Information Security Lab

Project – 1

Submitted by: Manish Choudhary
GTID: 902982487

Answer 1

The top-ranked domain visited initially was **"www.gabfirethemes.com".** Its Alexa's ranking is 16228. More information can be found at: http://www.alexa.com/siteinfo/gabfirethemes.com

The post exploitation malware was served via URL: **"porertiasw.tk/1.html"**

Answer 2

The intermediate URLs are:

www.gabfirethemes.com	// Initial top-ranked domain (With obfuscated JS)
gena.glx.nl /top2.html	// Redirecting to porertiasw.tk host (Doc Moved)
porertiasw.tk/77463790.html	// Applet redirecting to Jar file download
porertiasw.tk/24842.jar	// Java Exploit Download (3 times)
porertiasw.tk/24842.jar	
porertiasw.tk/24842.jar	
porertiasw.tk/1.html	// Malware distribution URL

This was a direct website compromise with malicious JavaScript embedded on the index webpage of the website.

Answer 3

The exploitation was based on a Java vulnerability (CVE-2012-0507) targeting following vulnerable versions:

JDK and JRE 7 Update 2 and earlier Java SE
JDK and JRE 6 Update 30 and earlier Java SE
JDK and JRE 5.0 Update 33 and earlier Java SE
SDK and JRE 1.4.2_35 and earlier Java SE
JavaFX 2.0.2 and earlier JavaFX

The exploit was served in a JAR file (**porertiasw.tk/24842.jar**) via an Applet on requesting the URL **porertiasw.tk/77463790.html**.
The virustotal scan result can be found at:
https://www.virustotal.com/en/file/43ffe7b4fc49f7b4111b933eb35b0117b32441a68480fec7f95f5d4d7f3f08f6/analysis/1410306734/

Answer 4

As per the scanners provided on virustotal, the malware is a Win32 Trojan downloader.

The results of Anubis scan can be found at:

https://anubis.iseclab.org/?action=result&task_id=11b241b366ca6e0a4c982fac698cc7281

The results of Threat Expert scan can be found at:

http://www.threatexpert.com/report.aspx?md5=72078c2991fe9259d159823b1b96bc01

The malware belongs to the **"Trojan.Karagany"** family and is generally used to download some other file on the system. As per Symantec and McAfee reports, it is a type of RAT (Remote Access Trojan) that opens a backdoor on the compromised system. This type of malware has been used recently to facilitate cyber espionage campaign.

Reasoning Behind the above answers and the network trace

The binary download was searched in PCAP by looking for PE and MZ in the packets. There were two binary downloads. The first was considered as the initial malware download and thus, the subject for analysis. The TCP stream confirmed that the download was a result of GET request for 1.html to the host "porertiasw.tk". This GET request was a post exploitation malware download attempt after the exploitation of a Java vulnerability (CVE-2012-0507). Following the same TCP stream upward revealed that the exploit was delivered in a JAR file on making a GET request for 24842.jar to the host porertiasw.tk. This JAR file was the exploit and can be confirmed by checking that the user agent is "Mozilla/4.0 (Windows XP 5.1) Java/1.6.0_10". In addition, check on virustotal, and the presence of the requests for Jar file and the malware in the same TCP session also help to conclude the same. Looking at the Jar file object and requests in PCAP confirmed that the request for the Jar file was forced via an applet served on a GET request for 77463790.html to the host porertiasw.tk. The request for this HTML page was made because of a redirection from the host gena.glx.nl.

The response page for a request for top2.html to gena.glx.nl contained:

<h1>Document moved here</h1>

This redirected us to the host porertiasw.tk. The request for gena.glx.nl/top2.html was embedded in the index page served on requested gabfirethemes.com. This website was compromised and contained obfuscated JavaScript to request for top2.html at gena.glx.nl.

Requests identified on scanning the index page on Wepawet can be found at:

https://wepawet.iseclab.org/view.php?hash=32341165f303eaab9485bdc7d9bf4c43&type=js&t=1409845027