

The New York Times

May 10, 2005

Internet Attack Called Broad and Long Lasting by Investigators

By [JOHN MARKOFF](#) and LOWELL BERGMAN

SAN FRANCISCO, May 9 - The incident seemed alarming enough: a breach of a [Cisco Systems](#) network in which an intruder seized programming instructions for many of the computers that control the flow of the Internet.

Now federal officials and computer security investigators have acknowledged that the Cisco break-in last year was only part of a more extensive operation - involving a single intruder or a small band, apparently based in Europe - in which thousands of computer systems were similarly penetrated.

Investigators in the United States and Europe say they have spent almost a year pursuing the case involving attacks on computer systems serving the American military, NASA and research laboratories.

The break-ins exploited security holes on those systems that the authorities say have now been plugged, and beyond the Cisco theft, it is not clear how much data was taken or destroyed. Still, the case illustrates the ease with which Internet-connected computers - even those of sophisticated corporate and government networks - can be penetrated, and also the difficulty in tracing those responsible.

Government investigators and other computer experts sometimes watched helplessly while monitoring the activity, unable to secure some systems as quickly as others were found compromised.

The case remains under investigation. But attention is focused on a 16-year-old in Uppsala, Sweden, who was charged in March with breaking into university computers in his hometown. Investigators in the American break-ins ultimately traced the intrusions back to the Uppsala university network.

The F.B.I. and the Swedish police said they were working together on the case, and one F.B.I. official said efforts in Britain and other countries were aimed at identifying accomplices. "As a result of recent actions" by law enforcement, an F.B.I. statement said, "the criminal activity appears to have stopped."

The Swedish authorities are examining computer equipment confiscated from the teenager, who was released to his parents' care. The matter is being treated as a juvenile case.

Investigators who described the break-ins did so on condition that they not be identified, saying that their continuing efforts could be jeopardized if their names, or in some cases their organizations, were disclosed.

Computer experts said the break-ins did not represent a fundamentally new kind of attack. Rather, they said, the primary intruder was particularly clever in the way he organized a system for automating the theft of computer log-ins and passwords, conducting attacks through a complicated maze of computers connected to the Internet in as many as seven countries.

The intrusions were first publicly reported in April 2004 when several of the nation's supercomputer laboratories acknowledged break-ins into computers connected to the TeraGrid, a high-speed data network serving those labs, which conduct unclassified research into a range of scientific problems.

The theft of the Cisco software was discovered last May when a small team of security specialists at the supercomputer laboratories, trying to investigate the intrusions there, watched electronically as passwords to Cisco's computers were compromised.

After discovering the passwords' theft, the security officials notified Cisco officials of the potential threat. But the company's software was taken almost immediately, before the company could respond.

Shortly after being stolen last May, a portion of the Cisco programming instructions appeared on a Russian Web site. With such information, sophisticated intruders would potentially be able to compromise security on router computers of Cisco customers running the affected programs.

There is no evidence that such use has occurred. "Cisco believes that the improper publication of this information does not create increased risk to customers' networks," the company said last week.

The crucial element in the password thefts that provided access at Cisco and elsewhere was the intruder's use of a corrupted version of a standard software program, SSH. The program is used in many computer research centers for a variety of tasks, ranging from administration of remote computers to data transfer over the Internet.

The intruder probed computers for vulnerabilities that allowed the installation of the corrupted program, known as a Trojan horse, in place of the legitimate program.

In many cases the corrupted program is distributed from a single computer and shared by tens or hundreds of users at a computing site, effectively making it possible for someone unleashing it to reel in large numbers of log-ins and passwords as they are entered.

Once passwords to the remote systems were obtained, an intruder could log in and use a variety of software "tool kits" to upgrade his privileges - known as gaining root access. That makes it possible to steal information and steal more passwords.

The operation took advantage of the vulnerability of Internet-connected computers whose security software had not been brought up to date.

In the Cisco case, the passwords to Cisco computers were sent from a compromised computer by a legitimate user unaware of the Trojan horse. The intruder captured the passwords and then used them to enter Cisco's computers and steal the programming instructions, according to the security investigators.

A security expert involved in the investigation speculated that the Cisco programming instructions were stolen as part of an effort to establish the intruder's credibility in online chat rooms he frequented.

Last May, the security investigators were able to install surveillance software on the University of Minnesota computer network when they discovered that an intruder was using it as a staging base for hundreds of Internet attacks. During a two-day period they watched as the intruder tried to break into more than 100 locations on the Internet and was successful in gaining root access to more than 50.

When possible, they alerted organizations that were victims of attacks, which would then shut out the intruder and patch their systems.

As the attacks were first noted in April 2004, a researcher at the University of California, Berkeley, found that her own computer had been invaded. The researcher, Wren Montgomery, began to receive taunting e-mail messages from someone going by the name Stakkato - now believed by the authorities to have been the primary intruder - who also boasted of breaking in to computers at military installations.

"Patuxent River totally closed their networks," he wrote in a message sent that month, referring to the Patuxent River Naval Air Station in Maryland. "They freaked out when I said I stole F-18 blueprints."

A Navy spokesman at Patuxent River, James Darcy, said Monday said that "if there was some sort of attempted breach on those addresses, it was not significant enough of an action to have generated a report."

Monte Marlin, a spokeswoman for the White Sands Missile Range in New Mexico, whose computers Stakkato also claimed to have breached, confirmed Monday that there had been "unauthorized access" but said, "The only information obtained was weather forecast information."

The messages also claimed an intrusion into seven computers serving NASA's Jet Propulsion Laboratory in Pasadena, Calif. A computer security expert investigating the

case confirmed that computers at several NASA sites, including the propulsion laboratory, had been breached. A spokesman said the laboratory did not comment on computer breaches.

Ms. Montgomery, a graduate student in geophysics, said that in a fit of anger, Stakkato had erased her computer file directory and had destroyed a year and a half of her e-mail stored on a university computer.

She guessed that she might have provoked him by referring to him as a "quaint hacker" in a communication with system administrators, which he monitored.

"It was inconvenient," she said of the loss of her e-mail, "and it's the thing that seems to happen when you have malicious teenage hackers running around with no sense of ethics."

Walter Gibbs, in Oslo, and Heather Timmons, in London, contributed reporting for this article.