Major NSA/Equation Group Leak

The NSA was badly hacked in 2013, and we're just now learning about it.

A group of hackers called "The Shadow Brokers" claim to have hacked the NSA, and are posting data to prove it. The data is source code from "The Equation Group," which is a sophisticated piece of malware exposed last year and attributed to the NSA. Some details:

> The Shadow Brokers claimed to have hacked the Equation Group and stolen some of its hacking tools. They publicized the dump on Saturday, tweeting a link to the manifesto to a series of media companies.
>
> The dumped files mostly contain installation scripts, configurations for command and control servers, and exploits targeted to specific routers and firewalls. The names of some of the tools correspond with names used in Snowden documents, such as "BANANAGLEE" or "EPICBANANA."

Nicholas Weaver has analyzed the data and believes it real:

> But the proof itself, appear 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 this data is authentic. And it does not appear to be information taken from comprised systems. 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.

I agree with him. This just isn't something that can be faked in this way. (Good proof would be for *The Intercept* to run the code names in the new leak against their database, and confirm that some of the previously unpublished ones are legitimate.)

This is definitely not Snowden stuff. This isn't the sort of data he took, and the release mechanism is not one that any of the reporters with access to the material would use. This is someone else, probably an outsider...probably a government.

Weaver again:

> 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. 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 possibly sources, it may have accidentally or deliberately eliminated this adversary's access.

Okay, so let's think about the game theory here. Some group stole all of this data in 2013 and kept it secret for three years. Now they want the world to know it was stolen. Which governments might behave this way? The obvious list is short: China and Russia. Were I betting, I would bet Russia, and that it's a signal to the Obama Administration: "Before you even think of sanctioning us for the DNC hack, know where we've been and what we can do to you."

They claim to be auctioning off the rest of the data to the highest bidder. I think that's PR nonsense. More likely, that second file is random nonsense, and this is all we're going to get. It's a lot, though. Yesterday was a *very* bad day for the NSA.

EDITED TO ADD: Snowden's comments. He thinks it's an "NSA malware staging server" that was hacked.

Tags: exploits, game theory, hacking, leaks, NSA
Posted on August 16, 2016 at 10:43 AM • 62 Comments

Comments

Alan • August 16, 2016 10:52 AM

Why do I feel that the Shadow Brokers might shortly suffer a rash of inexplicable fatal accidents? Messing with the NSA or CIA seems less advised than messing with the mob.

Lou Herford • August 16, 2016 11:16 AM

Interesting analysis from Snowden:

"This leak looks like somebody sending a message that an escalation in the attribution game could get messy fast."

Dave • August 16, 2016 11:30 AM

I had a chance to look at the files on Cryptome. What Cryptome is showing right now only seems to be a subset of the 301 MB file.

Those files seem to be text files showing how to use the various tools. There are some python programs but very basic stuff a good analogy would be a Torpedo without the warhead.

They do not actually have any "tools" or "implants" they are just guides.

It's my understanding that the NSA has an automated process for deploying Malware on the internet. If you do something that sets off a red flag then the ip address and mac address gets added to a targeting computer. This happens when you go to a specific website, call a phone, or text an individual already in the targeting computer.

If this is real, my thinking would be these are tools used to train individual red team members. It doesn't mean the NSA was hacked it could be a lapse in security where (training materials) were stolen.

I would bet a lot of money the NSA itself was not hacked.

Mandoch • **August 16, 2016 11:37 AM**

When these things happen, I find it fascinating to watch which companies scramble to comply with the NSA by rapidly shutting down the accounts used by the "perpetrators" to publish information and which companies leave the accounts open until a court order tells them otherwise. It says a lot about who's who and what they really stand for when the chips are down.

Closed accounts so far:
-Tumblr (https://theshadowbrokers.tumblr.com/)
-Github (https://github.com/theshadowbrokers/EQGRP-AUCTION)
-Dropbox (https://www.dropbox.com/s/g8kvfl4xtj2vr24/EQGRP-Auction-Files.zip)

Sam • **August 16, 2016 11:39 AM**

@Dave

> a good analogy would be a Torpedo without the warhead

Well ... good? At least a partly responsible disclosure then: it's much better than having a pile of Equation-Group-quality exploits floating around in the wild for anyone to use.

Clive Robinson • **August 16, 2016 11:51 AM**

@ Alan,

> Why do I feel that the Shadow Brokers might shortly suffer a rash of inexplicable fatal accidents?

You are presupposing that the Shadow Brokers are,

1, Civilians
2, Identifiable
3, Available
4, Unprotected

It may well be that they are military / IC of a country that has decided it's time to double down on the current US Gov Encumbrents hypocrisy and misatribution.

There has not realy been any real evidence presented on the Sony Pictures, Bangladeshi bank heist or DMC hacks, just rabid finger pointing.

Then there is the preceding China APT etc, from a non US perspective one has to wonder just how much room under the bed the US has for REDS. It all looks like a reheat of the old fifties and sixties "Red Scare" "un-american" nonsense.

If it is the IC / Mil of another nation turning the screw on the US --which the 1million BTC might suggest-- then we are going to need a realy comfortable sofa and a large supply of Cool-Aid and Coors along with a big supply of pizza and popcorn ;-)

Dennis • **August 16, 2016 11:53 AM**

@Dave:

"If this is real, my thinking would be these are tools used to train individual red team members. It doesn't mean the NSA was hacked it could be a lapse in security where (training materials) were stolen."

This is what Snowden says about the hack (in a nutshell: it's probably a hacked proxy hop server and it's happened before):

NSA is often lurking undetected for years on the C2 and ORBs (proxy hops) of state hackers. This is how we follow their operations. This is how we steal their rivals' hacking tools and reverse-engineer them to create "fingerprints" to help us detect them in the future. Knowing this, NSA's hackers (TAO) are told not to leave their hack tools ("binaries") on the server after an op. But people get lazy. What's new? NSA malware staging servers getting hacked by a rival is not new. A rival publicly demonstrating they have done so is.

Alex Mora • **August 16, 2016 11:54 AM**

Something about this reminded me of Sneakers(1992)

Then:
Dick Gordon: National Security Agency.
Martin Bishop: Ah. You're the guys I hear breathing on the other end of my phone.
Dick Gordon: Only No, that's the FBI. We're not chartered for domestic surveillance.
Martin Bishop: Oh, I see. You just overthrow governments. Set up friendly dictators.
Dick Gordon: No, that's the CIA. We protect our government's communications, we try to break the other fella's codes. We're the good guys, Marty.
Martin Bishop: Gee, I can't tell you what a relief that is... Dick.

Now:
Dick Gordon: National Security Agency.

Martin Bishop: Ah. You're the guys I hear breathing on the other end of my phone.

Dick Gordon: Officially, only if your making international calls, otherwise, that's the FBI. Or maybe it's the Brits or New Zealand, we spy on people in each others countries to all the time and "share" the information to get around the fact we were not officially charted for Domestic Surveillance.

Martin Bishop: Oh, I see. You also overthrow governments? Set up friendly dictators?

Dick Gordon: No, that's the CIA. Though they are a little off their game these days. They've been trying to overthrow Syria for years. Might have to due with everyone with some common sense leaving to protest the mass application of torture.

We at the NSA spend most of our time sifting through a mountain of noisy and mostly useless information, which at least makes us look busy, which is important because after that Snowden fiasco we are a household name. We used to talk about protecting our government's communications, but the people in our government can't follow basic security advice.

Don't worry Marty, all you need to know is were from the government and were here to help.

Martin Bishop: Gee, I can't tell you what a relief that is... Dick.

---

boseman • **August 16, 2016 11:57 AM**

it's much better than having a pile of Equation-Group-quality exploits floating around in the wild for anyone to use.

It's better to have the knowledge shared. A legitimate response by the networking hardware developers would be to study them, develop some kind of workaround, then close the exploits.

We all know by now, sometimes that is much easier said than done. But, more shared knowledge is better despite the temporary risks.

/b/paradise • **August 16, 2016 12:10 PM**

Lots of fascinating tidbits in the dump itself. In no particular order: (1) network profiling permits arbitrary unsupervised surveillance with no audit trail - in case you ever believed that crap about complying with applicable laws and regs. (2) It seems that even simple things like using non-default ports for your services can make you a harder target. (imagine what a little idiosyncratic compiling can do) (3) the tunneler, made executable with one click, is really going to advance the information freedom of the world, if ya get my drift. (4) Oh to be a fly on the wall when they think through the hugest implication of the dump, and PANIC.

---

r • **August 16, 2016 12:14 PM**

I haven't looked at the stuff, I was paranoid about the trolls when I first saw it (translate.google.com), I think it's funny how the trolls now used github - and were censored - I guess that answers my question: why not?

That aside,

Are these datatypes the type capable of being obtained through a honeypot?

It could've been a staging area, a forward asset that was compromised?

(so far, it IS a relatively small trove)

---

r • **August 16, 2016 12:19 PM**

/b/paradise said:

> "**non-default ports** for your services can make you a **harder target**. (imagine what a little **idiosyncratic compiling** can do"

+3

However, *uniqueness* can be an identifiable factor.

These are all points made (roughly) in the analysis.

Harvey • **August 16, 2016 12:26 PM**

@/b/paradise:

Yup, a few other nuggets I've stumbled across so far: the code they use to disable password checking when compromising telnet (really, in 2013?) or ssh in EXTRABACON; the technique they use to exfiltrate text data as binaries in Netprofiler; the script they use to automatically set up a default Apache server to stage an attack...

ALexT • **August 16, 2016 12:27 PM**

Few random thoughts...

It would see obvious that the 1mn bitcoin price tag is some sort of joke - there is simply no way anyone would be able to do cash about 10% (give or take, there is probably no consensus as of the total amount in actual circulation)

I am the only one who never heard of http://sxnc.com.cn/ ? Are the only serving the Chinese market ?

---

r • **August 16, 2016 12:32 PM**

@All,

OIC,

It was a staging area. ;)

https://twitter.com/Snowden/status/765513662597623808

---

tian tian • **August 16, 2016 12:42 PM**

To those who are suggesting that this is an innocuous responsible disclosure, I think you guys need to download the full version. Follow the links from their twitter account to the pastebin message to the

mega.nz upload. As well as the config files, there are binaries and fully working exploits in there.

Vesselin Bontchev • **August 16, 2016 12:44 PM**

Some observations:

1) The auction is an obvious scam. A Tullock lottery, really? And no determined time limit, either. Gimme a break. Nobody does this in real life.

2) The "stuff" (at least the freebe) looks real. Some are still unpatched 0days, even after so many years. The names match the ANT catalog, the file dates *predate* the leak of the ANT catalog. I definitely believe that this is NSA stuff.

3) The quality of the programs is shit. Did they use interns to write the programs using the exploits or what?! Using Python and the "[+]" notation, plus snarky remarks in some messages, too. How very 177t.

4) The text doesn't read like Russian English. More like Chinese English. Although it could be simple misdirection, of course.

5) This doesn't seem like an insider leak a la Snowden. It seems mostly like stuff discovered on an NSA-hacked appliance. Remember, the opponents of the NSA aren't exactly stupid, either. Stuff gets discovered all the time.

Oh, and in totally unrelated news, the NSA website is down. Only the front page works (and even that times out occasionally); all the links point to non-existent pages.

/b/paradise • **August 16, 2016 12:47 PM**

@r (12:14) see last night from the squid thread, somebody already ran the dump through the malware yara rules [see for yourself if you don't trust them, https://github.com/Yara-Rules/rules] There is no sign of tampering. And the sources, Cryptome and mega, are no honeypots.

---

r • **August 16, 2016 12:50 PM**

@Mr. Bontchev,

Non-cached access here (my mother-in-law's PC has never been there), even the main page displays:

> Invalid URL The requested URL "[no URL]", is invalid.
> Reference #9.f111cb8.1471369730.9a8d2

---

r • **August 16, 2016 12:52 PM**

@/b/

I believe you/that, I was careful about the 'news article'.

By the time (yesterday just before noon?) I clicked the github it was down.

---

r • August 16, 2016 12:53 PM

@/b/

EST ofc.

/b/paradise • August 16, 2016 12:56 PM

@r, no it's here

https://t.co/F9iwKLcmQ9 (passwd: theequationgroup)

https://cryptome.org/2016/08/nsa-malware-scripts.zip

Dave • August 16, 2016 1:10 PM

@ Dennis

NSA is often lurking undetected for years on the C2 and ORBs (proxy hops) of state hackers

This would explain how to get the implant (code), but not sure that gets you the tools themselves or the directions how to use the tools. I mean what Snowden is describing is a MITM attack on existing passive collection. Now a hack of a staging server ok I could see that and that makes sense. If TAO and its red teams are trained to erase all implants when they are done (why have the directions on anything you hack to begin with) I mean one would think they reside on the computer of the RT member only.

In my mind maybe this could be tools used for supply side interdiction.

Just a theory

(1) Bad actor buys a computer, server, firewall, or router.

(2) Device shows up at location NSA uses to install implants

(3) Device goes back on DHL or UPS truck mid shipment

(4) Actor gets computer NIB (with implant)

It's possible this is a toolkit used in supply side interdiction that just got out into the wild?

What is very clear is we are now in a public game of attribution diplomacy for the LUZ!

Bob • August 16, 2016 1:14 PM

@All:

The cryptome zip file is a tiny subset. The full dump can be downloaded from mega.nz:

https://mega.nz/#!zEAU1AQL!oWJ63n-D6lCuCQ4AY0Cv_405hX8kn7MEsa1iLH5UjKU. Make sure you sha256sum your download (http://pastebin.com/NDTU5kJQ).

---

rusty syrup • August 16, 2016 1:25 PM

How could a bad day get worse:

"It's not just you! http://nsa.gov looks down from here." (isup.me)

Raindance • August 16, 2016 1:40 PM

I've been browsing through the exploits, finding it all quite amusing until it suddenly hit me: "the exploits of today are the PhD theses of tomorrow and the next day blah blah bah." There is something very wrong about the fact that the 0-days behind these exploits have probably been developed somewhere abroad by a bunch of different mercenary security firms, bought with USD tax money and/or plagiarized from the tools used by countries that want to hack us, stolen again from us by those very countries that want to hack us, doxed, and ultimately used by script kiddies from around the world to design the ransomware that will grace an office work station near us in the next few days. It seems just wrong that we're all paying for the privilege with our tax dollars.

Bystander • August 16, 2016 1:44 PM

This is pretty interesting.

As it hasn't been linked yet, here is a comment of someone who played a little with the material provided.

---

yoshii • August 16, 2016 1:58 PM

To everyone here at this site and forum...

Please substantiate (back up with supporting information) all claims whenever possible, to avoid illogical sensationalism and the disruptive intellectual fallout that accompanies mismanaged propagation of information.

Opinions and hunches aren't facts. And hyping people up with claims that might not hold up to scrutiny when the evidence finally comes is not a good idea.

Times are tense enough without accidental or intentional instigators.
This is just a fair request.

Dali La • August 16, 2016 2:09 PM

From Nicholas Weaver's article

"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?"

It looks like the NSA is suffering a bit of an image problem, shifting from Neo to Mr Bean within a couple of years.

PerryD • **August 16, 2016 2:15 PM**

I admittedly don't know a lot of the details, but it seems that this might have been taken from an employee laptop that had been stolen or lost (or maybe bought at government auction).

AJWM • **August 16, 2016 2:26 PM**

Relying on the file timestamps -- which are easy to modify -- the most likely date of acquisition was June 11, 2013.

There are newer files than that. For example, Firewall/OPS/userscript.FW has a file timestamp of October 18, 2013. And, not to rely on file timestamps, that file itself has an internal change history suggesting changes made on or after June 11:

```
# 6/11/13 -- Modified layout of disk so TPATHS have been updated...

# 7/25/13 -- Removed blockme rules and added in support for BG3121 as we mo

# 8/18/13 -- Updated paths to match the new directory structures
```

Not that this proves anything either, the provenance and chain of custody of this stuff is questionable.

Rabbid Honeypotting • **August 16, 2016 2:28 PM**

@Dennis

> NSA's hackers (TAO) are told not to leave their hack tools ("binaries") on the server after an op. But people get lazy. What's new? NSA malware staging servers getting hacked by a rival is not new.

and @Vesselin

> 5) This doesn't seem like an insider leak a la Snowden. It seems mostly like stuff discovered on an NSA-hacked appliance. Remember, the opponents of the NSA aren't exactly stupid, either. Stuff gets discovered all the time.

I have more respect for the NSA's skills and workflow protocols to agree with this. Likewise I don't think Schneier should have presumed it was a group. That sounds like the thing I could have seen if Snowden hadn't taken immediate credit. I.e. rabid egos presume that only a 'group' could do something so monumental.

Amplifier • **August 16, 2016 2:36 PM**

@Raindance

> I've been browsing through the exploits, finding it all quite amusing until it suddenly hit me: "the exploits of today are the PhD theses of tomorrow and the next day blah blah bah." There is something very wrong about the fact that the 0-days behind these exploits have probably been developed somewhere abroad by a bunch of different mercenary security firms, bought with USD tax money and/or plagiarized from the tools used by countries that want to hack us, stolen again from us by those very countries that want to hack us, doxed, and ultimately used by script kiddies from around the world to design the ransomware that will grace an office work station near us in the next few days. It seems just wrong that we're all paying for the privilege with our tax dollars.

Ain't america grand?

Speculator • **August 16, 2016 2:41 PM**

@yoshiee "Opinions and hunches aren't facts. And hyping people up"

Anyone capable of being hyped up by comments in an (mostly) unmoderated thread with anonymous posts is someone who has a serious risk of dying on their way to work in the morning, even if they aren't trusted by their government to operate something as dangerous as a motor vehicle.

Max • **August 16, 2016 2:51 PM**

"The equation group" is the name used by Kapersky. Not saying that Kapersky is the leaker, but it's possible that this didn't come directly from the Russian government. Maybe it's a leak of a leak of a leak. Stuff gets around.

---

avnr • **August 16, 2016 2:56 PM**

Something to do with Snowden's recent private key tweet?

WhiskersInMenlo • **August 16, 2016 3:22 PM**

Given the dates these are "Pre-WindowZ-10", now I am curious if any apply to Win-10.

The future of patches for anything other than Win-10 now has a a limited life. So these may be almost worthless to the big boys.

If the tools were for a NIB system in transit install then the list of new in box operating systems needs to line up with tools. Time alone says they do not.

Same time issue is true for Apple and even Linux where a year or two would present an interesting set of changes and new set of exploit challenges.

For those that have looked at the bits are there strong
clues that anti virus tool vendors could jump on quickly?

Exploit of php and web services -- will we see a spate of bug fixes?

My personal expectation is one or more individual noticed that
knowledge of exploits is double edge and the rusty sharp edges
run all the way down the handle.

Groups like the DNC are embarrassed and have enough power
to illuminate the flawed thinking of some TLAs and adjust their budgets.

Groups like the DHS may have grokked the reality that homeland
security depends on defect free software (OK much improved).

Awareness of the Vulnerabilities Equities Process in the news
might have triggered less embarrassing back door disclosures.

Congress women have been embarrassed i.e.:
Nancy Pelosi: DCCC hacking brought on 'obscene and sick calls'
Her rolodex is full of good non random numbers:
She served on the Appropriations and Intelligence Committees, and was the
ranking Democrat on the Intelligence Committee until her election as Minority Leader

Now should I allow myself to succumb to curiosity and download
this pile of risks.

Andre Gironda • **August 16, 2016 3:28 PM**

It's more-likely that the data was stolen before 2013 and that the dates were modified to look like they were stolen around the time Snowden started talking to reporters.

Nicholas Weaver • **August 16, 2016 3:38 PM**

A couple of interesting notes:

I'll bet the other file is real and a threat: Do what we want or we dump the rest of this data.

There is a huge amount missing even if this was captured from a staging server: the obfuscators. The implants themselves are unobfuscated and unstripped. IN installing them the attacker would need to modify them to remove such tells and obfuscate the code itself. No such tool appears present.

Moreso, many of the exploits only work from within an institution. EXTRABACON, for example, requires ssh and SNMP-read access to the firewall, so you first need to exploit the sysadmin's computer and from there attack the firewall. So where is the code for that?

A good example of the quality is the EXTRABACON exploit, which is a reliable exploit for Cisco devices:
https://xorcatt.wordpress.com/2016/08/16/equationgroup-tool-leak-extrabacon-demo/

At the time it was a zero day, and it may STILL be a zero day?!?

Susan • August 16, 2016 3:39 PM

To me this smells like a Snowden leak. It's just a bit of too much coincidence that this leaked with his disappearance and those cryptic keys. Also it makes a lot of sense. He sure had all those files. The dates match. Russia might have forced him to release this material, who knows.

Nicholas Weaver • August 16, 2016 3:41 PM

Also, the date is at least 2013: there are bits there, like version strings etc, that only existed in 2013 or late 2012 at most. If someone has a historical listing of MAC address allocations the Firewall/BARGLEE/BARGLEE3100/Install/LP/maclist file could also confirm this, its a list of every ethernet mac address and the company which owns it.

Bystander • August 16, 2016 3:45 PM

@Nicholas Weaver

Re EXTRABACON exploit:

Look here please. :)

---

double cheese • August 16, 2016 4:13 PM

An interesting aspect of the code (which has already been highlighted by previous leaks) is that most of the exploits have been designed as extremely simple to use point-and-click solutions. They include step by step instructions (and even echo useful cut-and-paste options!) for users to append to their commands in the terminal. Although there obviously must be plenty of talent in the NSA, clearly not all operators are regarded as the brightest of sparks or entrusted with any degree of autonomy.

"To me this smells like a Snowden leak."
This couldn't be further removed from a Snowden leak. Snowden acted on ideological grounds, putting his life at risk and making his identity known to reveal the gross abuse of a governmental institution that had gotten out of control, acting against the interests of its own people. This leak is anonymous, includes a trove of exploits with no significant socio-political context, is apparently attempting to profit from the sale of exfiltrated data, does not involve the press partners that have worked with Snowden in the past, and would only seem to benefit a country that currently bears a grudge towards the USA about cyber-attack attribution.

Grauhut • August 16, 2016 4:51 PM

@Clive: Lots of popcorn, because of "it's time"? ;)

Did you work with me? Have we talked since 2013? Please recontact me securely, or talk to @bartongellman. It's time. https://t.co/AKmgF5AIDJ

— Edward Snowden (@Snowden) August 3, 2016

Ross Snider • August 16, 2016 5:19 PM

@Schneier

More interesting to me is Snowden's speculation that the release is part of the escalation over the DNC hacks - a warning that further escalation on the US's side will result in the disclosure of information implicating US intelligence in manipulating elections.

Of course such a disclosure would be nothing new, but as big breaking stories tend to unfold widespread public understanding of this could be a major 'soft power' blow to US legitimacy.

Grauhut • August 16, 2016 5:19 PM

@double cheese: "Snowden acted on ideological grounds, putting his life at risk and making his identity known to reveal the gross abuse of a governmental institution that had gotten out of control, acting against the interests of its own people. This leak is anonymous, includes a trove of exploits with no significant socio-political context, is apparently attempting to profit from the sale of exfiltrated data"

What if Snowden just wanted to say #nevertrump+#neverhillary ?

Maybe he felt the Bern and hated to see him get f*cked... ;)

"Look, this how it feels to be sold. It's time to pull the plug. They don't get these tools. Time to burn them, no pasaran!"

Marcos Malo • August 16, 2016 6:12 PM

I agree with others regarding the selling of the info: it's a joke. They could have made that clearer by putting it on Kickstarter. I highly doubt they expect anyone to make a serious bid.

Jonathan Wilson • August 16, 2016 6:35 PM

I do hope that any currently-unpatched exploits that are used by these pieces of malware get picked up on and fixed (assuming the programs they affect are still receiving security updates that is)

65535 • August 16, 2016 7:13 PM

If this indeed a true hack of the NSA then the agency has grown fat, dumb and happy.

The NSA has not be fighting true Nation State Adversary's such as the Russian and Chinese hardened indigenous cyber weapons facilities. The NSA has been working with the Facebook and other social media to identify soft targets including kiddy porn, vice drug busts, economic theft of trade secrets an so on [Not to mention spying of NATO allies].

I believe that it's now time for the NSA to have true congressional oversight. Barring true congressional oversight, a 35% cut in the NSA's budget would be the only thing to gets its attention –

and move resources from watching naked teen selfies to real “National Security” threats.

---

r • August 16, 2016 7:36 PM

@Susan, CC: 65535

> "To me this smells like a Snowden leak. It's just a bit of too much coincidence that this leaked with his disappearance and those cryptic keys. Also it makes a lot of sense. He sure had all those files. The dates match. Russia might have forced him to release this material, who knows."

What you're saying would make the assertion they're making about hacking the 'NSA' not a lie. I suppose they could've discovered a deadman's switch (as was surmised about tweets prior) and figured out how to force the issue.

Snowden tweeting about on-goings now would give him deniability if someone else wrestled the mechanism from a resting state, that might explain why it was deleted - the whole "speculation of my demise" being untrue.

We all know he didn't catalog everything he had taken possession of.

---

r • August 16, 2016 7:37 PM

@65535,

I bet you cut their budget and they run for unaccountable automation even harder.

65535 • August 16, 2016 7:39 PM

@ Bystander

https://xorcatt.wordpress.com/2016/08/16/equationgroup-tool-leak-extrabacon-demo/

Wow, cool ASA hack!

Winston Smith • August 16, 2016 7:40 PM

@ross snider

"More interesting to me is Snowden's speculation that the release is part of the escalation over the DNC hacks - a warning that further escalation on the US's side will result in the disclosure of information implicating US intelligence in manipulating elections."

The consequences and potential fallout of proof of IC manipulation of U.S. elections is simply salivating. May the truth prevail.

@double cheese

"To me this smells like a Snowden leak."
This couldn't be further removed from a Snowden leak. Snowden acted on ideological grounds, putting his life at risk and making his identity known to reveal the gross abuse of a governmental institution that had gotten out of control, acting against the interests of its own people. This leak is anonymous, includes a trove of exploits with no significant socio-political context, is apparently attempting to profit from the sale of exfiltrated data, does not involve the press partners that have worked with Snowden in the past, and would only seem to benefit a country that currently bears a grudge towards the USA about cyber-attack attribution.

Well said! Very well said, indeed.

Skeptical • August 16, 2016 7:55 PM

I haven't looked at the material of the dump itself, not that my views on it would be worth very much.

Nor do I have anything beyond a description of more plausible scenarios to add to the inevitable connection-to-Snowden question given aspects of timeframe.

Lots of plausible scenarios include no involvement by Snowden. Of course, a few plausible scenarios do - I mentioned a "two-track" approach being logical for Snowden, one involving the release of earlier materials that contained relatively little operational material ("relatively") and then a covert track that involved the actual release of acutely harmful information. There are others. But at present, there's really not much say on the matter. Maybe, maybe not. I wouldn't be inclined to bet unless given very good odds.

Regarding Snowdeen's idea as a shot across the bow of the US in any significant way: Very unlikely.

There's no signal here. This is the equivalent of a Russian jet doing a flyby of a Navy missile destroyer. The destroyer tolerates it, avoids an incident, and emerges without any significant differences in the estimate of enemy capabilities.

If anything, it would be a domestic signal: don't be afraid of the NSA, the Russian Bear is more than a match.

I view this as an attempt to burnish Putin's imagine as a strong leader, even as he lays the groundwork should the US utilize its cybercapabilities to respond in kind or, within the same domain, using different tactics to achieve the desired punishment.

It may be that Putin's ego demanded a better show of strength after the clamor that arose in the United States.

Of course, it could also be a gift from the PRC to North Korea - and the PRC did via Snowden, have access to various points of potential access to NSA servers, sensors, or implants within its territory. The North Koreans hate to lose face; perhaps this is their revenge for whatever might happened to some of their projects post-Sony.

But to the United States Government? Unless this reveals a penetration of a nature that casts doubt on the rest of its network infrastructure and capabilities - which would be a rather brash thing to show - I don't see how it changes much. This doesn't alter the balance of power between any two states.

As to a Russian threat to show the US attempted to influence an election, this would be clumsy way to deliver that threat. It would be more psersuasive delivered in person, with sufficient evidence. And the Russian warning would be this: we didn't cross the line, because you did the same to us, so if you take action beyond anything we did, then you are escalating things.

Or it could be as simple as their information ops people receiving a bag of goods to use to cast attention back towards the nefarious NSA and away from the cuddly CozyBear and FancyBear.

I'd say at this point - absent discovery of something of real significance in there that would alter the analysis - this is not a warning to the US but domestic politics and/or domestic face-recuperation, nothing more.

For all we know, frank talks between the Russian and US governments regarding the DNC document dump have already occurred and reached, one hopes, a resolution of the rules of the road on the matter of political campaigns.

---

supersaurus • August 16, 2016 8:23 PM

my perverse-o-meter is pegged today: suppose it is some subtle scam run by the NSA itself? "help...help...just look at this awful hack perpetrated upon us...we need more money and power..."

Winston Smith • August 16, 2016 8:30 PM

@Skeptical

I read your post. Did you ever consider that maybe this doesn't involve Russia at all, but rather, in-fighting among U.S. TLAs?

65535 • August 16, 2016 8:35 PM

@ supersaurus

"help...help...just look at this awful hack perpetrated upon us...we need more money and power..."

That’s my secondary though in my post. The solution is no more money for the duplicitous spies at the NSA. In fact, a reduction of funds is in order.

Sorge • August 16, 2016 8:39 PM

Sometime after the invasion of Iraq, the CBP РФ canceled the gentleman's agreement on mutual forbearance for clandestine operations. They've since been doing intel not just to counter US covert action but to expose US criminality. This disclosure is consistent with that approach: these files are a smoking gun for state acts that are illegal in US municipal and conventional international law. That doesn't mean the Russians did it. The SCO is now a de facto alliance and Eurasia has technical capacity coming out its ears. Eurasia is out to do what the Church and Pike committees tried and failed to do: get the US permanent government under control. They've got the support of the entire international community including unbought elements in the US satellites.

The international community understands that in the US rule of law has been superseded by a state

of exception involving crimes against humanity and peace: legally, that means acting like the Nazis. The Russians lost 20 million lives that time so curbing US Nazi tricks is a vital interest of the Russian state. For that reason containing the US threat to peace ultimately falls to them. The world would much prefer suasion to the alternative.

Wael • **August 16, 2016 8:39 PM**

It's none of the above (and I read nothing above, so take it with a grain of salt.)

During the Cold War era, superpowers used to have proxy wars. You know, get some little countries to fight together and test the weapons. Now, Cold War over, Cyber space in...

It's the start of direct cyber war! Can't trust the little countries with those sort of weapons.... It's evolution (not that I believe in it) in action. We're heading towards a Taste of Armageddon, as @Dirk Praet will tell you!

May the source be with you...

Wael • **August 16, 2016 9:07 PM**

@Winston Smith,

> in-fighting among U.S. TLAs?

+1

Azalo • **August 17, 2016 12:18 AM**

@Yoshii

There hasn't been many proclamations of fact here other than the dump itself and the blogpost depicting EXTRABACON in action.

I miss the silliness and irreverence of the older hacker groups. Too many people are far too serious these days with the endless gender politics shaming. Can't express ourselves without being demonized as childish or hateful in some manner. It sucks. Especially poisonous for creative communities of all stripes, including the hacker community.

Eliot Lear • **August 17, 2016 12:20 AM**

Let's call this release embarrassing, but I very much doubt that policy makers will take it into account when considering sanctions against Russia. No organization, **not even the NSA**, is entirely isolated. The NSA assuredly has multiple levels of security, depending on the sensitivity of the subject matter. We all knew that such code existed. I would expect them to have done a better job at firewalling the crown jewels, such as communications within foreign administrations.

A smaller release of more sensitive information would have sent a stronger message, and that such a release **didn't** happen leads me to believe they didn't get very far in. And even if they did, the idea that a policy maker would be blackmailed about information that wasn't personally about them doesn't

really ring true.

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"> • <cite> <i> • <b> • <sub> <sup> •   • <blockquote> <pre>

Preview Submit

← Powerful Bit-Flipping Attack