FBI suspected of cyber-attack on anonymous web-hosting and email services

Mark Blackwood
12 August 2013

On August 5 malicious software (malware) in the form of a Java Script (JS) attack code was discovered embedded in multiple websites hosted by the anonymous hosting company Freedom Hosting (FH), the largest hosting company on the anonymous Tor network. Initial research into the malware by experts suggests that it originated from and returned private data back to the Federal Bureau of Investigation (FBI) or other US government agencies.

The malicious script was specifically designed to attack and exploit vulnerabilities within the Firefox 17 web browser, included within older versions of the Tor Browser Bundle (TBB), which allows for anonymous Internet access.

An announcement of the attack was made by the Tor Anonymity project, which stated, “An attack that exploits Firefox vulnerability in JavaScript has been observed in the wild. Specifically, Windows users using the Tor Browser Bundle (which includes Firefox plus privacy patches) appear to have been targeted.” It advised anyone using an older version of the Tor Browser Bundle (TBB) to update to the latest August 9 release immediately.

The detection of the malicious code coincided with the arrest of Eric Eoin Marques, the alleged administrator of FH, on suspicion that the company, which hosts a vast array of servers, had been hosting sites linked to child pornography. Shortly after Marques’ arrest every website hosted by FH was taken offline simultaneously, including the anonymous email service Tor Mail.

Owing to the fact that the TBB can inhibit the collection of data on a person’s online activities and connect it to his or her name, address, age, phone number, etc., the software has become increasingly popular, as has the free anonymous means of online communication offered by Tor Mail.

This is especially the case in the wake of the US government’s persecution of whistleblower Edward Snowden. The former intelligence contractor exposed mass internet surveillance by the US government’s National Security Agency (NSA) and its allies internationally. For disclosing these activities, Snowden has been subjected to an unprecedented international manhunt, stripped off his passport, and forced to seek temporary asylum in Russia.

TBB is used to access services on the “deep net” (servers not indexed by standard search engines) such as Tor Mail, which until August 5 had the capacity to enable anyone to safely leak information relating to government corruption, oppression and human rights abuses, without fear of being detected or having their anonymity compromised.

The goal of Tor Mail was to provide for free a completely anonymous means of email communication to anyone who needed it. As such, it had earned a reputation as being the most anonymous email operation online.

The servers accessed by Tor, now portrayed as an arena inhabited solely by criminal elements, have been used widely by human rights groups, journalists, whistle-blowers, protesters and political dissidents worldwide, as well as members of the wider public who value their right to privacy.

That is why the circulation of a malicious code that has the capacity to unmask and compromise a person’s anonymity is of great concern to those who have relied on the TBB and Tor Mail as a means of anonymous communication.

Claims that the attack only affects, or should be of concern to, those engaged in criminal activities online is false.

In order to carry out the attack, the FH servers housing the websites and services were compromised, meaning that their owners have also been unmasked. Owing to the fact that FH was considered a trusted anonymous hosting service, the owners of Tor Mail will also have considered themselves anonymous and therefore could not have been forced to reveal anything about a Tor Mail user to law enforcement agencies.

Should Marques turn out to be the owner of FH as has been reported, however, it would confirm that FH security has been breached. That being the case, every owner of "deep net" websites and services including Tor Mail housed on FH could have lost their mask of anonymity in the attack. Since the attack, Tor Mail has remained inaccessible.

The attack code released last week, according to *Wired.org*, "exploited memory management vulnerability, forcing Firefox to send a unique identifier to a third-party server using a public IP address that can be linked back to the person's ISP."

Vlad Tsrklevich, a reverse-engineer who analysed the code, explained how the attack works. It "contained several hallmarks of professional malware development, including 'heap spraying' techniques to bypass Windows security protections and the loading of executable code that prompted compromised machines to send the identifying information to a server located in Virginia." Many specialized functions of the FBI and other US spy agencies are located at facilities in Virginia.

As *Wired.org* points out, the malware "is likely the first sample captured in the wild" of the FBI's Computer and Internet Protocol Address Verifier or CIPAV. On August 8 *Wired.org* cited court documents and FBI files released under the Freedom of Information Act which described 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."

As alarming as this is, it is only one part of the massive state assault being carried out against internet privacy.

Only last week Lavabit, the secure communications company used by Snowden, reluctantly shut down its email services after having been subjected to a gag order and pressure from the US government to open up its servers to the authorities for inspection.

Likewise Silent Circle, in a pre-emptive move to protect its secure email users, also shut down its secure email services, out of fear that it could be next on the US government's hit list.

The most recent developments takes these attacks to another level. As technology experts have pointed out, under the guise of ridding the deep net of illegal content, Tor Mail has effectively been put out of action as the apparent outcome of a cyber-attack enacted by US law enforcement agencies.