statewatch

Analysis

State Trojans: Germany exports “spyware with a badge”

Kees Hudig

German police have been using software to surveil people's internet activity beyond what is allowed by the law. There has also been increased cross-border cooperation with the police forces of neighbouring countries, with an informal working group meeting twice a year without the knowledge of parliamentarians.

Since 2005 German police have been remote-spying on individuals and organisations by installing software (malware or Trojans) on their computers. [1] There was no legal base for these activities, and in February 2008 the Federal Constitutional Court (Bundesverfassungsgericht) ruled that the state of North-Rhine Westphalia (Nordrhein-Westfalen) was acting unconstitutionally and that ‘remote searches’ (online durchsuchung) are only allowed under very strict conditions. [2] Germany has a strong civic movement on the protection of 'digital privacy' and the disclosure has triggered heated public debate on state intelligence and security institutions intercepting private computers and mobile phones.

In October 2011, the computer watchdog Chaos Computer Club (CCC) published research conducted on data sent by people who had found Trojans installed on their computers (see Appendix). According to the CCC, the malware was able to spy in ways that exceeded the limits set out by the Federal Constitutional Court in 2008. “The CCC's analysis showed that the Trojan can log keystrokes, take screenshots, record Skype conversations and even activate webcams or computer microphones to survey private events in a person's home.” [3] The malware was also constructed in such a way that it could open a 'backdoor' in the targeted person's computer, allowing it to install software. The CCC said that the software, which was developed by the private company DigiTask based in the regional state of Hessen, was badly designed and “could allow the software to be used by third parties.”

Following the CCC’s disclosure, the Bavarian state acknowledged the existence of the Trojan and other states soon followed. The Minister of Justice, Sabine Leutheusser-Schnarrenberger (Liberal Party, Freie Demokratische Partei), initiated an investigation. The German news service *Deutsche Welle* reported on the extent of the known use of Trojans. [4]

The interior ministers of the states of Baden-Württemberg, Brandenburg, Schleswig-Holstein and Lower Saxony said that regional police had used the software within the parameters of the law. In Lower Saxony, the software had been in use for two years, according to the public broadcaster NDR.

Authorities in Brandenburg told the daily *Berliner Morgenpost* newspaper that they were using the spyware in a single, on-going investigation. Baden-Württemberg had also used such software to investigate "individual cases," according to *Badische Zeitung*.

The interior ministry in the western state of North Rhine-Westphalia also admitted that police had used the software in two instances, both of which had been approved by a judge. The news agency *dpa* reported that both cases had involved serious drug crimes.

Officials in the southern German state of Bavaria confirmed that their agencies have been using a spyware program since 2009. It remains unclear whether all four states had been using the same software.

The president of the Federal Criminal Police Authority (Bundeskriminalamt), Jörg Ziercke, was quick to state that he had dissuaded the regional states' criminal police units from using the programme. What he did not say, and only became clear after parliamentary questions from the Left party Die Linke, was that it was not only police officers from Baden-Württemberg and Bavaria that had been meeting in an informal working group for DigiTask software users, but also officers from Belgium, the Netherlands and Switzerland. This working group had initially been called the DigiTask User Group and had been active for three years. It was later renamed the Remote Forensic Software User Group. The group met twice a year and parliamentarians were not aware of its existence. [5]

Before parliament was informed of the existence of this international working group, DigiTask had told German media that the software had been sold to other countries. The Dutch liberal party (D66) asked its Minister of Justice whether the software was being used in the Netherlands, but the answer is pending. [6]

Criminal prosecution cases have also disclosed information about these operations. At a court case involving two left-wing activists from Switzerland, who were using a server in Nürnberg to encrypt their communications, it was revealed that Swiss police used hardware and software for a so-called "deep packet inspection", which captures all communications made with the server. The legal file revealed that DigiTask software had been used and that the Swiss and Bavarian police forces, who had been arguing over who would foot the bill, shared the costs. [7] What remains unclear, however, is whether the informal working groups are also being used to coordinate joint international operations.

Informal groups rule

The EU has a long history of using informal rather than formal and transparent working groups to coordinate its police forces. [8] Heise reports that the European Cooperation Group on Undercover activities (ECG) "facilitate[s] cross border exchange of undercover investigators." This relatively informal group has countries participating from both inside and outside the EU. There is also a Cross-Border-Surveillance Working Group (CSW) that meets twice a year and is - according to the German government [9] - focused on "cross border observation and problems connected to that." It aims to "optimise the working results." The methods used for 'remote searches' by Europol are unknown.

One of the communication networks that concerns criminal investigators is Skype, which is more difficult to intercept than regular phones. The Trojan seems to be designed to be able to listen in to people communicating with this Voice over IP-system by capturing their key-logs, or sending a constant stream of images of the computer screen. After parliamentary questions on 19 October

2011, the German deputy interior minister, Ole Schröder, disclosed that some of the police collaboration with Italian forces was specifically around this issue. The Germans were concerned that Skype was giving more information to the Italians than to them (which later appeared to be untrue). Skype hands over information to every government that requests it, but the company checks whether the request is legitimate, following specific public guidelines. [10] For information requests, government institutions have to send a request to the organisation's head office in Luxembourg, and Skype advises the applicant not to send a notice to the phone-user that they are investigating. [11]

The 'Federal Trojan' scandal has had the positive side effect of revealing details about the way police and the secret services operate in the opaque area of 'cyber-espionage.' Sometimes the practice turns out to be very 'analogue,' because installing a Trojan on the computer of a targeted person is difficult. The common method of sending an email with an attachment in the hope the target person opens it, allowing its content to install itself on his or her computer, is increasingly unsuccessful because people are aware of the risk of infecting their computer with malware. The monthly newspaper AK writes that some Trojans had been installed by hand on peoples' computers. In one case, this happened when a person passed through customs at Munich airport. In another case, police installed it during a court-ordered house search.

The German news website *Heise.de* [12] reports that the Ministry of Interior acknowledges the existence of more informal working groups involving the German BKA and other countries' police authorities. In November 2007, the President of the European Commission issued a statement to "encourage" the practice of remotely searching computers and in September 2010 the EU Anti-Terrorism Coordinator called for the construction of a "common juridical framework for certain intelligence techniques" and pointed explicitly to remote searches. [13]

Endnotes

1 Geheimdienste *spitzeln schon seit Jahren (Secret services spy since years already):*

http://www.stern.de/digital/online/online-durchsuchungen-geheimdienste-spitzeln-schon-seit-jahren-587865.html?nv=ct_mt

2 Press release Bundesverfassungsgericht

http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg08-022.html

3 Deutsche Welle 11/10/11 http://www.dw-

world.de/dw/article/0,,15449054,00.html

4 See above

5 Kleine Anfrage der Linken enthüllt: Bundeskriminalamt treibt den Einsatz von Schadprogrammen der Firma DigiTask international voran:

http://www.jungewelt.de/2011/11-14/047.php

6 Gebruikt Nederlandse overheid ook spyware?

http://www.d66.nl/europa/nieuws/20111011/gebruikt_nederlandse_overheid_ook?ctx=vghpm7u9vdea

7 Matthias Monroy, Landeskriminalamt Bayern schnüffelt mit DigiTask für Schweizer Polizei http://www.heise.de/tp/artikel/35/35712/1.html

8 See, for example, Trevi, Europol and the European state by Tony Bunyan in Statewatching the New Europe, 1993/14

9 http://dipbt.bundestag.de/dip21/btd/17/056/1705677.pdf

10 http://cryptome.org/isp-spy/skype-spy.pdf

11 Matthias Monroy, Internationaler Trojaner-Stammtisch

http://www.heise.de/tp/artikel/35/35805/1.html

12 Internationaler Trojaner-Stammtisch http://www.heise.de/tp/artikel/35/35805/1.html

13 http://register.consilium.europa.eu/pdf/de/10/st13/st13318-re01.de10.pdf

Background

Lemma Wikipedia on 'Online Durchsuchung in Germany' http://de.wikipedia.org/wiki/Online-Durchsuchung_%28Deutschland%29

The tricky issue of spyware with a badge: meet 'policeware'

http://arstechnica.com/security/news/2007/07/will-security-firms-avoid-detecting-government-spyware.ars

APPENDIX

The announcement from the Chaos Computer Club

Chaos Computer Club analyses government malware

http://www.ccc.de/en/updates/2011/staatstrojaner (08/10/11)

The largest European hacker club, "Chaos Computer Club" (CCC), has reverse engineered and analyzed a "lawful interception" malware program used by German police forces. It has been found in the wild and submitted to the CCC anonymously. The malware can not only siphon away intimate data but also offers a remote control or backdoor functionality for uploading and executing arbitrary other programs. Significant design and implementation flaws make all of the functionality available to anyone on the internet.

Even before the German constitutional court ("Bundesverfassungsgericht") on February 27 2008 forbade the use of malware to manipulate German citizen's PCs, the German government introduced a less conspicuous newspeak variant of the term spy software: "Quellen-TKÜ" (the term means "source wiretapping" or lawful interception at the source). This Quellen-TKÜ can by definition only be used for wiretapping internet telephony. The court also said that this has to be enforced through technical and legal means.

The CCC now published the extracted binary files [0] of the government malware that was used for "Quellen-TKÜ", together with a report about the functionality found and our conclusions about these findings [1]. During this analysis, the CCC wrote its own remote control software for the trojan.

The CCC analysis reveals functionality in the "Bundestrojaner light" (Bundestrojaner meaning "federal trojan" and is the colloquial German term for the original government malware concept) concealed as "Quellen-TKÜ" that go much further than to just observe and intercept internet based telecommunication, and thus violates the terms set by the constitutional court. The trojan can, for example, receive uploads of arbitrary programs from the Internet and execute them remotely. This means, an "upgrade path" from Quellen-TKÜ to the full Bundestrojaner's functionality is built-in right from the start. Activation of the computer's hardware like microphone or camera can be used for room surveillance.

The analysis concludes, that the trojan's developers never even tried to put in technical safeguards to make sure the malware can exclusively be used for wiretapping internet telephony, as set forth by the constitution court. On the contrary, the design included functionality to clandestinely add more components over the network right from the start, making it a bridge-head to further infiltrate the computer.

“This refutes the claim that an effective separation of just wiretapping internet telephony and a full-blown trojan is possible in practice – or even desired," commented a CCC speaker. "Our analysis revealed once again that law enforcement agencies will overstep their authority if not watched carefully. In this case functions clearly intended for breaking the law were implemented in this malware: they were meant for uploading and executing arbitrary code on the targeted system."

The government malware can, unchecked by a judge, load extensions by remote control, to use the trojan for other functions, including but not limited to eavesdropping. This complete control over the infected PC – owing to the poor craftsmanship that went into this trojan – is open not just to the agency that put it there, but to everyone. It could even be used to upload falsified "evidence" against the PC's owner, or to delete files, which puts the whole rationale for this method of investigation into question.

But the trojan's built-in functions are scary enough, even without extending it by new moduls. For the analysis, the CCC wrote its own control terminal software, that can be used to remotely control infected PCs over the internet. With its help it is possible to watch screenshots of the web browser on the infected PC – including private notices, emails or texts in web based cloud services.

The official claim of a strict separation of lawful interception of internet telephony and the digital sphere of privacy has no basis in reality. [NB: The German constitutional court ruled that there is a sphere of privacy that is afforded total protection and can never be breached, no matter for what reason, for example keeping a diary or husband and wife talking in the bedroom. Government officials in Germany argued that it is possible to avoid listening in on this part but still eavesdrop electronically. The constitutional court has created the concept of "Kernbereich privater Lebensgestaltung", core area of private life. The CCC is basically arguing that nowadays a person's laptop is intrinsically part of this core area because people put private notes there and keep a diary on it] The fact that a judge has to sign the warrant does not protect the privacy, because the data are being taken directly from the core area of private life.

The legislator should put an end to the ever growing expansion of computer spying that has been getting out of hand in recent years, and finally come up with an unambiguous definition for the digital privacy sphere and with a way to protect it effectively. Unfortunately, for too long the legislator has been guided by demands for technical surveillance, not by values like freedom or the *question of how to protect our values in a digital world. It is now obvious that he is no longer able to oversee the technology, let alone control it.*

The analysis also revealed serious security holes that the trojan is tearing into infected systems. The screenshots and audio files it sends out are encrypted in an incompetent way, the commands from the control software to the trojan are even completely unencrypted. Neither the commands to the trojan nor its replies are authenticated or have their integrity protected. Not only can unauthorized third parties assume control of the infected system, but even attackers of mediocre skill level can connect to the authorities, claim to be a specific instance of the trojan, and upload fake data. It is even conceivable that the law enforcement agencies' IT infrastructure could be attacked through this channel. The CCC has not yet performed a penetration test on the server side of the trojan infrastructure.

“We were surprised and shocked by the lack of even elementary security in the code. Any attacker could assume control of a computer infiltrated by the German law enforcement authorities", commented a speaker of the CCC. "The security level this trojan leaves the infected systems in is comparable to it setting all passwords to '1234'".

To avoid revealing the location of the command and control server, all data is redirected through a rented dedicated server in a data center in the USA. The control of this malware is only partially within the borders of its jurisdiction. The instrument could therefore violate the fundamental principle of national sovereignty. Considering the incompetent encryption and the missing digital signatures on the command channel, this poses an unacceptable and incalculable risk. It also poses the question how a citizen is supposed to get their right of legal redress in the case the wiretapping data get lost outside Germany, or the command channel is misused.

According to our hacker ethics and to avoid tipping off criminals who are being investigated, the CCC has informed the German ministry of the interior. They have had enough time to activate the existing self destruct function of the trojan.

When arguing about the government authorized infiltration of computers and secretly scanning suspects' hard drives, the former minister of the interior Wolfgang Schäuble and Jörg Ziercke, BKA's president (BKA, German federal policy agency), have always claimed that the population should not worry because there would only be "a handful" of cases where the trojan would be used at all. Either almost the complete set of government malware has found their way in brown envelopes to the CCC's mailbox, or the truth has been leapfrogged once again by the reality of eavesdropping and "lawful interception".

The other promises made by the officials also are not basis in reality. In 2008 the CCC was told that all versions of the "Quellen-TKÜ" software would manually be hand-crafted for the specifics of each case. The CCC now has access to several software versions of the trojan, and they all use the same hard-coded cryptographic key and do not look hand-crafted at all. Another promise has been that the trojan would be subject to exceptionally strict quality control to make sure the rules set forth by the constitutional court would not be violated. In reality this exceptionally strict quality control has neither found that the key is hard coded, nor that the "encryption" is uni-directional only, nor that there is a back door for uploading and executing further malware. The CCC expressed hope that this farce is not representative for exceptionally strict quality control in federal agencies.

The CCC demands: The clandestine infiltration of IT systems by government agencies must stop. At the same time we would like to call on all hackers and people interested in technology to further analyze the malware, so that at least some benefit can be reaped from this embarrassing eavesdropping attempt. Also, we will gladly continue to receive copies of other versions of government malware off your hands. [4]

Links:

[0] Binaries

[1] Analysis of the government malware (German)

http://www.ccc.de/system/uploads/76/original/staatstrojaner-report23.pdf

[4] BigBrotherAwards 2009, Category Business: companies selling internet and phone surveillance technology

http://www.bigbrotherawards.de/2009/.com

[5] 0zapftis (at) ccc.de use the PGP key below

This article was first published in Statewatch Journal volume 21 no 4, March 2012