evil. *Both* are foremost friendly to each other and *both* want to continue ending the us-american hegemony.

As for China I'd like to remind you that they had (and probably still have) quite some internal conflicts, to. It might hence be quite realistic to assume that the old anti Xi faction stabbed the us american spooks so as to create problems for Xi. Similarly, powerful groups might have stabbed the us spooks *because* they don't like Xi's "making friendly" to washington.

- from what we know and see, Putin is almost obsessed with legality. While it might be quite realistic to assume that russian intelligence services hacked the nsa they would very clearly not be allowed to play the Shadow Broker game.

We can't know. Simple as that. As for guessing my personal take is us-american infighting plus a generous dose of spreading suspicion against Russia and China.

Who? • May 30, 2017 9:33 AM

> *That's not what we're seeing here; it's simply a bunch of exploit code, which doesn't have the political or ethical implications that a whistleblower would want to highlight.*

Bruce, are you sure?

Most whistleblowers want to embarrash the agencies that hired them. This is the reason they publish documentation that shows the bad —usually illegal— practices of their IC. I agree with you here. However leaking code is something a whistleblower may do too. Look at it this way, Edward Snowden and Chelsea Manning leaked information about the way the U.S. Government acts that may or may not help changing these activities for the good in the future. Shadow Brokers leaked code that will improve the world helping closing bugs that are being actively exploited by the IC in the software we run each day. Both are different approaches to the same problem.

Who? • May 30, 2017 9:41 AM

I want to be more clear: Snowden and Manning took a political approach, Shadow Brokers are more on the technical side. In both cases leaks can be used for the good or for the evil. Snowden leaks provided a long-term overview of how IC acts, and helps developing strategies against global surveillance. Shadow Brokers provide short-term leaks that will help us fixing bugs that are being exploited right now (of course, iff OEMs care enough about their clients security, Cisco will not patch old devices that will remain exploitable forever).

Soufiane Tahiri • May 30, 2017 9:47 AM

It doesn't have to be Russia, China , Iran, NK and especially in this fully connected word ; At least I hope its a civil operation which is being conducted.

The scariest story is not knowing what ShadowBrokers will be leaking, to some point the leak is "democratizing" what NSA is capable of, anyway the exploits and the cyber warfare is being widely used against us every single minute why the hell caring about who are SB, the real question is what does NSA really have? What are they really capable of? and Why the hell not caring about stooping.

If the leaks come between "cyber criminals" hands, at least this make things a little bit balanced, not only NSA can use the leaked exploit and this is quit satisfying from a certain point of view.

Fausto Carrera • May 30, 2017 9:59 AM

If the main purpose of the ShadowBrokers is profit from the NSA tools, they would have used any of the numerous dark web markets to handle it. Why they tried to have an auction and now a monthly subscription?

Morgado • May 30, 2017 10:00 AM

2 farfetched hypotheses:

- "A nation state": Russia, or a "lone hacker", putting these 2 options together... Could it be Mr. Snowden?

- What are the chances that the NSA itself, has a new and so powerfull capability that they decided to leak, both because these leaks are now obsolete to them and to watch who are the other foreign actors who lay behind them at this point, giving themselves up by trying to catch this recent leaks?

As I said, these are farfetched theories, but who knows right?

Who? • May 30, 2017 10:14 AM

> *As with the Snowden documents, though, they only know what the attackers could have taken and not what they did take. But they did alert Microsoft about the Windows vulnerability the Shadow Brokers released months in advance. Did they have eavesdropping capability inside whoever stole the files, as they claimed to when the Russians attacked the State Department? We have no idea.*

If I remember right, Shadow Broker published a list of stolen files a few months before releasing them to the public. I think it was last december, perhaps january. NSA does not need eavesdropping capability to alert Microsoft this time.

Who? • May 30, 2017 10:43 AM

@ Morgado

> *- "A nation state": Russia, or a "lone hacker", putting these 2 options together... Could it be Mr. Snowden?*

No. Snowden left the NSA on the first months of 2013, some leaks are from the last months of that year.

Scott • May 30, 2017 10:54 AM

The Shadow Brokers' messages have a syntax consistent with a language represented by Cyrillic characters. Their origin isn't exactly a mystery.

Steve • May 30, 2017 11:03 AM

Like **mostly harmful**, I find perhaps the most disturbing part of this story is the blurblet Dr Schneier quotes from the WaPo: *That individual also has been arrested, but his case has not been made public.* So much for various bits of the 4th through the 8th Amendments, it would seem.

Evan • May 30, 2017 11:08 AM

@Steven C. Buttgereit
I think it's at least somewhat plausible. Consider this scenario: by plan or by happenstance (investigating cyber attack, doing malware scans, etc) they discover NSA assets that they are able to compromise. Being less than scrupulous, they take everything they can with the intent of finding a way to monetize it later. Unfortunately, not being "true" black hats, they have no big-league criminal or espionage ties, and they're too scared to use the tools to enrich themselves in case it gets tracked back to them. The leaks are to establish a reputation and hook some buyers, and the proposed "subscription model" strikes me as a desperate move to try and get some cash out of the whole thing.

The pros of the theory are that it would explain the amount of time elapsed and why they don't seem to be trying to leverage their exploits for anything. The cons are that it can't be that hard to sell exploits on darknet, can it?

---

herman • May 30, 2017 11:11 AM

"That individual also has been arrested, but his case has not been made public."

Who is this poor sod and since when has he been chucked into which dungen?

---

albert • May 30, 2017 11:25 AM

So, to sum up:

Who are the Shadow Brokers?

. .. . .. --- ....

Rachel • May 30, 2017 11:52 AM

Ab Praeceptis

"if I may...."

Bruce could have written a more concise article.

'We don't know who they are, what they look like, or what they want. But we know they are out there..'

Scissors • May 30, 2017 12:04 PM

@Evan
I find it hard to believe that the Shadow Brokers' main objective is financial gain. With the likes of Zerodium, it's trivial to find legal (or legal enough) avenues of selling 0days anonymously and quietly.

Unless the thieves were quite inept they could create seeming original proof-of-concepts based on the stolen tools that wouldn't raise suspicion for the first several 'transactions'. Even if Zerodium had provided the 0days to the NSA, they'd have to pay them to keep them from talking.

Thomas • **May 30, 2017 12:37 PM**

One thing that had - in my opinion - not discussed extensivly is, that the Shadowbroker really just are ciminals that try to squeeze as much money out of their data as possible. In my opinion that fits to the many "oh we are sad that nobody send us BTC" message from the last month. The subscription-model they now introduced might be a way to sell stuff that they know is getting worthless by every day. What do you think?

Subscribe to comments on this entry

Leave a comment

Login

Name (required):

E-mail Address:

URL:

□ **Remember personal info?**

Fill in the blank: the name of this blog is Schneier on ___________ (required):

Comments:

Allowed HTML: <a href="URL"> • <em> <cite> <i> • <strong> <b> • <sub> <sup> • <ul> <ol> <li> • <blockquote> <pre>

Preview Submit

← Tainted Leaks

Schneier on Security is a personal website. Opinions expressed are not necessarily those of IBM Resilient.