This Content Component encountered an error

SERGEY NIVENS - FOTOLIA

FBI accused of paying Carnegie Mellon $1M to hack Tor network

2

by
Michael Heller
Senior Reporter

Published: 13 Nov 2015

The Tor Project said that the Carnegie Mellon researchers behind an attack on the hidden service subsystem carried out last year were paid $1 million by the FBI to hack Tor network.

THIS ARTICLE COVERS
Web Security Tools and Best Practices

LOOKING FOR SOMETHING ELSE?
Windows 10 security fixes longtime OS vulnerabilities
Google wants sites to disable SSLv3 to boost Web security
Hackers hijack website analytics for black hat SEO and more

+ Show More

The Tor Project claimed it has learned more about an attack on its Deep Web hidden service subsystem that was detected in July of 2014. The Tor Project

said that the Carnegie Mellon researchers responsible for the attempt to hack Tor's network were hired by the FBI and paid "at least $1 million."

According to a Tor Project blog post by Roger Dingledine, Tor Project director, the FBI paid researchers to attack hidden services users in an effort to find data that would allow the FBI to then accuse people of crimes. Dingledine said it is unlikely that a valid warrant could have been obtained for the attack because "it was not narrowly tailored to target criminals or criminal activity, but instead appears to have indiscriminately targeted many users at once."

In July 2014, the Tor Project announced that it had found evidence that attackers were attempting to deanonymize users, and linked the servers used in the attacks to the techniques described in a cancelled talk at Black Hat 2014 by Carnegie Mellon researchers Alexander Volynkin and Michael McCord, which claimed to demonstrate such a way to hack Tor.

Carnegie Mellon refused to comment to SearchSecurity on the subject of Tor, but Ed Desautels, senior writer/editor for the public relations department of Carnegie Mellon University's Software Engineering Institute, did not exactly deny the allegations.

"I'd like to see the substantiation for their claim," Desautels told Wired. "I'm not aware of any payment."

A
is
cl

"\
a
o
e

weaknesses in the software and designs."

However, Dingledine said in the blog post that this could be a case of law enforcement believing it can "circumvent the rules of evidence" by hiring universities to perform police work.

"If academia uses 'research' as a stalking horse for privacy invasion, the entire enterprise of security research will fall into disrepute," Dingledine wrote. "Legitimate privacy researchers study many online systems, including social networks -- if this kind of FBI attack by university proxy is accepted, no one will have meaningful Fourth Amendment protections online and everyone is at risk."

Robert Hansen, vice president of WhiteHat Labs at WhiteHat Security, said the questions over invasion of privacy are made much more difficult because the Deep Web can be used for both legitimate and illegal activity.

"No one doing anything illegal should have an expectation of privacy unless the law specifically protects that speech -- for instance while talking to your lawyer," Hansen said. "However, there is much about Tor that is simply used to prevent people from tracking you, which is not at all illegal and may actually be critical to your own well-being. For instance, people who are regularly cyber-stalked by abusive exes, or political dissidents, as an example, have not only an expectation of privacy but a deep need for it."

Dingledine also said that the attacks may have crossed an ethical line.

"Such action is a violation of our trust and basic guidelines for ethical research," Dingledine wrote. "We strongly support independent research on our software and network, but this attack crosses the crucial line between research and endangering innocent users."

Hansen said that while it is still unclear if Carnegie Mellon was behind the attacks or whether the FBI paid the university, there could be legal implications for anyone found responsible.

"It's quite possibly a case of hacking, and as such they would be just as culpable under existing hacking laws as any other hacker," Hansen said. "There may be some carve-out for national security that the government could use to shield [Carnegie Mellon], as the government did with the case the EFF brought against them regarding the AT&T and NSA partnership. Carnegie Mellon may have fully believed they were doing something that the government needed and saw it as a civic duty."

Dr. Chase Cunningham, head of threat research and development for Armor Defense Inc., said that answering questions over who was responsible and whether the FBI paid for attempts to hack Tor can have major ramifications on how the actions are viewed.

"The main difference is really a philosophical one; did [Carnegie Mellon] do it solely because they got paid and essentially had a bug contract out on Tor? Or did they do it because they saw a chance to break something that everyone said was basically unbreakable," Cunningham said. "From what I know, I'm sure the money didn't hurt, but there have always been lots of groups, schools, and organizations wanting to break Tor simply to say 'we did it.' The folks at Carnegie Mellon just happened to have the right talent, timing and techniques to actually do it. The money was really just universal grease; it

eased the need for tools personnel, and access to make the break happen."

Michael Heller asks:

What policies does your enterprise have in place around using Tor?

0 Responses

Join the Discussion

Next Steps

Learn why one security researcher believes the security industry is broken.

Find out how Tor vulnerabilities made the Dark Web too risky for the black market.

Learn more about how the Dark Web is enabling the malware industry.

Dig Deeper on Web Security Tools and Best Practices

ALL | NEWS | GET STARTED | EVALUATE | PROBLEM SOLVE

- Windows 10 security fixes longtime OS vulnerabilities
- Google wants sites to disable SSLv3 to boost Web security
- Hackers hijack website analytics for black hat SEO and more
- IT pros don't get cybersecurity risks around certificate authorities

Load More

2 comments

Oldest ▼

Share your comment

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

ncberns — 13 Nov 2015 6:17 AM

It's really hard to wrap my head around the absurdity of this. One of the organizations tasked with preventing data breaches just shelled out $1M to hack a network...? Yes, they're right, there are things going on there that they might not like. I, on the other hand, don't like anyone breaking into my space, no matter the validity of the hack.

ToddN2000 — 13 Nov 2015 7:23 AM

Let's get the lawyers involved ! I wouldn't be surprised. With what Snowden was saying about the NSA, this would not shock me one bit. If you are doing illegal acts on the internet then it's a use at your own risk. If they have to got outside to find help to hack a system, how good is their own protection?? I would say not as good as what they are trying to hack.

Latest TechTarget resources

CLOUD SECURITY

NETWORKING

CIO

CONSUMERIZATION

ENTERPRISE DESKTOP

CLOUD COMPUTING

COMPUTER WEEKLY

SearchCloudSecurity

How to craft an enterprise cloud change management policy

Though few enterprises have one, a cloud change management policy can be a lifesaver when confronted with transitions and ...

Blue Coat acquires Elastica in $280 million CASB deal

After acquiring Perspecsys this summer, Blue Coat Systems makes another CASB deal for Elastica to further strengthen its cloud ...