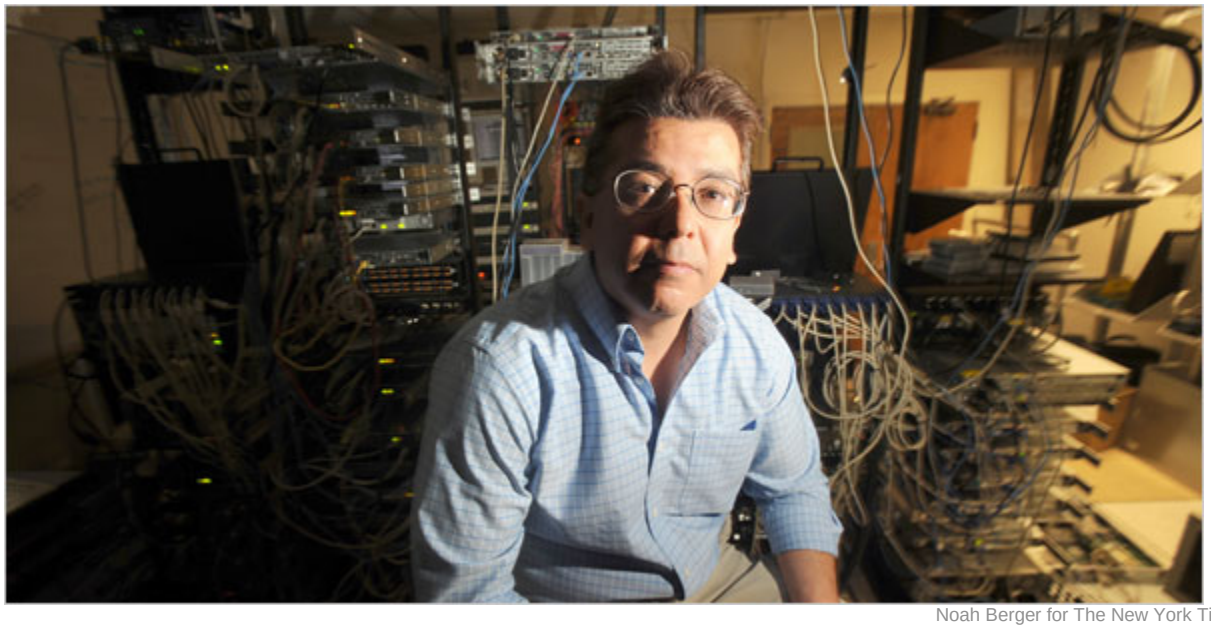
Thieves Winning Online War, Maybe Even in Your Computer



Noah Berger for The New York Times

Phillip Porras, a computer security expert at SRI International, a science and technology research group.

By JOHN MARKOFF
Published: December 5, 2008

SAN FRANCISCO — Internet security is broken, and nobody seems to know quite how to fix it.

Despite the efforts of the computer security industry and a half-decade struggle by Microsoft to protect its Windows operating system, malicious software is spreading faster than ever. The so-called malware surreptitiously takes over a PC and then uses that computer to spread more malware to other machines exponentially. Computer scientists and security researchers acknowledge they cannot get ahead of the onslaught.

As more business and social life has moved onto the Web, criminals thriving on an underground economy of credit card thefts, bank fraud and other scams rob computer users of an estimated $100 billion a year, according to a conservative estimate by the Organization for Security and Cooperation in Europe. A Russian company that sells fake antivirus

software that actually takes over a computer pays its illicit distributors as much as $5 million a year.

With vast resources from stolen credit card and other financial information, the cyberattackers are handily winning a technology arms race.

“Right now the bad guys are improving more quickly than the good guys,” said Patrick Lincoln, director of the computer science laboratory at SRI International, a science and technology research group.

A well-financed computer underground has built an advantage by working in countries that have global Internet connections but authorities with little appetite for prosecuting offenders who are bringing in significant amounts of foreign currency. That was driven home in late October when RSA FraudAction Research Lab, a security consulting group based in Bedford, Mass., discovered a cache of half a million credit card numbers and bank account log-ins that had been stolen by a network of so-called zombie computers remotely controlled by an online gang.

In October, researchers at the Georgia Tech Information Security Center reported that the percentage of online computers worldwide infected by botnets — networks of programs connected via the Internet that send spam or disrupt Internet-based services — is likely to increase to 15 percent by the end of this year, from 10 percent in 2007. That suggests a staggering number of infected computers, as many as 10 million, being used to distribute spam and malware over the Internet each day, according to research compiled by PandaLabs.

Security researchers concede that their efforts are largely an exercise in a game of whack-a-mole because botnets that distribute malware like worms, the programs that can move from computer to computer, are still relatively invisible to commercial antivirus software. A research report last month by Stuart Staniford, chief scientist of FireEye, a Silicon Valley computer security firm, indicated that in tests of 36 commercial antivirus products, fewer than half of the newest malicious software programs were identified.

There have been some recent successes, but they are short-lived. On Nov. 11, the volume of spam, which transports the malware, dropped by half around the globe after an Internet service provider disconnected the McColo Corporation, an American firm with Russian ties, from the Internet. But the respite is not expected to last long as cybercriminals regain control of their spam-generating computers.

“Modern worms are stealthier and they are professionally written,” said Bruce Schneier, chief security technology officer for British Telecom. “The criminals have gone upmarket, and they’re organized and international because there is real money to be made.”

The gangs keep improving their malware, and now programs can be written to hunt for a specific type of information stored on a personal computer. For example, some malware uses the operating system to look for recent documents created by a user, on the assumption they will be more valuable. Some routinely watch for and then steal log-in and password information, specifically consumer financial information.

The sophistication of the programs has in the last two years begun to give them almost lifelike capabilities. For example, malware programs now infect computers and then routinely use their own antivirus capabilities to not only disable antivirus software but also remove competing malware programs. Recently, Microsoft antimalware researchers disassembled an infecting program and were stunned to discover that it was programmed to turn on the Windows Update feature after it took over the user’s computer. The infection was ensuring that it was protected from other criminal attackers.

And there is more of it. Microsoft has monitored a 43 percent jump in malware removed from Windows computers just in the last half year.

The biggest problem may be that people cannot tell if their computers are infected because the malware often masks its presence from antivirus software. For now, Apple’s Macintosh computers are more or less exempt from the attacks, but researchers expect Apple machines to become a larger target as their market share grows.

The severity of the situation was driven home not long ago for Ed Amaroso, AT&T's chief security official. "I was at home with my mother's computer recently and I showed her it was attacking China," he said. " 'Can you just make it run a little faster?' she asked, and I told her 'Ma, we have to reimage your hard disk.' "

Beyond the billions of dollars lost in theft of money and data is another, deeper impact. Many Internet executives fear that basic trust in what has become the foundation of 21st century commerce is rapidly eroding. "There's an increasing trend to depend on the Internet for a wide range of applications, many of them having to deal with financial institutions," said Vinton G. Cerf, one of the original designers of the Internet, who is now Google's "chief Internet evangelist."

"The more we depend on these types of systems, the more vulnerable we become," he said.

The United States government has begun to recognize the extent of the problem. In January, President Bush signed National Security Presidential Directive 54, establishing a national cybersecurity initiative. The plan, which may cost more than $30 billion over seven years, is directed at securing the federal government's own computers as well as the systems that run the nation's critical infrastructure, like oil and gas networks and electric power and water systems.

That will do little, however, to help protect businesses and consumers who use the hundreds of millions of Internet-connected personal computers and cellphones, the criminals' newest target.

Despite new technologies that are holding some attackers at bay, several computer security experts said they were worried that the economic downturn will make computer security the first casualty of corporate spending cuts. Security gets hit because it is hard to measure its effectiveness, said Eugene Spafford, a computer scientist at Purdue University.

He is pessimistic. “In many respects, we are probably worse off than we were 20 years ago,” he said, “because all of the money has been devoted to patching the current problem rather than investing in the redesign of our infrastructure.”

The cyber-criminals appear to be at least as technically advanced as the most sophisticated software companies. And they are faster and more flexible. As software companies have tightened the security of the basic operating systems like Windows and Macintosh, attackers have moved on to Web browsers and Internet-connected programs like Adobe Flash and Apple QuickTime.

This has led to an era of so-called “drive-by infections,” where users are induced to click on Web links that are contained in e-mail messages. Cyber-criminals have raised the ability to fool unsuspecting computer users into clicking on intriguing messages to a high art.

Researchers note that the global cycle of distributing security patches inevitably plays to the advantage of the attacker, who can continually hunt for and exploit new backdoors and weaknesses in systems. This year, computer security firms have begun shifting from traditional anti-virus program designs, which are regularly updated on subscribers’ personal computers, to Web-based services, which can be updated even faster.

Security researchers at SRI International are now collecting over 10,000 unique samples of malware daily from around the globe. “To me it feels like job security,” said Phillip Porras, an SRI program director and the computer security expert who led the design of the company’s Bothunter program, available free at www.bothunter.net.

“This is always an arm race, as long as it gets into your machine faster than the update to detect it, the bad guys win,” said Mr. Schneier.