German researchers develop defense software: Potential protection against the "Hacienda" intelligence program

August 15 2014

Scientists have developed free software that can help to prevent cyberattacks. (Photo: Artur Marciniec/Fotolia.com) Scientists have developed free software that can help to prevent cyberattacks.Credit: Artur Marciniec/Fotolia.com

Today, a group of journalists has reported the existence of the

"Hacienda" spy program. According to this report, five western intelligence agencies are using the Hacienda software to identify vulnerable servers across the world in order to control them and use them for their own purposes. Scientists at the Technische Universität München (TUM) have developed free software that can help prevent this kind of identification and thus the subsequent capture of systems.

Port scanners are programs that search the Internet for systems that exhibit potential vulnerabilities. According to the report published today by journalists at Heise Online, Hacienda is one such port scanning program. The report says that this program is being put into service by the "Five Eyes," a federation of the secret services of the USA, Canada, the UK, Australia and New Zealand. "The goal is to identify as many servers as possible in other countries that can be remotely controlled," explains Dr. Christian Grothoff, Emmy Noether research group leader at the TUM Chair for Network Architectures and Services.

New Free Software "TCP Stealth"

Grothoff and his students at TUM have developed the "TCP Stealth" defense software, which can inhibit the identification of systems through both Hacienda and similar cyberattack software and, as a result, the undirected and massive takeover of computers worldwide, as Grothoff explains. "TCP Stealth" is free software that has as its prerequisites particular system requirements and computer expertise, for example, use of the GNU/Linux operating system. In order to make broader usage possible in the future, the software will need further development.

But even now, through "TCP Stealth," the researchers are already putting an additional defensive tool into the hands of system administrators, as firewalls, virtual private networks (VPNs) and other existing techniques provide only limited protection against such cyberattacks.

The connection between a user and a server on the Internet occurs using the so-called Transmission Control Protocol (TCP). The user's computer first has to identify itself to a service by sending a data packet to the server. "This is the user asking, 'Are you there?'" explains Grothoff. The service then answers the user's request; within this response alone, there is often information transmitted that adversaries can use for an attack.

Secret Token is Transmitted Invisibly

The free software developed by TUM researchers is based on the following concept: There exists a number that is only known to the client computer and the server. On the basis of this number, a secret token is generated, which is transmitted invisibly while building the initial connection with the server. If the token is incorrect, the system simply doesn't answer, and the service appears to be dead. While similar defensive measures are already known, the protection capabilities of the new software is higher than that of extant techniques.

In particular, in contrast to existing defensive software, "TCP Stealth" also protects against a further variant of this kind of cyberattack. The attack occurs when an adversary interposes himself between the user and the server into an already existing connection. The data sent by the user to the server is then captured and replaced with other information. This is analogous to pulling an envelope from the mailbox after it has been deposited, removing the contents from that envelope, and replacing them with a different letter.

In order to prevent this, a verification code is also sent while building the initial connection. The server can then use this to detect whether or not it has received the correct data.

More information: Experts who would like to review, deploy or further develop the software can download it at gnunet.org/knock xperts

who would like to review, deploy or further develop the software can download it at gnunet.org/knock

Provided by Technical University Munich