

The Washington Post

SATURDAY, OCTOBER 5, 2013

Files show NSA targeted Tor encrypted network

**BY BARTON GELLMAN,
CRAIG TIMBERG
AND STEVEN RICH**

On Nov. 1, 2007, the National Security Agency hosted a talk by Roger Dingledine, principal designer of one of the world's leading Internet privacy tools. It was a wary encounter, akin to mutual intelligence gathering, between a spy agency and a man who built tools to ward off electronic surveillance.

According to a top-secret NSA summary of the meeting, Dingledine told the assembled NSA staff that his service, called Tor, offered anonymity to people who needed it badly — to keep business secrets, protect their identities from oppressive political regimes or conduct research without revealing themselves. In the minds of NSA officials, Tor was offering protection to terrorists and other intelligence targets.

As he spoke to the NSA, Dingledine said in an interview Friday, he suspected the agency was attempting to break into Tor, which is used by millions of people around the world to shield their identities. Documents provided to The Washington Post by former agency contractor Edward Snowden show that he was right.

Beginning at least a year before Dingledine's visit, the NSA has mounted increasingly successful attacks to unmask the identities and locations of users of Tor. In some cases, the agency has succeeded in blocking access to the anonymous network, diverting Tor users to insecure channels. In others, it has been able to "stain" anonymous traffic as it enters the Tor network, enabling the NSA to identify users as it exits.

Tor works by encrypting traffic repeat-

edly as it flows across a global network of servers, mostly run by volunteers. The traffic, which can include e-mails, information from a Web site and almost anything else on the Internet, is supposed to arrive at its destination with no identifying information about its origin or the path it took.

The Snowden documents, including a detailed PowerPoint presentation, suggest that the NSA cannot see directly inside Tor's anonymous network but that it has repeatedly unmasked users by circumventing Tor's protections. The documents also illustrate the power of the NSA to at least partially penetrate what have long been considered the most secure corners of the Internet.

The U.S. Naval Research Laboratory first developed Tor more than a decade ago as a tool to allow anonymous communications and Web browsing. It was embraced by privacy advocates, including the Electronic Frontier Foundation, and continues to receive substantial federal funding. Tor is now maintained by Dingledine's non-profit group, the Tor Project.

The State Department trains political activists worldwide on how to use Tor to protect communications from the intelligence services of repressive governments. But the anonymity service also has become popular with criminals — especially dealers of illicit drugs, military-grade weapons and child pornography — and terrorists seeking to evade tracking by Western intelligence services.

One of the documents provided by Snowden said an NSA technique code-named EGOTISTICALGIRAFFE had succeeded in unmasking 24 Tor users in a single weekend. The same operation allowed

the NSA to discover the identity of a key propagandist for al-Qaeda in the Arabian Peninsula, as the group's offshoot in Yemen is known, after he posted information and instructions on the group's Web site.

NSA anti-anonymity techniques are now also being used by law enforcement agencies. In August, civilian security researchers detected an FBI operation against an alleged child pornography ring that used a Tor-based Web server called Freedom Hosting. The FBI mounted a cyber-attack to unmask the location and owner of that anonymous server, using precisely the technique described as EGOTISTICALGI-RAFFE.

The Washington Post is not releasing certain details from the documents, including the name of the al-Qaeda operative. Documents about the NSA's attempts to penetrate Tor were also shared with the British newspaper the Guardian, which published a report on the effort Friday.

In a statement, Director of National Intelligence James R. Clapper Jr., who oversees the NSA and other intelligence agencies, said that the intelligence community "seeks to understand" tools that facilitate anonymous communication. He added that it does so because of the "undeniable fact that these are the tools our adversaries use to communicate and coordinate attacks against the United States and our allies."

The intelligence community "is only interested in communication related to valid foreign intelligence and counterintelligence purposes," Clapper said.

There is no evidence that the NSA is capable of unmasking Tor traffic routinely on a global scale. But for almost seven years, it has been trying.

Since 2006, according to a 49-page research paper titled simply "Tor," the agency has worked on several methods that, if successful, would allow the NSA to uncloak anonymous traffic on a "wide scale" — effectively by watching communications as they enter and exit the Tor system, rather than trying to follow them inside. One type of attack, for example, would identify users by minute differences in the clock times on

their computers.

Dingledine expressed no surprise that the NSA has tried to defeat efforts at anonymity. In the interview, he said the weaknesses in Tor described in the PowerPoint presentation likely could be exploited only against a relatively small number of individual users. That, he said, is reassuring.

"If those documents actually represent what they can do, they are not as big an adversary as I thought," he said.

The Tor Browser Bundle, available for free at www.torproject.org, was downloaded 40 million times last year. Until a recent security upgrade to the Firefox browser, which is incorporated in the bundle, the NSA could trick the browser into leaking the real Internet address of a targeted user. One slide described these tactics as "pretty much guaranteed to succeed."

Mozilla, the nonprofit organization that develops Firefox, declined to comment.

One document provided by Snowden included an internal exchange among NSA hackers in which one of them said the agency's Remote Operations Center was capable of targeting anyone who visited an al-Qaeda Web site using Tor.

"The ROC currently [operates] against certain extremist web forums at the moment," the employee wrote. "I am under the impression that they can serve up an exploit" — hacker jargon for malicious code — "to pretty much anyone that visits the particular web forum, though."

"Like any tool, [Tor] can be used for something good, and it can be used for something bad," said Garth Bruen, a Boston-based investigator who studies Internet crimes. "It's all about how people are using it, and criminals have been using it to great advantage. ... It's a nightmare."

An FBI agent told an Irish court last month that Freedom Hosting, unmasked with NSA-devised techniques, was among the largest purveyors of child pornography in the world, according to news reports. Silk Road, an online marketplace some called "the eBay of illicit substances," also relied on Tor — and was targeted by the FBI. Federal officials arrested the alleged founder

and shut down the site Wednesday.

Privacy advocates, however, say Tor is valuable and should be protected even if it is sometimes used by criminals. “Tor is networking technology,” said Christopher Soghoian, an American Civil Liberties Union technology expert. “It is no different from a postage stamp or a highway. Good people use highways, and bad people use highways.”

The NSA documents portray a years-long program to defeat what the agency called “The Tor Problem,” with the agency repeatedly updating its tactics as Tor’s developers made changes to the network.

The NSA also altered tactics as Mozilla introduced new versions of Firefox. In anticipation of a new release of Firefox, one agency official wrote in January that a new exploit was under development: “I’m confident we can have it ready when they release something new, or very soon after :).”

In late 2006, when the NSA prepared a working paper on methods to defeat Tor, the anonymous network had an estimated 200,000 users and 1,000 servers. Among the secret NSA documents were lists of hundreds of servers the agency believed to be “nodes” on that network.

Along with EGOTISTICALGIRAFFE, the agency’s cover names for Tor attacks have included MJOLNIR, MOTHMONSTER and EGOTISTICALGOAT. A similar program at Britain’s Government Com-

munications Headquarters, the NSA’s close counterpart, was called STUNT WORM.

One NSA PowerPoint presentation provided by Snowden is titled “Peeling Back the Layers of TOR with EGOTISTICALGIRAFFE.”

The agency began identifying browsers that were using Tor by noting how the encryption program reset what’s called the BuildID — a 14-digit code representing the exact date and time when that version of Firefox was released. On versions using Tor, the BuildID is reset to “0.” That feature made it hard to distinguish one Tor user from another, but it also allowed the NSA to pick out Tor-enabled browsers from among all others in use at any given moment.

“It’s easy!” a slide describing the technique said.

Mozilla issued a patch to Firefox that would protect newer versions of the browser against such an attack, though the NSA documents make clear that research into new exploits remains active.

One PowerPoint slide sums up a multistep method for learning the identity and location of Tor users and implanting NSA code in the browser. It ends with a final bullet point saying, “Win!”

bart.gellman@washpost.com

timbergc@washpost.com

steven.rich@washpost.com

Ashkan Soltani and Julie Tate contributed to this report.