COMPUTER FRAUD & SECURITY

October 2003

ISSN 1361-3723

Managing Security Budget pg — 8

Future abuses of Biometrics pg — 12

Editorial Office:
Elsevier Advanced Technology, PO Box 150 Kidlington, Oxford OX5 1AS, UK
Tel: +44-(0)1865-843645
Fax: +44-(0)1865-843971
Email: s.hilley@elsevier.com

Subscription Price for one year:
(12 issues) US$782/¥96,000/€722.00
including first class airmail delivery subject to our prevailing exchange rate

Price valid to end of 2003

Subscription Enquiries:
Orders and Payments:

For customers residing in the Americas (North, South and Central America):
Elsevier Journals Customer Service
6277 Sea Harbor Drive
Orlando, FL 32887-4800, USA
North American customers:
Tel: +1 (877) 839-7126
Fax: +1 (407) 363-1354
Customers outside US:
Tel: +1 (407) 345-4020
Fax: +1 (407) 363-1354
Email: usinfo-f@elsevier.com

For customers in the rest of the World:
Elsevier Science Customer Support Department
PO Box 211, 1000 AE Amsterdam, The Netherlands
Tel: (+31) 20-3853757
Fax: (+31) 20-4853432
Email: nlinfo-f@elsevier.com

To order from our website:
www.compseconline.com

ELSEVIER

Publishers of
Network Security
Computers & Security
Computer Fraud & Security
Computer Law & Security Report
Information Security Technical Report

Viruses Bottleneck Prosecution

Catherine Everett

Viruses and Trojan horses are presenting an increasing challenge to law enforcement agencies as they introduce an element of doubt into what would otherwise be cut-and-dried legal cases.

A recent example of this in the UK involves criminal proceedings relating to Julian Green, who was accused of having child pornography images on his PCs, but was subsequently acquitted due to the presence of Trojan horses on his hard drive.

Another US-based case involved Eugene Pitts, an Alabama-based accountant who was found innocent by a jury of nine counts of tax evasion and filing fraudulent personal and business state income tax returns.

He claimed that a computer virus was to blame for under-reporting the income of his firm, Pitts, Daniels & Co between 1997 and 1999, although state prosecutors noted that the alleged virus did not affect the tax returns of customers, even though they were prepared on the same machine.

Trojan horses, such as the infamous BackOriface, install a so called backdoor on a computer that enables hackers to take control of the machine in order to upload information, access personal data, or even use the machine as a proxy for spam so that such usage cannot be traced back to them.

Continued on page 2...

DHS Security Efforts under Fire

Wayne Madsen

The US Department of Homeland Security is being slammed by US National Security Experts for losing prominent cybersecurity experts, and placing the cybersecurity division down the list in terms of political weight.

At a July hearing of the US House Homeland Security Subcommittee on Cybersecurity, Science, and Research and Development, Representative Zoe Lofgren of California questioned the Department' of Homeland's commitment to cyber security. She highlighted the fact that during the first half of 2003, four of the Bush administration's cyber-security officials - Richard Clarke, the Special Advisor to the President for Cybersecurity; Howard Schmidt, the vice-chairman of the President's Critical Infrastructure Advisory Board; Ron Dick, the director of the National Infrastructure Protection Center (NIPC) and John Tritak, the director of the Critical Infrastructure

Continued on page 2...

Contents

In Brief

CITIBANK CUSTOMERS FACE HOAX SPAM

Citibank customers are being targeted by a hoax email requesting they provide their social security details or else face account shutdown. The scam directs customers to a spoofed website, that is an imitation of the real Citibank site and asks them to enter their name and ATM card number. Citibank has issued a statement warning customers to be on the look out for the scam.

RIAA SUE 261 FOR FILE SWAPPING

The Recording Industry Association of America (RIAA) has sued 261 people for exchanging music files in peer-to-peer networks. This is the first time that the RIAA has targeted individuals as in the past Kazaa and other P2P sites bore the brunt of its legal action. The RIAA is only suing file swappers who have allowed access to their hard drive so others can download their collection. It is not filing lawsuits against people who only download music from others without sharing.

WORM AIMS AT BRITISH PM

A new low-risk email worm targets the British Prime Minister, Tony Blair. The worm tries to launch a denial-of-service attack on www.number-10.gov.uk, the official website of Blair.

Continued from page 1 top

Trevor Mascarenhas, a partner at Philippsohn Crawford Berwald, explains: "Trojan horses have the potential to call into question the whole system of evidence for computer cases."

While in a civil case, prosecutors have to show that the defendant is guilty on a balance of probability, in a criminal suit, they have to demonstrate this beyond all reasonable doubt.

As a result, Mascarenhas warns: "A defendant might well be able to produce enough evidence to cast doubt over the prosecution's case and effectively destroy it."

Peter Sommer, research fellow at the London School of Economics and an expert witness for the police since 1985, says he has come across Trojan horse-related cases for more than three years and is aware of the potential ambiguity they can cause.

"If you're caught with child porn on your computer, you know that if you're found guilty, your life is going to undergo uncomfortable changes, so you're probably going to be fairly desperate to light on any excuse. But I've also come across cases where people have had a practical joke played on them or someone uploaded porn onto their computer out of malice," he explains.

However, there are certain procedures that computer forensics experts follow to try and establish innocence or guilt. The first stage is to make a copy of the computer in question as early as possible to ensure that it is not contaminated. Next it is mounted as a second disk onto another machine so experts can examine it and run a standard anti-virus program to see what results.

"This is the first point of failure for an argument because if you can't find a Trojan, the defence doesn't go any further. If you find one, however, it becomes necessary to look at the totality of the circumstances and the quantity of incriminating material found," Sommer says.

Such circumstances include establishing if a defendant is vulnerable, for example, as a result of using an always-on connection rather than a dial-up modem and looking at the time and date stamps of offending material to identify whether and how much material has been uploaded on a regular basis or over a limited number of sessions.

Continued from page 1 bottom

Assurance Office (CIAO) - all left the government.

Lofgren criticized the Bush administration for placing the National Cybersecurity Division far down in the chain of command in DHS and dividing responsibilities for cybersecurity between various entities within the Department, including the Science and Technology Directorate and the Homeland Security Advanced Research Projects Agency. She said, "the NCSD is located within the DHS Information Analysis and Infrastructure Protection Directorate, reporting to the assistant secretary for infrastructure protection." Lofgren added, "some cybersecurity-related R&D activities, however, will take place within the DHS Science and Technology Directorate. I believe that this situation, where it's buried within the bureaucracy . . . once a person is finally chosen to lead the division he or she may not receive the high level access to Secretary Ridge and the White House that is warranted."

At the same hearing Daniel G. Wolf, NSA's Deputy Director for Information Assurance proposed the creation of a National Software Assurance Center (NSAC), which would likely be under

02065
Printed by Mayfield Press (Oxford) Ltd