Main Menu ▾   My Stories: 24 ▾   Forums   Subscribe   Jobs   Log In
                                                                                    Search

LAW & DISORDER / CIVILIZATION & DISCONTENTS

Alleged Tor hidden service operator busted for child porn distribution

Freedom Hostings's alleged founder held in Ireland, facing extradition to US.

by **Sean Gallagher** - Aug 4 2013, 8:00pm UTC   HACKING   INTERNET CRIME   THE WEB   34

Catherine Scott

On Friday, Eric Eoin Marques, a 28 year-old Dublin resident, was arrested on a warrant from the US on charges that he is, in the words of a FBI agent to an Irish court, "the largest facilitator of child porn on the planet." The arrest coincides with the disappearance of a vast number of "hidden services" hosted on Tor, the anonymizing encrypted network.

Marques is alleged to be the founder of Freedom Hosting, a major hidden services hosting provider. While Marques' connection to Freedom Hosting was not brought up in court, he has been widely connected to the service—as well as the Tormail anonymized e-mail service and a Bitcoin exchange and escrow service called Onionbank—in discussions on Tor-based news and Wiki sites. All those services are now offline. And prior to disappearing, the sites hosted by Freedom Hosting were also distributing malware that may have been used to expose the users of those services.

Tor hidden services are a lesser known part of the Tor "darknet." They are anonymized Web sites, mail hosts, and other services which can only be reached by computers connected to Tor, or through a Tor hidden services proxy website, such as tor2web.org, and they have host names ending in .onion.

Hidden services are used for a wide range of purposes, both for good and ill. The *New Yorker*, for example, uses a hidden service to host its Strongbox communications setup, which allows anonymous communication with editors. (Full disclosure: The *New Yorker*, like Ars, is a Condé
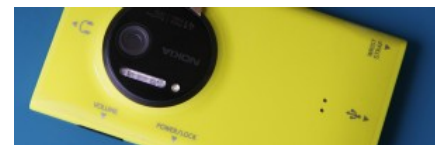
Nast publication). Other hidden services are often used to conceal criminal enterprises; The Hidden Wiki provides an index of a variety of hidden services offering "skimmed" credit card numbers, anonymized Bitcoin "wallet" services, and fake IDs.

Freedom Hosting was one of a number of hosting providers specializing in hidden services. The business—which is in no way connected to the Tor Project, which encompasses the operators of the Tor network itself—also became notorious for allegedly hosting a significant number of child pornography sites, as well as Hidden Wiki sites that were used to provide child porn traffickers with a way to post links to their wares for distribution. For that reason, it became a major target of members of Anonymous, who launched denial of service attacks on Freedom Hosting and tried to "dox" child pornographers using the service.

According to a Sunday blog post by the Tor Project's Executive Director, Andrew Lewman, the servers of Freedom Hosting were breached before the service went offline. "From what is known so far, the breach was used to configure the server in a way that it injects some sort of JavaScript exploit in the Web pages delivered to users," Lewman wrote. "This exploit is used to load a malware payload to infect user's computers. The malware payload could be trying to exploit potential bugs in Firefox 17 ESR, on which our Tor Browser is based. We're investigating these bugs and will fix them if we can."

The malware injected by the exploit could have been used as part of an attempt to expose the users of Freedom Hosting's services. The JavaScript initially redirected requests to Freedom Hosting sites to an IP address of a Verizon Business customer located outside Washington, DC.

The servers themselves are likely run on a "bulletproof" hosting service in Romania or Russia; Irish law enforcement authorities told the court Friday that Marques had transferred large sums of money to accounts in Romania and had been investigating obtaining a visa to enter Russia. Marques, for his part, claimed that he was helping out friends in Romania, including an ex-girlfriend, by sending them money, and that his visa inquiries were out of curiosity over the plight of NSA whistleblower Edward Snowden.

READER COMMENTS   34

| 57 | 6 | 155 | | 2 |
| Like | | Tweet | | |

Sean Gallagher / Sean is Ars Technica's IT Editor. A former Navy officer, systems administrator, and network systems integrator with 20 years of IT journalism experience, he lives and works in Baltimore, Maryland.

Follow @thepacketrat

← OLDER STORY   NEWER STORY →

YOU MAY ALSO LIKE
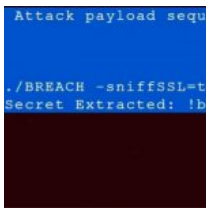
Gone in 30 seconds: New attack plucks secrets from HTTPS-protected pages

"NASDAQ is owned." Five men charged in largest financial hack ever

Arrested suspect denies that DEA-seized bitcoins are his

Hard drive-wiping malware that hit South Korea tied to military espionage

Rampant Apache website attack hits visitors with highly malicious software

UK prime minister lambasts search engines, seeks porn filter blacklist

"The cutting edge of cybercrime" —Lulzsec hackers get up to 32 months in jail

Japanese police ask ISPs to start blocking Tor

SITE LINKS

About Us

Advertise with us

Contact Us

Reprints

SUBSCRIPTIONS

Subscribe to Ars

MORE READING

RSS Feeds

Newsletters

CONDE NAST SITES

Reddit

Wired

Vanity Fair

Style

Details

Visit our sister sites ▼

Subscribe to a magazine ▼

VIEW MOBILE SITE