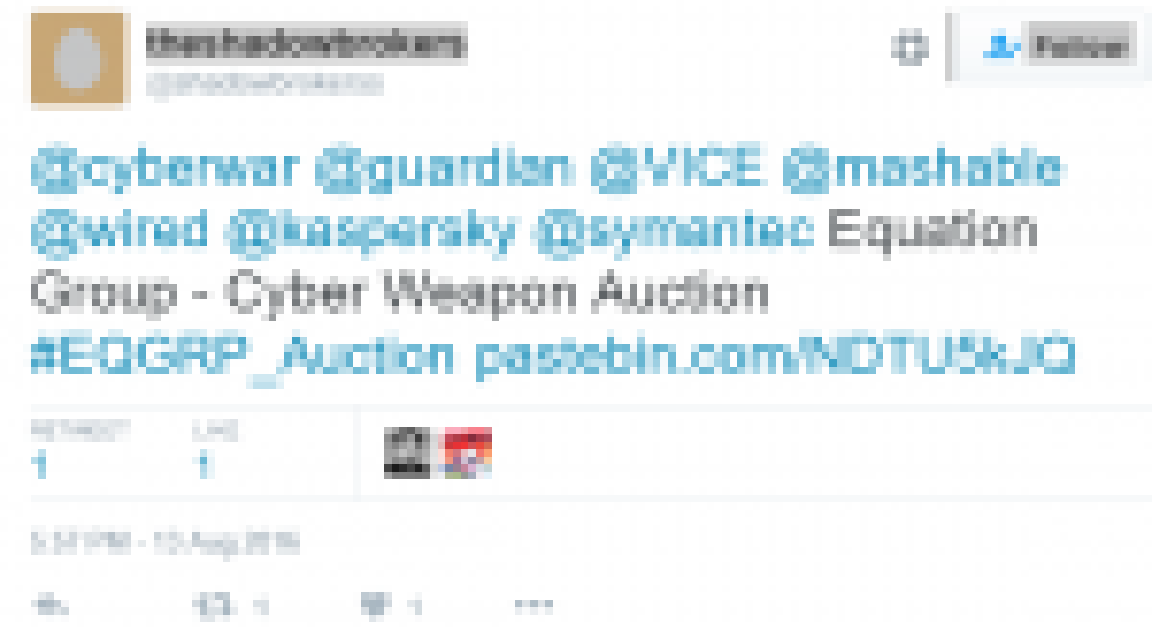
Lifting the Shadows of the NSA's Equation Group?

August 15, 2016 By RBS

This week a hacker group going by the name The Shadow Brokers has surfaced and appears to be auctioning off computer exploits it claims are stolen from the Equation Group. The Equation Group, a group of hackers believed to be operated by the National Security Agency, was named by Kaspersky after their analysis of "APT" activity leading up to 2015. According to Wikipedia:

> "The Equation Group is a highly sophisticated threat actor described by its discoverers at Kaspersky Labs as one of the most sophisticated cyber attack groups in the world and "the most advanced … we have seen", operating alongside but always from a position of superiority with the creators of Stuxnet and Flame"

The group that leaked the new exploit files goes by the name The Shadow Brokers and operates the Twitter account @theshadowbrokerss. Based on their Tweets, it appears that they have been preparing for this release since at least the start of August. It started with the creation of a Reddit account on the 1st of August and then over the next 13 days it appears they created accounts at GitHub, Twitter, and Imgur.



On the 13th of August they they announced the leak of this data, which stands out from other leaks because it appears to be a teaser and advertisement to promote the online auction of a larger portion of the data they got a hold of. The leak and auction announcement has been posted to various sites, including Twitter, GitHub, Tumblr, Reddit, Imgur, and Pastebin:

> 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.

The data was uploaded to several sites including MEGA, which shows that it was last modified on their system on the 1st of August further suggesting they have had it for some time.**The Auction**While we have increasingly

seen the data from hacked companies be put up for auction, it is rare to see this big of a teaser posted publicly. Many breaches only end up publicly disclosing a very small sample of data to show their authenticity, but the Equation Group teaser data includes a significant trove of exploits designed to compromise firewalls. This data alone has incredible value to a wide variety of companies, both offensive and defensive. The hacked data release came with a FAQ and a set of instructions for the auction:

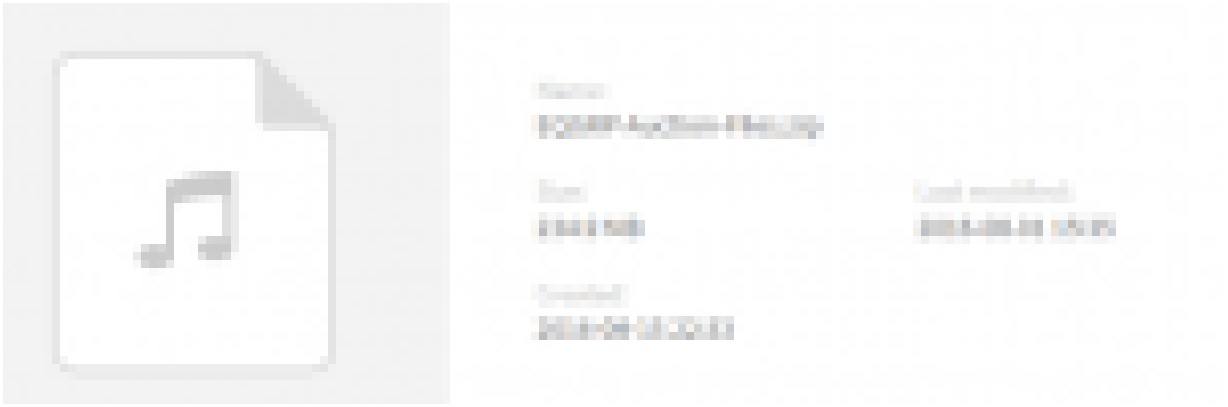
> We auction best files to highest bidder. Auction files better than stuxnet. Auction files better than free files we already give you. The party which sends most bitcoins to address: 19BY2XCgbDe6WtTVbTyzM9eR3LYr6VitWK before bidding stops is winner, we tell how to decrypt. Very important!!! When you send bitcoin you add additional output to transaction. You add OP_Return output. In Op_Return output you put your (bidder) contact info. We suggest use bitmessage or I2P-bote email address. No other information will be disclosed by us publicly. Do not believe unsigned messages. We will contact winner with decryption instructions. Winner can do with files as they please, we not release files to public.

The FAQ has several interesting points:

> Q: Why I want auction files, why send bitcoin? A: If you like free files (proof), you send bitcoin. If you want know your networks hacked, you send bitcoin. If you want hack networks as like equation group, you send bitcoin. If you want reverse, write many words, make big name for self, get many customers, you send bitcoin. If want to know what we take, you send bitcoin.Q: What is in auction files? A: Is secret. Equation Group not know what lost. We want Equation Group to bid so we keep secret. You bid against Equation Group, win and find out or bid pump price up, piss them off, everyone wins.Q: What if bid and no win, get bitcoins back? A: Sorry lose bidding war lose bitcoin and files. Lose Lose. Bid to win! But maybe not total loss. Instead to losers we give consolation prize. If our auction raises 1,000,000 (million) btc total, then we dump more Equation Group files, same quality, unencrypted, for free, to everyone. Q: When does auction end? A: Unknown. When we feel is time to end. Keep bidding until we announce winner.
> Q: Why I trust you? A: No trust, risk. You like reward, you take risk, maybe win, maybe not, no guarantees. There could be hack, steal, jail, dead, or war tomorrow. You worry more, protect self from other bidders, trolls, and haters.

The Exploits The compressed data is a little over 256MB and contains both the teaser data (eqgrp-free-file.tar.xz.gpg) as well as the data being auctioned (eqgrp-auction-file.tar.xz.gpg). While both are encrypted, the Shadow Brokers only provided the password for the teaser data, and only the auction winners presumably receive the password for the rest. Highlights:

- Free data file extracts to a folder named “Firewall”
- The date stamps on the encrypted files are July 25, 2016.
- The decrypted “free file” has file dated as far back as 2013.
- Directories are dated back to 2010.
- The data structure is same as shown in Imgur preview.



While many companies and analysts rush to figure out what exploits were released, with some already publishing their initial analysis, a few of the highlights based on our cursory examination are below. The directory structure uses four letter code names for specific exploits. Some of the codes, exploit names, and relevant details:

EGBL: EGREGIOUSBLUNDER version 3.0.0.1 – A web-based exploit that targets Fortigate firewalls (various builds of firmware FGT_60-v300) including models 60, 60M, 80C, 200A, 300A, 400A, 500A, 620B, 800, 5000, 1000A, 3600, and 3600A. One researcher notes that Avast calls it CVE-2006-6493, which is a vulnerability in OpenLDAP.

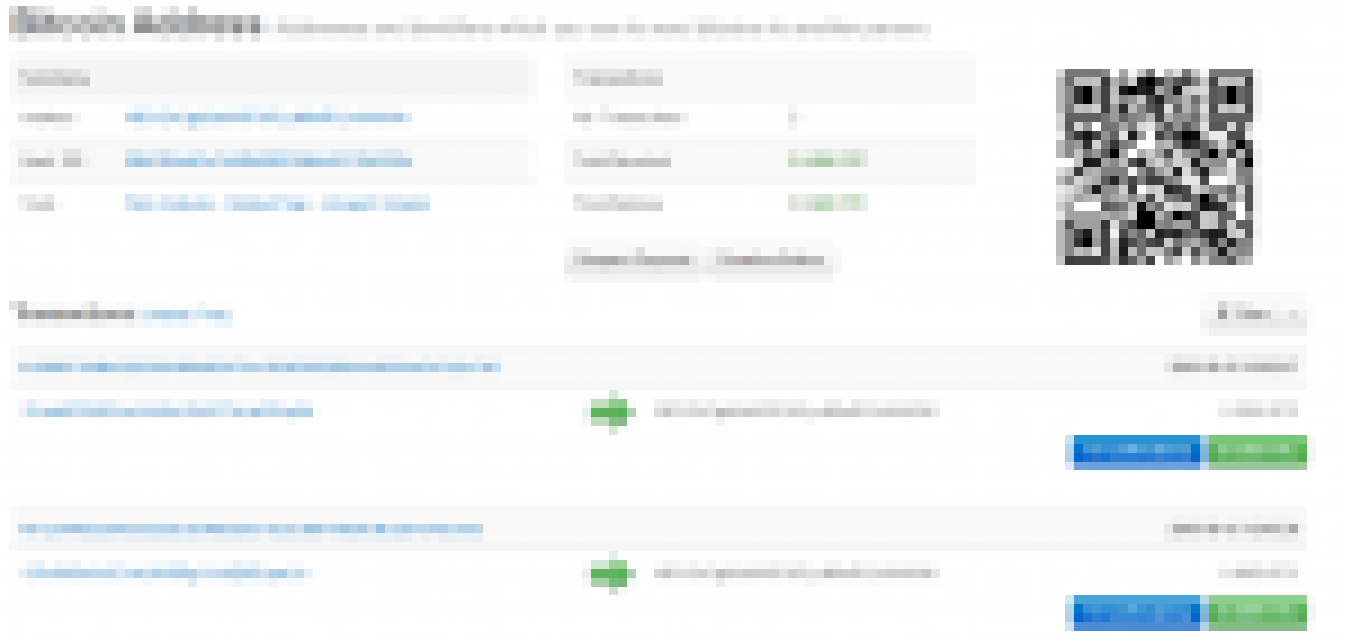
ELBA: ELIGIBLEBACHELOR – An exploit against an unspecified vendor, affecting versions 3.2.100.010, 3.3.001.050, 3.3.002.021 and 3.3.002.030. This exploit uses the third-party library from Keld Simonsen called ISO/IEC 14652 i18n FDCC-set.
ELBO: ELIGIBLEBOMBSHELL version 1.2.0.1 – A web-based exploit reported to be against the Chinese made TOPSEC firewall and affects versions 3.3.005.057.1 to 3.3.010.024.1. Some payloads are noted as having been added as far back as 2009 and have their own code name designations, including WOBBLYLLAMA, FLOCKFORWARD, HIDDENTEMPLE, CONTAINMENTGRID, and GOTHAMKNIGHT. Notes in the exploit include information “FOR DEVELOPERS ONLY”.

ELCA: ELIGIBLECANDIDATE version 1.1.0.1 – A line in the exploit describes itself as “*What is the sound of a single thread blocking?*” This web-based exploit targets the /cgi/maincgi.cgi script of Chinese made TOPSEC firewalls version 3.3.005.057.1 to 3.3.010.024.1.ELCO: ELIGIBLECONTESTANT version 1.1.0.1 – A line in the exploit describes itself as “*A packet drops in a router. Does anyone hear it?*” This web-based exploit targets the /cgi/maincgi.cgi script of Chinese made TOPSEC firewalls before version 3.3. The exploit also has warnings for the user that the “*User may be logged in. PLEASE REVIEW SYSTEM INFO*“.
EPBA: EPICBANANA version 2.1.0.1 – This exploit targets several models of Cisco PIX Firewalls and Cisco Adaptive Security Appliance (ASA) devices. It uses the pexpect.py Python module written by Noah Spurrier and includes an extensive list of credits for helping develop the module. The affected ASA device images include 711, 712, 721, 722, 723, 724, 80432, 804, 805, 822, 823, 824, 825, 831, and 832. The affected PIX device images include 711, 712, 721, 722, 723, 724, and 804.

ESPL: ESCALATEPLOWMAN version 1.1.0.1 – A local exploit against an unknown vendor, with one very interesting line in the *params.py* file. One of the configurable parameters is “callback” and the example in the header of the file says “callback (“30.40.50.60:9342”) parse to: callback_ip, callback_port”. That IP address is registered to the DoD Network Information Center located in Columbus, Ohio that is part of the Defense Logistics Agency. This may be a telling piece of information, or an unfortunate sample IP address as we see it used in at least one book on administering data centers. One researcher notes that it appears to be

unroutable and potentially just a placeholder.

EXBA: EXTRABACON version 1.1.0.1 – An exploit against the SNMP service of Cisco Adaptive Security Appliance (ASA) devices that affects version 8.0(2) to 8.4(4).The exploit dump contains many other tools and scripts, along with other wonderful codenames such as BANANAGLEE (impacting Juniper devices), BARGLEE, BLATSTING, BUZZDIRECTION, SCREAMPLOW, and BANANADAIQUIRI.**Bidding and Bitcoin** Several researchers have taken to monitoring the BTC (bitcoin) transactions associated with the auction of the leaked data, and have pointed out it can be monitored on the blockchain. At the time of publishing, the auction currently has two transactions worth a total 0.0424 BTC ($23.56US). The first transaction bid was 0.0355 BTC and the second one was 0.0069 BTC. The current high bid comes from Mike Damm, who has announced it on twitter.



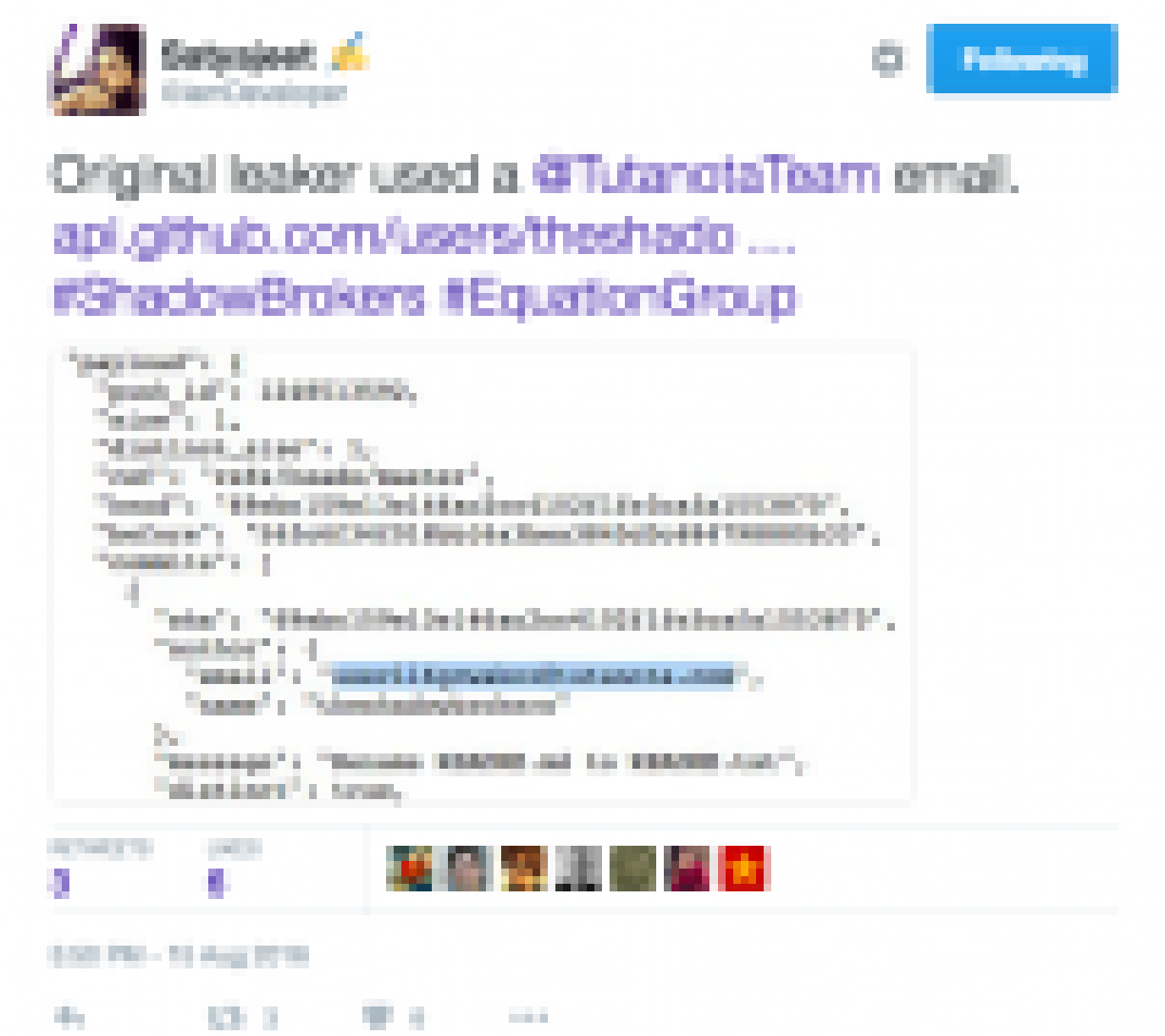
Final Thoughts As we wrap up this initial blog post, the amount of attention and analysis this leak is receiving is considerable. The ShadowBrokers GitHub page has been suspended already, but copies of the leaked data are already spread far and wide. In the coming days and weeks, we expect to see a variety of blogs further analyzing the exploits as well as the affected vendors scrambling to evaluate the information to provide patches.
While this leak seems extremely damaging to the NSA on the surface, we caution readers to remember that false flag operations are a critical part of high-level hacking activity. As one analyst notes, this leaked information likely comes from a compromised system hosting the exploits rather than the NSA getting hacked directly.

The Dust Has Settled, Or Has It? (August 16) After a furious first day with many researchers analyzing the published data, there seem to be as many questions as answers. However, a fair amount of points and facets of the dump have been discussed and discovered. With so many disjointed analyses taking place, we have attempted to recap the highlights in this update.We start first with some other recaps and pieces worthy of a read:**Published Leak**As originally mentioned, the leak and auction announcement were posted to various sites, including:

- Twitter – The original Twitter account is still up and running, despite claims otherwise.
- GitHub – Some level of censoring and data removed ~ 5:30P EST – August 15th.
- Tumblr – theshadowbrokers.tumblr.com is no longer available as of ~ 5:50P EST – August 15th.

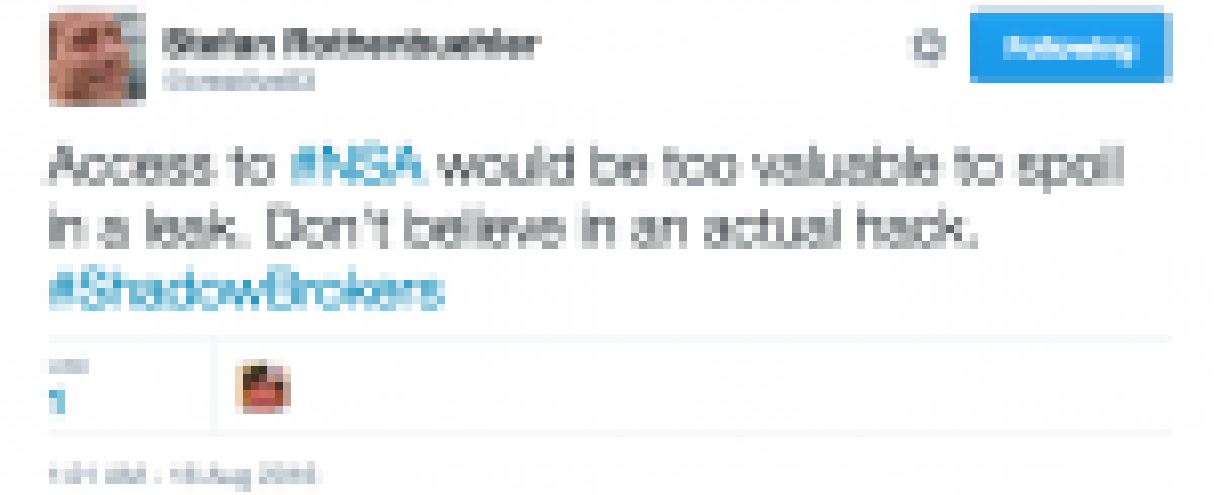
- Imgur – The picture posted is still up.
- Pastebin – The content is still up.
- MEGA – The content is still up.

When looking at the leak and public event on Github, one can see the original leaker used a @TutanotaTeam email. We took note of it in our analysis, and it was later pointed out by Twitter user @iamdeveloper.



You can also see a list of 'file by modified time' on Github from the archive. When reviewing, it is evident they are older files from approximately September 2013 and directories listed are from 2010. According to @pwnallthethings, "*The most recent "last modified" timestamp in the EQUATION GROUP hacking tool set is 2013:10:18 14:48:09+02:00 – i.e. October 18, 2013.*" This suggests it is very questionable to think that the NSA was actually hacked directly or recently. It is much more likely given the file dates and content that this is a quite old compromise, or – as many would believe – the hackers compromised a launch box used for attacks that wasn't cleaned up.

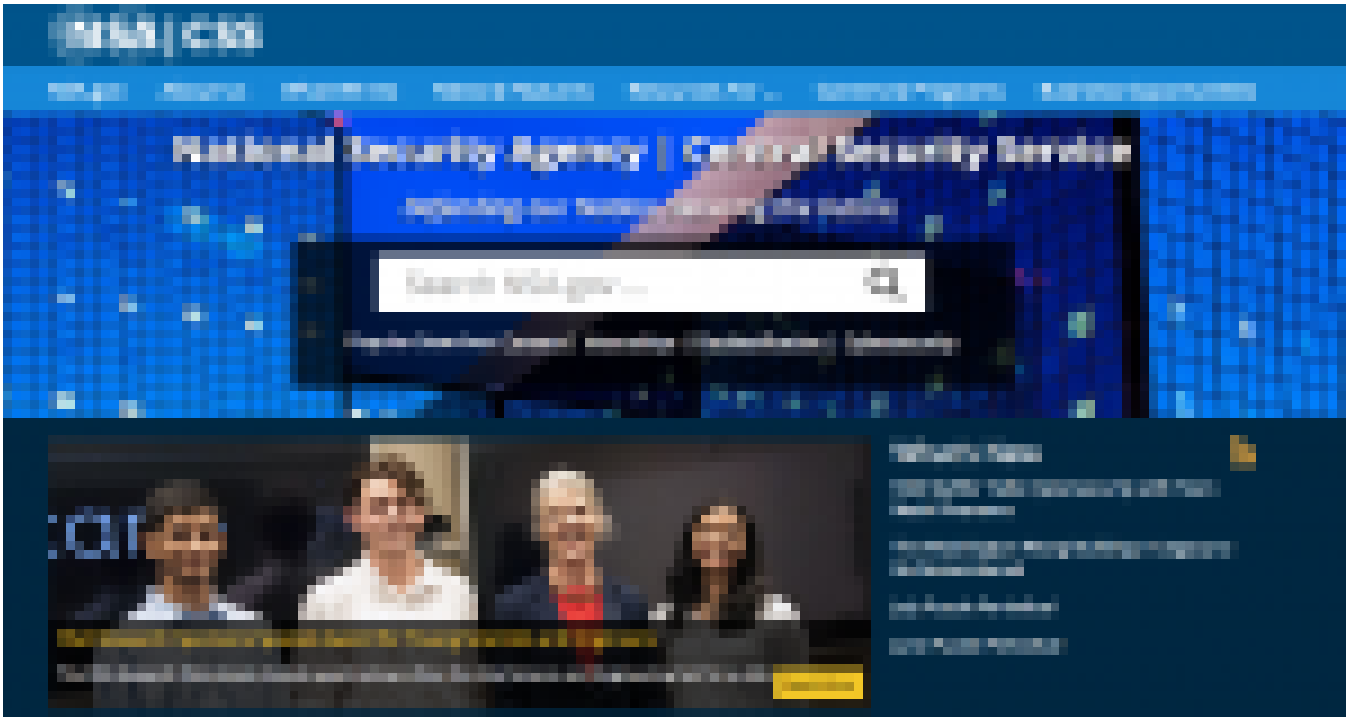
Furthermore, as Twitter user @creative83 points out, it would be far too valuable to give up access to the NSA if the attackers actually had it:



So far, most coverage is pointing to the NSA being compromised either directly, or indirectly via misleading headlines. As mentioned earlier, it's very likely the NSA was **not** hacked, but it does look more and more like the exposed data is from the NSA.

Twitter user @RidT points out JETPLOW and BANANAGLEE appear in only one file in the Snowden leaks.

NSA Website Down



For those readers who have never been to the NSA's website, there is a screen shot above. It is quite extensive and appears to have a lot of references and content. However, Twitter user @ericgeller pointed out something very interesting about the NSA's website yesterday:

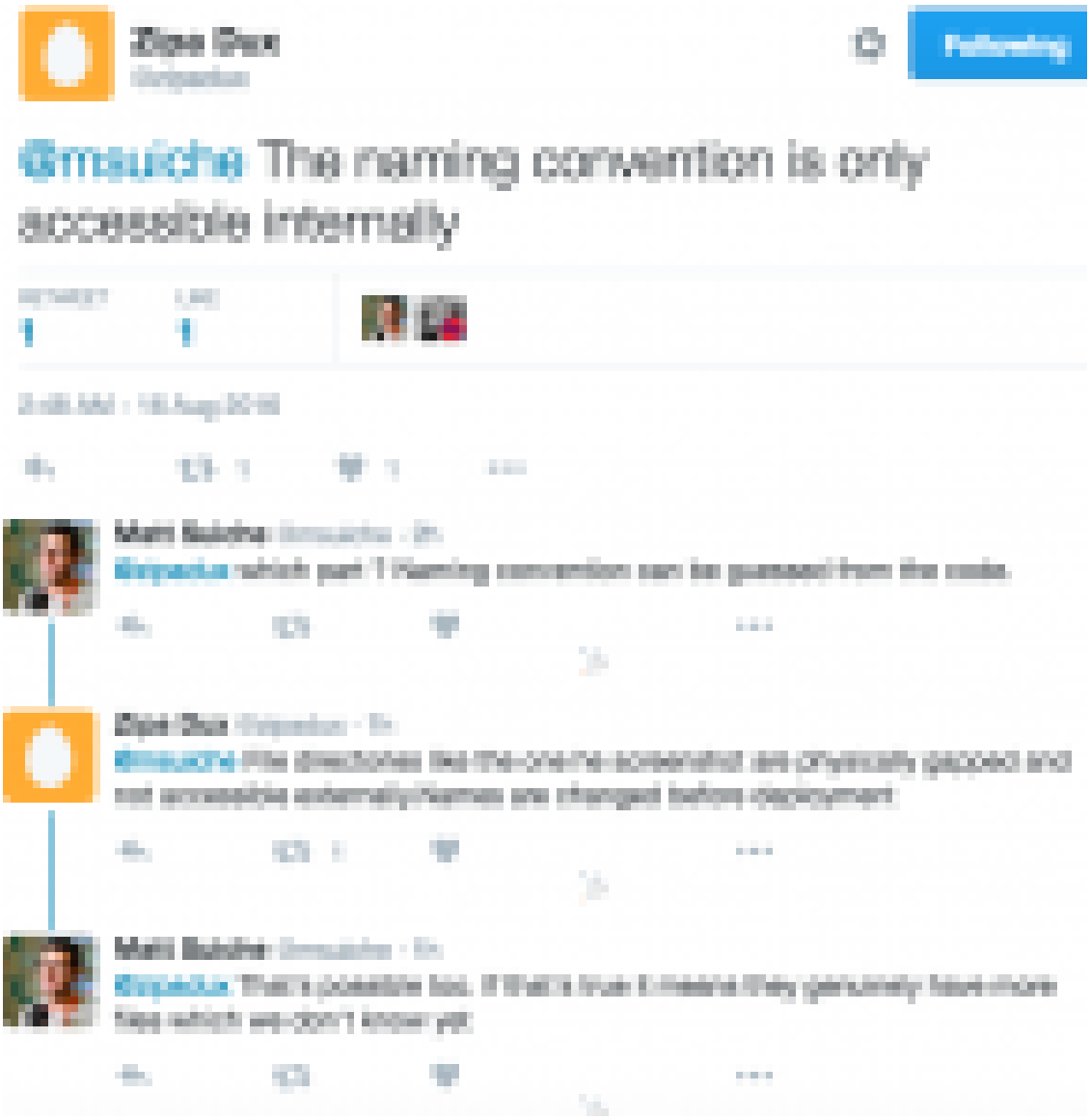
It seems too crazy to be true, so we did personally verify that the main page of the NSA is loading, all other pages are not loading and returning a "*Service Unavailable*" message.

It got us questioning when the website was last working properly and whether this is connected to the leak. Looking at the Way Back Machine, between August 1st and 16th we can see that the site appears to have

been properly serving content:

Just now a Twitter account @zipadux (registered since November 2005, but inactive until just now) stated that "*ShadowBrokers is an insider who grabbed the data via USB and is trying to pass himself off as a foreign group.*"

And then a bit more conversation about the naming structure of the leak:



Data being removed from the NSA on a USB, sounds familiar right? It's difficult to tell if @zipadux is speaking from authority or an educated guess, but the lack of Twitter activity until now is certainly interesting.

Snowden

There has been quite a bit of speculation on whether Edward Snowden is involved with this leak or had knowledge of it as Wikileaks claims. Based on recent behavior from his Twitter account, while there is no evidence at all, it is easy to see why many are asking the question. It is also worth noting that Snowden's original leak happened in June, 2013, and most of the files in the newly leaked archive are dated 2013. While the archive has files dated up to October, 2013 and Snowden had already left the NSA and flew to Russia by June, 2013, it still makes some wonder if he was involved.

Here is the timeline of events of now mostly removed Tweets:
August 3rd, 2016: Snowden says "It's time."

August 5th, 2016: Snowden tweeted a "dead man switch" key, or so people thought.
"ffdae96f8dd292374a966ec8b57d9cc680ce1d23cb7072c522efe32a1a7e34b0"

No Tweets for 10 days from Snowden.
August 13, 2016: The ShadowBrokers release the NSA tool archive .

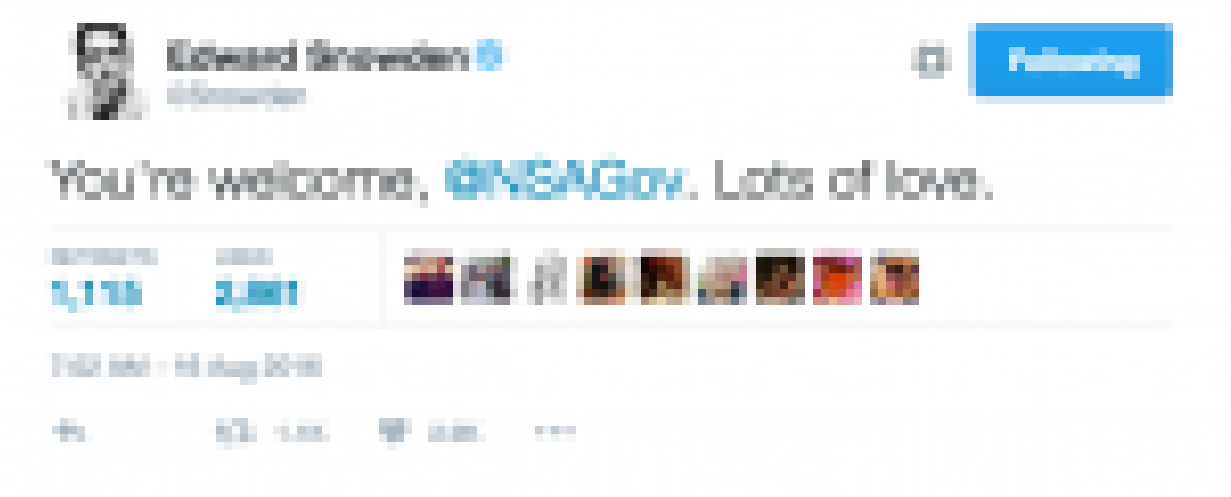
Today, Snowden is back with some thoughts on this leak, confirming that he believes this is a compromise of

an NSA malware staging server.

He goes on to tweet quite a bit more adding more context and sharing his thoughts that include:

- 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 rivals' hacking tools and reverse-engineer them to create "fingerprints" to help us detect them in the future.
- Here's where it gets interesting: the NSA is not made of magic. Our rivals do the same thing to us — and occasionally succeed.
- 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.
- Why did they do it? No one knows, but I suspect this is more diplomacy than intelligence, related to the escalation around the DNC hack.
- Circumstantial evidence and conventional wisdom indicates Russian responsibility. Here's why that is significant:
- This leak is likely a warning that someone can prove US responsibility for any attacks that originated from this malware server.
- That could have significant foreign policy consequences. Particularly if any of those operations targeted US allies.
- Particularly if any of those operations targeted elections.
- Accordingly, this may be an effort to influence the calculus of decision-makers wondering how sharply to respond to the DNC hacks.
- TL;DR: This leak looks like a somebody sending a message that an escalation in the attribution game could get messy fast.
- Bonus: When I came forward, NSA would have migrated offensive operations to new servers as a precaution – it's cheap and easy. So? So…
- The undetected hacker squatting on this NSA server lost access in June 2013. Rare public data point on the positive results of the leak.

He ends with one last tweet aimed at the NSA.



Now he will most likely go back to focusing on where he can speak next!

Vulnerability Details, Attribution, and Bitcoin Goals (August 17)
Day three of the Shadow Brokers dump of the purported Equation Group exploits, and as expected, technical analysis and wild speculation are prevalent. In this update we cover the attribution angle in more detail below, but one point that is square in many minds is how this auction quickly removed the recent George Soros / Open Society Foundations leak from the news. In the rapidly evolving face of American politics, with several political leaks at play, the notion of a new breach or leak stealing news cycles is certainly feasible. Either to bury a previous story, or to add more weight to a string of stories that may embarrass a political party. Regardless, the timing of the Shadow Brokers couldn't have been any better for George Soros and the Open Society Foundations.

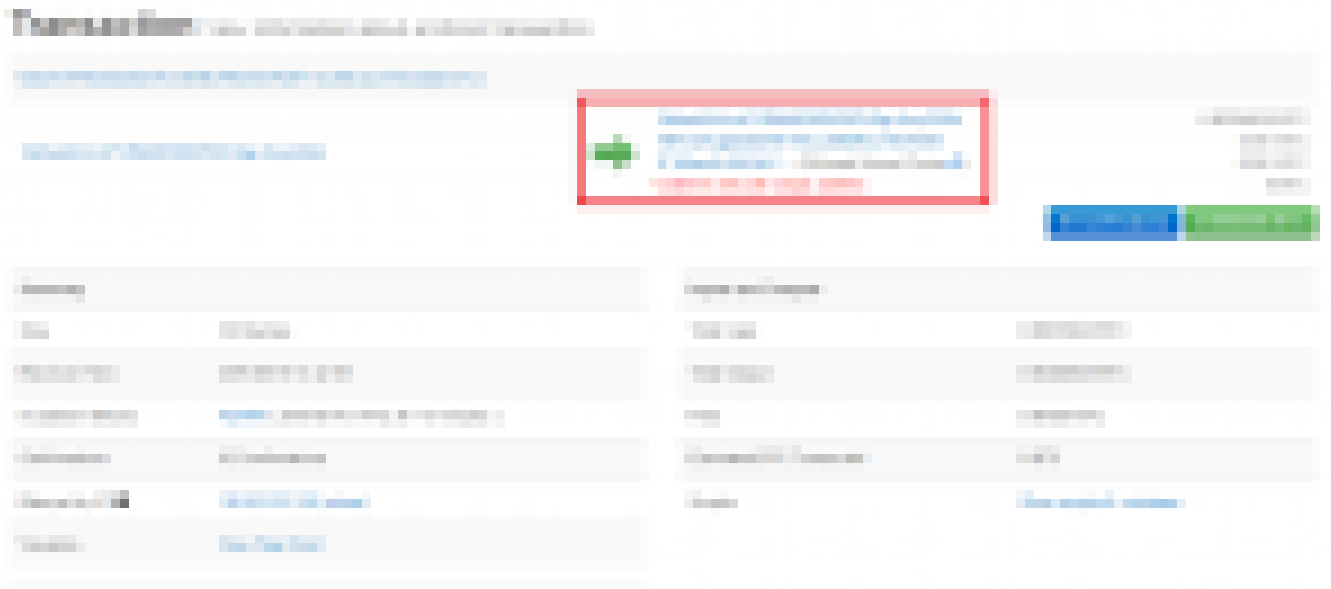
As a quick follow-up to our previous update, Vice published an article detailing why Github removed the links to the Shadow Brokers' data dump, citing that it violated the user-agreement. Per GitHub's agreement, that certainly seems like grounds for shutting down the account and falls well outside of conspiracy theory:

> "Per our Terms of Service (section A8), we do not allow the auction or sale of stolen property on GitHub. As such, we have removed the repository in question," Kate Guarente, from Github's communications team, told Motherboard in a statement.

Sometime today, the NSA has restored their website content and you can navigate the site to learn more about what they do, and what they consider the threat to be. As we continue to digest the leaked data and understand the implications, one question that will remain front and center is, "*what is going to happen next*"?

Bitcoin Update Two days later, the auction for the rest of the exploit archive is still a bit short of their one million BTC goal (a total, not single bidder) and the promise of releasing them to everyone. Fifteen transactions later and the highest bid is 1.5 BTC, a majority of the balance, with a final balance at 1.629 BTC or US$947.41.

Dee Kay notes that one of the Bitcoin addresses bidding on the archive has also sent Bitcoins to an address that was part of the Silk Road seizure:



As Wired notes, no one is really bidding on the stolen NSA “cyberweapons”.

Vulnerability Analysis

With several days to analyze the leaked data, more details are emerging about each of the codenamed exploits. One of the more important things to note is that with every released exploit, it requires access to an interface that is typically restricted to privileged networks or the internal network in general. These exploits would only be valuable against a remote target over the Internet if the firewall was severely misconfigured, making the vulnerable services Internet addressable. While certainly valuable, the initial impression that these exploits were for remotely compromising firewalls is now drastically overstated. Despite that, some are offering absurd “expert advice” or masterful trolls.

The current tally of vulnerabilities, many of which appear to be 0days stands at:1 Fortigate: EGREGIOUSBLUNDER1 WatchGuard: ESCALATEPLOWMAN2 Cisco ASA / PIX: EXTRABACON, EPICBANANA4 TOPSEC: ELIGIBLECANDIDATE, ELIGIBLEBOMBSHELL, ELIGIBLECONTESTANT, ELIGIBLEBACHELOR

So far, according to Chris Bing, Cisco is the only vendor that has made a public statement acknowledging the vulnerabilities included in the leak.

EXBA: EXTRABACON version 1.1.0.1 – An exploit against the SNMP service of Cisco Adaptive Security Appliance (ASA) devices that affects version 8.0(2) to 8.4(4). XORcat has done a great analysis of this exploit and reports that the exploit requires read access to SNMP as well as access to telnet or SSH to access the

resulting shell. If the exploit fails to gain a shell, it may crash the device. The resulting shell grants user privileges, so the 'enable' password or a separate privilege escalation vulnerability is required for privilege escalation afterwards. According to Hector Martin, he believes the exploit may be related to the "*cufwUrlfServerStatus OID or just general SNMP parsing*". XORcat does not believe this is CVE-2015-4238 based on the information available, meaning this is very likely a 0day. According to Mustafa Al-Bassam, it relies on knowing the target machine's uptime and software version.

ELCA: ELIGIBLECANDIDATE version 1.1.0.1 – A line in the exploit describes itself as "*What is the sound of a single thread blocking?*" This web-based exploit targets the /cgi/maincgi.cgi script of Chinese made TOPSEC firewalls version 3.3.005.057.1 to 3.3.010.024.1. Mustafa Al-Bassam adds that the vulnerability more specifically resides in HTTP cookie handling.

ELBO: ELIGIBLEBOMBSHELL version 1.2.0.1 – A web-based exploit reported to be against the Chinese made TOPSEC firewall and affects versions 3.3.005.057.1 to 3.3.010.024.1. Some payloads are noted as having been added as far back as 2009 and have their own code name designations, including WOBBLYLLAMA, FLOCKFORWARD, HIDDENTEMPLE, CONTAINMENTGRID, and GOTHAMKNIGHT. Notes in the exploit include information "*FOR DEVELOPERS ONLY*". Mustafa Al-Bassam adds that like ELCA, this injects code via cookies into the web interface and detects the version based on the E-Tag header.

ELCO: ELIGIBLECONTESTANT version 1.1.0.1 – A line in the exploit describes itself as "*A packet drops in a router. Does anyone hear it?*" This web-based exploit targets the /cgi/maincgi.cgi script of Chinese made TOPSEC firewalls before version 3.3 via a POST parameter. The exploit also has warnings for the user that the "*User may be logged in. PLEASE REVIEW SYSTEM INFO*". Mustafa Al-Bassam says this exploit can be tried after ELIGIBLECANDIDATE.

ELBA: ELIGIBLEBACHELOR – An exploit against Shaanxi Networkcloud Information Technology TOPSEC Firewall running the TOS operating system, based on a version included in the script and/or "tos_configd" in the script. The exploit works against versions 3.2.100.010, 3.3.001.050, 3.3.002.021 and 3.3.002.030. This exploit uses the third-party library from Keld Simonsen called ISO/IEC 14652 i18n FDCC-set. Mustafa Al-Bassam adds that the exploit is designed to install an implant called BLATSTING, which uses a custom-made tool dubbed NOPEN for opening a shell on the victim machine. While the attack vector is unknown, he says it has an XML-like payload that starts with <?tos length="001e:%8.8x"?> and is sent to the custom protocol operating on TCP port 4000. Al-Bassam goes on to note that the exploit author included some humor in the NOPEN payload shell/tunnel.

EGBL: EGREGIOUSBLUNDER version 3.0.0.1 – A web-based authentication cookie overflow leading to remote code execution exploit that targets Fortigate firewalls (various builds of firmware FGT_60-v300) including models 60, 60M, 80C, 200A, 300A, 400A, 500A, 620B, 800, 5000, 1000A, 3600, and 3600A. One researcher notes that Avast calls it CVE-2006-6493, which is a vulnerability in OpenLDAP, and others are fairly sure it is not. One researcher has independently confirmed the exploit works, but requires access to the web management interface.

ESPL: ESCALATEPLOWMAN version 1.1.0.1 – A local privilege escalation exploit against WatchGuard firewalls, with one very interesting line in the params.py file. One of the configurable parameters is "callback" and the example in the header of the file says "callback ("30.40.50.60:9342") parse to: callback_ip, callback_port". That IP address is registered to the DoD Network Information Center located in Columbus, Ohio that is part of the Defense Logistics Agency. This may be a telling piece of information, or an unfortunate

sample IP address as we see it used in at least one book on administering data centers. One researcher notes that it appears to be unroutable and potentially just a placeholder.

EPBA: EPICBANANA version 2.1.0.1 – This exploits a buffer overflow in line editing functionality in several models of Cisco PIX Firewalls and Cisco Adaptive Security Appliance (ASA) devices. It uses the pexpect.py Python module written by Noah Spurrier and includes an extensive list of credits for helping develop the module. The affected ASA device images include 711, 712, 721, 722, 723, 724, 80432, 804, 805, 822, 823, 824, 825, 831, and 832. The affected PIX device images include 711, 712, 721, 722, 723, 724, and 804.

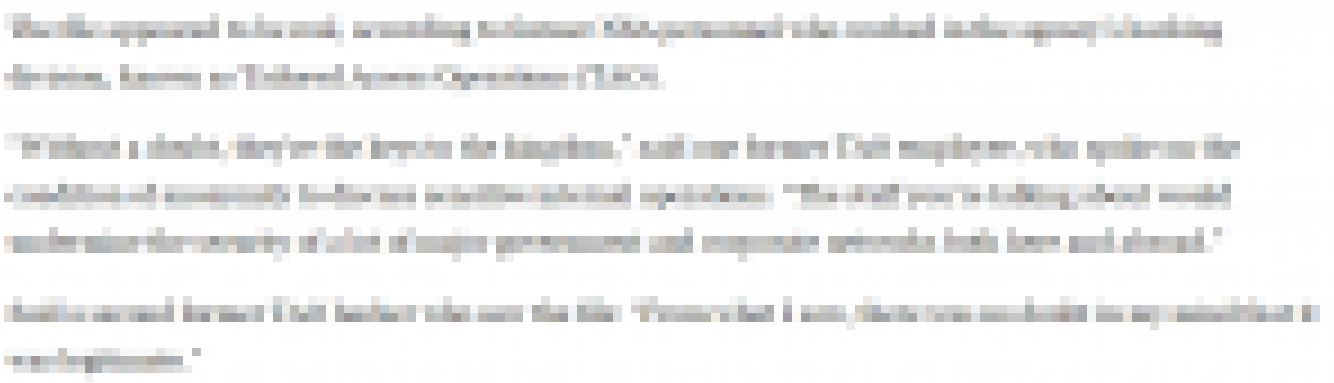
The exploit dump contains many other tools and scripts, along with other wonderful codenames such as BANANAGLEE (impacting Juniper devices), BARGLEE, BLATSTING, BUZZDIRECTION, DurableNapkin (post-firewall injection packet injection tool), SCREAMPLOW, Teflon Door (self-destructing exploitation payload), FalseMorel (tool to bypass Cisco enable password), BANANAUSURPER, BUZZDIRECTION, and BANANADAIQUIRI. The NOPEN tool referenced earlier, appears to be a tunnel to hide the source of attacks via TCP port 32754 by default, according to one researcher.

According to another researcher, among the tools is a script named stager.sh that includes code showing the Equation Group masquerades as Chinese actors by default, query Chinese domains. As with everything else in this leak, it has to be questioned if this is really a sign the scripts were authored by Western powers versus any other nation-state. After all, if the tools are lost, as these were, wouldn't it make sense to plant false-flags?

Attribution

There are three facets of attribution facing this leak. First, is the leaked data truly from the Equation Group, second, who leaked the data, and third, is the Equation Group is really part of the National Security Agency (NSA). While most people interested in attribution are focusing on who leaked the data, Kaspersky Lab's Global Research & Analysis Team has posted convincing evidence that the leaked data directly correlates to the Equation Group's tools analyzed in February of 2015. One of the more unique aspects of the Equation Group's arsenal is the use of the RC5 and RC6 algorithms, which also appears in the new dump. Kaspersky's team breaks down several uses of the same algorithms and code bits that make a compelling argument that the newly released files are indeed from the same group. It is interesting to note that in all of this time, Kaspersky has never officially said that the Equation Group was the NSA. Strong implications and third-party articles making that conclusion (some with ex-NSA sources) are prevalent, but Kaspersky has never publicly stated that connection.

Like last year's analysis and conclusions, the Washington Post has gone on the record to say the leaked Equation Group files are directly tied to the NSA:

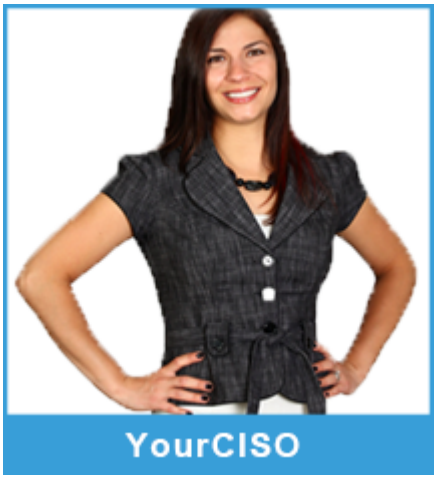


The more popular attribution argument centers around who leaked the data. The last few years have

demonstrated that a few obvious culprits will be named in **any** 'cyber' incident; China and Russia. It's only a matter of time before these names are bantered about, and this time is no exception. Edward Snowden said Russia is the primary suspect in this leak in a series of Tweets covered yesterday, and further covered in a Forbes article today. CTO of Immunity Inc, Dave Aitel, who is a former NSA employee, makes an argument that the leak can be attributed to Russia too, but many have already responded that it is not a compelling argument at all.

Others are approaching the leaker attribution question from a more analytical standpoint, looking at the text accompanying the leak. Anup Ghosh says he is looking forward to "linguistic analysis of the Shadow Broker's broken English." User 'kafkaesq' on the Hacker News Y Combinator makes observations about the language used, and others chime in with their knowledge of speaking multiple languages. While such analysis is very interesting, it has to be taken with a grain of salt. Advanced adversaries that perform such a leak should be assumed to be wise enough to use various techniques to throw off would-be detectives and may use such language purposefully. As Nick Galbreath points out, "spelling is opsec". Even in the actual code, as mentioned with the stager.sh script above, it is important to note that attribution proof must be solid as Greg Barnes notes.

While technical evidence may be completely lacking and speculation ruling the day, it cannot be ignored that the timing of this leak in the current U.S. political climate is suspect. With the last few weeks of U.S. news dominated by Donald Trump and questionable ties to Russia and Vladimir Putin, as well as Trump's speeches calling for Russia to hack U.S. government resources (in jest or not), it begs the question if the Equation Group leaks are part of a political agenda. The Register is one of many news outlets to put that theory forward, in addition to hundreds of Twitter denizens. This is the type of speculation that is important to discuss, but prudence demands that it remain part of the discussion until evidence surfaces.



Affordable SaaS security solution providing a complete Information Security Program with access to a CISO.

Risk Based Security's risk management solutions are a combination of data analytics, risk assessment and improvement strategies.

Not just security, the right security

Resources: