SECURITYWEEK NETWORK:

- Information Security News
- Infosec Island
- Suits and Spooks

Security Experts:

WRITE FOR US

RECOMMENDED CONTENT

SECURITYWEEK

INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS

- Subscribe (Free)
- CISO Forum 2016
- ICS Cyber Security Conference
- Contact Us

- Malware & Threats
  - Vulnerabilities
  - Email Security
  - Virus & Malware
  - White Papers
  - Endpoint Security
- Cybercrime
  - Cyberwarfare
  - Fraud & Identity Theft
  - Phishing
  - Malware
  - Tracking & Law Enforcement
  - Whitepapers
- Mobile & Wireless
  - Mobile Security
  - Wireless Security
- Risk & Compliance
  - Risk Management
  - Compliance
  - Privacy
  - Whitepapers

- Security Architecture
  - Cloud Security
  - Identity & Access
  - Data Protection
  - White Papers
  - Network Security
  - Application Security
- Management & Strategy
  - Risk Management
  - Security Architecture
  - Disaster Recovery
  - Training & Certification
  - Incident Response
- SCADA / ICS

RECOMMENDED CONTENT

me › Cyberwarfare

Industry Reactions to Shadow Brokers Leak: Feedback Friday

By Eduard Kovacs on August 26, 2016

Share 30 G+1 3 Tweet RSS

A group calling itself Shadow Brokers has leaked many exploits, implants and other tools allegedly stolen from the NSA-linked Equation Group, and it claims to possess much more information that it's prepared to sell for 1 million Bitcoins.

Security firms, firewall vendors and documents released by Edward Snowden have shown that the leaked files are genuine. Cisco, Juniper Networks, WatchGuard and Fortinet have analyzed the exploits targeting their products and Cisco even identified an ASA software zero-day vulnerability, which it started patching this week.

It's still unclear who is behind Shadow Brokers, but some believe it could be Russia, while others suspect another NSA insider.

Industry professionals contacted by *SecurityWeek* have shared their thoughts on various aspects of the incident, including attribution, implications and defense methods.

And the feedback begins...

Israel Barak, CISO, Cybereason:

"One goal that the adversary could be trying to achieve is to make the agency believe that it has accessibility to some of their covert infrastructure, which may lead the agency to tear down some of its assets, without exactly disclosing which infrastructure they have accessibility to. Better yet, the adversary could be on a hactivism crusade, looking more to embarrass the agency more than anything else."

Chenxi Wang, Chief Strategy Officer, Twistlock:

"The information thus far leaked by the "ShadowBrokers" appears legitimate, and has included real vulnerabilities that firewall vendors are now racing to fix. However, this series of events begs a darker question: if NSA has zero-day vulnerability information on all the top firewall brands, what other kinds of information do they have at their disposal to conduct surveillance on civilians and organizations at their discretion?

RECOMMENDED CONTENT

With the ShadowBroker leak of the NSA hacking tool, it has become clear that we are entering into a new "cyber reality," one in which cyber security weapons are not only used for financial gains and industrial espionage, but also to tip the political landscape and gain international influence. And every day, it seems that there are new revelations to this evolving cyberwar. First, political campaigns can be hacked and now we see attackers target popular public opinion media.

Going forward, what if hackers had such power that they could disrupt an entire nation's political stability at their whim? This is previously unchartered and dangerous territory for us. And what's next? Could electronic voting records -- which are certainly enticing in an election year -- be the next target? If a perpetrating group can conduct cyberattacks to influence a nation's political future, financial records, and public opinions, one must ask - "is there anything that is sacred and safe?"

One thing, however, is clear: every nation will be shoring up cyber defenses as well as bolstering aggression capabilities. Where that will lead us in terms of international relations is anyone's guess at this point."

Chris Roberts, Chief Security Architect at Acalvio:

"Frankly, this whole situation is a mess, and armchair experts are getting in the way. When you have a cache of exploits, you have options for financial gain, selling to opposing governments, cash in via bug bounties, or sell to exploit market in general. You don't put it up on the public Internet with a BIN of $500M+. Something is not right somewhere. If you want publicity, you drop one or two of them out…not the entire thing.

If it's Russia, then it doesn't make senses. Same as if it's China or ANY nation state. Why give away your secrets? It's like publishing a list of where ALL your nuclear stuff is stored. There's no logic to it.

One thing is for sure, with all the potential issues, the whole concern of perimeter security being the “way forward” is getting blown to bits. Deceptive security is about to come into the spotlight. We know we can’t keep people out and this just proves it even further!”

Stephen Cobb, senior security researcher at ESET:

“I have no specific data about Shadow Broker but three points need to be made. First, attribution in cyberspace is notoriously difficult, which is extremely frustrating, but that frustration should not tempt people to jump to conclusions. Second, there is clearly a need for greater transparency and wiser policy around government use and/or abuse of zero days. Like many security professionals, I am not comfortable with a government agency withholding information that would help companies secure their data against criminals and foreign adversaries.

RECOMMENDED CONTENT

Third, like many people who have spent a lot of time over the past few decades fighting the deleterious effects of malicious code on our economy, I am not comfortable with the government making and distributing it, as they have been doing for many years now. This is fundamentally a bad idea, and I see no indication that the people who authorize this use of malicious code truly grasp the categorical difference between cyberspace weapons and conventional meatspace weapons.

The situation with government-sponsored malware today is a bit like atomic scientists in the 50s and 60s arguing that radioactive weaponry is a bad idea. Just about everyone agrees that things can and will go wrong, but there is this one particular mindset that thinks it knows better and can manage the risks. Sadly, that same mindset drastically underestimates technology risks in general.”

Greg Leah, principle threat researcher, Cloudmark:

“I believe this is the first time we have seen an auction for cyber weapons or for any data stolen by criminals from a breach. The angle of using bitcoin for the auction I also believe is new.

The criminals clearly feel that the data they have stolen is quite valuable as they suggested in their manifesto that the auction may reach 1 million bitcoin. They also offered to release additional data if the bidding does reach the million bitcoin mark. As of this morning however they had only raised just over 1.76 BTC which is around $1016 USD.

There is also a fair bit of speculation that whoever wrote the manifesto was a native English speaker but was trying to hide that fact by breaking down their English. I am not a linguistics expert but I do find this interesting. I can’t comment on the motivations as to why someone would do that but it does add another angle to the story.”

Andrew McDonnell, Vice President, Security Solutions, AsTech Consulting:

> “It's difficult to be definitive in cases such as this because actors like the NSA have even less incentive to disclose compromise details than corporate victims. From what we can tell, it seems likely that Edward Snowden's analysis is correct in that whoever was responsible for this leak ceased activity around the time of the NSA's response to Snowden. It's possible that we are seeing a single Mass Effect fan who pluralized that identity to confuse investigators.”

Peter Tran, Senior Director at RSA:

> “Assessing and determining hacking legitimacy is a double edged sword and is often judged by the hacker revealing and proving their trove is a unique ground zero "data grab" and not just attributing a hacking group to a government agency based on malware code or tool kit "likeness".
>
> The dark web and hacker underground is an unpredictable and a dynamic arena and motives are difficult to determine as to whether this claim is an attempt to gain mind share for being "loud and proud" much like you would see in hacktivist behavior or a hybrid motive with geopolitical intent. Until the real wizard reveals itself and there are unique bread crumbs to follow, it’s a hacker's game of Chutes and Ladders at best.”

Michael Gorelik, VP of R&D at Morphisec:

> “The Equation Group dump is the next big thing after the publication of the Hacking Team dump (I would go so far as to claim that the Equation dump is even more significant than Hacking Team). Besides the fact that the dump has been analyzed openly by security researchers throughout the community over social outlets like Twitter (unprecedented, in my opinion), this dump revealed Zero-Days (e.g. CVE-2016-6366), and I suspect there are more Zero-Days in the dump (maybe Fortinet?).
>
> It seems that all the exploits and attacks worked smoothly, and the attacks are very well documented and easily applied for the latest versions of Firewall products (like Cisco). This Wednesday, Cisco released a patch for its versions, therefore I strongly recommend to update as soon as possible.
>
> I also assume that the group that leaked the dump has much more Zero-Days in their arsenal, so there is concern about those getting into the wrong hands.”

Jo Webber, CEO, Spirion:

> "First, the contents of this leak should serve as a reminder of the porous nature of endpoint security. It's clear, based on the tools the NSA and undoubtedly others have stockpiled, that attacking and circumventing endpoint security is the path of least resistance into an organization. While it's important to implement endpoint security, there needs to be a greater focus on locating and placing controls on data not simply on the walls around it.

> Second, time and time again sensitive government information with national security and defense implications has been compromised and put on display for the world to see. While the Snowden leaks are in the rear view mirror, the government understands all-too-well that they are a high-profile target for both domestic and international threat actors. With each and every data breach that makes headlines, it becomes painfully clear that there's a staggering gap between understanding where important assets reside and actually taking the steps to protect that information.

> While no single piece of data is 100 percent safe, very few organizations even have the faintest idea of they would identify and categorize their most important data. The example of the Shadow Broker leaks shines a bright light on the fractured state of data security and we will continue to see organizations suffer the same fate until they can get a better grasp on their data sprawl."

bin Daniels, CMO of Vera:

> "We need a renaissance when it comes to security. Information is fluid, and we need to rethink how we approach security because traditional security methods around building bigger walls isn't working. We need to figure out what we're trying to protect, and protect the content itself. Look at the NSA - the National Security Agency has now been breached via inside and outside threats, despite probably having giant walls. Something isn't working when it comes to security and we need to change that. It's a great time to be in security with new security companies looking to solve this problem with many different angles."

Kon Leong, President, CEO and Co-founder of ZL Technologies:

> “A surprising number of data breaches today result from internal behavior and not external threats. Some disagree on which is more difficult to stop— the insider trade or insider raid? Insider raid may be a lot more challenging because it involves understanding, locating, classifying and locking down sensitive information across the organization. To succeed, it’s necessary to have a comprehensive strategy and platform for managing information across the organization.”

Share 30 G+1 3 Tweet RSS

Previous Columns by Eduard Kovacs:
[Industry Reactions to Shadow Brokers Leak: Feedback Friday]
[Mozilla Launches Website Security Testing Tool]
[Security Firm Discloses Medical Device Flaws as Part of Investment Strategy]
[Millennium Hotels & Resorts Investigating Possible PoS Breach]
[Attackers Can Target Enterprises via GroupWise Collaboration Tool]

Tags:
[Cyberwarfare](#) [NEWS & INDUSTRY](#)

0 Comments **SecurityWeek provides information security news and analysis.** 1 **Login**

Recommend Share Sort by Best

Start the discussion…

Be the first to comment.

RECOMMENDED CONTENT

ALSO ON **SECURITYWEEK PROVIDES INFORMATION SECURITY NEWS AND ANALYSIS.**

Dridex Trojan Returns From Summer Vacation

1 comment • 7 days ago•

Scott Kosciuk — Good article. It is also important to point out that the reason for Dridex's resurgence is the fact that AV …

Maxthon Browser Sends Sensitive Data to China

6 comments • a month ago•

realmadpuppy — "malicious actors" ??? The first time I read it in the article I thought typo, but, it is repeated throughout the …

Hadoop Audit and Logging "Back in Time"

1 comment • 2 months ago•

Big Data Analytics Guide — Excellent article, Eddie. Thanks!

UEFI Zero-Day Allows Hackers to Disable Security Features

1 comment • 2 months ago•

Former MS Idiot/Bigot — Once you go Mac, you never go back.

Subscribe Add Disqus to your site Add Disqus Add Privacy

Search

Subscribe to SecurityWeek

Enter Your Email Address Subscribe

RECOMMENDED CONTENT

Most Recent Most Read

- F-Secure's Mikko Hypponen Talks Cyber Crime and Cyber Unicorns
- Industry Reactions to Shadow Brokers Leak: Feedback Friday
- Locky Ransomware Switches to DLLs for Distribution
- Mozilla Launches Website Security Testing Tool
- Answering the "So What" Question on Cyber Threat Intelligence
- Machine Learning CrowdStrike Joins VirusTotal
- Apple Issues Emergency Fix for iOS Zero-Days: What You Need to Know
- Security Firm Discloses Medical Device Flaws as Part of Investment Strategy
- Critical Vulnerabilities Affect Open Source Base Transceiver Stations
- Millennium Hotels & Resorts Investigating Possible PoS Breach

Discussion

- People
- Recent
- Popular

Recent Comments

- Gurupreet Malhotra

  very nice article, thanks...

  What Your Security Team Can Learn From the Olympics · 1 day ago

- Marcus Bloodworth

  VERY interesting, informative, and well thought article. I noticed little commentary, and I have included your work as a cited reference to my blog. http://mdbloodworth.wixsite.co......

  Firmware, Controllers, and BIOS: Subterranean Malware Blues · 2 days ago

- Joe Colby

  Great article and history lesson! As big data gets bigger and threat actors get more creative machine learning and behavior analytics options are on the rise. You have to have a baseline of what...

  Shall We Play a Game? It's a SIEM-ple Question. · 3 days ago

community on DISQUS

Popular Topics

- Information Security News
- IT Security News
- Risk Management
- Cybercrime
- Cloud Security
- Application Security
- Smart Device Security

Security Community

- IT Security Newsletters
- Suits and Spooks
- ICS Cyber Security Conference

- CISO Forum
- InfosecIsland.Com

Stay Intouch

- Twitter
- Facebook
- LinkedIn Group
- Cyber Weapon Discussion Group
- RSS Feed
- Submit Tip
- Security Intelligence Group

RECOMMENDED CONTENT

bout SecurityWeek

- Team
- Advertising
- Events
- Writing Opportunities
- Feedback
- Contact Us

Wired Business Media