By Bob Sullivan

A well-regarded Germany-based hacker group claims a German government-created Trojan horse program is capable of secretly spying on Web users without their consent.

The group says on its website that it obtained and analyzed a piece of software that is supposed to be a "lawful interception" program designed to listen in on Internet-based phone calls as part of a legal wiretap, but its capabilities go far beyond legal bounds.

The program is capable of logging keystrokes, activating Webcams, monitoring Web users' activities and sending mountains of data to government officials, the club said.

To cover its tracks, the data is routed through rented servers located in the United States, the club alleges.

"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 Club said on its website.

The German government has yet to comment on the findings, but already, antivirus companies are reacting to them. Security firm F-Secure will detect and disable the alleged government monitoring software if found on clients' computers, it announced on Saturday.

"Yes, it is possible the Trojan found by CCC is written by the German government. We just can't confirm that," said Mikko Hypponen, F-Secure's chief technology officer, via Twitter.

The program, labeled a "backdoor" because it can open a computer to surreptitious access, targets certain applications for keylogging, including Firefox, Skype, MSN Messenger, ICQ and others, according to F-Secure.

"We do not know who created this backdoor and what it was used for," Hypponen wrote on

F-Secure's blog . "(But) We have no reason to suspect CCC's findings."

German courts have long allowed use of a backdoor program known as "Bundestrojan" — "federal Trojan," in English — which permits government investigators to listen in on Skype-based phone calls as part of a legal wiretap order. Skype and other kinds of Internet phone calls that can be encrypted are particularly troubling for law enforcement, because they can be used by suspects to evade wiretaps.

After a court battle in 2008, Bundestrojan was ruled legal as long as it screened only very specific communications — essentially, Internet telephone calls.

But the Chaos Computer Club announced Saturday that it had obtained a copy of what it believed was a copy Bundestrojan, and that the program has capabilities that go far beyond legal wiretapping. In addition to keylogging and screen shots, the software is also capable of remote control and upgrade.

"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.... 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," said the club on its site. "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 club also criticized security measures put in place by programmers of the alleged Trojan. Poor encryption implementation means a malicious third-party could intercept the government communications, or take control of government-infected machines, it said.

"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," the club said. "The security level this trojan leaves the infected systems in is comparable to it setting all passwords to '1234.' "

Worse yet, the flaws make it possible to place false evidence on a suspect's computer.

"(This) puts the whole rationale for this method of investigation into question," the club said.

The well-regarded hacker group, founded in the 1970s, didn't say where it had obtained the program, but said it had analyzed several different copies. It said the German Ministry of the Interior had been informed about the findings, and the club publicly demand that the German government stop using the program and initiate its self-destruction capabilities.

While Bundestrojan is designed to tap communications of suspects after a government official obtain permission from a German court, there is no technical reason that the software could not be used on U.S. citizens traveling in Germany, or even on Web users who are outside of Germany.

Government use of voice-over-IP monitoring software first came to light in 2006 when the Swiss government announced it was considering software written by Swiss-based ERA IT Solutions. At the time, Switzerland said the program's use would require a court order.

Antivirus companies have long held that they would detect and disable any such government-monitoring software found on users' machines. That public stance dates from 2001, when an msnbc.com report revealed that the FBI had developed a Trojan called Magic Lantern, which had capabilities similar to Bundestrojan. F-Secure's policy statement on Bundestrojan references Magic Lantern
.

Still, the firm said it has not yet faced a direct confrontation with a government agency over the policy.

“We have never before analyzed a sample that has been suspected to be governmental backdoor," it said Saturday. "We have also never been asked by any government to avoid

detecting their backdoors."

The Chaos Computer Club used the announcement to make a generic plea for less electronic monitoring by government officials.

"The (government) 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," it said. "Unfortunately, for too long the (government) 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."

Source