GlobalResearch
Center for Research on Globalization

Germany. Calls for "Less Democracy": Police Caught Planting Spyware on Personal Computers

German secret state agencies installing spyware capable of transforming PC webcam and microphone into listening device

By Tom Burghardt
Global Research, October 16, 2011
Antifascist Calling... 16 October 2011

Region: Europe
Theme: Intelligence, Police State & Civil Rights

Revelations by the Chaos Computer Club (CCC) that German secret state agencies are installing spyware on personal computers capable of transforming a PC's webcam and microphone into a listening device, sparked outrage across the political spectrum.

It has since emerged that despite legal requirements that police do so only with a warrant and only if surveillance intercepts are used to prevent threats to "life, limb or liberty," authorities are not complying with strict limits laid down by Germany's Supreme Court.

And while these disclosures may have ignited a political firestorm in Berlin, they will come as no surprise to readers of *Antifascist Calling*.

Three years ago, I reported that Germany's foreign intelligence service, the *Bundesnachrichtendienst* or BND, was caught up in a major scandal after the whistleblowing web site WikiLeaks, published documents which revealed that the agency had extensively spied on, and even recruited, journalists for use in illicit intelligence operations.

Recalling the CIA's long-running Operation Mockingbird program that enrolled journalists as spies in what are now euphemistically called "influence operations," the covert manipulation of the domestic and foreign press according to WikiLeaks, showed "the extent to which the collaboration of journalists with intelligence agencies has become common and to what dimensions consent is manufactured in the interests of those involved."

BBC News reported that "Bavaria has admitted using the spyware, but claimed it had acted within the law." And *Deutsche Welle* disclosed that "several additional German states have admitted to deploying spyware," including "Baden-Württemberg, Brandenburg, Schleswig-Holstein and Lower Saxony," but like their counterparts in Bavaria, those officials also claimed they had operated "within the parameters of the law"

As I have written many times, the secret state is bound by their own set of "laws." Normal rules and procedures which are supposed to protect citizens from unwarranted government intrusions are deemed inoperative for reasons of "national security."

In the United States, constitutional protections designed to guarantee the right of citizens to protest, enjoy a modicum of privacy in their daily lives or, at the most basic level, have their day in court before being executed, have been overthrown by two successive administrations who assert the right to conduct the affairs of state in secret, according to a

set of legal guidelines which are unreviewable by any court.

It would appear that similar moves are underway in Germany.

‘Backdoor Functionality’

The Chaos Computer Club revealed in their analysis that when they reverse engineered the program, variously dubbed “0zapftis”, “Bundestrojaner” or “R2D2,” they discovered that the spyware “found in the wild” and “submitted to the CCC anonymously,” 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.”

Club researchers learned 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.”

“The government malware can,” analysts noted, “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, 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.”

Their study 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.”

“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,” a CCC spokesperson commented. “The security level this trojan leaves the infected systems in is comparable to it setting all passwords to ‘1234’.”

Nothing ‘Magical’ about this ‘Lantern’

There are glaring similarities between the “R2D2” package deployed by German police and “Magic Lantern” software used by the FBI. As with Bureau spyware, the German program is a keystroke logging virus installed via a malicious email attachment or by exploiting operating system vulnerabilities.

When news of the FBI program first broke back in 2000, the Electronic Privacy Information Center (EPIC) obtained documents under a Freedom of Information Act request relating to the system, which were part of a suite of surveillance tools then called Carnivore.

At the time, EPIC revealed that the FBI "had developed an Internet monitoring system that would be installed at the facilities of an Internet Service Provider (ISP) and would monitor all traffic moving through that ISP."

Once a user is spoofed into installing the malicious Trojan, it is activated when PGP encryption is used to enhance email security. When switched on, the Trojan will log the PGP password which will then allow the agents to read the encrypted communications unbeknownst to the sender. Since its first iteration in the 1990s, such programs are exponentially more sophisticated and are now capable of scooping-up virtually everything a user stores on a computer or handset.

A 2007 exposé by *Wired Magazine* revealed that Magic Lantern's "computer and internet protocol address verifier" or CIPAV, "gathers a wide range of information, including the computer's IP address; MAC address; open ports; a list of running programs; the operating system type, version and serial number; preferred internet browser and version; the computer's registered owner and registered company name; the current logged-in user name and the last-visited URL."

And once that data was obtained, it was siphoned-off to the Bureau's technology laboratory in Quantico, Virginia via fiber optic splitter cables.

As whistleblower Babak Pasdar revealed in 2008, following earlier disclosures by AT&T whistleblower Mark Klein, Verizon, and other giant telecommunications firms, including AT&T, maintained a high-speed DS-3 digital line that handed the Bureau and other security agencies "unfettered" access to the carrier's wireless network, including billing records and customer data "transmitted wirelessly."

Just after the scandal broke, *Wired Magazine* disclosed that "two years before the Bavarian state in Germany began using a controversial spy tool to gather evidence from suspect computers, German authorities approached the Federal Bureau of Investigation to discuss a similar tool the U.S. law enforcement agency was using."

"Bavarian authorities," *Wired* reported, "began using their spyware in 2009. It's not known if that spyware is based on the FBI's, but in July 2007, German authorities contacted the FBI seeking information about its tool."

The FBI's assistant legal attache in Frankfurt "sent an email to Bureau colleagues on July 24, 2007, writing, 'I am embarrassed to be approaching you again with a request from the Germans … but they now have asked us about CIPAV (Computer Internet Protocol Address Verifier) software, allegedly used by the Bu[reau]'."

The email uncovered by *Wired* was part of a huge cache of files obtained by the Electronic Frontier Foundation (EFF) in response to their 2007 Freedom of Information Act request for data on CIPAV.

In the years since those disclosures, secret state surveillance is more pervasive than ever and and now includes the "lawful interception" of GPS locational data streamed automatically to their manufacturers or hosting services by smart phones.

It appears that German secret state officials are playing a similar game. According to *Der Spiegel*, at least two agencies, the Bundeskriminalamt, or BKA, the federal crime investigation agency equivalent to the FBI, and some 16 Landeskriminalamt or LKAs,

regional investigative bureaus, may have deployed the malware during wide-ranging investigations unrelated to terrorism.

Following Chaos Computer Club revelations, it is clear that German authorities have been caught red-handed violating a landmark decision by the Supreme Court. “The court,” *Der Spiegel* noted, “specified that online spying was only permissible if there was concrete evidence of danger to individuals or society.”

In a follow-up piece, *Der Spiegel* disclosed that the firm DigiTask was the spyware’s developer. Along with hundreds of similar firms, DigiTask is a niche security outfit that develops applications for the so-called “lawful interception” market.

In 2008, WikiLeaks released two documents concerning “interception technology for Skype and SSL in Bavaria, Germany. The first document is a communication by the Bavarian Ministry of Justice to the prosecutors office, relating to cost distribution for the interception licenses between police and prosecution. The second document allegedly presents the offer made by Digitask, the German company developing the technology, and holds information on pricing and license model, high-level technology descriptions and other detail.”

According to the WikiLeaks analysis, the DigiTask offer “introduces a basic description of the cryptographic workings of Skype, and concludes that new systems are needed to spy on Skype calls.”

We were informed in that letter that German police were interested in standing-up a “*Skype Capture Unit*.”

“In a nutshell: malware is installed onto a target machine, to intercept Skype Voice and Chat. Another feature introduced is a recording proxy, that is not part of the offer, yet would allow for anonymous proxying of recorded information to a target recording station. Access to the recording station is possible via a multimedia streaming client, supposedly offering real-time interception.”

“Another part of the offer,” WikiLeaks noted, was related to “an interception method for SSL based communication, working on the same principle of establishing a man-in-the-middle attack on the key material on the client machine. According to the offer, this method works for Internet Explorer and Firefox web browsers. Digitask also recommends using overseas proxy servers, to cover the tracks of all activities.”

As it turns out those proxy servers were conveniently located in the United States. This raises the distinct possibility that information captured by German secret state officials is also being shared with “partner agencies” of their close NATO ally, the CIA, FBI and NSA.

This was confirmed by CCC’s analysis of R2D2’s code. “To avoid 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.”

“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.”

The short answer is, they *can't.*

Aside from lining the pockets of DigiTask shareholders, there are more sinister uses for the malware. As the *World Socialist Web Site* noted "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."

This would certainly be a convenient way to "neutralize" a troublesome politician, journalist or over-eager anticorporate campaigner.

'Less Democracy'

Following similar efforts in the United States, evidence that police are illegally spying on German citizens using sophisticated malware developed for the government are neither benign nor accidental events.

As a recent article in *German Foreign Policy* disclosed, leading voices in Europe's largest state are "pleading for a transition toward 'less democracy'." A recent book, published under the title, *Dare Less Democracy*, claims that the "voice of the people" and the "'emancipatory Zeitgeist, putting everything into question,' has a too 'paralyzing influence" on current governance'."

"The author," the critical online leftist magazine observes, "demands to 'correct the system' for 'more efficient policy making.' These 'corrections' must include the dismantlement of democratic participation."

Author Laszlo Trankovits, the bureau chief of the Deutsche Presse Agentur in South Africa, who had previously worked for the agency in Washington "as its White House correspondent," explained "it should never be suggested that a 'democratic society can do away with inequality and establish social justice'."

"Trankovits," *German Foreign Policy* notes, is "a member of the elitist Rotary-Club." He demands that "the elite clearly 'commits itself to capitalism and profit,' and that 'intelligent forms of public relations' be used to communicate policy measures to the population. However, the demand for more 'transparency' is 'counterproductive and paralyzing' for any 'governance efficiency' and must be rejected."

That drivel such as this was penned by a journalist for Germany's leading news agency, to whit, that the media should serve as a propaganda mouthpiece for casino capitalist interests, is one more sign that democratic norms, already seriously eroded in the West, are now being rapidly jettisoned by our political masters.

With the global capitalist system on the verge of a repeat performance of the 2008 meltdown, and with a worldwide resurgence of opposition to the one-sided costs of saving a system of financial plunder borne by the working class, elite calls for "less democracy" are warning signs that stern measures, including blanket surveillance and naked police violence, are in the offing.

Tom Burghardt *is a researcher and activist based in the San Francisco Bay Area. In*

addition to publishing in Covert Action Quarterly and Global Research, Montreal, he is a Contributing Editor with Cyrano's Journal Today. His articles can be read on Dissident Voice, The Intelligence Daily, Pacific Free Press, Uncommon Thought Journal, and the whistleblowing website WikiLeaks. He is the editor of Police State America: U.S. Military "Civil Disturbance" Planning, distributed by AK Press and has contributed to the new book from Global Research, The Global Economic Crisis: The Great Depression of the XXI Century.

Comment on Global Research Articles on our Facebook page

Become a Member of Global Research

Articles by: Tom Burghardt
http://antifascist-calling.blogspot.com/