FBI Admits It Controlled Tor Servers Behind Mass Malware Attack

Kevin Poulsen ⋮ 7-9 minutes ⋮ 9/13/2013

It wasn't ever seriously in doubt, but the FBI yesterday acknowledged that it secretly took control of Freedom Hosting last July, days before the servers of the largest provider of ultra-anonymous hosting were found to be serving custom malware designed to identify visitors.

Freedom Hosting's operator, Eric Eoin Marques, had rented the servers from an unnamed commercial hosting provider in France, and paid for them from a bank account in Las Vegas. It's not clear how the FBI took over the servers in late July, but the bureau was temporarily thwarted when Marques somehow regained access and changed the passwords, briefly locking out the FBI until it gained back control.

The new details emerged in local press reports from a Thursday bail hearing in Dublin, Ireland, where Marques, 28, is fighting extradition to America on charges that Freedom Hosting facilitated child pornography on a massive scale. He was denied bail today for the second time since his arrest in July.

Freedom Hosting was a provider of turnkey “Tor hidden service” sites — special sites, with addresses ending in .onion, that hide their geographic location behind layers of routing, and can be reached only over the Tor anonymity network. Tor hidden services are used by sites that need to evade surveillance or protect users' privacy to an extraordinary degree – including human rights groups and journalists. But they also appeal to serious criminal elements, child-pornography traders among them.

On August 4, all the sites hosted by Freedom Hosting -- some with no connection to child porn -- began serving an error message with hidden code embedded in the page. Security researchers dissected the code and found it exploited a security hole in Firefox to identify users of the Tor Browser Bundle, reporting back to a mysterious server in Northern Virginia. The FBI was the obvious suspect, but declined to comment on the incident. The FBI also didn't respond to inquiries from WIRED today.

But FBI Supervisory Special Agent J. Brooke Donahue was more forthcoming when he appeared in the Irish court yesterday to bolster the case for keeping Marques behind bars, according to local press reports. Among the many arguments Donahue and an Irish police inspector offered was that Marques might reestablish contact with co-conspirators, and further complicate the FBI probe. In addition to the wrestling match over Freedom Hosting's servers, Marques allegedly dove for his laptop when the police raided him, in an effort to shut it down.

Donahue also said Marques had been researching the possibility of moving his hosting, and his residence, to Russia. "My suspicion is he was trying to look for a place to reside to make it the most difficult to be extradited to the U.S.," said Donahue, according to the *Irish Independent*.

Freedom Hosting has long been notorious for allowing child porn to live on its servers. In 2011, the hactivist collective Anonymous singled out the service for denial-of-service attacks after allegedly finding the firm hosted 95 percent of the child porn hidden services on the Tor network. In the hearing yesterday, Donahue said the service hosted at least 100 child porn sites with thousands of users, and claimed Marques had visited some of the sites himself.

Reached by phone, Marques' lawyer declined to comment on the case. Marques faces federal charges in Maryland, where the FBI's child-exploitation unit is based, in a case that is still under seal.

The apparent FBI-malware attack was first noticed on August 4, when all of the hidden service sites hosted by Freedom Hosting began displaying a “Down for Maintenance” message. That included at least some lawful websites, such as the secure email provider TorMail.

Some visitors looking at the source code of the maintenance page realized that it included a hidden `iframe` tag that loaded a mysterious clump of Javascript code from a Verizon Business internet address. By midday, the code was being circulated and dissected all over the net. Mozilla confirmed the code exploited a critical memory management vulnerability in Firefox that was publicly reported on June 25, and is fixed in the latest version of the browser.

Though many older revisions of Firefox were vulnerable to that bug, the malware only targeted Firefox 17 ESR, the version of Firefox that forms the basis of the Tor Browser Bundle – the easiest, most user-friendly package for using the Tor anonymity network. That made it clear early on that the attack was focused specifically on de-anonymizing Tor users.

Tor Browser Bundle users who installed or manually updated after June 26 were safe from the exploit, according to the Tor Project's security advisory on the hack.

The payload for the Tor Browser Bundle malware is hidden in a variable called "magneto."

Perhaps the strongest evidence that the attack was a law enforcement or intelligence operation was the limited functionality of the malware.

The heart of the malicious Javascript was a tiny Windows executable hidden in a variable named “Magneto.” A traditional virus would use that executable to download and install a full-featured backdoor, so the hacker could come in later and steal passwords, enlist the computer in a DDoS botnet, and generally do all the other nasty things that happen to a hacked Windows box.

But the Magneto code didn't download anything. It looked up the victim’s MAC address -- a unique hardware identifier for the computer’s network or Wi-Fi card -- and the victim's Windows hostname. Then it sent it to a server in Northern Virginia server, bypassing Tor, to expose the user's real IP address, coding the transmission as a standard HTTP web request.

“The attackers spent a reasonable amount of time writing a reliable exploit, and a fairly customized payload, and it doesn’t allow them to download a backdoor or conduct any secondary activity," said Vlad Tsyrklevich, who reverse-engineered the Magneto code, at the time.

The malware also sent a serial number that likely ties the target to his or her visit to the hacked Freedom Hosting-hosted website.

The official IP allocation records maintained by the American Registry for Internet Numbers show the two Magneto-related IP addresses were part of a ghost block of eight addresses that have no organization listed. Those addresses trace no further than the Verizon Business data center in Ashburn, Virginia, 20 miles northwest of the Capital Beltway.

The code's behavior, and the command-and-control server's Virginia placement, is also consistent with what's known about the FBI’s "computer and internet protocol address verifier," or CIPAV, the law enforcement spyware first reported by WIRED in 2007.

Court documents and FBI files released under the FOIA have described the CIPAV as software the FBI can deliver through a browser exploit to gather information from the target’s machine and send it to an FBI server in Virginia. The FBI has been using the CIPAV since 2002 against hackers, online sexual predators, extortionists, and others, primarily to identify suspects who are disguising their location using proxy servers or anonymity services, like Tor.

Prior to the Freedom Hosting attack, the code had been used sparingly, which kept it from leaking out and being analyzed.

No date has been set for Marques' extradition hearings, but it's not expected to happen until next year.