Assignment 3 - Analyze a malware download

Submit Assignment

Due Sep 21 by 11:59pm **Points** 7 **Submitting** a text entry box or a file upload
Available after Sep 14 at 12am

For this project you will perform an analysis of a drive-by download (DDL) event. An event is represented as a packet capture (PCAP) file whose network activity begins with a visit to an Alexa top-ranked domain and ends with the download of malicious software.

Once you have retrieved a copy of the PCAP file representing your event (listed below), create an analysis report that answers the questions below. You will get credit for the completeness and correctness of your report.

This project is to be completed individually.

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

Note: The traffic you are analyzing is real-world event data that contains actual exploit content and malicious software. Use a Linux or Mac OS X environment to perform the analysis.

Use of tools such as Wireshark are allowed and encouraged for this project. However, excepting the MITRE CVE website and VirusTotal, Internet resources such as Google are prohibited. Please contact the instructor if you require clarification on one or more of the above questions.

This assignment was originally written by Paul Royal.

f779851715edabc1541a2be06453f7ca.pcap