Hacker group accuses German government of using illegal Trojan horse

October 11 2011, by Bob Yirka

(PhysOrg.com) -- Governments all over the world are wrestling with the legalities of computer snooping in their efforts to catch people doing illegal things, or to prove that wrongful acts have been committed after the fact. Now comes a blog posting by a well-known hacker group that calls itself the Chaos Computer Club (CCC), accusing the German government of overstepping its bounds by infecting suspected criminal's computers with a Trojan horse program that allows it to do more than has been granted by law.

The program, which the group calls "Bundestrojaner" or *State Trojan* in German, is purportedly able to scrape a hard drive looking for data, grab screen shots, insert a program to run or turn on a computer's microphone and video camera. German law allows law enforcement to use a Trojan program to monitor Skype type conversations, but nothing else. Thus, if the accusations by the CCC turn out to be true, someone in government in Germany is going to be in a lot of hot water.

So far two separate antivirus companies (Sophos and F-Secure) have verified that the Trojan does exist and that it does what the CCC claims it does, but neither is willing to suggest that there is proof the German government is behind its development and/or use. For its part, representatives of the German government, at least at the federal level, have denied using any illegal software to catch criminals.

The posting by the CCC came about when the group was approached by a lawyer who had a client who believed he'd been hacked - screen shots

of his computer were presented at trial. The lawyer handed over the computer to the CCC who examined it and found the Trojan. Thus, it appears that if the Trojan was commissioned and used by the government, it likely it was done at a more local level.

So far, three German states have admitted using a Trojan program to gather information from computers used by suspects, but all of them insist that they've only used the type allowed by law, i.e. to monitor Skype conversations, similar to old-fashioned telephone wire-tapping.

Also, a company called DigiTask was unveiled recently by Wikileaks, as a maker of such Trojan type software programs, and when queried admitted they had created a Trojan called Quellen-TKU, which they says only allows for Skype type activities on computers. A spokesman for the company says it is looking into whether it's Trojan may have been modified into the Bundestrojaner by a third-party.

The German government is apparently looking into the whole matter and further announcements are likely to come as more information becomes available.

© 2011 PhysOrg.com