

The New York Times

January 13, 2010

Hacking Risks Persist Even if Companies Withdraw From China

By JEREMY KIRK of [IDG News Service](#) \London Bureau, [IDG](#)

[Google](#) and other enterprises still face a bleak computer security landscape that makes their companies vulnerable to hackers, whether they do business in China or not, analysts say.

Google's chief legal officer revealed on Tuesday that the company and more than 20 other technology, financial and software companies were targeted by hackers, motivated to steal intellectual property and intelligence on human rights activists.

In protest, Google said it would stop censoring search engine results as demanded by the Chinese government and is considering halting its business within the country.

"I think the logic is clear: Google is disappointed, perhaps, with the result of its policy to agree to be censored in China," said Whit Andrews, lead Google analyst for [Gartner](#). "They are no doubt frustrated by security breaches which they perceive are related to their existence in China."

But Andrews and others analysts say the distributed nature of the Internet means Google and other enterprises are at no less risk from hackers sympathetic to Chinese policy by not doing business in that country.

"My sense is that there would be relatively no major impact on Google's ability to defend itself based on whether it has business operations in China or not," Andrews said.

To steal information from computers, hackers often try to trick people into installing malicious software. Hackers can do that through social engineering, such as constructing an e-mail that appears to come from a friend or colleague but that carries a malicious program or file as an attachment.

The technique is known as spear phishing. Last year, researchers from the SecDev Group, a think tank, and the Munk Center for International Studies at the University of Toronto revealed a deep spying network dubbed GhostNet that in part used spear phishing to infect computers in 103 countries. Although some of the computers involved in GhostNet were found to be in China, the government there denied any involvement in the massive spying network.

In one example, computers belonging to Tibetan activists were sent e-mails containing a malicious Microsoft Word document that would exploit a vulnerability in that application, installing other software that allowed hackers to steal documents.

"Since then, of course, we've attempted to take a number of security precautions so that this type of incident doesn't happen again," said Tenzin Taklha, spokesman for the Office of His Holiness the Dalai Lama in Dharamsala, India. "It's an ongoing effort. It's not just something that you do in one day."

The attacks can be difficult to trace, as hackers route their probes through worldwide networks of other hacked computers known as botnets. Up to 25 percent of computers infected with botnet code are in enterprise networks, said Rik Ferguson, senior security adviser for [Trend Micro](#).

Because commands to those bots are encrypted, it can be difficult for investigators to identify who is behind the attacks, he said.

"It's a shifting landscape all the time," Ferguson said. "The more success that law enforcement and the security industry had, the more we oblige the criminal element to innovate and find new ways to do things."

The attacks against Google were low-volume operations, which means it is trivial for the perpetrators to cover their tracks, said Scott Borg, director and chief economist for the U.S. Cyber Consequences Unit, an independent nonprofit research institute that assesses the impact of cyberattacks.

"Almost anyone who is willing to go to enough trouble can obtain anonymous Internet access, even in China," Borg said. "It is possible that the senior Chinese leaders are right now trying to find out who did what."

Even with stronger security, there will always be a small window of opportunity for hackers.

While many software companies now create patches faster for vulnerable software, there still is a gap of time in between when the vulnerability is found and when the fix is ready. If a vulnerability is already being exploited when it is publicly disclosed and there is no patch, it is known as a zero-day attack, the most dangerous type of problem.

It's doubtful there will be a day when software will be free of vulnerabilities said Andre' M. DiMino, co-founder of Shadowserver, a volunteer-run organization that tracks botnets.

"As long as there are unpatched applications and operating systems, poorly secured networks and Web sites, as well as users not taking basic precautions, we'll continue to see system compromises," DiMino said.

Google's revelations are further affirmation of what other analysts have said is an uptick in industrial espionage using computers.

"Let's be honest: If you can hack Google, there must be a lot of technology companies that should be similarly worried about their systems," said Tom Watson, a Labour Member of Parliament for West Bromich East.

Watson put forth an early-day motion in the U.K.'s Parliament on Wednesday, a motion that other U.K. lawmakers can sign on to show their support for Google's decision to stop censoring search engine results in China.

Copyright 2010 IDG. All Rights Reserved.

[Copyright 2010](#)

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