



January 20, 2010

Fearing Hackers Who Leave No Trace

By [JOHN MARKOFF](#) and [ASHLEE VANCE](#)

MOUNTAIN VIEW, Calif. — The crown jewels of [Google](#), [Cisco Systems](#) or any other technology company are the millions of lines of programming instructions, known as source code, that make its products run.

If hackers could steal those key instructions and copy them, they could easily dull the company's competitive edge in the marketplace. More insidiously, if attackers were able to make subtle, undetected changes to that code, they could essentially give themselves secret access to everything the company and its customers did with the software.

The fear of someone building such a back door, known as a Trojan horse, and using it to conduct continual spying is why companies and security experts were so alarmed by Google's disclosure last week that hackers based in China had stolen some of its intellectual property and had conducted similar assaults on more than two dozen other companies.

"Originally we were saying, 'Well, whoever got it has the secret sauce to Google and some 30 other California companies, and they can replicate it,'" said Rick Howard, director of security intelligence at [VeriSign](#) iDefense, which helped Google investigate the Chinese attacks. "But some of the more devious folks in our outfit were saying, 'Well, they could also insert their own code — and they probably have.'"

For example, a foreign intelligence agency might find it extremely useful to know who was asking particular questions of Google's search engine.

Security researchers took particular interest in the fact that the Silicon Valley company [Adobe Systems](#) was one of the companies hit by the recent wave of attacks.

Computer users around the globe have Adobe's Acrobat or Reader software sitting on their machines to create or read documents, and Adobe's Flash technology is widely used to present multimedia content on the Web and mobile phones.

"Acrobat is installed on about 95 percent of the machines in the world, and there have been a lot of vulnerabilities found in Flash," said Jeff Moss, a security expert who sits on the Homeland Security Advisory Council. "If you can find a vulnerability in one of these products, you're golden."

Products from [Microsoft](#), including Windows, Office and Internet Explorer, have long been favored targets for hackers because so many people use them. But McAfee, a leading software security firm, predicts that

Adobe's software will become the top target this year, as Microsoft has improved its products after years of attacks and Adobe's software has become ubiquitous.

Adobe said it was still investigating the attacks but so far had no evidence that any sensitive information had been compromised.

Brad Arkin, the director of product security at Adobe, said the company generally expected to face increasing attention from hackers given the growing popularity of its products. But he added that the company employed industry-leading practices to respond to threats. "The security of our customers will always be a critical priority for Adobe," he said.

Given the complexity of today's software programs, which are typically written by teams of hundreds or thousands of engineers, it is virtually impossible to be perfectly confident in the security of any program, and tampering could very well go undetected.

Companies are understandably reluctant to discuss their security failures. But one notable incident shows just how damaging the secret tampering with source code can be.

Before the 2004 Summer Olympics in Athens, an unidentified hacker inserted secret programs into four telephone switching computers operated by the [Vodafone Group](#), the world's largest cellphone carrier. The programs created a clandestine tapping system that allowed unknown snoops to eavesdrop on cellphone calls and track the location of about 100 prominent Greek citizens, including the prime minister, military officials, the mayor of Athens, activists and journalists.

The infiltration was uncovered in a government investigation after a Vodafone engineer was found dead in 2005 under suspicious circumstances.

Although the recent round of attacks against Google and other companies appears to have come from China, the threat is not limited to that country, according to computer security researchers. A host of nations, private corporations and even bands of rogue programmers are capable of covertly tunneling into information systems.

"Our conventional military dominance drives our adversaries to cheat, lie and steal," said James Gosler, a fellow at Sandia National Laboratories and a visiting scientist at the [National Security Agency](#), in a speech last year to Pentagon employees. "The offensive technical capability to play this game is well within the reach of the principal adversaries of the United States. In fact, one could argue that some of our adversaries are better at this game than we are." Over the years, Chinese attackers have shown the most interest in military and technology-related assets, leaving assaults on financial systems to hackers in Russia and Eastern European countries.

A look at the source code of software at a company like Adobe or Cisco can help attackers find new ways to burrow into products before the companies can fix errors in their software. In addition, the hackers can gain insights into how to insert their own code into the software so that they can have ready access to machines down the road. "One of the U.S. government's biggest worries is that the attackers will place that source code back into products," said George Kurtz, the chief technology officer at McAfee.

For example, the widespread appearance of counterfeit Cisco routers, which direct traffic on computer networks, has become a major concern in recent years.

Cisco is required by law to include technology in its networking products that allows investigators to tap the hardware for information. The fear is that a country like China could sell counterfeit routers containing slightly modified software that would allow hackers to dial into the systems. “That could provide the perfect over-the-shoulder view of everything coming out of a network,” Mr. Moss said.

A Cisco spokesman, Terry Alberstein, said that the company has extensively tested counterfeit Cisco routers. “We have not found a single instance of software or hardware that was modified to make them more vulnerable to security threats,” he said.

Alan Paller, director of research at the SANS Institute, a security education organization, said United States technology companies had gotten better about protecting their most prized intellectual property by creating more complex systems for viewing and changing source code. Such systems can keep a detailed account of what tweaks have been made to a software product.

But such security can be undermined by employees who open malicious files sent to them in e-mail, said Mr. Kurtz. “One of the greatest vulnerabilities remains the people element,” he added.

[Copyright 2010 The New York Times Company](#)

[Privacy Policy](#) | [Terms of Service](#) | [Search](#) | [Corrections](#) | [RSS](#) | [First Look](#) | [Help](#) | [Contact Us](#) | [Work for Us](#) | [Site Map](#)