Web Malware Investigation

**Manual Analysis**

Identify 2 obfuscated PHP files on all snapshots of the website, deobfuscate them, and identify the attacker's behavior.

The snapshots of the provided website were scanned using PHP scanner and report generated show –

**Version:** 0.10.4  
**Scan date:** 2023-03-13 22:25:35  
**Files analyzed:** 305 **| Files infected:** 296

****

**Cron.php –**

Cron is often used to ensure timely execution of important tasks including executing or scheduling a code snippet. Cron jobs are very helpful at scheduling jobs in PHP.  Cron jobs let you automate several tasks which aid in the efficient running of your website.

**Block injection in seen in cron.php using code –**

****

**Deobfuscated cron.php –**

****

Using this code, unauthenticated attacker seems to perform remote code execution on default Drupal installations using elevated privileges. He execute arbitrary code base64-encoded in the post-parameter "cookies\_p". The intent may be an attempt to attack the visitor of the site.

Drupal site does not seem to be up to date and was exploited by the vulnerability known as Druppalgeddon 2 (aka SA-CORE-2018-002), which is used to fiddle with the system and inject this php. This vulnerability is related to PHP’s improper sanitization in the handling of arrays in parameters (in GET/POST).

**Impact** – The returning / new users to this website will be affected (redirected to other websites in array because of the cookies set by this injected code.

**index.php –**

The index. php file for a template contains a mixture of code that will be delivered as it is, and PHP code that will be modified before it is delivered. The code will be familiar to anyone who has designed a simple HTML web page. There are 2 main sections - the <head> and <body>

**Block injection in seen in index.php using code –**

****

**Deobfuscated cron.php –**

****

Identify all binaries and apks (if any) in this website repository for all snapshots, submit them to VirusTotal and collect the reports.

find . -type f | perl -lne 'print if -B'



**Analysis using Tool –**

**Tool name - Malware detector**

root@Ubuntu1:/home/vboxuser/Desktop# python3.6 Malware\_detector.py /home/vboxuser/Desktop/website-682886/www.joncomet.com

root@Ubuntu1:/home/vboxuser/Desktop# ls -lrt

total 1372

drwxrwx--- 5 755 vboxuser 4096 Mar 12 07:39 website-682886

-rw-r--r-- 1 root root 1614 Mar 31 15:12 all-files.py

-rw-r--r-- 1 root root 4860 Mar 31 15:34 1

-rw-r--r-- 1 root root 4919 Mar 31 16:39 Malware\_detector.py

-rw-r--r-- 1 root root 702956 Mar 31 16:55 Target

-rw-r--r-- 1 root root 635369 Apr 1 11:22 target\_files

-rw-r--r-- 1 root root 33110 Apr 1 11:22 suspicious\_files

Identify 2 obfuscated PHP files on all snapshots of the website, deobfuscate them, and identify the attacker's behavior.

**274 suspicious PHP files detected by Malware detector tool.**