🔍

ARSGERA - FOTOLIA

The Shadow Brokers cancels the auction of NSA cyber weapons

💬 | 🔗

by
Michael Heller
Senior Reporter

Published: 17 Oct 2016

🐦 G+ in ✉

The first auction of NSA cyber weapons didn't generate much money for the Shadow Brokers, so the group is changing tactics with a direct sale of the files.

THIS ARTICLE COVERS
Malware ▶▶

+ Show More

f

🐦

G+

in

🖶

The auction of NSA cyber weapons didn't go as planned but the Shadow Brokers are still hoping for a big payday by ditching the auction format in favor of a more direct crowdfunding scheme.

The Shadow Brokers have a cache of cyber weapons and exploits from the advanced persistent threat group known as the Equation Group, which was said to be tied to the NSA. Per the rules of the original auction, the highest bidder would receive the files and the Shadow Brokers promised to release more files if the total bidding reached 1 million bitcoin. However, the auction went badly with bids totaling just 1.76 bitcoin and a high bid of 0.08 bitcoin.

"We prefer sell in bulk to more responsible party. One more likely to disclose than hurt peoples," the Shadow Brokers wrote before ending the auction. "Maybe a government, security company, wealth[y] individual step up, do [right] thing, get seen doing it. If not, we assume no one interested and we start selling on the underground. Lots of transparency and disclosure there. This how much they care about peoples personal data, financial info, and security, 1.5btc."

With the new conditions of sale the Shadow Brokers have a much more modest goal of 10,000 bitcoin and if that goal is met, they will publicly post the password to the dump of NSA cyber weapons. The Equation Group files have been verified with a limited release of the data and the Shadow Brokers claim to have more unreleased files; Shadow Brokers has claimed that it released only 60% of its alleged cache of cyberweapons.

PRO+
Content

E-Handbook
How to prevent ransomware or recover from a ransomware breach

E-Handbook
How to buy the best antimalware tools to protect endpoints

E-Zine
Emerging security threats from every which way

"You seeing 'Firewalls' toolkit, includes remote exploits, privilege escalations, persistence mechanisms, [remote access Trojans], LPs, and post-exploit collection utilities. Complete package for to run own operations. TheShadowBrokers is having more Equation Group tool kits for other platforms Windows, Unix/Linux, Routers, Databases, Mobile, Telecom. Newer revisions too," the Shadow Brokers wrote. "The auction file is toolkit for one of other platforms. Includes remote exploits, local exploits/privilege escalations, persistence mechanisms, RATs, LPs, post-exploit collection utilities. Value estimated in millions of euros/dollars."

The Shadow Brokers initially released 300Mb of files which experts said were genuine and included exploits for Cisco and Juniper product vulnerabilities.

Michael Heller asks:

What do you think of the sale of NSA cyber weapons by the Shadow Brokers?

0 Responses

Join the Discussion

⮷ Next Steps

Learn more about the leaked Cisco vulnerability found in the Shadow Brokers dump.

Find out what the NSA cyber weapons release means for advanced attack defense.

Get info on the questions surrounding the Shadow Brokers cyber weapons dump.

⮷ Dig Deeper on Malware, Viruses, Trojans and Spyware

ALL   NEWS   GET STARTED   EVALUATE   MANAGE   PROBLEM SOLVE
▲

📄 **Odinaff banking Trojan linked to Carbanak group, attacks SWIFT**

📄 **Release of Mirai IoT botnet malware highlights bad password security**

📄   **Even with rise in crypto-ransomware, majority do not pay**

📄   **How did a malicious app slip past Google Play app store security?**

Load More

💬 **0 comments**   Oldest ▼

☑ Send me notifications when other members comment.

Register or **Login**

E-Mail

email@techtarget.com

Username / Password

Username

Password

Comment

By submitting you agree to receive email from TechTarget and its partners. If you reside outside of the United States, you consent to having your personal data transferred to and processed in the United States. Privacy

LOUD SECURITY   NETWORKING   CIO   CONSUMERIZATION   ENTERPRISE DESKTOP   CLOUD COMPUTING

SearchCloudSecurity

PaaS security: Four rules for lowering enterprise risks

Securing a platform as a service can sometimes get overlooked within enterprises. Expert Char Sample offers four simple rules for...

How to handle cloud-based big data strategies according to the CSA

Assembling big data strategies is a nuanced process, but the Cloud Security Alliance offers guidance on some best practices. ...

About Us   Contact Us   Privacy Policy   Videos   Photo Stories   Guides

Advertisers   Business Partners   Media Kit   Corporate Site   Experts   CPE and CISSP Training

Reprints   Archive   Site Map   Events   E-Products