

## Popular Articles

- ➔ Week 26 In Review
- ➔ Week 22 In Review
- ➔ Week 23 In Review
- ➔ Week 17 In Review - 2011
- ➔ Los Angeles Security Community
- ➔ Week 18 In Review - 2011
- ➔ Week 25 In Review

## Subscribe to Infosec Events



Stay up to date with all of the latest security news by subscribing to our RSS Feed. Alternatively, you can have updates sent directly to your email address.



942 readers  
BY FEEDBURNER

## Recent Articles

- ➔ Week 29 In Review
- ➔ Week 28 In Review
- ➔ Week 27 In Review
- ➔ Week 26 In Review
- ➔ Information Security Events For July
- ➔ Week 25 In Review
- ➔ Week 24 In Review

# Operation Aurora, Zero-day IE Flaw and Google Hacking – Don't Panic!

Published: January 28th, 2010 | Category: Security Vulnerabilities

The past couple of weeks have been a whirlwind of news about the events happening around Google, Microsoft and Operation Aurora. Story upon story had been published on news sites, analysis upon analysis pored over in blog posts and opinions upon opinions voiced out by security professionals around the globe. It's a bit heady to wrap my head around all of this so I'm going to break it down a bit so we can all consume it in bite-sized pieces.

### The Beginning

Last January 12, 2010, Google reported that they suffered a **highly sophisticated attack** on their corporate infrastructure. The attack was believed to have originated from China during the middle of December last year. The breach targeted the search giant as well as at least 20 other large, publicly listed companies in order to steal intellectual property and source code. The main goal of this attack was to gather data from Gmail accounts of human rights activists from China, Europe and other parts of the world.

It was a tense time between Google and China when the attack came. The Chinese government had long been mandating Google to filter its search results on its Chinese site, something that went squarely against the search company's advocacy for free speech. It also came at a time when Google had been struggling to overthrow Baidu as the top search site in China. Google had stated that they were going to stop censoring search results in China going forward and were willing to walk away from the largest internet market in the world if the Chinese government felt otherwise.

Almost at the same time, Adobe posted a similar **security incident** that happened to them but did not mention if it was related to the attack on Google. **The Washington Post** revealed that Yahoo, Symantec, Dow Chemical and Northrop Grumman were also targeted by the same exploit. No other details were revealed by the companies as to the nature of the attacks.

### The Attack Vector

In a report by **Wired.com**, the attack was allegedly the result of a zero-day vulnerability in Adobe Reader, which was later found to be incorrect. **McAfee's Security Insights** blog explained that hackers actually exploited a security hole in Internet Explorer, **CVE-2010-0249**. The attack was quite complex and utilized a host of zero-day exploits and social engineering techniques to initiate a targeted strike on certain individuals within the companies mentioned. Another **blog** even pointed out that the friends of the targets were also exploited to increase their chance of success.

Once the breach was successful, it deposited several malware on the host computer to open a backdoor so that the hacker could steal valuable corporate information from that system as well as others in its network. The attack was designed to be as stealthy as possible and avoided detection by encrypting itself and its remote communications. In addition, the operation took place during December, a time when most corporate offices would have reduced staff and would not be able to deal with such a threat effectively.

As for the name Aurora, it was the folder where the original exploit was located in the attacker's machine and McAfee concluded that this must have been the hackers' internal name for this operation.

### Response from Redmond and Others

Microsoft quickly released a **security advisory** on the situation explaining that the vulnerability affected Internet Explorer 6, 7 and 8 but stressed that IE 6 was the most vulnerable to this exploit. They moved quickly and announced an **out-of-band patch** to mitigate the effects of this flaw. The German government raised concerns on this vulnerability and urged its citizens to **stop using Internet Explorer** for the meantime.

**Some researchers claim** that the attack vector used wasn't new at all, though what really stood out was the outcome of the attack. All of the pieces used in the attack were already easily available, from the obfuscation to the malware used. The attackers did a bold move as they launched their attack simultaneously on at least 33 other companies besides Google. Their time table might have mandated the concurrent assault but it also made them highly visible to their targets which lead to a quicker response.

Another thing that surprised analysts and researchers about this attack was that it was directed against commercial entities. Previous attacks of this nature often targeted governments rather than companies. The media took notice and corporations were shaken that they can also be targets of such a high-level attack. Businesses are now aware that they too are vulnerable to a breach like this and so they need to ramp up their security accordingly.

### Anatomy of an Exploit

**McAfee** and **Wired's Threat Level** gave us some insight as to how the actual attack was performed. Social engineering techniques were used to fool users in to clicking a malicious link within an email or instant message that was believed to be from a trusted source. This then opened up an infected site in Internet Explorer which drops the payload onto the computer, a piece of Javascript. The exploit would afterwards send an encrypted message to a remote server to activate itself and run as an executable. It would download and launch 10 different malware files into the infected system, each having its own task to perform.

One of those files deployed a backdoor and used the computer's SSL protocol to enable hackers to control the infected system remotely. Once inside, the machine was then used as an access point to infect and breach others in the system. The attack itself lasted for three weeks after which the hackers commanded the vectors to shut themselves off.

### Proof-of-Concept Attacks

New versions of the attack code had been created and were able to **bypass Microsoft's Data Execution Protection** (DEP) which was the main protection for the original exploit. **Microsoft countered** these claims though and have announced that these are only proof-of-concept code and not a threat. They stressed that DEP is not the only protection for these attacks. Windows also utilizes Address Space Layout Randomization (ASLR) and Internet Explorer Protected Mode to give further security versus the malicious code.

Over at **Metasploit's** blog, Chief Architect HD Moore tried to reproduce the attack once it became available in **Wepawet**. The objective was to test workarounds and develop fixes for this vulnerability. He was able to successfully duplicate the breach on Internet Explorer 6 though it did not work for newer versions of the browser and on patched systems. It's now available on Metasploit, just run an **update** to get the exploit.

### Aurora Copycats

Once the attack was made public, it was only a matter of time until the source code itself was published online. This was soon confirmed by **McAfee** that the exploit code was now being used by certain individuals and organizations in their own "Aurora"-based websites. **Symantec** had also found that hundreds of websites were already utilizing this malicious code. **ESET** found more than 650 different versions of the exploit through their antivirus software as well as 220 different sites where it was used. The modified attack code executes the same way as the original one but is mainly used to steal passwords for online games. **Websense** added that targeted emails using this exploit are also still rampant in the wild and users should be on the alert.

It had also been revealed that a **gov.cn website** was hosting code that exploits the IE flaw. This points out that even Chinese websites are affected though it had not been confirmed if these attacks are from the Chinese government or if they were just infiltrated by hackers.

### Defense and Common Sense

I agree with what Dino Dai Zovi explained in his **blog post**. While this attack is certainly alarming in its scale, there's nothing to panic about. Threats come and go and security holes will be exploited on way or another. If Microsoft updated the IE flaw right away, I'm sure these hackers will just use another technique to get in. **Verizon** even confirmed that there were 34 other browser vulnerabilities revealed last year that could become avenues for such an attack. If anything, this news should make you aware that authorities and security software companies respond quickly when such threats arise and are actively seeking out to fix vulnerabilities in software, both those publicly known and unknown.

One of the best defenses against security threats is to be aware. Rarely will dangerous exploits infiltrate your system unless you go ahead and let them in. Most malicious software are already blocked by your operating system, firewalls, and antivirus software. If something feels fishy regarding a certain attachment, link or email, don't tinker with it and refer to your IT resource person for help. Here are a few more tips you can follow that apply to this security threat as well as to others like it.

- If you receive an unexpected email from a colleague which contains phrases like "Helping Serve Your Customers", "I just saw the news", "I just saw it today" or "Obama Slips in Polls", do not click on the link included. Also analyse the content of the email, e.g. if Bob never sends you news links, inform him that his computer is infected and ignore those emails from him.
- Refrain from using Internet Explorer 6. If possible upgrade to IE 7 or 8 or use an alternative browser as your default. Google Chrome is a good option as it sandboxes untrusted data to prevent it from harming your computer.
- Update your antivirus software to make it more resilient. These attacks are known to disable AV protection so make sure they are robust enough to fight these threats.
- Check your firewalls and other security measures as well. **Enable DNS and content filtering**, turn on **DEP** and ASLR and, if required, make sure users are on **Protected Mode** when using Internet Explorer.
- If you're an IT resource for your company, take this time to reiterate IT security policies to the people in your company. If they want access to the Internet for non-business matters, you can setup an external WiFi network for use with their personal devices.

Analysts were surprised that the companies affected by the attack chose to announce publicly that they were breached. Most companies would opt to keep matters of security private to prevent any further attacks. Maybe it was because California, where Google and Adobe are located, requires **swift disclosure when a data breach** occurs? In any case, it's good though that they spoke out and I hope other companies follow Google's lead on quickly disclosing breaches in data security, especially when customer data is at stake. At least more people are now aware that security is not just a matter for IT and that everyone should be involved in keeping our data safe and away from cyber criminals.



[RSS feed](#) | [Trackback URI](#)

## 1 Comment »

Name (required)

E-mail (required - never shown publicly)

URI

Your Comment (smaller size | larger size)

You may use [<a href="" title="">](#) [<abbr title="">](#) [<acronym title="">](#) [<b>](#) [<blockquote cite="">](#) [<code>](#) [<del datetime="">](#) [<em>](#) [<i>](#) [<q cite="">](#) [<strike>](#) [<strong>](#) in your comment.

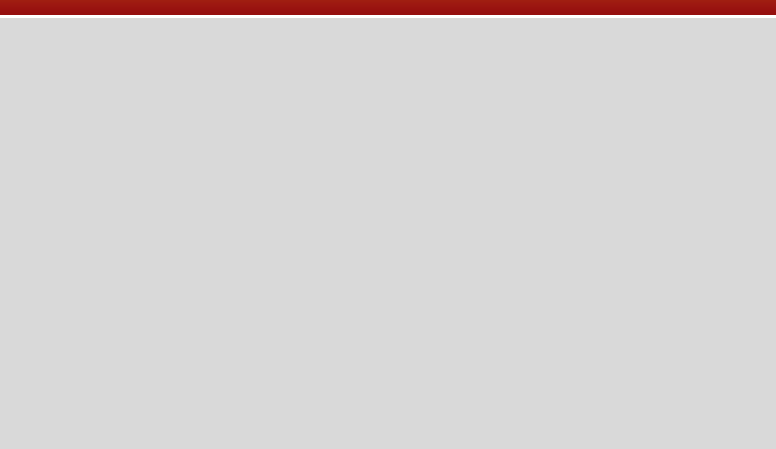
### Trackback responses to this post

[Operation Aurora, Zero-day IE Flaw and Google Hacking – Don't ... Zero Me](#)

## Recent Commentators

- ➔ Vijay Prozak commented on Houston Security Community
- ➔ Dan Tentler commented on San Diego Security Community
- ➔ gyakusetsu commented on Indianapolis Security Community
- ➔ stuff commented on Des Moines Security Community
- ➔ Saint commented on Helena Security Community

## Recent Visitors



## Favorite Links

- ➔ Security Bloggers Network
- ➔ Top Network Security News