World Socialist Web Site wsws.org

German state deploys illegal spy software

Sybille Fuchs
14 October 2011

German security services are placing spyware on personal computers, even though this violates fundamental rights and has been expressly forbidden by Germany's Supreme Court. Writing in the *Süddeutsche Zeitung*, Heribert Prantl refers to this as "a new form of state crime".

The so-called Trojan software used by the state can be remotely controlled. It can also be used to plant programs on infected computers and monitor all processes they are running. It can access the keyboard, microphone and camera, meaning the security services can read emails, listen to Skype conversations, and create screenshots, also using the camera and microphone to spy on what is happening near the computer.

In a landmark ruling on 27 February 2008, the Supreme Court banned such general on-line surveillance. However, the ruling makes an exception for so-called source telecommunications surveillance (Quellen-TKÜ), allowing the security agencies to intercept communications on the computer of a suspect before they are encrypted.

However, the court has imposed strict guidelines on Quellen-TKÜ operations, requiring judicial authorization and limiting them to cases of serious crime and terrorism. Moreover, "technical precautions and legal requirements" must ensure that "only limited monitoring data from an on-going telecommunication process" occurs. The 2009 BKA law allows the authorities to use Trojans under the conditions laid down by the Supreme Court with respect to threats to "life, limb or liberty" or when the "existence of the state" is threatened.

It has been clear since last weekend that the security authorities are not complying with these requirements. The Chaos Computer Club (CCC) has analyzed the spy software on the hard drive of an infected computer.

From this, the CCC established that the authorities were deliberately violating the statutory requirements. There was "no attempt to use software technology to ensure that the collection of data was strictly limited to telecommunications, but - on the contrary - the secret extension of the functionality of the computer bugging software was planned from the outset", the CCC declared.

This refutes state claims that there was "effective separation of the exclusive interception of telecommunications and a broader snooping using Trojans".

The CCC warned that the remote-control function could be used to load and execute malicious software, and to plant bogus digital evidence on the computer, which can then be detected if the computer was seized. A suspect would have no way of proving that this had happened.

What is possible was shown by a case at HSH Nordbank, where private detectives planted child pornography onto a computer.

The function making it possible to scour the hard drive for files or use the microphone and camera as surveillance tools was consciously disguised by the programmers of the Trojan analyzed by the CCC.

While the rest of the Trojan software had no significant safeguards against its functions being explored by machine code analysis, the programmers tried to camouflage the remote software loading function and hide the way it worked. To this end, the individual software components had been scattered around like puzzle pieces.

"Those who commissioned and programmed the Trojan were apparently aware of the massive constitutional violation and tried to cover up their actions", according to the *Frankfurter Allgemeine Zeitung*.

The Bavarian state government admitted to deploying the Trojans analyzed by the CCC in five cases. In Baden-Württemberg, Lower Saxony, Brandenburg and Schleswig-Holstein, the same or similar versions of the software were also used.

These were not cases of serious crime or terrorism, but about a dozen routine criminal cases, such as the commercial trade in narcotics, handling stolen property and theft of drugstore products, clothing and doping agents. In one case, the 15 accused had offered to sell equipment on the Internet, which was never delivered, thus depriving 200 customers of their money.

© World Socialist Web Site

Bavarian Interior Minister Joachim Herrmann and the head of the Bavarian Office of Criminal Investigation Peter Date have defended these actions, claiming they were in line with the laws of criminal procedure and the decisions of the Supreme Court. However, the district court in Landshut regarded capturing the image of the computer screen every few seconds as a clear violation of the law. According to Date, this raised “a legal and political debate.”

The manufacturer of the Trojan investigated by the CCC is now known. It is the company DigiTask, based in Haiger in the state of Hesse.

DigiTask apparently does very good business with the German authorities. Its clients include the customs authorities, who rendered assistance in a case in Bavaria, installing the Trojan on a suspect’s computer during a customs inspection. According to press reports, from March 2008 to January 2009, the Cologne Customs Office awarded DigiTask €2.7 million in contracts for hardware and software for telecommunications surveillance. According to *Spiegel Online*, the Federal Network Agency has also placed orders with DigiTask.

In early 2008, a price list of the Trojans created by DigiTask was leaked to the Pirate Party. According to this, the monthly rental price for the software is €3,500, a one-time installation on site costs €2,500, and the cost for decoding “per location and per instance” is also €2,500.

According to CCC estimates, the Trojans contain glaring security holes, making it possible for any attacker to easily “take control of a computer infiltrated by the German authorities”.

The Trojans could accept commands without any security or authentication. The screenshots and audio data are encoded in an incompetent way, and the commands used to control the Trojans are even completely unencrypted. Therefore, third parties could easily control the computer if they knew that it contained one of these Trojans.

The use of Trojans makes any “evidentiary chain of custody” out of the question. Even if one assumes that the judges and authorities act according to law, manipulation by a third party cannot be excluded.

The authorities and politicians caught up in this scandal, who have campaigned for years for online monitoring, are now in damage-control mode.

Interior Minister Hans-Peter Friedrich (Christian Social Union, CSU) hastened to claim that the federal authorities had not used the software in question, and recommended that the states no longer use the program examined by CCC.

Justice Minister Sabine Leutheuser-Schnarrenberger (Free Democratic Party, FDP), complained that the requirements laid down by the Supreme Court were not being observed, undermining the confidence of German citizens. The FDP had always warned against the dangers of government snooping software, she claimed—although as a governing party, the FDP has for decades agreed to every tightening of state security laws.

The chairman of the Parliamentary Committee on Internal Affairs Wolfgang Bosbach (Christian Democratic Union, CDU) spoke of serious allegations, but defended the use of secretly-installed computer programs: “They are an investigative tool which the state cannot reject on principle, otherwise it could no longer collect evidence in a series of cases.”

The Social Democratic Party (SPD) called for a parliamentary debate, and SPD General Secretary Andrea Nahles spoke of a “blatant violation of fundamental rights”, although the SPD has always argued for online monitoring.

The illegal spying on citizens using Trojans is neither an accident nor an isolated case. It is part of a systematic stepping up of the powers of the state, supported by all the mainstream parties. Under the pretext of combating crime and terrorism, preparations are being made for a confrontation with broad sections of the population who are increasingly unwilling to bear the burden of the economic and financial crisis.

To contact the WSWS and the Socialist Equality Party visit:

wsws.org/contact