SECURITY January 13, 2010 3:00 AM

Google Attack Part of Widespread Spying Effort

By Robert McMillan, IDG News

Google's decision Tuesday to risk walking away from the world's largest Internet market may have come as a shock, but security experts see it as the most public admission of a top IT problem for U.S. companies: ongoing corporate espionage originating from China.

PEOPLE WHO READ THIS ALSO READ:

- Law Firm in Green Dam Suit Targeted With Cyber-attack
- Google Attack Highlights Strength of Targeted Malware
- The Google-China Challenge: How It Came to This
- China Emphasizes Laws as Google Defies Censorship
- The U.S.-South Korea Cyberattack: How Did It Happen?
- Google Could Leave China over Censorship, E-mail Attacks

Recommendations by loomia

It's a problem that the U.S. lawmakers have complained about loudly. In the corporate world, online attacks that appear to come from China have been an ongoing problem for years, but big companies haven't said much about this, eager to remain in the good graces of the world's powerhouse economy.

Google, by implying that Beijing had sponsored the attack, has placed itself in the center of an international controversy, exposing what appears to be a state-sponsored corporate espionage campaign that compromised more than 30 technology, financial and media companies, most of them global Fortune 500 enterprises.

The U.S. government is taking the attack seriously. Late Tuesday, U.S. Secretary of State Hillary Clinton released a statement asking the Chinese government to explain itself, saying that Google's allegations "raise very serious concerns and questions."

"The ability to operate with confidence in cyberspace is critical in a modern society and economy," she said.

The search-engine company first learned it had a security problem in mid-December, coincidentally just days after hosting a closed-door symposium on circumventing censorship. Soon the company's security team realized that it was dealing with more than just a few hacked workstations.

"First, this attack was not just on Google. As part of our investigation we have discovered that at least twenty other large companies from a wide range of businesses -- including the Internet, finance, technology, media and chemical sectors -- have been similarly targeted," wrote Google Chief Legal Officer David Drummond in a Tuesday blog posting. "Second, we have evidence to suggest that a primary goal of the attackers was accessing the Gmail accounts of Chinese human rights activists."

Drummond said that the hackers never got into Gmail accounts via the Google hack, but they did manage to get some "account information (such as the date the account was created) and subject line."

That's because they apparently were able to access a system used to help Google comply with search warrants by providing data on Google users, said a source familiar with the situation, who spoke on condition of anonymity because he was not authorized to speak with the press. "Right before Christmas, it was, 'Holy s***, this malware is accessing the internal intercept [systems],'" he said.

That, in turn led to a Christmas Eve meeting led by Google co-founder Larry Page to assess the situation. Three weeks later, the company had decided that things were serious enough that it would risk walking away from the largest market of Internet users in the world.

Drummond, in his blog post, said that -- in part due to this incident -- Google would no longer censor search results in China, a move that could cause its Web site to be blocked by the Chinese government.

Corporate IT workers have come to expect all sorts of Internet attacks from China in recent years, but because of the distributed nature of the Internet, it's very hard to determine the true source of a cyber attack. For several hundred dollars, criminals from any country can buy so-called bulletproof hosting in China. These servers are guaranteed not to be taken down, even if they are linked to spam or other illegal online activity.

In this case, however, Google believes the attacks really were state sponsored, said Leslie Harris, president and CEO of the Center for Democracy and Technology. "They wouldn't be taking an action suggesting that they cannot operate in China ... if it was not related to the Chinese government," she said.

Google's security team eventually managed to gain access to a server that was used to control the hacked systems, and discovered that it was not the only company to be hit. In fact, 33 other companies had also been compromised, including Adobe Systems, according to several sources familiar with the situation.

On Jan. 2 Adobe learned of "a computer security incident involving a sophisticated, coordinated attack against corporate network systems managed by Adobe and other companies," the company said in a blog post published just minutes after Google went public with its account of the hacking incident. An Adobe spokeswoman declined to comment on whether or not the Google and Adobe attacks were related.

Other companies that have been hit include "Internet, finance, technology, media and chemical sectors," Drummond said.

On Tuesday Yahoo -- another likely target -- declined to say whether it had been hit, but the company did issue a brief statement in support of Google. These "kinds of attacks are deeply disturbing," Yahoo said.

Microsoft said even less about the incident. "We have no indication that any of our mail properties have been compromised," the company said via e-mail.

"We've never seen any attacks that were on this large of a scale and were this successful against private companies," said Eli Jellenc, head of international threat intelligence with Verisign's iDefense security unit.

IDefense was called in to help some of the victim companies that Google had uncovered. According to Jellenc, the hackers sent targeted e-mail messages to victims that contained a malicious attachment containing what's known as a zero-day attack. These attacks are typically not detected by antivirus vendors because they exploit a previously unknown software bug.

"There is an attack exploiting a zero-day vulnerability in one of the major document types," Jellenc said. "They infect whichever users they can, and leverage any contact information or any access information on the victim's computer to misrepresent themselves as that victim." The goal is to "infect someone with administrative access to the systems that hold the intellectual property that they're trying to obtain," he added.

Once they have the data they move it out of the corporate network.

The attacks followed the same game plan that security experts have seen in attacks on non-governmental organizations and the defense industry, where contractors and government agencies have been hit with similar targeted spying attacks for years now. Some of Verisign's defense partners said that they'd seen some of the same IP addresses used in previous, "very similar attacks," Jellenc said.

"Whomever is doing this, this isn't their first attack," he said. "These contractors also confirmed the China origin of the attacks."

This type of attack was described in detail in an October Northrop Grumman report, (pdf) commissioned by the US-China Economic and Security Review Commission. Analysts concluded that "China is likely using its maturing computer network exploitation capability to support intelligence collection against the U.S. government and industry by conducting a long term, sophisticated computer network exploitation campaign."

At least 10 to 20 terabytes of sensitive data had been taken from U.S. government networks as part of what the report's authors called a "long term, persistent campaign to collect sensitive but unclassified information."

For the past few years, China has been focused on moving its economy to the next level, said James Mulvenon, director of Defense Group Inc.'s Center for Intelligence Research and Analysis. China built its economy processing products for export, but it is not known for cutting-edge research and development. The country has been taking steps to spur innovation within its borders, pressuring multinational companies to build research labs in China and developing the talent to eventually replace these businesses with indigenous competitors.

Mulvenon doesn't find it implausible that a nation such as China would spy on U.S. companies.

"If you're having trouble [innovating] or if you want to prime the pump, the best way is to go out and steal cutting-edge IP," he said. "It's a plausible explanation for why they would go after Silicon Valley companies on such a broad scale because they're really trying to jump start IT innovation in China."

John Ribeiro in Bangalore and Jeremy Kirk in London contributed to this story.

Comments Readers reply with their ideas and expertise. Add Yours

SUBSCRIBE TO THIS DISCUSSION VIA EMAIL OR RSS

Jalek posted Wed Jan 13 11:46:43 PST 2010

Who uses GMail or any web-based mail system for anything of consequence?

I guess if they did, they should probably rethink it anyway, though even POP3 isn't perfect. The mail files are cleared, but if a provider is running "intercept" copies or archives, the mail never really leaves the internet.

ColinABQ posted Thu Jan 14 07:56:58 PST 2010

Thank you, Mr. McMillan, for providing one of the very, very few articles on this topic to even touch on the issue of "bulletproof" hosting in China and the alarming volume of black hattery sponsored by such operations. I do not doubt Google's appraisal of the specific attacks in question as not falling in that category but, if not for that important distinction, Google's China Cabinet would have 33,000 bulls in it, rather than the 33 or so that have been identified. In fact, I would challenge the operators of any public-facing, Internet-based services on any continent to scour their firewall, security appliance, and server logs and NOT find evidence of "attacks that appear to originate in mainland China."

I wonder how many enterprise IT admins and security consultants are scrambling

A survey of app developers finds that Android is quickly closing the gap as the platform that developers are pursuing, while widening its lead over iOS as the mobile platform considered to have the most potential for the future.

NET WORK - SEPTEMBER 27, 2010 6:17 AM
Sharp Galapagos Android Devices to Enter Tablet Fray

Sharp is launching two Android-based devices dubbed "Galapagos", and the strategy seems to be to fly under the iPad radar by declaring them e-readers rather than tablets.

All Blogs »

this week, looking for evidence of the attacks. It could be interesting to see, over the coming days and weeks, how many companies come forward, falsely claiming to have been victims of “the Google 33” attacks. Even lacking that, would a sudden leap into public view of bulletproof hosting schemes do any good? I would guess not, but it would be interesting all the same.

JudyK42 posted Thu Jan 14 10:18:52 PST 2010

And behind what door have you been standing since probably about 1991-2. Once on-line communication moved from a internal-to-corporate/computer industry technological environment, there became definitely provable security breaches. Commercialising the web without predetermining the structural restrictions exacerbated a growing problem. That the ISPs have REMOVED certain of the capabilities of the end user to monitor what are basically incoming "searches" creates further breaches. Combine that with the contractual structure; and my opinion is that you have a "bombshell" just waiting to explode legally. Look at some of your most popular end-user applications in coordination to the application spyware (illicit or otherwise) let alone the programming capabilities that provide through our own public education system. (IE engineering certification WITHOUT registration) Looks to me like we've opened the door to the activity via our own carelessness. Obviously, the "honors system" the computer industry originally employed isn't sufficient. The whys and wherefores (Yes?) are many and varied. I'd say it's time we re-educated our employment base. Yes, that includes the "call centers" based outside the United States to which our batched transactions are forwarded for data entry.

GregoryCreaser posted Tue Jan 19 14:59:55 PST 2010

One of our discussion at VeriSign is recognizing successful technique of hackers, which generally involve phishing and social engineering. The method of determining a targets, in order to direct a spear phish email to a specific employee posing as someone from the inside or a vendor. And we all aware of the consequences from there.

So right, not the work of kiddy hackers or money monger crimals - now a eye-opening event that supports the idea that the breach is being sponsored by foreign governments who have a much bigger agenda.

I think we all agree that these attacks were very complex and warrant ongoing investigation, research and analysis.

Our take here: “Update on the Google Breach” at http://blogs.verisign.com/idefense/

WinTard posted Tue Jan 19 15:14:14 PST 2010

I wouldn't put it past ANY government to have hidden agendas, obfuscated under various http://en.wikipedia.org/wiki/McCarthyism or Patriotic subterfuges. And the Chinese government certainly appears to have the motives and the resources to mount such a sophisticated attack.

However, it is interesting to note that:

Excerpt from:
http://www.theregister.co.uk/2010/01/19/google_china_attack_malware_analysis/

The Operation Aurora attack targeted systems running IE6, which begs the question of why Google and the other affected concerns were running a version of Microsoft's browser software first released in 2001 and not Chrome. IE6 is famously outdated, and it's tempting to think Google and Yahoo! were only running it because it was the only browser supported by government systems connected with lawful interception (wiretapping).

~~~~~~~~~~
~~~~~~~~~~

When fascism comes to America, it will be wrapped in the flag and carrying a cross.

~ Sinclair Lewis

Censorship in any form is the opening wedge for fascism, since it places arbitrary and unwarranted power in the hands of individuals.

~ Jack Parsons from the book "Freedom Is a Two-edged Sword."

The inherent vice of capitalism is the unequal sharing of blessings; the inherent virtue of socialism is the equal sharing of miseries.

~ Winston Churchill

What do you think?

Sign in to post a comment. New to PCWorld Comments? Register here.

Sign in to post a comment. New to PCWorld Comments? Register here.

Connect with Facebook

6 Ways to Improve Your W-iFi Network

Google Chrome: 5 Must-Have Tips and Tricks

Apple iPad: The Low-Price Leader?

PCWorld

PCWorld.com is the Web's trusted resource for management-level buyers and users of technology products, reaching an average of more than 11 million unique visitors per month (HitBox, January - June 2009).

More About Us » FAQ »

Resources

- Twitter
- RSS
- Newsletters
- Contact Us
- Magazine Customer Service
- Advertise

Network

- PCWorld
- PCWorld Business Center
- Macworld
- MacUser
- Mac OS X Hints
- iPhone Central