Server IP: 45.33.37.149
Analyst: Gbenga Ojo

Analysis Summary

- Backed up files and db
- Cannot access apache log files; inadequate permissions
- https://www.wordfence.com/docs/how-to-clean-a-hacked-wordpress-site-using-wordfence/
- Ran manual diff on clean wordpress files versus infected
- Upgraded wp, themes, plugins; created another backup
- Reset admin password to ‘password’ to gain access
- Deleted or updated the following:
    - Only in html/wp-admin/css/colors/light: article11.php *(obfuscated; see below for details)*
    - Files wordpress/wp-content/index.php and html/wp-content/index.php differ *(arbitrary file upload; see below for details)*
    - Only in html/wp-includes/customize: lhvy.php *(spam relay)*
    - Only in html/wp-includes/SimplePie: bOR_uPNDa.php *(arbitrary code execution)*
    - Only in html/wp-includes/Text/Diff: dmdm.php *(spam relay)*
    - Only in html/wp-includes/Text/Diff/Engine: lmaow.php *(spam relay)*
    - Only in html/wp-includes: ueuo.php *(spam relay)*
    - Only in html: wp-tmp.php *(arbitrary code execution)*
- Download latest WP and re-ran diff
    - Only benign differences in readme, theme, plugin, cache, and log files
- Scan db dump file for ‘base64’, ‘eval’, ‘<script>’, ‘pills’, ‘viagra’, ‘cialis’, etc.
    - *Found malware links and attempted redirects; deleting (from both posts and revisions):*
        - http://45.33.37.149/index.php/2008/09/11/a-post-with-a-right-aligned-image/
            - http://cheap-pills-norx.com
            - http://buyviagraonlinenow.net
        - http://45.33.37.149/index.php/2008/09/11/a-post-with-a-right-aligned-image/
            - http://cheap-pills-norx.com
        - http://45.33.37.149/index.php/2008/09/17/another-post-with-everything-in-it/
            - http://buycialisonlinehq.net
            - http://buycialisonlinefree.net
            - http://hepatitis-genericsovaldion.net
            - http://cialis24online.net
            - http://viagracoupongeneric.net
            - http://buycialisonlinehq.net
            - http://tadalafilforsale.net
            - http://viagragenericedpills.net
            - http://sovaldihepatitisc.net
            - http://buyviagraonlinefree.net
            - http://hepatitis-genericsovaldion.net
            - http://viagraonlinebuy.net
        - http://45.33.37.149/index.php/2008/09/17/an-ordered-list-post/
        - http://45.33.37.149/index.php/2016/03/29/hello-world/
            - script redirects to http://google.com
- Restored admin password

Select File Details

/wp-admin/css/colors/light/article11.php

A string is defined on the first line that obfuscates characters as hexadecimal representations of ASCII characters. Individual hex elements from the string are referenced via array format to produce the remainder of the file's code. Data is stolen from the WordPress installation, and the code is further obfuscated using variable functions combined with the following language constructs and functions:

- string chr (int $ascii)
- int ord (string $string)
- int strlen (string $string)
- string ini_set (string $varname , string $newvalue)
- string phpversion ([string $extension])
- mixed unserialize (string $str [, array $options])
- string base64_decode (string $data [, bool $strict = false])
- bool set_time_limit (int $seconds)

Data that appears capable of theft includes:

- HTTP GET data
- HTTP POST data
- Request specific cookies
- Request specific file uploads
- Logged in user specific data (admin in this case)

Further deobfuscation of this file could yield more information regarding its purpose.

/wp-content/index.php

This appears to be a primary attack vector candidate, allowing for the arbitrary upload of files to various locations on the server. Access to logs could provide more clues as to how the server was initially compromised.