The Hacker News™
Security in a serious way
+1,680,990 270,800 1,102,000

Former Tor Developer Cr to Unmask Tor Users

Wednesday, April 27, 2016 Swati Khandelwal

IN BRIEF

According to an investigation, Matthew Edman, a cyber security expert and former employee of the Tor Project, helped the FBI with Cornhusker a.k.a Torsploit malware that allowed Feds to hack and unmask Tor users in several high-profile cases, including Operation Torpedo and Silk Road.

Do you know who created malware for the FBI that allowed Feds to unmask Tor users?

It's an insider's job... A former Tor Project developer.

In an investigation conducted by Daily Dot journalists, it turns out that **Matthew J. Edman**, a former part-time employee of Tor Project, created malware for the Federal Bureau of Investigation (FBI) that has been used by US law enforcement and intelligence agencies in several investigations, including Operation Torpedo.

Matthew Edman is a computer scientist who specializes in cyber security and investigations and joined the Tor Project in 2008 to build and enhance Tor software's interactions with Vidalia software, cross-platform GUI for controlling Tor.

After 2009, Matthew was hired by a contractor working for defense and intelligence agencies, including the FBI, to develop an anti-Tor malware.

> The Tor Project has also confirmed the same, saying, "It has come to our attention that Matt Edman, who worked with the Tor Project until 2009, subsequently was employed by a defense contractor working for the FBI to develop anti-Tor malware."

Moreover, the team said Edman worked only on the Vidalia project that Tor dropped in 2013 and replaced it with other tools designed to improve the user experience.

Also Read: How Hacking Team and FBI planned to Unmask A Tor User.

Cases Solved with the Help of Former Tor Developer

Since 2012, Edman has been working at Mitre Corporation as a senior cyber security engineer assigned to the FBI's internal team, dubbed *Remote Operations Unit*, that develops or purchases exploits and hacking tools for spying on potential targets.

Due to his work for the Tor Project, Edman became an FBI contractor assigned a task to hack Tor as part of Operation Torpedo, a sting operation to identify owners and patrons of Dark Net child pornography websites that used Tor.

Also Read: How Spies Could Unmask Tor Users without Cracking Encryption.

Besides working on Operation Torpedo, Edman also helped the federal agency shut down Silk Road, the first most popular DarkNet drug marketplace, and arrest its convicted creator Ross Ulbricht.

According to testimony, it was Edman who did almost everything from tracking *$13.4 Million in Bitcoins from Silk Road* to tracing Ulbricht's laptop, which played a significant role in Ulbricht being convicted and sentenced to the life term in prison.

Cornhusker/Torsploit Malware to Unmask Tor Users

To unmask Tor users, Edman worked closely with FBI Special Agent Steven A. Smith to develop and deploy malware, dubbed "**Cornhusker**" or "**Torsploit**," that collect identifying information on Tor users.

Tor is an anonymity software used by millions of people, including government officials, human rights activists, journalists and, of course, criminals around the world to keep their identity hidden while surfing the Internet.

This is why, the Tor software is used by people to visit Dark Net websites, like child pornography sites, which are inaccessible via standard web browsers.

The Cornhusker malware exploited vulnerabilities in Adobe Flash Player to reveal Tor users' actual IP address to an FBI servers outside the Tor network.

Also Read: FBI paid $1 Million to University Researchers for Unmasking Tor Users.

The agency hijacked and placed Cornhusker on three servers that ran multiple anonymous child pornography websites. The malware then targeted the flaws in Flash inside the Tor Browser.

Adobe Flash Player has long been considered as unsafe by many security experts, and the Tor Project has long warned against using it. However, many people, including the dozens revealed in Operation Torpedo, make use of Flash inside their Tor Browser.

Though, according to court documents, Cornhusker is no longer in use, the FBI is using its own funded "Network Investigative Technique" (NIT) to obtain IP and MAC addresses of Tor users in the course of investigations.

However, the so-called network investigative technique has been considered as invalid by the court during a hearing on the burst of the world's largest dark web child pornography site, **PlayPen**.

On Monday, the opposition lawyers have filed a motion against the FBI to reveal the full source code of the malware it used to hack suspected visitors of PlayPen, or simply drop the case.

About the Author:

Swati Khandelwal Swati Khandelwal is Senior Technical Writer and Security Analyst at The Hacker News. She is a Technology Enthusiast with a keen eye on the Cyberspace and other tech related developments.

Adobe Flash Player, Child Pornography, Cornhusker, Dark Web Search Engine, FBI, Malware, Matt Edman, Silk Road, Tor Anonymity Network, Tor Hidden Service, Torsploit, Unmask Tor User

Latest Stories

In-Brief: Telegram Vulnerability, Malware in Nuclear Plant, Anti-Tor Malware and Hotpatching Exploit

Child Porn Suspect Held in Jail for 7 Months for refusing to Decrypt Hard Drives

Former Tor Developer Created Malware for FBI to Unmask Tor Users

PLATINUM Hackers Hijack Windows Hotpatching to Stay Hidden

This Tiny Computer has no Battery, Powered Wirelessly from Radio Waves

For the First time, FBI discloses a Flaw to Apple, but it's already Patched!

Pro-ISIS Hackers release 'Kill List' Of 43 United States Officials

In-Brief: Spotify Hack, Secret of Chrome OS, MIT Bug Bounty, Nanowire Batteries

Laser Gun to Detect Bombs and Chemical Weapons from 100 Feet Away

DDoS Extortionists made $100,000 without Launching a Single Attack

Comments (7)

6 Comments Sort by Oldest

Add a comment...

Ilyass TheCoder - Researcher at Kaspersky Lab
Mother F*******
Like · Reply · 4 · 20 hrs

Ricardas Svetainius - Vilnius, Lithuania
Axujet
Like · Reply · 18 hrs

Carl Vancil - Little Rock, Arkansas
...and you can bet that within seconds of Matt Edman's name being published that several entities worldwide put a price on his head. If you're going to go up against some of the most powerful and intelligent cyber-criminals in the world, you should do *everything* to ensure that your own identity is **never compromised**.

I would bet that elements of ISIS, the Syrian Electronic Army, and anyone connected to the Tor based murder-for-hire boards will be actively hunting to get into Matt's life and destroy him, utterly, for what he's participated in. While the media and law enforcement are a... See More
Like · Reply · 1 · 18 hrs

George Cantrell
Hopefully it will be a brutal execution for such a traitor to the human race and the cause of privacy.
Like · Reply · 12 hrs

Ayush Sharma - Assistant Manager at Jovial Folks Creations
And now he'd be a criminal for criminals!
Like · Reply · 1 · 15 hrs

George Cantrell
I hope to read about this lowlife scumbag motherfucker being found dead from a brutal murder, along with as many of his handlers as possible, of course. A bastard like this and his employers do not deserve to breathe the same atmosphere as the human race.
Like · Reply · 12 hrs

Kira Slith
Figures, this guy is going to end up with a lot of hits out on his ass now his name has been revealed, worse still the FBI isn't going to reveal it's exploit code because it's the same one they've been using to hunt terrorists. so its gone and caused a whole fuss and officially the FBI won't be able nail the PlayPen case.
Like · Reply · 4 hrs

Facebook Comments Plugin

TRENDING STORIES

Bank with No Firewall. That's How Hackers Managed to Steal $80 Million

Hacker Installed a Secret Backdoor On Facebook Server to Steal Passwords

How Did Hackers Who Stole $81 Million from Bangladesh Bank Go Undetected?

In-Brief: Spotify Hack, Secret of Chrome OS, MIT Bug Bounty, Nanowire Batteries

This Tiny Computer has no Battery, Powered Wirelessly from Radio Waves

I keep 200+ Browser Tabs Open, and My Computer Runs Absolutely Fine. Here's My Secret.

FBI paid Hacker $1.3 Million to Unlock San Bernardino Shooter's iPhone

DDoS Extortionists made $100,000 without Launching a Single Attack

Opera Browser Now Offers Free and Unlimited Built-in VPN Service

More than 1 million People now access Facebook Over Tor Network