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)

+5
5 Votes

Symantec Official Blog

Hydraq - An Attack of Mythical Proportions

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

Created 15 Jan 2010

0 Comments

Share

Over the past couple of days, media outlets have been abuzz with news of a cyber attack on Google. A number of people have theorized political intent and the implications of these attacks.

First, a little background. The critical infrastructures of large corporations are attacked on a daily basis. Some companies are targeted more than others, but all of them are targeted by either hackers who like to put a large feather in their cap, or by hackers trying to steal information for monetary gain. As in all cases with large companies the attacks are investigated thoroughly to make certain that networks and data are not compromised.

As with all targeted attacks, this particular attack was tailored to target a small number of corporate users. The attack vector in this instance could be one of many. A hacker only requires an unpatched computer to visit a website of the hacker's choice, or open a document crafted by the hacker. This can be done by sending a malicious document attached to an email or sending a spoofed email message with a link to a malicious website. Once this is done the hacker installs a back door on the computer that allows him to gain complete control. This grants access to all information stored or passing through the compromised computer. It is vital to note that such hackers don't try to take over all computers within a corporation. All they need is one computer in order to enter an intranet and then seek the information of their choosing. The current case is no different. A very small number of people were attacked using a combination of such vectors, resulting in back door Trojans being installed. More details of the Trojan, detected by Symantec as Trojan.Hydraq (http://www.symantec.com/business/security_response/writeup.jsp?docid=2010-011114-1830-99) and Trojan.Hydraq!gen1 (http://www.symantec.com/business/security_response/writeup.jsp?docid=2010-011411-3125-99), can be obtained from our Threat Expert blog (http://blog.threatexpert.com/2010/01/trojanhydraq-exposed.html).

There is evidence to show that documents attached to an email message were a method of infection. There are also reports of an unpatched vulnerability (http://www.microsoft.com/technet/security/advisory/979352.mspx) in Microsoft's Internet Explorer, which allowed even fully patched computers to become infected once they were lured into visiting a website of the hacker's choosing. We've also seen multiple variants of the Trojan, which confirm that the authors of the malware were constantly improving control of compromised computers by updating the Trojan. This can mean only one thing: the hackers didn't employ one technique across the board, but used different files along with different combinations of attack vectors in order to compromise a network.

We've seen changes happening in cyber attacks for several years now. This attack just brings to light the stark difference we see today as compared to Trojans from a decade ago. In the past, malware authors wanted everyone to know their name and so were doing things such as changing the desktop backgrounds of computers to showcase their ability to compromise a computer. Today, the cyber world is a very different place. Today’s malware authors would rather stay under the radar on one computer for as long as possible, than risk their exposure by trying to infect 100 computers.

We will continue to do whatever we can to protect our customers' assets as more information comes to light about the cyber attack on Google. We advise customers to apply patches where they can, and update their security suite solutions on a regular basis. There are a number of Symantec solutions that can help, such as Data Loss Prevention Network Prevent, which is effective at detecting or blocking the exfiltration of user data via a network protocol following a successful hack into a server; Critical System Protection, which can harden servers that contain critical data and stop unauthorized applications and services from accessing information or prevent data from being moved off the server; and Control Compliance Suite (CCS), which can be used to protect against incursions by hackers or targeted malware by ensuring that patches and configurations of externally facing devices such as firewalls are up to date. Additionally, there are service programs such as Security Program Assessment, which evaluates the maturity of an information security program. We also urge customers to block traffic to known malicious sites where possible.

Next: 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)

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)

Subscriptions (0)

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

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

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

Login (https://www-secure.symantec.com/connect/user/login?destination=node%2F1158381) or Register (https://www-secure.symantec.com/connect/user/register?destination=node%2F1158381) to post comments.

Contact Us (/connect/contact) Privacy Policy (http://www.symantec.com/about/profile/policies/privacy.jsp) Terms and Conditions (/connect/legal) Earn Rewards (/connect/points) Rewards Terms and Conditions (/connect/blogs/symantec-connect-rewards-program-terms-and-conditions)