NSA targets anyone interested in online privacy

Joseph Santolan
4 July 2014

An article published on July 3 by German public broadcaster *Das Erste* reveals that the National Security Agency (NSA) is using its surveillance program XKeyScore to target users of the traffic anonymizing software Tor and the Tails operating system, for deep packet inspection, data retention, and heightened surveillance.

The article is based on “exclusive access to top secret NSA source code, interviews with former NSA employees, and the review of secret documents of the German government.” This is the first leak regarding NSA surveillance, which includes a portion of the programming source code being used by the spy agency.

The leaked code is written in a custom programming grammar with embedded fragments of the computer language C++. Reference is made in the code to the grammar being “version 5.”

The code clearly reveals, yet again, that the claim made by the NSA and the Obama White House that XkeyScore is collecting “only metadata” is a lie.

The portion of the XKeyScore code released in the article targets users in the United States, in the so-called Five Eyes countries, and anywhere else in the world. What is more, anyone who conducts a search for information on Tails or Tor, or who visits the Tor web site torproject.org, is digitally fingerprinted, and their IP address is flagged for surveillance. The target of this surveillance is anyone who seeks to maintain the privacy of their communications.

The released code routinely inspects the contents of emails sent from Tor, even if the email was both sent and received within the United States, a flagrant violation of the Fourth Amendment’s prohibition of “unreasonable searches and seizures” by the government.

Ordinarily when a user accesses the Internet they are assigned an IP address by their Internet service provider (ISP). This can easily be used to identify the user online. Even if a user encrypts his Internet traffic the NSA can see, for example, that Bob’s IP sent an email to Alice's IP, or that he accessed a particular web site.

Tor makes this traffic anonymous. It is a network of thousands of servers, called nodes, which are used to relay connections through three encrypted “hops” that effectively hide the origin and destination of Internet traffic.

The user connects to a Tor entry node that removes all trace of the user’s IP and passes the data forward to a relay, which in turn removes all traces of the entry node and passes the data to an exit node, which finally passes the data to the desired web site. In this manner a user can effectively send and receive data anonymously.

The NSA can see when a user has accessed Tor. It can also see that one of the millions of Tor users at an exit node accessed a web site. It cannot, however, determine which user did so.

Tails is a portable operating system (OS), which is based on open source Linux OS, and which runs off of a USB stick. Tails encrypts communications and routes all traffic through Tor.

Tor updates the list of relays on an hourly basis through a series of nine Directory Authority servers worldwide. When a user logs in, Tor will connect with a Directory Authority server for a fresh list of relay servers.

The NSA lists the IP addresses of the Directory Authority servers in its XkeyScore code, including the server (128.31.0.34) hosted in the United States at the Massachusetts Institute of Technology (MIT). Anyone accessing a Directory Authority is flagged for Deep

Packet Inspection (DPI) and data retention. DPI means that it is not merely the metadata of the communication but the content, which is inspected.

Not only are Tor and Tails users targeted, but anyone interested in the well-known programs is as well. Searches for information about Tails and Tor will flag a user for surveillance, even if that search brought them to Wikipedia, or to this article.

The XkeyScore code flags two user discussion forums for targeted surveillance. The first is the Tails discussion forums at tails.boum.org. The second is the Linux programming forum, Linux Journal, a monthly online magazine dedicated to using the Linux OS. A comment contained in the XkeyScore code states that Tails is “a comsec mechanism advocated by extremists on extremist forums.”

That Tor and Tails, which are used by millions of people to ensure their anonymity online, are portrayed as a mechanism for “extremists,” and that Linux Journal is depicted as an “extremist forum,” reflects the fact that the ruling class sees threats to its existence everywhere. They are terrified of the emergence of an organized movement of the working class in opposition to capitalism, and see in encrypted and anonymous communications a potential political threat.

The leaked code is only a snippet, a rule set, from the XkeyScore program, which doubtless contains thousands more such rule sets. The same coding could be, and almost certainly is, used to identify political websites and search terms also deemed “extremist.”

There is widespread speculation that this leak of Xkeyscore code did not come from NSA whistleblower Edward Snowden. It is in many regards unlike the previous data released. Leading security expert Bruce Schneier, who is reported to be one of five people who have a complete set of the Snowden documents, wrote today, “I do not believe that this came from the Snowden documents ... I think there's a second leaker out there.”