Security firm outlines how attack against Google was pulled off

January 17 2010, By Pete Carey

A Silicon Valley Internet security firm has described for the first time how hackers from China were able to crack Google's defenses, saying the attackers took advantage of a flaw in Microsoft's Web browser to probe deeply into the company's network.

The new description of the attack raises questions about the security of Google's increasingly popular computing "cloud," a term that refers to the clusters of servers it uses to store user's information. Google, however, insisted that the cloud is safe, and it will continue to use it for its business operations.

The cyber attack, which Google said emanated from China and in part targeted Chinese dissidents, led the search giant to reassess its operations in that country and threaten to pull out because of mounting frustrations over censorship and other issues.

According to the Associated Press, a Chinese official Thursday endorsed the country's current rules governing Internet content, giving little indication it's willing to loosen controls over the Web.

"China's Internet is open," said Jiang Yu, a foreign ministry spokeswoman, according to the AP. "China welcomes international Internet enterprises to conduct business in China according to law."

Microsoft confirmed the nature of the attack and said it is working to patch the flaw, which affects some versions of its Internet Explorer browser.

The intruders gained access to Google by targeting a few key individuals at the company who had access to intellectual property, McAfee said in a corporate blog. Once they clicked on a malicious link, they were taken to a Web site where malicious software was downloaded onto their computer through the flaw in their browsers.

The software established "complete control" over the target's computer, said George Kurtz, McAfee's worldwide chief technology officer, and let them potentially gain "access to sensitive intellectual property and to move that property to another location outside of that network and company."

The software used in the attack "looks very sophisticated," Kurtz said. "There's multiple layers of encryption. The whole purpose is to attack and burrow into a company's network and go undetected as long as possible."

Google discovered the attack in mid-December.

Google spokesman Scott Rubin said, "This not about cloud computing. This is about hacking." Since the attack, the company has taken "additional steps to protect our users," Rubin said. "We believe that Google services are safe to use. That's why we use them all day every day."

In addition to the Google network, the high-profile intrusion also targeted Gmail accounts in the United States and other countries. This may prompt users to demand better security for electronic mail and other personal data that's stored on Internet clouds, some advocates say.

"The problem up until now is that people like Google have emphasized speed and efficiency and ease of use," said John M. Simpson, an advocate with Consumer Watchdog. "In too many cases they have let security and privacy become a secondary issue. This situation is a wakeup call for everybody."

Tuesday night, just after announcing the widespread security breach from China on its official blog, Google announced that it would allow Gmail users to always encrypt their mail as it travels between a user's Web browser and Google's servers. While such encryption would not have prevented the malware or phishing intrusion of human rights activists' Gmail accounts, Google said the feature would help protect data from being snooped by others in places such as public wifi hotspots.

Mark Shavlik, CEO of Shavlik Technologies, which helps companies with cloud computing initiatives, said, the penetration of Google "is not unique for cloud computing, as attacks can occur anywhere on the Internet. However, if you do use cloud computing you should make sure your provider is using industry standard processes and solutions to automate and secure their (and your) environment."

"I don't think this is an event that will dissuade people from leveraging the cloud," added Kurtz of McAfee, "but it will shed light on the fact that companies and organizations need to make sure their cloud providers have adequate security measures in place."

(c) 2010, San Jose Mercury News (San Jose, Calif.).
Distributed by McClatchy-Tribune Information Services.

Citation: Security firm outlines how attack against Google was pulled off (2010, January 17) retrieved 20 March 2024 from https://phys.org/news/2010-01-firm-outlines-google.html provided for information purposes only.