theguardian

Attacking Tor: how the NSA targets users' online anonymity

Secret servers and a privileged position on the internet's backbone used to identify users and attack target computers

Bruce Schneier
theguardian.com, Friday 4 October 2013 15.50 BST

Tor is a well-designed and robust anonymity tool, and successfully attacking it is difficult. Photograph: Magdalena Rehova/Alamy

The online anonymity network Tor is a high-priority target for the National Security Agency. The work of attacking Tor is done by the NSA's application vulnerabilities branch, which is part of the systems intelligence directorate, or SID. The majority of NSA employees work in SID, which is tasked with collecting data from communications systems around the world.

According to a top-secret NSA presentation provided by the whistleblower Edward Snowden, one successful technique the NSA has developed involves exploiting the Tor browser bundle, a collection of programs designed to make it easy for people to install and use the software. The trick identified Tor users on the internet and then executes an attack against their Firefox web browser.

The NSA refers to these capabilities as CNE, or computer network exploitation.

The first step of this process is finding Tor users. To accomplish this, the NSA relies on its vast capability to monitor large parts of the internet. This is done via the agency's partnership with US telecoms firms under programs codenamed Stormbrew, Fairview, Oakstar and Blarney.

The NSA creates "fingerprints" that detect http requests from the Tor network to particular servers. These fingerprints are loaded into NSA database systems like XKeyscore, a bespoke collection and analysis tool which NSA boasts allows its analysts to see "almost everything" a target does on the internet.

Using powerful data analysis tools with codenames such as Turbulence, Turmoil and Tumult, the NSA automatically sifts through the enormous amount of internet traffic that it sees, looking for Tor connections.

Last month, Brazilian TV news show Fantastico showed screenshots of an NSA tool that had the ability to identify Tor users by monitoring internet traffic.

The very feature that makes Tor a powerful anonymity service, and the fact that all Tor users look alike on the internet, makes it easy to differentiate Tor users from other web users. On the other hand, the anonymity provided by Tor makes it impossible for the NSA to know who the user is, or whether or not the user is in the US.

After identifying an individual Tor user on the internet, the NSA uses its network of secret internet servers to redirect those users to another set of secret internet servers, with the codename FoxAcid, to infect the user's computer. FoxAcid is an NSA system designed to act as a matchmaker between potential targets and attacks developed by the NSA, giving the agency opportunity to launch prepared attacks against their systems.

Once the computer is successfully attacked, it secretly calls back to a FoxAcid server, which then performs additional attacks on the target computer to ensure that it remains compromised long-term, and continues to provide eavesdropping information back to the NSA.

Exploiting the Tor browser bundle

Tor is a well-designed and robust anonymity tool, and successfully attacking it is difficult. The NSA attacks we found individually target Tor users by exploiting vulnerabilities in their Firefox browsers, and not the Tor application directly.

This, too, is difficult. Tor users often turn off vulnerable services like scripts and Flash when using Tor, making it difficult to target those services. Even so, the NSA uses a series of native Firefox vulnerabilities to attack users of the Tor browser bundle.

According to the training presentation provided by Snowden, EgotisticalGiraffe exploits a type confusion vulnerability in E4X, which is an XML extension for Javascript. This vulnerability exists in Firefox 11.0 – 16.0.2, as well as Firefox 10.0 ESR – the Firefox version used until recently in the Tor browser bundle. According to another document, the vulnerability exploited by EgotisticalGiraffe was inadvertently fixed when Mozilla removed the E4X library with the vulnerability, and when Tor added that Firefox version into the Tor browser bundle, but NSA were confident that they would be able to find a replacement Firefox exploit that worked against version 17.0 ESR.

The Quantum system

To trick targets into visiting a FoxAcid server, the NSA relies on its secret partnerships with US telecoms companies. As part of the Turmoil system, the NSA places secret servers, codenamed Quantum, at key places on the internet backbone. This placement ensures that they can react faster than other websites can. By exploiting that speed difference, these servers can impersonate a visited website to the target before the legitimate website can respond, thereby tricking the target's browser to visit a Foxacid server.

In the academic literature, these are called "man-in-the-middle" attacks, and have been known to the commercial and academic security communities. More specifically, they are examples of "man-on-the-side" attacks.

They are hard for any organization other than the NSA to reliably execute, because they require the attacker to have a privileged position on the internet backbone, and exploit a "race condition" between the NSA server and the legitimate website. This top-secret NSA diagram, made public last month, shows a Quantum server impersonating Google in this type of attack.

The NSA uses these fast Quantum servers to execute a packet injection attack, which surreptitiously redirects the target to the FoxAcid server. An article in the German magazine Spiegel, based on additional top secret Snowden documents, mentions an NSA developed attack technology with the name of QuantumInsert that performs redirection attacks. Another top-secret Tor presentation provided by Snowden mentions QuantumCookie to force cookies onto target browsers, and another Quantum program to "degrade/deny/disrupt Tor access".

This same technique is used by the Chinese government to block its citizens from reading censored internet content, and has been hypothesized as a probable NSA attack technique.

The FoxAcid system

According to various top-secret documents provided by Snowden, FoxAcid is the NSA codename for what the NSA calls an "exploit orchestrator," an internet-enabled system capable of attacking target computers in a variety of different ways. It is a Windows 2003 computer configured with custom software and a series of Perl scripts. These servers are run by the NSA's tailored access operations, or TAO, group. TAO is another subgroup of the systems intelligence directorate.

The servers are on the public internet. They have normal-looking domain names, and can be visited by any browser from anywhere; ownership of those domains cannot be traced back to the NSA.

However, if a browser tries to visit a FoxAcid server with a special URL, called a FoxAcid tag, the server attempts to infect that browser, and then the computer, in an effort to take control of it. The NSA can trick browsers into using that URL using a variety of methods, including the race-condition attack mentioned above and frame injection attacks.

FoxAcid tags are designed to look innocuous, so that anyone who sees them would not be suspicious. An example of one such tag [LINK REMOVED] is given in another top-secret training presentation provided by Snowden.

There is no currently registered domain name by that name; it is just an example for internal NSA training purposes.

The training material states that merely trying to visit the homepage of a real FoxAcid server will not result in any attack, and that a specialized URL is required. This URL would be created by TAO for a specific NSA operation, and unique to that operation and target. This allows the FoxAcid server to know exactly who the target is when his computer contacts it.

According to Snowden, FoxAcid is a general CNE system, used for many types of attacks other than the Tor attacks described here. It is designed to be modular, with flexibility that allows TAO to swap and replace exploits if they are discovered, and only run certain exploits against certain types of targets.

The most valuable exploits are saved for the most important targets. Low-value exploits are run against technically sophisticated targets where the chance of detection is high. TAO maintains a library of exploits, each based on a different vulnerability in a system. Different exploits are authorized against different targets, depending on the value of the target, the target's technical sophistication, the value of the exploit, and other considerations.

In the case of Tor users, FoxAcid might use EgotisticalGiraffe against their Firefox browsers.

FoxAcid servers also have sophisticated capabilities to avoid detection and to ensure successful infection of its targets. One of the top-secret documents provided by Snowen demonstrates how FoxAcid can circumvent commercial products that prevent malicious software from making changes to a system that survive a reboot process.

According to a top-secret operational management procedures manual provided by Snowden, once a target is successfully exploited it is infected with one of several payloads. Two basic payloads mentioned in the manual, are designed to collect configuration and location information from the target computer so an analyst can determine how to further infect the computer.

These decisions are made in part by the technical sophistication of the target and the security software installed on the target computer; called Personal Security Products or PSP, in the manual.

FoxAcid payloads are updated regularly by TAO. For example, the manual refers to version 8.2.1.1 of one of them.

FoxAcid servers also have sophisticated capabilities to avoid detection and to ensure successful infection of its targets. The operations manual states that a FoxAcid payload with the codename DireScallop can circumvent commercial products that prevent malicious software from making changes to a system that survive a reboot process.

The NSA also uses phishing attacks to induce users to click on FoxAcid tags.

TAO additionally uses FoxAcid to exploit callbacks – which is the general term for a computer infected by some automatic means – calling back to the NSA for more instructions and possibly to upload data from the target computer.

According to a top-secret operational management procedures manual, FoxAcid servers configured to receive callbacks are codenamed FrugalShot. After a callback, the FoxAcid server may run more exploits to ensure that the target computer remains compromised long term, as well as install "implants" designed to exfiltrate data.

By 2008, the NSA was getting so much FoxAcid callback data that they needed to build a special system to manage it all.

More from the Guardian

What's this?

Miley Cyrus: Bangerz – review
03 Oct 2013

A window on weird: step inside the Unseen Photo fair in Amsterdam
02 Oct 2013

Sex repulses me
30 Sep 2013

Silk Road closure will be 'devastating' for Australians trying to buy Nembutal
04 Oct 2013