January 2004 to September 2015

f-secure.com/weblog/archives/00002249.html

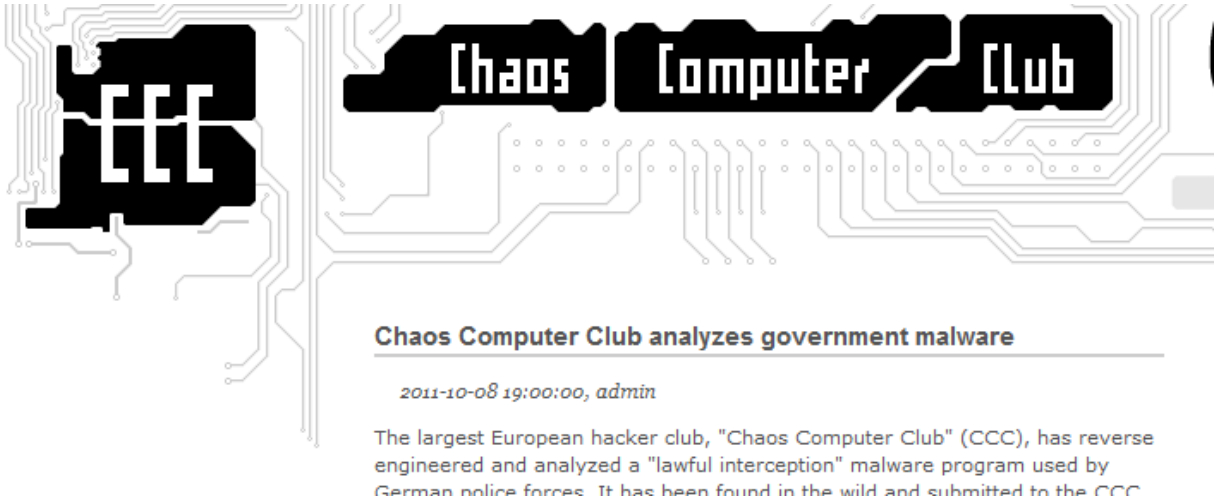
F-SECURE LABS

<<< NEWS FROM THE LAB - Saturday, October 8, 2011 >>>

ARCHIVES | **SEARCH**

Possible Governmental Backdoor Found ("Case R2D2")	Posted by Mikko @ 20:42 GMT

Chaos Computer Club from Germany has tonight announced that they have located a backdoor trojan used by the German Government.



The announcement was made public on ccc.de with a detailed 20-page analysis of the functionality of the malware.
Download the report in PDF (in German).

The malware in question is a Windows backdoor consisting of a DLL and a kernel driver.

The backdoor includes a keylogger that targets certain applications. These applications include **Firefox, Skype, MSN Messenger, ICQ** and others.

The backdoor also contains code intended to take screenshots and record audio, including recording Skype calls.

In addition, the backdoor can be remotely updated. Servers that it connects to include 83.236.140.90 and 207.158.22.134.

We do not know who created this backdoor and what it was used for.

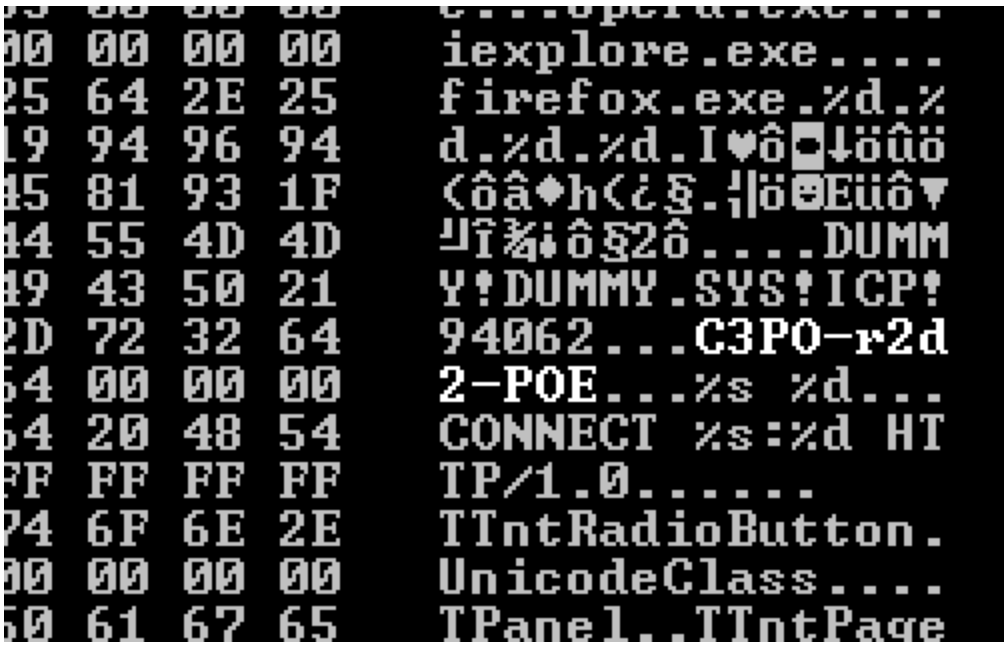
We have no reason to suspect CCC's findings, but we can't confirm that this trojan was written by the German government. As far as we see, the only party that could confirm that would be the German government itself.

Our generic policy on detecting governmental backdoors or "lawful interception" police trojans can be read here.

We have never before analyzed a sample that has been suspected to be governmental backdoor. We have also never been asked by any government to avoid detecting their backdoors.

Having said that, we detect this backdoor as Backdoor:W32/R2D2.A

The name R2D2 comes from a string inside the trojan: "C3PO-r2d2-POE". This string is used internally by the trojan to initiate data transmission.



We are expecting this to become a major news story. It's likely there will be an official response from the German government.

MD5 hashes: *930712416770A8D5E6951F3E38548691* and *D6791F5AA6239D143A22B2A15F627E72*