WIKIPEDIA
The Free Encyclopedia

Main page
Contents
Featured content
Current events
Random article
Donate to Wikipedia
Wikipedia store

Interaction
Help
About Wikipedia
Community portal
Recent changes
Contact page

Tools
What links here
Related changes
Upload file
Special pages
Permanent link
Page information
Wikidata item
Cite this page

Print/export
Download as PDF
Printable version

Languages
Français
Italiano
မြန်မာဘာသာ
Nederlands
日本語
Українська
中文
Edit links

Operation Aurora

From Wikipedia, the free encyclopedia

Not to be confused with Aurora Generator Test.

Operation Aurora	
Date	June–December 2009
Location	*Not specified – occurred on a worldwide scale.*
Result	Diplomatic incident between the United States and China
Belligerents	
United States • Google • Adobe Inc. • Juniper Networks • Rackspace • Yahoo! (allegedly) • Symantec (allegedly) • Northrop Grumman (allegedly) • Morgan Stanley (allegedly) • Dow Chemical Company (allegedly)	China • PLA Unit 61398
Casualties and losses	
Google intellectual property stolen[1]	

Operation Aurora was a series of cyber attacks conducted by advanced persistent threats such as the Elderwood Group based in Beijing, China, with ties to the People's Liberation Army.[2] First publicly disclosed by Google on January 12, 2010, in a blog post,[1] the attacks began in mid-2009 and continued through December 2009.[3]

The attack was aimed at dozens of other organizations, of which Adobe Systems,[4] Juniper Networks[5] and Rackspace[6] have publicly confirmed that they were targeted. According to media reports, Yahoo, Symantec, Northrop Grumman, Morgan Stanley[7] and Dow Chemical[8] were also among the targets.

As a result of the attack, Google stated in its blog that it plans to operate a completely uncensored version of its search engine in China "within the law, if at all", and acknowledged that if this is not possible it may leave China and close its Chinese offices.[1] Official Chinese sources claimed this was part of a strategy developed by the U.S. government.[9]

The attack was named "Operation Aurora" by Dmitri Alperovitch, Vice President of Threat Research at cyber security company McAfee. Research by McAfee Labs discovered that "Aurora" was part of the file path on the attacker's machine that was included in two of the malware binaries McAfee said were associated with the attack. "We believe the name was the internal name the attacker(s) gave to this operation," McAfee Chief Technology Officer George Kurtz said in a blog post.[10]

According to McAfee, the primary goal of the attack was to gain access to and potentially modify source code repositories at these high tech, security and defense contractor companies. "[The SCMs] were wide open," says Alperovitch. "No one ever thought about securing them, yet these were the crown jewels of most of these companies in many ways—much more valuable than any financial or personally identifiable data that they may have and spend so much time and effort protecting."[11]

Contents [hide]

History [edit]

Flowers left outside Google China's headquarters after its announcement it might leave the country

On January 12, 2010, Google revealed on its blog that it had been the victim of a cyber attack. The company said the attack occurred in mid-December and originated from China. Google stated that over 20 other companies had been attacked; other sources have since cited that more than 34 organizations were targeted.[8] As a result of the attack, Google said it was reviewing its business in China.[1] On the same day, United States Secretary of State Hillary Clinton issued a brief statement condemning the attacks and requesting a response from China.[12]

On January 13, 2010, the news agency All Headline News reported that the United States Congress plans to investigate Google's allegations that the Chinese government used the company's service to spy on human rights activists.[13]

In Beijing, visitors left flowers outside of Google's office. However, these were later removed, with a Chinese security guard stating that this was an "illegal flower tribute".[14] The Chinese government has yet to issue a formal response, although an anonymous official stated that China is seeking more information on Google's intentions.[15]

Attackers involved [edit]

Main article: PLA Unit 61398

Technical evidence including IP addresses, domain names, malware signatures, and other factors, show Elderwood was behind the Operation Aurora attack, one of numerous attacks conducted by the Elderwood gang and others such as PLA Unit 61398 (also known as APT1), a Shanghai-based advanced persistent threat group also called "Comment Crew", named after the technique often used by the group involving internal software "comment" features on web pages, which are used to infiltrate target computers that access the sites. The two largest groups may employ hundreds of people, and work to compromise security and siphon business ideas, advanced designs, and trade secrets from various foreign computer networks.[16] The group behind the Operation Aurora attacks were dubbed "Elderwood" by Symantec after a source-code variable used by the attackers, and "Beijing Group" by Dell Secureworks. The group obtained some of Google's source code, as well as access to information about Chinese activists.[17] Along with other groups such as Unit 61398, also targeted numerous other companies in the shipping, aeronautics, arms, energy, manufacturing, engineering, electronics, financial, and software sectors.[2][18]

While APT1 was active at the time of the attack on Google, the group was not responsible for it. The "APT" designation for the Chinese threat actors responsible for attacking Google is APT17. [19]

Elderwood specializes in attacking and infiltrating second-tier defense industry suppliers that make electronic or mechanical components for top defense companies. Those firms then become a cyber "stepping stone" to gain access to top-tier defense contractors. One attack procedure used by Elderwood is to infect legitimate websites frequented by employees of the target company – a so-called "water hole" attack, just as lions stake out a watering hole for their prey. Elderwood infects these less-secure sites with malware that downloads to a computer that clicks on the site. After that, the group searches inside the network to which the infected computer is connected, finding and then downloading executives' e-mails and critical documents on company plans, decisions, acquisitions, and product designs.[2]

Attack analysis [edit]

In its blog posting, Google stated that some of its intellectual property had been stolen. It suggested that the attackers were interested in accessing Gmail accounts of Chinese dissidents. According to the *Financial Times*, two accounts used by Ai Weiwei had been attacked, their contents read and copied; his bank accounts were investigated by state security agents who claimed he was under investigation for "unspecified suspected crimes".[20] However, the attackers were only able to view details on two accounts and those details were limited to things such as the subject line and the accounts' creation date.[1]

Security experts immediately noted the sophistication of the attack.[10] Two days after the attack became public, McAfee reported that the attackers had exploited purported zero-day vulnerabilities (unfixed and previously unknown to the target system developers) in Internet Explorer and dubbed the attack "Operation Aurora". A week after the report by McAfee, Microsoft issued a fix for the issue,[21] and admitted that they had known about the security hole used since September.[22] Additional vulnerabilities were found in Perforce, the source code revision software used by Google to manage their source code.[23][24]

VeriSign's iDefense Labs claimed that the attacks were perpetrated by "agents of the Chinese state or proxies thereof".[25]

According to a diplomatic cable from the U.S. Embassy in Beijing, a Chinese source reported that the Chinese Politburo directed the intrusion into Google's computer systems. The cable suggested that the attack was part of a coordinated campaign executed by "government operatives, public security experts and Internet outlaws recruited by the Chinese government."[26] The report suggested that it was part of an ongoing campaign in which attackers have "broken into American government computers and those of Western allies, the Dalai Lama and American businesses since 2002."[27] According to The Guardian's reporting on the leak, the attacks were "orchestrated by a senior member of the Politburo who typed his own name into the global version of the search engine and found articles criticising him personally."[28]

Once a victim's system was compromised, a backdoor connection that masqueraded as an SSL connection made connections to command and control servers running in Illinois, Texas, and Taiwan, including machines that were running under stolen Rackspace customer accounts. The victim's machine then began exploring the protected corporate intranet that it was a part of, searching for other vulnerable systems as well as sources of intellectual property, specifically the contents of source code repositories.

The attacks were thought to have definitively ended on Jan 4 when the command and control servers were taken down, although it is not known at this point whether or not the attackers intentionally shut them down.[29] However, the attacks were still occurring as of February 2010.[3]

Response and aftermath [edit]

The German, Australian, and French governments publicly issued warnings to users of Internet Explorer after the attack, advising them to use alternative browsers at least until a fix for the security hole was made.[30][31][32] The German, Australian, and French governments considered all versions of Internet Explorer vulnerable or potentially vulnerable.[33][34]

In an advisory on January 14, 2010, Microsoft said that attackers targeting Google and other U.S. companies used software that exploits a hole in Internet Explorer. The vulnerability affects Internet Explorer versions 6, 7, and 8 on Windows 7, Vista, Windows XP, Server 2003, Server 2008 R2, as well as IE 6 Service Pack 1 on Windows 2000 Service Pack 4.[35]

The Internet Explorer exploit code used in the attack has been released into the public domain, and has been incorporated into the Metasploit Framework penetration testing tool. A copy of the exploit was uploaded to Wepawet, a service for detecting and analyzing web-based malware operated by the computer security group at the University of California, Santa Barbara. "The public release of the exploit code increases the possibility of widespread attacks using the Internet Explorer vulnerability," said George Kurtz, CTO of McAfee, of the attack. "The now public computer code may help cyber criminals craft attacks that use the vulnerability to compromise Windows systems."[36]

Security company Websense said it identified "limited public use" of the unpatched IE vulnerability in drive-by attacks against users who strayed onto malicious Web sites.[37] According to Websense, the attack code it spotted is the same as the exploit that went public last week.[*clarification needed*] "Internet Explorer users currently face a real and present danger due to the public disclosure of the vulnerability and release of attack code, increasing the possibility of widespread attacks," said George Kurtz, chief technology officer of McAfee, in a blog update.[38] Confirming this speculation, Websense Security Labs identified additional sites using the exploit on January 19.[39] According to reports from Ahnlab, the second URL was spread through the Instant Messenger network Misslee Messenger, a popular IM client in South Korea.[39]

Researchers have created attack code that exploits the vulnerability in Internet Explorer 7 (IE7) and IE8—even when Microsoft's recommended defensive measure (Data Execution Prevention (DEP)) is turned on.[*dubious – discuss*] According to Dino Dai Zovi, a security vulnerability researcher, "even the newest IE8 isn't safe from attack if it's running on Windows XP Service Pack 2 (SP2) or earlier, or on Windows Vista RTM (release to manufacturing), the version Microsoft shipped in January 2007."[40]

Microsoft admitted that the security hole used had been known to them since September.[22] Work on an update was prioritized[41] and on Thursday, January 21, 2010, Microsoft released a security patch aiming to counter this weakness, the published exploits based on it and a number of other privately reported vulnerabilities.[42] They did not state if any of the latter had been used or published by exploiters or whether these had any particular relation to the Aurora operation, but the entire cumulative update was termed critical for most versions of Windows, including Windows 7.

Security researchers continued to investigate the attacks. HBGary, a security firm, released a report in which they claimed to have found some significant markers that might help identify the code developer. The firm also said that the code was Chinese language based but could not be specifically tied to any government entity.[43]

On February 19, 2010, a security expert investigating the cyber-attack on Google, has claimed that the people behind the attack were also responsible for the cyber-attacks made on several Fortune 100 companies in the past one and a half years. They have also tracked the attack back to its point of origin, which seems to be two Chinese schools, Shanghai Jiao Tong University and Lanxiang Vocational School.[44] As highlighted by *The New York Times*, both of these schools have ties with the Chinese search engine Baidu, a rival of Google China.[45] Both Lanxiang Vocational and Jiaotong University have denied the allegation.[46][47]

In March 2010, Symantec, which was helping investigate the attack for Google, identified Shaoxing as the source of 21.3% of all (12 billion) malicious emails sent throughout the world.[48]

To prevent future cyberattacks such as Operation Aurora, Amitai Etzioni of the Institute for Communitarian Policy Studies has suggested that the United States and China agree to a policy of mutually assured restraint with respect to cyberspace. This would involve allowing both states to take the measures they deem necessary for their self-defense while simultaneously agreeing to refrain from taking offensive steps; it would also entail vetting these commitments.[49]

See also [edit]

- Chinese intelligence activity in other countries
- Chinese Intelligence Operations in the United States
- Cyber-warfare
- Economic and Industrial Espionage
- GhostNet
- Honker Union
- Titan Rain
- Vulcanbot

References [edit]

1. ^ a b c d e "A new approach to China". Google Inc. 2010-01-12. Retrieved 17 January 2010.
2. ^ a b c Clayton, Mark (14 September 2012). "Stealing US business secrets: Experts ID two huge cyber 'gangs' in China". *Christian Science Monitor*. Retrieved 24 February 2013.
3. ^ a b "'Aurora' Attacks Still Under Way, Investigators Closing In On Malware Creators". *Dark Reading*. DarkReading.com. 2010-02-10. Retrieved 2010-02-13.
4. ^ "Adobe Investigates Corporate Network Security Issue". 2010-01-12. Retrieved 17 January 2010.
5. ^ "Juniper Networks investigating cyber-attacks". MarketWatch. 2010-01-15. Retrieved 17 January 2010.
6. ^ "Rackspace Response to Cyber Attacks". Archived from the original on 18 January 2010. Retrieved 17 January 2010.
7. ^ "HBGary email leak claims Morgan Stanley was hacked". Retrieved 2 Mar 2010.
8. ^ a b Cha, Ariana Eunjung; Ellen Nakashima (2010-01-14). "Google China cyberattack part of vast espionage campaign, experts say". *The Washington Post*. Retrieved 17 January 2010.
9. ^ Hille, Kathrine (2010-01-20). "Chinese media hit at 'White House's Google'". *Financial Times*. Retrieved 20 January 2010.
10. ^ a b Kurtz, George (2010-01-14). "Operation "Aurora" Hit Google, Others". McAfee, Inc. Archived from the original on 11 September 2012. Retrieved 17 January 2010.
11. ^ Zetter, Kim (2010-03-03). "'Google' Hackers Had Ability to Alter Source Code". *Wired*. Retrieved 4 March 2010.
12. ^ Clinton, Hillary (2010-01-12). "Statement on Google Operations in China". US Department of State. Archived from the original on 2010-01-16. Retrieved 17 January 2010.
13. ^ "Congress to Investigate Google Charges Of Chinese Internet Spying". All Headline News. 13 January 2010. Archived from the original on 28 March 2010. Retrieved 13 January 2010.
14. ^ Robertson, Matthew (2010-01-14). "Flowers Laid, and Removed, at Google Headquarters in China". *The Epoch Times*. Retrieved 18 January 2010.
15. ^ "Chinese govt seeks information on Google intentions". *China Daily*. Xinhua. 2010-01-13. Retrieved 18 January 2010.
16. ^ Martin, Adam (19 February 2013). "Meet 'Comment Crew,' China's Military-Linked Hackers". *New York*. Retrieved 24 February 2013.
17. ^ Nakashima, Ellen. "Chinese hackers who breached Google gained access to sensitive data, U.S. officials say". *WashingtonPost*. Retrieved 5 December 2015.
18. ^ Riley, Michael; Dune Lawrence (26 July 2012). "Hackers Linked to China's Army Seen From EU to D.C." Bloomberg. Retrieved 24 February 2013.
19. ^ Gertz, Bill. "New Chinese Intelligence Unit Linked to Massive Cyber Spying Program". *Washington Free Beacon*. Retrieved 5 November 2019.
20. ^ Anderlini, Jamil (January 15, 2010). "The Chinese dissident's 'unknown visitors'". *Financial Times*.
21. ^ "Microsoft Security Advisory (979352)". Microsoft. 2010-01-21. Retrieved 26 January 2010.
22. ^ a b Naraine, Ryan. Microsoft knew of IE zero-day flaw since last September, ZDNet, January 21, 2010. Retrieved 28 January 2010.
23. ^ "Protecting Your Critical Assets, Lessons Learned from "Operation Aurora", By McAfee Labs and McAfee Foundstone Professional Services" (PDF). *wired.com*.
24. ^ "'Google' Hackers Had Ability to Alter Source Code". *Wired*. Retrieved 27 July 2016.
25. ^ Paul, Ryan (2010-01-14). "Researchers identify command servers behind Google attack". Ars Technica. Retrieved 17 January 2010.
26. ^ Shane, Scott; Lehren, Andrew W. (28 November 2010). "Cables Obtained by WikiLeaks Shine Light Into Secret Diplomatic Channels". *The New York Times*. Retrieved 28 November 2010.
27. ^ Scott Shane and Andrew W. Lehren (November 28, 2010). "Leaked Cables Offer Raw Look at U.S. Diplomacy". *The New York Times*. Retrieved 2010-12-26. "The Google hacking was part of a coordinated campaign of computer sabotage carried out by government operatives, private security experts and Internet outlaws recruited by the Chinese government. They have broken into American government computers and those of Western allies, the Dalai Lama and American businesses since 2002, ..."
28. ^ US embassy cables leak sparks global diplomatic crisis *The Guardian* 28 November 2010
29. ^ Zetter, Kim (2010-01-14). "Google Hack Attack Was Ultra Sophisticated, New Details Show". *Wired*. Retrieved 23 January 2010.
30. ^ One News (19 January 2010). "France, Germany warn Internet Explorer users". TVNZ. Retrieved 22 January 2010.
31. ^ Relax News (18 January 2010). "Why you should change your internet browser and how to choose the best one for you". *The Independent*. London. Retrieved 22 January 2010.
32. ^ "Govt issues IE security warning". ABC (Australia). 19 January 2010. Retrieved 27 July 2016.
33. ^ NZ Herald Staff (19 January 2010). "France, Germany warn against Internet Explorer". *The New Zealand Herald*. Retrieved 22 January 2010.
34. ^ Govan, Fiona (18 January 2010). "Germany warns against using Microsoft Internet Explorer". *The Daily Telegraph*. London. Retrieved 22 January 2010.
35. ^ Mills, Elinor (14 January 2010). "New IE hole exploited in attacks on U.S. firms". CNET. Retrieved 22 January 2010.
36. ^ "Internet Explorer zero-day code goes public". Infosecurity. 18 January 2010. Retrieved 22 January 2010.
37. ^ "Security Labs – Security News and Views – Raytheon – Forcepoint". Retrieved 27 July 2016.
38. ^ Keizer, Gregg. "Hackers wield newest IE exploit in drive-by attacks". Retrieved 27 July 2016.
39. ^ a b "Security Labs – Security News and Views – Raytheon – Forcepoint". Retrieved 27 July 2016.
40. ^ Keizer, Gregg (19 January 2010). "Researchers up ante, create exploits for IE7, IE8". Computerworld. Retrieved 22 January 2010.
41. ^ "Security – ZDNet". Retrieved 27 July 2016.
42. ^ "Microsoft Security Bulletin MS10-002 – Critical". Retrieved 27 July 2016.
43. ^ "Hunting Down the Aurora Creator". TheNewNewInternet. 13 February 2010. Retrieved 13 February 2010.(Dead link)
44. ^ Markoff, John; Barboza, David (18 February 2010). "2 China Schools Said to Be Tied to Online Attacks". New York Times. Retrieved 26 March 2010.
45. ^ "Google Aurora Attack Originated From Chinese Schools". itproportal. 19 February 2010. Retrieved 19 February 2010.
46. ^ Areddy, James T. (4 June 2011). "Chefs Who Spy? Tracking Google's Hackers in China" – via www.wsj.com.
47. ^ University, Jiao Tong. "Jiao Tong University -【Shanghai Daily】Cyber expert slams "spy" report". *en.sjtu.edu.cn*.
48. ^ Sheridan, Michael, "Chinese City Is World's Hacker Hub", *London Sunday Times*, March 28, 2010.
49. ^ Etzioni, Amitai, "MAR: A Model for US-China Relations," *The Diplomat*, September 20, 2013, [1].

External links [edit]

- Google China insiders may have helped with attack news.cnet.com
- Operation Aurora – Beginning Of The Age of Ultra-Sophisticated Hack Attacks! Sporkings.com January 18, 2010
- In Google We Trust Why the company's standoff with China might change the future of the Internet. Rafal Rohozinski interviewed by Jessica Ramirez of Newsweek on 2010.1.29
- Recent Cyber Attacks – More than what meets the eye? Sporkings.com February 19, 2010
- ‘Google’ Hackers Had Ability to Alter Source Code Wired.com March 3, 2010
- 'Aurora' code circulated for years on English sites Where's the China connection?
- Gross, Michael Joseph, "Enter the Cyber-dragon", *Vanity Fair*, September 2011.
- Bodmer, S., Kilger, M., Carpenter, G., & Jones, J. (2012). *Reverse Deception: Organized Cyber Threat Counter-Exploitation*. New York: McGraw-Hill Osborne Media. ISBN 0-07-177249-9, ISBN 978-0-07-177249-5
- The Operation Aurora Internet Explorer exploit – live!
- McAfee Operation Aurora Overview
- Operation Aurora Explained by CNET

v·t·e McAfee [show]
v·t·e Hacking in the 2000s [show]

Categories: Cyberattacks | Advanced persistent threat | Cyberwarfare in China | Cyberwarfare in the United States | 2009 controversies | 2009 crimes | 2009 in technology | McAfee