Equation Group cyberweapons auctioned off; WikiLeaks promises release

by Michael Heller
Senior Reporter
Published: 16 Aug 2016

Cyberweapons purportedly stolen from the NSA-linked Equation Group have been put up for auction; WikiLeaks promises it will publish 'pristine copy in due course.'
A group attempting to auction off cyberweapons allegedly used by the NSA-linked Equation Group and Edward Snowden said this may be the beginning of the fallout.

The group, calling itself The Shadow Brokers, claims it hacked one of the most advanced and longstanding cyberespionage actors, the Equation Group. There has been speculation that the Equation Group is part of the National Security Agency (NSA).

The Shadow Brokers posted images of the files stolen and some of the code (the GitHub repository has since been disabled) and experts have matched the code samples with exploits catalogued in the NSA's Advanced Network Technology (ANT) Division data leaked by Edward Snowden in 2013.

Claudio Guarnieri, a researcher at the University of Toronto's Citizen Lab, said on Twitter "some of those programs in the dump are parts related to network appliance implants from the ANT catalog." Guarnieri was careful to note he hadn't seen any evidence in the code of the source of the data but the latest file modification date in the code was from June 2013, before the ANT catalog was published.

The Shadow Brokers set up an auction for the data asking bidders to send bitcoin and promising to release the code to the highest bidder, but they would not refund losing bids. And, if the bidding reached 1 million bitcoin (approximately $581 million), the Shadow Brokers would "dump more Equation Group files, same quality, unencrypted, for free, to everyone." Though, as of this publication, the auction address had only received 1.6 bitcoin.
Rick Holland, vice president of strategy for Digital Shadows, the London-based cybersecurity firm, said even "if the data is false, the notoriety surrounding the ad alone could be enough for Shadow Brokers to generate some profit."

"From what we have observed previously, this is a common tactic amongst cyber actors who want to profit from what they often claim is stolen information," Holland told SearchSecurity via email. "The highest bidder might be able to collect whatever data is for sale and either release it to the public or create their own sale in an attempt to generate a return on their investment (while also maintaining the illusion that the data is legitimate)."

The original announcement by the Shadow Brokers has disappeared from Tumblr, though the Google cache of the page is still available. In suspicious timing that may just be coincidence, the NSA.gov website has been down for most of the day and WikiLeaks claims to have the Equation Group data.

Edward Snowden himself commented on the happenings on Twitter while being careful to not specifically confirm the claims made by the Shadow Brokers. Snowden described how the NSA hacks others and claimed the NSA itself is not immune to being hacked.

5) 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.
Snowden went on to conjecture, as others have, who might be behind such an attack on the NSA, but Guarnieri said any claims of attribution are nothing more than speculation.

Igor Baikalov, chief scientist for Securonix, the Dallas security analytics firm, told SearchSecurity that "too many things around this announcement don't make sense."

"There's no proof whatsoever that the code is in any way connected to [Equation Group] or NSA," Baikalov said. "Researchers who've seen it say it's good, but there's a lot more analysis [that] has to be done before any definitive conclusions, specifically on the lineage with any known code base. The most I'd give to The Shadow Brokers is that they've stumbled upon an old backup from 2013 -- that'd explain the most recent file date and names unchanged since the leak."

However, Snowden suggested that whoever may be behind this release might be sending a "warning that someone can prove U.S. responsibility for any attacks that originated from this malware server. That could have significant foreign policy consequences. Particularly if any of those operations targeted U.S. allies."

Edward Snowden
@Snowden

6) What's new? NSA malware staging servers getting hacked by a rival is not new. A rival publicly demonstrating they have done so is.
1:44 PM - 16 Aug 2016
1,208 1,334

Nex ~ Claudio
@botherder

Everybody who's calling out Russia/China on this #ShadowBrokers dump has no evidence. Can we stop this trend of freestyle attribution?
7:52 PM - 15 Aug 2016
18 26

Michael Heller asks:

What do you think about the auction of alleged Equation Group cyberweapons?
12) Accordingly, this may be an effort to influence the calculus of decision-makers wondering how sharply to respond to the DNC hacks.

13) TL;DR: This leak looks like a somebody sending a message that an escalation in the attribution game could get messy fast.

Edward Snowden
@Snowden
1:49 PM - 16 Aug 2016

Edward Snowden
@Snowden
Follow

Next Steps

Learn more about what the NSA's Tailored Operations Access unit means for enterprise.

Find out how Edward Snowden accessed secret NSA files.

Get info on how to prevent insider information leak incidents.

Dig Deeper on Hacker Tools and Techniques: Underground Sites and Hacking Groups

timing attack

Russian hacker arrests linked to ransomware and exploit kit shutdowns

Can credit card hacking be stopped with Chip and PIN alone?
DDoS mitigation services: What to consider before implementation

Before implementing DDoS mitigation services, there are a few things enterprises should consider. Expert Ed Moyle discusses the ...

Fireglass demonstrates techniques to beat AWS CloudTrail

At Black Hat 2016, Fireglass researchers demonstrated how attackers can take advantage of AWS account jumping and abuse ...