Answers to Assignment 3

Christopher Adam Craig

I just graded Assignment 3. Those of you who turned it in did extremely well. The score is up to 5 extra points on your final grade. Here are the answers:

1. Which top-ranked domain was initially visited (hint: look for the first use of the DNS)? What URL (domain or IP address and path) served the (first) post- exploitation malware download? The answers to these two questions represent the start and end points of a chain of requests for the DDL event.

The initial visit was to askmen.com and the malware was downloaded from 1991374732-6.headexclusive.uni.me

2. Which URLs comprise the intermediate chain of requests that connect the top- ranked domain to the malware distribution URL? Was an ad network involved or was the DDL the result of direct website compromise? If an ad network was involved, specify which one (e.g., Clicksor, DoubleClick).

There was not an ad network involved, it was a direct compromise of askmen.com. The domain names in the chain (it asks for URLs, but I accepted domain names) are:

1. askmen.com
2. **www.askmen.com** (http://www.askmen.com) - this included a compromised javascript named geoAnalytics.js that included a sequence of integers that were the ASCII values for
3. static.nasrul.web.id
4. static.smallorange.co.za - this included javascript with a ROT13 encoding of
5. 1991374732-6.headexclusive.uni.me

3. What software component targeted during the event resulted in successful exploita- tion? Upload the corresponding threat artifact (e.g., PDF file, jar file, Flash file) you extract from the PCAP to VirusTotal and provide a link to its detections. Which CVE does this artifact target?

There were two exploits downloaded.

The first was a PDF file that targeted CVE-2010-0188 in Adobe Reader/Adobe Acrobat. This could have been found by looking up the PDF on VirusTotal and then checking the Microsoft Knowledge Base for the exploit name in Windows Defender.

The second was a jar file that targeted CVE-2012-0507 in Java. This CVE was actually included in the exploit name from several engines directly in VirusTotal.

4. What malware instance was pushed to the exploited system? To answer this question, use reports from VirusTotal.

This asks about the **malware**, not the exploit (several of you missed that). It was a Zbot variant, also known as Bagsu!rfn.

Search entries or author | Unread

Reply