Überwachung

Secret documents reveal: German foreign spy agency BND attacks the anonymity network Tor and advises not to use it

The German spy agency BND developed a system to monitor the Tor network and warned federal agencies that its anonymity is „ineffective“. This is what emerges from a series of secret documents that we are publishing. The spies handed a prototype of this technology over to the NSA, in expectation of a favor in return.

am 15.09.2017 Andre Meister / keine Kommentare / Teilen

— Public Domain Caroline Attwood

This is a translated version of our original German reporting. Translation support by Anna Biselli and Kirsten Fiedler.

„If you’re an Internet newcomer and want to get up to speed without all the intimidating technical jargon, The Internet For Dummies has you covered.“ That is how the publisher promotes its book in the popular „For Dummies“ series. Like many people, the German foreign spy agency Bundesnachrichtendienst (BND) buys a copy in 2005, to „get familiar“ with this internet. That is what the engineer Harald Fechner testified in the German parliamentary committee investigating the NSA spying scandal two years ago.

This is a creative version of the truth. Until his retirement in June 2009, Fechner was head of the BND's Signals Intelligence Directorate and therefore responsible for the spy agency's internet surveillance. He had more than a thousand spies „specifically intercepting communication streams" – via radio waves, telephone cables and tapped fibre-optic cables.

Secret BND hacker unit

His command of the SIGINT Directorate also includes a secret hacker unit, responsible for „operative technological attacks on IT systems" all over the world. Like every department of the spy agency, these hackers are constantly changing their name: until August 2008, they were called „Unit 26E" (Operational Support and Listening Technology), then „Working Group TX" (IT Operations) and finally „Sub-Directorate T4" (Cyber Intelligence).

Within the spy agency, the hackers became famous in 2007 when one of them eavesdropped on his girlfriend's romantic e-mails with a Bundeswehr soldier, this so-called LOVEINT incident makes the rounds internally. The public learned about the hacker unit one year later, when it is revealed that they infiltrated the computer network of the Afghan Ministry of Trade. Not only did the spies read the e-mails of the minister – officially a friend of Germany – but also mails from the German journalist Susanne Koelbl.

Harald Fechner remembers this well, as the hacking attack against the journalist led him to the last step of his 28-year career at the BND. On the same day, the magazine Der Spiegel revealed this scandal, the former head of the SIGINT Directorate Dieter Urmann was demoted. Fechner became his successor and kept that position until his retirement.

Gathering of the spies

While these events unfolded in Germany, the BND agent operating under the initials „H.F." was on a work trip to the USA. The President was still George W. Bush – and his hand-picked CIA-support abroad was sometimes Edward Snowden. H.F. was the NSA's guest at its headquarters in Fort Meade, attending the annual SIGINT Development Conference, where more than a thousand agents discussed the latest developments in surveillance technology. While the BND was under pressure in Germany, it could shine here.

At the invitation of the NSA, H.F. presented an attack on the Tor network which the BND hackers developed shortly before. The „onion router" is a network to anonymize internet traffic and has become „the king of high-secure, low-latency internet anonymity". Millions of people around the world use Tor to protect against surveillance and censorship.

Tor was originally created by the US military to disguise spy agencies activities on the internet, and still receives a large part of its funding from the US government, to circumvent „technologies of internet repression, monitoring and control" in authoritarian states. But Tor is not only an annoyance for dictators, agencies of western countries also want to de-anonymize Tor users. And the BND is keen to help.

Attack on the Tor network

A few weeks prior to the conference, the BND hackers from Unit 26E „developed the idea of how the Tor network could be monitored relatively easily", according to internal BND documents. Tor was already well known at the time and had 200,000 active users all over the world. When project leader Roger Dingledine explained the development at the CCC Congress and in a police station in Stuttgart, the hackers of the BND listened carefully.

In March 2008, the spy agency filled in its partners from the USA and UK. When a foreign delegation visited Munich, the SIGINT unit presented „the anonymity network Tor and a possible disbandment of the anonymity feature", the BND writes in its internal report. In order to implement the plan, the BND hoped for „an international cooperation with several foreign intelligence agencies".

Both NSA and GCHQ expressed „a high interest" and offered support. The three spy agencies decided on further meetings and the creation of a project group, while the BND planned to set up its own Tor exit node server, as well as a „test capture" and „evaluation with the NSA".

Far ahead of the Yanks

In April, the BND agent H.F. presented the work of the German hackers to the anti-terror coalition of the European spy agency club SIGINT Seniors Europe. Afterwards, he was invited to the SIGDEV conference by the NSA at its headquarters. Yet again, his presentation was a success: The other spy agencies showed themselves „impressed with our work on Tor servers“, the BND writes, its work being „far ahead of the Yanks“.

As a result, the NSA promised „a technical review by its experts“, with the goal to implement the project. Only a week later, H.F. was again invited by the NSA, this time accompanied by „M.S.“ from the hacker unit, and this time to the BND's Bad Aibling station in Bavaria, where the NSA liaison unit SUSLAG has a building for itself. H.F. and M.S. joined a video conference with NSA experts to clarify further questions and ideas. Among other documents, we are publishing the report of this conference.

Both BND and NSA agree that „the Tor network is the most established system for anonymity on the internet“ and „other systems only play a minor role“. The spy agencies expected a continued growth of the Tor network, which would „continue to pose a problem for several years“. The spies assumed that „efforts for an attack are worthwhile“. Their goal was to break Tor's anonymity.

Efforts to find an attack angle

How exactly the spy agencies want to crack Tor remains vague. Tor is transparent and open in order to promote research and feedback. Not only are design, specification and source code public, but also a bibliography of research papers on anonymity. This openness not only helps researchers, but also Tor itself: the system is regularly analyzed – and if a vulnerability is identified, it is fixed.

The BND hackers told the NSA about „a possibility to penetrate the Tor network“, a term commonly used for the infiltration of IT systems. In this case, the documents suggest that the spy agencies wanted to exploit a design decision Tor publicly specified.

The principle of „onion routing“ is to transmit internet traffic through three intermediary servers, so that no point in the network knows both sender and receiver. With this technique, Tor prevents many surveillance and censorship measures, better than a „Virtual Private Network“ (VPN) with only one intermediate server. But of course not all.

A global passive adversary

Like all low-latency anonymity systems used in practice, Tor cannot protect against „a global passive adversary“. This is defined in the design document. The software documentation warns: „If your attacker can watch the traffic coming out of your computer, and also the traffic arriving at your chosen destination, he can use statistical analysis to discover that they are part of the same circuit.“ The goal of NSA's and GCHQ's internet surveillance is to achieve exactly that.

A number of researchers have demonstrated this attack in practice, either by simply counting transmitted packets, by analyzing time windows, or correlation attacks with only a fraction of traffic. All this research is public. The spy agencies followed this research, used it for their own purpose and turned theoretical vulnerabilities into real-world surveillance systems.

The BND hackers based their attack on „a paper by an American university“, which they handed over to the NSA. During the video conference in Bad Aibling, the BND responded to questions and presented a timetable with further steps. The Germans planned to set up their own Tor network in a lab within „six to eight weeks“ in order to better understand the system and to verify the research paper.

Test network and proof of concept

The NSA was clearly enthusiastic about the BND's presentation, wanted to work closely together, and especially wanted access to the test results. The Americans were „visibly astonished“ by the activity of the Germans. Although the BND considered its progress „a little more advanced than the NSA“, Pullach also wanted Fort Meade to participate: The project „would have a considerably greater prospect for success in a combined effort with partners“.

The NSA agreed to contact the university to learn more about the research paper. The BND started its work, set up the test network and developed a „proof of concept“ for the attack, a prototype. The Germans wanted to deliver

first results only a month after the video conference. SIGINT chief Harald Fechner planned to visit the USA in October and discuss the issue with NSA Director Keith Alexander.

But then the project experienced a setback. The hacker unit „IT operations“ was reorganized and the people involved in the Tor project were „dispersed within the unit“ into two different areas. Nevertheless, the NSA headquarter hosted another meeting on the topic in December 2008, „by far the most intense in terms of the number of participants and competence. The room was packed.“

A promise to the Yanks

The transition of US presidency from George W. Bush to Barack Obama set the project in motion again. On the day of the inauguration, the BND's „leadership support“ prepared another visit of SIGINT chief Fechner to the NSA in Fort Meade. In internal e-mails, the hackers were ordered to reactivate the project. After all, the BND had to keep „a promise the the Yanks“.

From that point, M.S. took over the project. He complained that „brilliant staff“ was a „scarce resource“ and about the lack of interest within the BND. After he presented the system internally, „there was no more feedback“. From then on, he stated, „further development is primarily geared to the needs of the partner“, meaning the NSA. The proof of concept was already „a good status to talk to the experts of the Yanks“.

For BND's leadership, this was opportune. While they hoped that BND analysts could be „pushed“ to work on Tor, their true goal was bigger. The BND wanted something from the NSA: a technology from the „field of cryptanalysis“, to decipher encrypted communication. The Germans knew from experience that Fort Meade would not easily hand over the object of desire. So they collected of items to trade for the Americans, the attack against Tor was „another building block“ for this gift package.

Vegetable chopper against onions

The BND's leadership gave M.S. the order to write up a concept paper within one month. And he delivered. On 20 February 2009, the 16-page „concept for tracking internet traffic, which has been anonymized with the Tor system“ was finalized. The cover is far from modest: He placed a vegetable chopper over an onion, the logo of the Tor network.

To justify the attack on Tor, M.S. quoted a law enforcement conference in Berlin from this year that took place under the motto „WWW – the virtual crime scene“. For the chapter on „How the Tor network works“, the author kept it simple, he copied the text from Wikipedia and took images from the Tor website.

Precisely how the BND plans to „chop“ Tor is unfortunately redacted in the document we obtained. But as before, the spy agency refers to public research. To implement the attack, it is likely that the spies runs their own servers in the Tor network. M.S. points to passive snooping servers, which are presumably operated by the NSA, and emphasizes the „protection of the anonymity“ of the spy agencies.

Highly interested in access

Three weeks after the concept paper, the British reiterated their demand. The GCHQ resident in Berlin and three other high-ranking spies of the queen visited Pullach on 11 March 2009. At the BND headquarters, they were welcomed by SIGINT chief Harald Fechner, who brought seven other senior SIGINT staff members. The purpose of the meeting was to develop their SIGINT cooperation, especially „regarding anonymity services“.

The British wanted to participate: The GCHQ „is very interested in the SIGINT unit's access to the Tor network“, the internal report says. Both parties agreed to arrange further technical discussions and a „joint workshop on possible technical and operational procedures“.

Five days after the visit from the island, SIGINT chief Fechner flew across the Atlantic, the concept paper of M.S. in his bag. The Americans gladly accepted his offer – the NSA and GCHQ took over the project. Whether the BND received the compensation it hoped for, remains unknown. When we confronted the BND with a set of specific questions, we received only the boilerplate answer: „As a matter of principle, the BND talks about operational aspects of its work only with the Federal Government and the competent authorities of Parliament.“

Very high level of surveillance

One and a half years later, the BND warned German federal agencies not to use Tor. The hacker unit „IT operations“ entitled its report: „The anonymity service Tor does not guarantee anonymity on the internet“. The six-page paper was sent to the chancellery, ministries, secret services, the military and police agencies on 2 September 2010.

According to the executive summary, Tor is „unsuitable“ for three scenarios: „obfuscating activities on the internet“, „circumventing censorship measures“ and „computer network operations for intelligence services“ – spy agency hacking. The BND assumes „a very high level of surveillance within the network“, including the possibility that anyone can „set up their own so-called exit nodes for monitoring“.

In a technical description, BND explains how Tor works. The pictures are copied again: from a personal website and the Electronic Frontier Foundation, however in outdated formats. Moreover, the BND gets it partly wrong: their statement that „information about the running Tor nodes is downloaded from a server in unencrypted form“ has not been true for over two years at the time of writing. After Iran identified and blockedthese, they were encrypted from 2007.

Not convinced of the legality

In its announcement, the spy agency presents a strong hypothesis. According to the BND, „Tor is predominantly used to conceal activities, where users are not convinced of the legality of their actions. The number of Tor users who aim at preserving anonymity out of mere privacy considerations is relatively small.“ The BND bases this statement on „several pieces of intelligence“, but does not underpin it with any facts.

We reached out to several people from the Tor project but nobody had any idea how the BND came up with this hypothesis. „That sounds like nonsense,“ IT security advisor Jens Kubieziel says, who is a system administrator for the Tor project and runs large Tor exit nodes. The Chaos Computer Club also operates some of the major servers of the Tor network. „Compared to the amount of traffic and the millions of connections anonymized by Tor every day, the number of inquiries about illegal activities is negligibly low,“ lawyer Julius Mittenzwei says, one of the project managers and former member of Tor’s board of directors.

Spy agencies and other agencies worldwide „have ways to counter anonymity. One of them is to set up own Tor nodes and monitor those intensively to gather intelligence and evidence“, the BND continues. The spies do not treat this as a secret: „Some agencies have already reported about installing their own Tor nodes and using the logged data for different projects and criminal investigations.“

Disguise not provided

The BND sees clear proof that spy agencies operate Tor servers by looking at the location of various servers, especially „in the vicinity of Washington, D.C.“. The spies assume that „various agencies provide these nodes“. The document does not specify whether the spy agency only suspects this, read it on the internet, was told so by NSA – or gave that idea to the NSA in the first place.

However, the BND is so convinced that it warns the most important German federal agencies not to use Tor. The conclusion of its assessment: „Users of anonymity software expect a level of disguise, which known and widely used anonymity services do not provide.“

Not only does the BND think Tor is unsafe, they also advise against using hacked systems as proxy servers: „The use of a compromised system for camouflage by spy agencies is known to be ultimately ineffective and appears only plausible for diversion maneuvers.“ The „IT operations“ department must know this of course – and so they warn their fellow state hacker colleagues from federal police, domestic spy agency and military.

Tempora and XKeyscore

Looking at the activities of the NSA and GCHQ, the BND’s concern might just be justified. Two years after the Germans presented their gift, the spy agencies continue their work on breaking Tor. The efforts of the British team is documented in the GCHQ’s internal wiki, published by German magazine Der Spiegel from the Snowden archive. Their goal is to deanonymize Tor, or in their own words: „if given some traffic from a Tor exit node, […] find the IP address of the user associated with that traffic.“

According to the wiki, the research began in December 2010. The British gave up on trying to follow the path of a circuit through the Tor network. Instead, they launched „an entry-exit correlation attack“, correlating the internet traffic from the sender to the network and from the network to the receiver. As the GCHQ massively intercepts internet traffic and runs its own Tor servers, this is not difficult. As early as June 2011, they finalized an 18-page study and source code in the statistical programming language R, completed by a presentation with slides.

The NSA also scores a success. In 2011, they implemented „several fingerprints and a plugin“ in their powerful XKeyscore system, in order to recognize and deanonymize Tor users. German public broadcasters published some of these XKeyscore rules. According to the code, the NSA monitors all internet users who visit the Tor website, use the Tor software, or simply search for Tor or the Tor operating system Tails.

Egotistical giraffe

Despite all attacks, the NSA still honors Tor as „king of high-secure, low-latency internet anonymity“. Even if spy agencies that intercept large parts of the internet might deanonymize some Tor users some of time, it is unlikely that they are able to deanonymize all Tor users all of the time. The NSA writes, it has „no smoking gun yet :-(„

Anonymity and encryption share a common feature: Both are easier to circumvent than to crack. Anyone who breaks into a computer can decrypt its communication and identify its users. NSA and GCHQ do exactly this since at least 2013: Under the code name Egotistical Giraffe, they hack the Firefox-based Tor Browser, infect the operating system and thereby solve their self-proclaimed „Tor problem“. Even the FBI carried out and admitted such attacks.

But sometimes it is enough to take advantage of mistakes that surveilled targets make. LulzSec hacker Hector Monsegur was identified because he revealed his IP address just once. Stratfor hacker Jeremy Hammond was identified because the FBI correlated the times when his home WIFI was in use. Silk Road founder Ross Ulbricht was identified because he gave away his pseudonym. A recent study researches these „technical limitations of anonymity and the operational security challenges that Tor users will encounter“.

No purely technical measures

The domestic German spy agency was however less successful. Even though the „Federal Office for the Protection of the Constitution“ received the memo from the BND, they still experience problems to identify Tor users two years later. While visiting Washington in June 2012, a delegation asked the NSA if they could „identify“ or „decrypt“ Tor. The American answer did not satisfy them. In the assessment of the trip, the Germans write that the visit was „strategically important“, but „was more about relationship management“.

Well-funded international spy agencies continue to refine their attacks. But the Tor community also continues to improve the project and fight off attacks – in close collaboration with the privacy research community. Project leader Roger Dingledine is skeptical as to whether spy agencies are able to make their attacks „work at scale“. Nevertheless, the documents show „that we need to keep growing the Tor network so it’s hard for even larger attackers to see enough Tor traffic to do these attacks.“

But that is not enough, according to Dingledine: „We as a society need to confront the fact that our spy agencies seem to feel that they don’t need to follow laws. And when faced with an attacker who breaks into Internet routers and endpoints like browsers, who takes users, developers, teachers, and researchers aside at airports for light torture, and who uses other ‚classical‘ measures – no purely technical mechanism is going to defend against this unbounded adversary.“

The original documents we published are available in full text attached to the German version of this reporting. (Redactions are not by us.)

– –

Über den Autor/ die Autorin

andre

Andre ist schon lange bei netzpolitik.org, seit 2012 auch als festangestellter Redakteur. Er hat einen Master in Sozialwissenschaften, ist Mitgründer der Vereine Digitale Gesellschaft, Gesellschaft für Freiheitsrechte und netzpolitik.org sowie Mitglied im Chaos Computer Club und Beobachter bei European Digital Rights. Außerdem arbeitet er als System-Administrator, so hat er u.a. den Mail-Server von Frag Den Staat aufgesetzt und nutzt ihn gerne. Und irgendwas mit Landesverrat. **Kontakt:** E-Mail, OpenPGP, Telefon, CryptoPhone, Twitter, Flattr, Bitcoin.

Veröffentlicht
15.09.2017 12:23 Uhr
Zuletzt aktualisiert
15.09.2017 17:08 Uhr

Kategorie
Überwachung

Schlagworte
Abteilung TA, Angriff, Anonymisierung, Arbeitsgruppe TX, BND, CCC, Cyber-Intelligence, Dieter Urmann, english, exklusiv, GCHQ, geheim, H.F., hacker, Harald Fechner, Informationstechnische Operationen, IT-Operationen, Jens Kubieziel, Julius Mittenzwei, M.S., NSA, Operative Unterstützung und Lauschtechnik, Referat 26E, Roger Dingledine, SIGINT, Susanne Koelbl, Technische Aufklärung, Tor, Tor Project, Überwachung, Unterabteilung T4

0 Kommentare