Security Response Blog (/connect/symantec-blogs/security-response)

(https://twitter.com/threatintel)

(http://www.symantec.com/connect/item-feeds/blog/2261/feed/all/en/all)

+16
18 Votes

Symantec Official Blog

The Trojan.Hydraq Incident

By: Symantec Security Response (/connect/user/symantec-security-response) SYMANTEC EMPLOYEE

Created 18 Jan 2010

0 Comments

Share

It has been about a week since news of the mysterious Hydraq Trojan (also known as Aurora) attack broke with the unveiling of a threat by Google to pull its operations out of China. In between then and now there has been a lot of rumour and debate about all aspects of this attack with many truths and mistruths being carried in public.

As the fallout from this event begins to settle a little, it helps to step back a bit and try to figure out exactly what happened and when. We will try and tell you the facts about this Trojan as we see it.

Large companies are common targets for hackers and attackers of various kinds and it is not uncommon for these companies to be actively monitoring traffic to and from their critical IT infrastructure. So it comes as no surprise that Google announced in its blog on the 12th January 2010 that it was the target of what it termed as a “highly sophisticated” attack on its business assets. In addition the blog also mentioned that a host of other large corporations were also targets of this same attack.

Although concrete details of the attacks are not yet public, Google made reference to a number of Gmail accounts that were compromised during or after the attacks. These accounts belonged to individuals or organizations dealing with information that may have been politically sensitive. Because of the seemingly political nature of the attacks, the posting suggested that Google may cease the censoring of certain sensitive topics related to China, and also raised the possibility of the search giant pulling out of China altogether.

The story of the attacks went public following the announcement from Google, with news media organizations worldwide choosing to place the story prominently on the front pages of numerous Web sites and printed publications. Far from being confined to security-related mailing lists and blogs, the story became part of the week's headlines with its news of potentially politically motivated "information warfare" in conjunction with the possibility of significant change ahead for one of the world's most prominent companies.

Anatomy of the Attack

For a number of years targeted attacks have nearly always followed the same modus operandi. An email is sent to an individual, or small group of individuals, within an organisation. All efforts are made to make the email look legitimate, that is, it will appear as though it was sent by somebody the recipient trusts and the subject matter will often be related to the recipient's area of business. In order to install the malware, the user must be tricked into either clicking a malicious link or launching a malicious attachment. In the more sophisticated attacks, the attacker will use a new zero day vulnerability, as obviously this will have a greater success rate.

The Trojan.Hydraq incident was no different and was almost textbook in its execution of a targeted attack. While there is much talk of the most recent incident, we observed a Trojan.Hydraq based attack in July 2009. In this attack a PDF file was used to exploit the Adobe Acrobat, Reader, and Flash Player Remote Code Execution Vulnerability (CVE-2009-1862/BID35759). This PDF installed a Trojan horse which was an earlier version of the current Trojan.Hydraq.

Trojan.Hydraq itself is very much a standard backdoor Trojan. Considering the efforts that the attackers put into staging the attack as a whole, the end malware is not so sophisticated. It doesn't use any anti-debugging or anti-analysis tricks. It just uses some basic obfuscation in the form of spaghetti code on some of its components.

Infected machines will typically have the following components installed:

Files:

- %System%\[RANDOM].dll: main file. Runs as a service and has back door capabilities
- %System%\acelpvc.dll: Streams live desktop feed to the attacker
- %System%\VedioDriver.dll: Helper dll for acelpvc.dll

Service:
RaS[FOUR RANDOM CHARACTERS]

Registry Key:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RaS[FOUR RANDOM CHARACTERS]

Motives for the Attack
Based on the functionality of the Trojan we can safely surmise that the intent of the Trojan is to open a back door on a compromised computer allowing a remote attacker to monitor activity and steal information from the compromised computer. Once installed inside a corporate network, the back door feature of the Trojan can also allow the attacker to use the initially compromised computer as a springboard to launch further forays into the rest of the infrastructure, meaning that the wealth of information that may be stolen could potentially be far greater than that existing on a single machine.

Capabilities

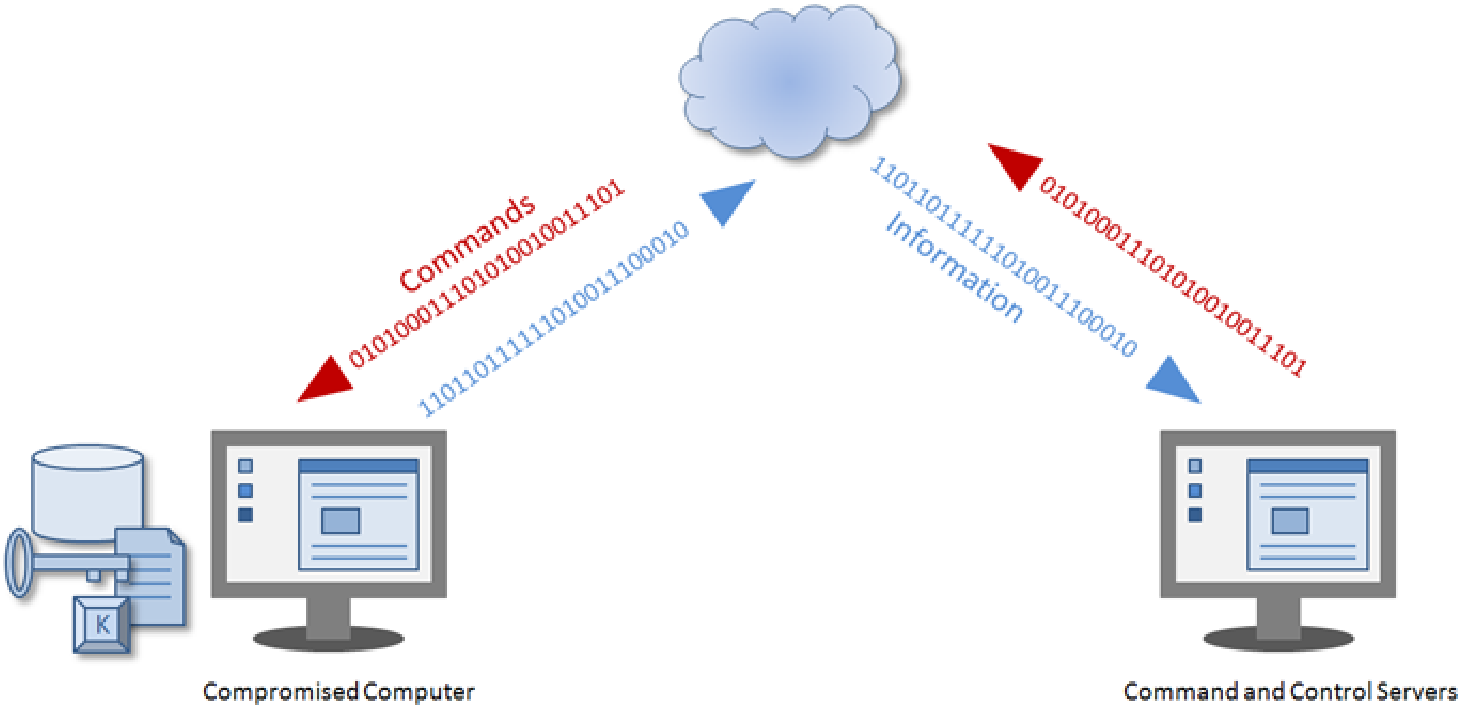
- As mentioned in our earlier technical report on Trojan.Hydraq, the back door allows the attacker to perform any of the following activities:
- Adjust token privileges.
- Check status, control, and end processes and services.
- Create, modify, and delete registry subkeys.
- Retrieve a list of logical drives.
- Read, write, execute, copy, change attributes of, and delete files.
- Restart and shut down the computer.
- Uninstall itself by deleting the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RaS[FOUR RANDOM CHARACTERS] subkey.
- Gather information about the compromised machines, such as:
  1. Client IP
  2. Computer Name
  3. OS Version Information

4. Main Processor Speed
5. RAM Memory size (in Mb)

- Clear all system event logs.
- Check if %System%\acelpvc.dll is present. If so, load it and call its EntryMain() export.
- Check if %System%\VedioDriver.dll is present.
- Open, read, and delete the %System%\drivers\etc\networks.ics file.
- Download a remote file, save it as %Temp%\mdm.exe, and then execute it.

The final item in the above list opens up the opportunity for installing updates and/or other malicious software with additional capabilities.

In addition to this, we know that one of the components of this Trojan is based on the code of VNC (Virtual Network Computing, an open source remote desktop access application) and this component has the ability to stream a live feed of a desktop to a remote computer. This means the remote attacker has the ability to see in real time any user interface activity as if they were sitting right next to the user.



Network Activities

Upon installation on a computer, Trojan.Hydraq attempts to make contact with a hardcoded C&C (command and control) server in order to receive instructions and to upload any information that it may have collected.

We know that it attempts to communicate with the following addresses which are all unavailable at this time but are known to be command and control servers for this attack:

- yahooo.8866.org
- sl1.homelinux.org
- 360.homeunix.com
- li107-40.members.linode.com
- ftp2.homeunix.com
- update.ourhobby.com
- blog1.servebeer.com

Data exchanged between a client and its server has the following format:

Header (0x14 bytes):

```
+00 DWORD MajorCode
+04 DWORD MinorCode
+08 DWORD SubCode
+0C DWORD ExtraSize
+10 WORD  ExtraChecksum
+12 BYTE  ExtraKey
+13 BYTE  Padding
```

Extra data follows:

```
+14 BYTE[Header.ExtraSize]
```

Client TO Server:

- The header's data is encrypted by inverting the bytes (bitwise NOT operation)
- If the client sends extra data to the server, the data is compressed and byte-XOR encrypted with ExtraKey (randomly generated by the client).
- A 16-bit checksum of the compressed and encrypted extra data is set.

Server TO Client:

- The header's data is encrypted by XOR-ing the bytes with 0xCC.
- If the server sends extra data, it may be byte-XOR encrypted with ExtraKey, but it's not compressed and the checksum is not set.

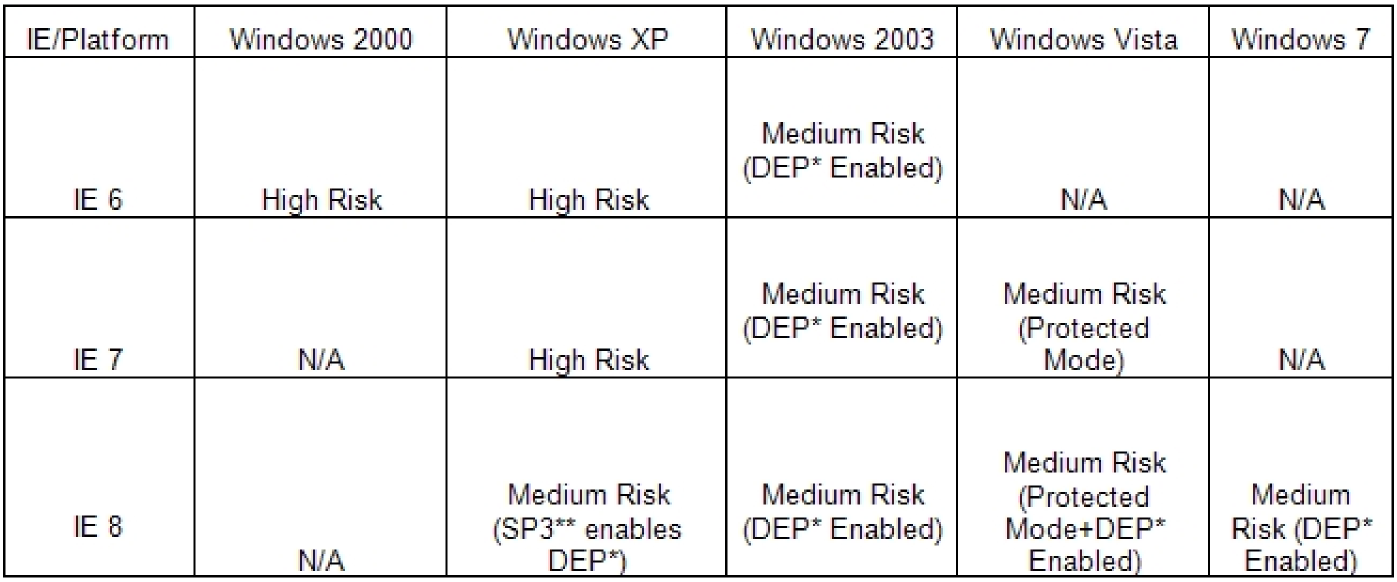
Situational Awareness

At this time, the command and control servers are no longer active so any of the Trojans still remaining in the field are effectively neutralised. The Trojans use of static backchannel URL addresses for communication with free Dynamic DNS sites to route traffic to control servers, has allowed the Dynamic DNS sites being abused to revoke their usage. The backchannel URL addresses have been changed by the Dynamic DNS sites to resolve to a loopback address (127.0.0.2). This in effect severs the connection to the control servers. The control server has also been taken down by the Virtual Private Server (VPS) hosting company.

Antivirus vendors have released signatures to catch Trojan.Hydraq variants. As new variants may emerge at any time, keeping your anti-virus products up-to-date is crucial to protect your machines.

As described in the previously posted blog (Hydraq - An Attack of Mythical Proportions (https://www-secure.symantec.com/connect/blogs/hydraq-attack-mythical-proportions)), an unpatched Internet Explorer vulnerability (BID 37815 (http://www.securityfocus.com/bid/37815)) was used as one of the propagation vectors for this particular Trojan.Hydraq attack. According to Microsoft, the vulnerability affects Internet Explorer 6, 7, and 8, which together make up the bulk of the versions used today. This security hole allows remote exploitation, which means that attackers can run any malicious code of their liking on a victim's machine by taking advantage of the vulnerability. Currently a patch is not available to plug this security hole but Microsoft has posted an advisory (http://www.microsoft.com/technet/security/advisory/979352.mspx) and is working on the patch. Also the advisory discusses possible workarounds users can use while waiting for the patch.

BID 37815 (http://www.securityfocus.com/bid/37815) affected platforms



IE/Platform	Windows 2000	Windows XP	Windows 2003	Windows Vista	Windows 7
IE 6	High Risk	High Risk	Medium Risk (DEP* Enabled)	N/A	N/A
IE 7	N/A	High Risk	Medium Risk (DEP* Enabled)	Medium Risk (Protected Mode)	N/A
IE 8	N/A	Medium Risk (SP3** enables DEP*)	Medium Risk (DEP* Enabled)	Medium Risk (Protected Mode+DEP* Enabled)	Medium Risk (DEP* Enabled)

* Data Execution Protection

** Service Pack

We expect to see the exploit being used more widely as the exploit code was made public last week.

Another propagation vector reportedly used was a vulnerability in Acrobat, Reader, and Flash Player. Adobe has already released a patch (Adobe APSB09-10) so also make sure to keep your Adobe products up to date.

Prevalence

From our intelligence sources, we have established that the numbers affected by this attack is extremely limited. The number of computers we have observed being attacked or have been attacked is low as borne out by our field detection statistics.
Number of factors may have contributed the low detection rates:

- This is a targeted attack. Only a limited number of organisations was targeted.
- The use of browsers other than Internet Explorer by an increasingly large number of people may have helped limit the "attack surface" by reducing the number of computers vulnerable to the Internet Explorer vulnerability used in this attack.

Prevention & Mitigation

Trojan.Hydraq has been known to be spread through specially crafted PDF files and also through malicious Web sites. In both methods software vulnerabilities were leveraged to deliver the Trojan onto the targeted computer.

Flash Vulnerability

Summary of the vulnerability:
Adobe Acrobat, Reader, and Flash Player Remote Code Execution Vulnerability (CVE-2009-1862 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1862)/BID35759 (http://www.securityfocus.com/bid/35759))
Acrobat, Reader, and Flash Player are prone to a remote code-execution vulnerability that arises in the Adobe ActionScript Virtual Machine and affects the 'flash9f.dll' and 'authplay.dll' modules. The attacker can exploit this issue by supplying a malicious Flash ('.swf') file or by embedding a malicious Flash application in a PDF file.

Potential attack scenario:
When using this vulnerability the most likely attack vector used in this case is targeted emails containing legitimate looking PDF documents sent to high level employees. When the document is opened, the vulnerability is leveraged to execute and install Trojan.Hydraq.

Antivirus

Trojan.Pidief.G (http://www.symantec.com/security_response/writeup.jsp?docid=2009-072209-2512-99) - July 2, 2009

Trojan Horse (http://www.symantec.com/security_response/writeup.jsp?docid=2004-021914-2822-99) - July 13, 2009

Bloodhound.Exploit.266 (http://www.symantec.com/security_response/writeup.jsp?docid=2009-080301-5619-99) - August 2, 2009

Intrusion Prevention System

- HTTP MSIE Memory Corruption Code Exec (BID 37815) (http://www.symantec.com/business/security_response/attacksignatures/detail.jsp?asid=23599) - January 16, 2010
- HTTP Acrobat PDF Suspicious File Download 4 (http://www.symantec.com/business/security_response/attacksignatures/detail.jsp?asid=23412) - July 17, 2009

Patches

Adobe APSB09-10 (http://www.adobe.com/support/security/bulletins/apsb09-10.html)

Mitigation

- Turn on Data Execution Protection (DEP) if available.
- Disable JavaScript, Flash and 3D and Multimedia support in Adobe Reader

Further Information

- Next-Generation Flash Vulnerability (https://www-secure.symantec.com/connect/blogs/next-generation-flash-vulnerability)
- SecurityFocus BID 35759 (http://www.securityfocus.com/bid/35759)

Internet Explorer Vulnerability

Summary of the vulnerability:

Internet Explorer CVE-2010-0249 Remote Code Execution Vulnerability (CVE-2010-0249 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0249)/BID37815 (http://www.securityfocus.com/bid/37815))

Internet Explorer is prone to a remote code-execution vulnerability caused by a memory-corruption error. The issue is triggered by an invalid pointer to a deleted object. Attackers can exploit this issue by enticing an unsuspecting user into opening a specially crafted webpage.

Potential attack scenario:

The most likely attack vector used in this case is targeted emails containing legitimate looking attachments or links to Web sites sent to high level employees. When the Web site is opened, the vulnerability is leveraged to execute and install Trojan.Hydraq.

Antivirus

Downloader (http://www.symantec.com/security_response/writeup.jsp?docid=2002-101518-4323-99) - January 15, 2010

Intrusion Prevention System

HTTP MSIE Memory Corruption Code Exec (BID 37815) (http://www.symantec.com/business/security_response/attacksignatures/detail.jsp?asid=23599) - January 16, 2010

Patches

None available yet

Mitigation

Turn on Data Execution Protection (DEP) if available.
Change Internet zone security setting in Internet Explorer to High.

Further Information

Protect yourself against exploit targeting new IE 0-day vulnerability (https://www-secure.symantec.com/connect/blogs/protect-yourself-against-exploit-targeting-new-ie-0-day-vulnerability)
SecurityFocus BID 37815 (http://www.securityfocus.com/bid/37815)

Trojan.Hydraq

Antivirus

- Trojan Horse (http://www.symantec.com/security_response/writeup.jsp?docid=2004-021914-2822-99) - July 13, 2009
- Trojan.Hydraq (http://www.symantec.com/business/security_response/writeup.jsp?docid=2010-011114-1830-99) - January 11, 2010
- Trojan.Hydraq!gen1 (http://www.symantec.com/business/security_response/writeup.jsp?docid=2010-011411-3125-99) - January 14, 2010

Further Reading

Hydraq - An Attack of Mythical Proportions (https://www-secure.symantec.com/connect/blogs/hydraq-attack-mythical-proportions)
Protect Yourself Against Exploit Targeting New IE Zero-Day Vulnerability (http://www.symantec.com/connect/blogs/protect-yourself-against-exploit-targeting-new-ie-zero-day-vulnerability)
The Hydraq VNC Connection (http://www.symantec.com/connect/blogs/hydraq-vnc-connection)
The Trojan.Hydraq Incident: Analysis of the Aurora 0-Day Exploit (http://www.symantec.com/connect/blogs/trojanhydraq-incident-analysis-aurora-0-day-exploit)
Seeing Past Trojan.Hydraq's Obfuscation (http://www.symantec.com/connect/blogs/seeing-past-trojanhydraq-s-obfuscation)
How Trojan.Hydraq Stays On Your Computer (http://www.symantec.com/connect/blogs/how-trojanhydraq-stays-your-computer)

Tags: Security (/connect/communities/security), Security Response (/connect/named-blogs/security-response), Endpoint Protection (AntiVirus) (/connect/products/endpoint-protection-antivirus), Emerging Threats (/connect/blog-tags/emerging-threats), PDF (/connect/blog-tags/pdf), Vulnerabilities & Exploits (/connect/blog-tags/vulnerabilities-exploits)

Subscriptions (0)

(/connect/user/symantec-security-response)

Symantec Security Response (/connect/user/symantec-security-response)

View Profile (/connect/user/symantec-security-response)