If You Used This Secure Webmail Site, the FBI Has Your Inbox

27. Januar 2014

By Kevin Poulsen, wired.com

While investigating a hosting company known for sheltering child porn last year the FBI incidentally seized the entire e-mail database of a popular anonymous webmail service called TorMail.

Now the FBI is tapping that vast trove of e-mail in unrelated investigations.

The bureau's data windfall, seized from a company called Freedom Hosting, surfaced in court papers last week when prosecutors indicted a Florida man for allegedly selling counterfeit credit cards online. The filings show the FBI built its case in part by executing a search warrant on a Gmail account used by the counterfeiters, where they found that orders for forged cards were being sent to a TorMail e-mail account: “platplus@tormail.net.”

Acting on that lead in September, the FBI obtained a search warrant for the TorMail account, and then accessed it from the bureau's own copy of “data and information from the TorMail e-mail server, including the content of TorMail e-mail accounts,” according to the complaint sworn out by U.S. Postal Inspector Eric Malecki.

The tactic suggests the FBI is adapting to the age of big-data with an NSA-style collect-everything approach, gathering information into a virtual lock box, and leaving it there until it can obtain specific authority to tap it later. There's no indication that the FBI searched the trove for incriminating evidence before getting a warrant. But now that it has a copy of TorMail's servers, the bureau can execute endless search warrants on a mail service that once boasted of being immune to spying.

“We have no information to give you or to respond to any subpoenas or court orders,” read TorMail's homepage. “Do not bother contacting us for information on, or to view the contents of a TorMail user inbox, you will be ignored.”

In another e-mail case, the FBI last year won a court order compelling secure e-mail provider Lavabit to turn over the master encryption keys for its website, which would have given agents the technical ability to spy on all of Lavabit's 400,000 users – though the government said it was interested only in one. (Rather than comply, Lavabit shut down and is appealing the surveillance order).

TorMail was the webmail provider of choice for denizens of the so-called Darknet of anonymous and encrypted websites and services, making the FBI's cache extraordinarily valuable. The affair also sheds a little more light on the already-strange story of the FBI's broad attack on Freedom Hosting, once a key service provider for untraceable websites.

Freedom Hosting specialized in providing 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 those seeking to evade surveillance or protect users' privacy to an extraordinary degree – human rights groups and journalists as well as serious criminal elements.

By some estimates, Freedom Hosting backstopped fully half of all hidden services at the time it was shut down last year - TorMail among them. But it had a reputation for tolerating child pornography on its servers. In July, the FBI moved on the company and had the alleged operator, Eric Eoin Marques, arrested at his home in Ireland. The U.S. is now seeking his extradition for allegedly facilitating child porn on a massive scale; hearings are set to begin in Dublin this week.

According to the new document, the FBI obtained the data belonging to Freedom Hosting's customers through a Mutual Legal Assistance request to France – where the company leased its servers – between July 22, 2013 and August 2 of last year.

That's two days before all the sites hosted by Freedom Hosting , including TorMail, began serving an error message with hidden code embedded in the page, on August 4.

Security researchers dissected the code and found it exploited a security hole in Firefox to de-anonymize users with slightly outdated versions of Tor Browser Bundle, reporting back to a mysterious server in Northern Virginia. Though the FBI hasn't commented (and declined to speak for this story), the malware's behavior was consistent with the FBI's spyware deployments, now known as a "Network Investigative Technique."

No mass deployment of the FBI's malware had ever before been spotted in the wild.

The attack through TorMail alarmed many in the Darknet, including the underground's most notorious figure - Dread Pirate Roberts, the operator of the Silk Road drug forum, who took the unusual step of posting a warning on the Silk Road homepage. An analysis he wrote on the associated forum now seems prescient.

"I know that MANY people, vendors included, used TorMail," he wrote. "You must think back through your TorMail usage and assume everything you wrote there and didn't encrypt can be read by law enforcement at this point and take action accordingly. I personally did not use the service for anything important, and hopefully neither did any of you." Two months later the FBI arrested San Francisco man Ross William Ulbricht as the alleged Silk Road operator.

The connection, if any, between the FBI obtaining Freedom Hosting's data and apparently launching the malware campaign through TorMail and the other sites isn't spelled out in the new document. The bureau could have had the cooperation of the French hosting company that Marques leased his servers from. Or it might have set up its own Tor hidden services using the private keys obtained from the seizure, which would allow it to adopt the same .onion addresses used by the original sites.

The French company also hasn't been identified. But France's largest hosting company, OVH, announced on July 29, in the middle of the FBI's then-secret Freedom Hosting seizure, that it would no longer allow Tor software on its servers. A spokesman for the company says he can't comment on specific cases, and declined to say whether Freedom Hosting was a customer.

"Wherever the data center is located, we conduct our activities in conformity with applicable laws, and as a hosting company, we obey search warrants or disclosure orders," OVH spokesman Benjamin Bongoat told WIRED. "This is all we can say as we usually don't make any comments on hot topics.”