

Exemples de résultats pour la recherche par IP dans les logs du serveur web

Attaque Wordpress

Fichier xmlrpc.php

Dans cet exemple de résultat, on constate avec la recherche par IP que celui-ci attaque un site Wordpress avec le fichier xmlrpc.php de celui-ci.

Pour résoudre le problème, vous pouvez:

- Bloquer l'accès au fichier xmlrpc.php à l'aide d'un fichier .htaccess
- Bloquer l'adresse IP avec le firewall du serveur.

```
/var/log/httpd/domains/mon_domaine.com.log:1244:54.36.38.246 - -  
[05/May/2020:09:39:50 -0400] "POST /xmlrpc.php HTTP/1.1" 200 631 "-"  
"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like  
Gecko) Chrome/80.0.3987.149 Safari/537.36"  
/var/log/httpd/domains/mon_domaine.com.log:1246:54.36.38.246 - -  
[05/May/2020:09:39:50 -0400] "POST /xmlrpc.php HTTP/1.1" 200 631 "-"  
"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like  
Gecko) Chrome/80.0.3987.149 Safari/537.36"  
/var/log/httpd/domains/mon_domaine.com.log:1248:54.36.38.246 - -  
[05/May/2020:09:39:51 -0400] "POST /xmlrpc.php HTTP/1.1" 200 631 "-"  
"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like  
Gecko) Chrome/80.0.3987.149 Safari/537.36"  
/var/log/httpd/domains/mon_domaine.com.log:1250:54.36.38.246 - -  
[05/May/2020:09:39:51 -0400] "POST /xmlrpc.php HTTP/1.1" 200 631 "-"  
"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like  
Gecko) Chrome/80.0.3987.149 Safari/537.36"  
/var/log/httpd/domains/mon_domaine.com.log:1252:54.36.38.246 - -  
[05/May/2020:09:39:51 -0400] "POST /xmlrpc.php HTTP/1.1" 200 631 "-"  
"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like  
Gecko) Chrome/80.0.3987.149 Safari/537.36"  
/var/log/httpd/domains/mon_domaine.com.log:1254:54.36.38.246 - -  
[05/May/2020:09:39:52 -0400] "POST /xmlrpc.php HTTP/1.1" 200 631 "-"  
"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like  
Gecko) Chrome/80.0.3987.149 Safari/537.36"  
/var/log/httpd/domains/mon_domaine.com.log:1256:54.36.38.246 - -  
[05/May/2020:09:39:52 -0400] "POST /xmlrpc.php HTTP/1.1" 200 631 "-"  
"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like  
Gecko) Chrome/80.0.3987.149 Safari/537.36"  
/var/log/httpd/domains/mon_domaine.com.log:1258:54.36.38.246 - -  
[05/May/2020:09:39:53 -0400] "POST /xmlrpc.php HTTP/1.1" 200 631 "-"  
"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like  
Gecko) Chrome/80.0.3987.149 Safari/537.36"
```

```
/var/log/httpd/domains/mon_domaine.com.log:1260:54.36.38.246 - -  
[05/May/2020:09:39:53 -0400] "POST /xmlrpc.php HTTP/1.1" 200 631 "-"  
"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like  
Gecko) Chrome/80.0.3987.149 Safari/537.36"  
/var/log/httpd/domains/mon_domaine.com.log:1262:54.36.38.246 - -  
[05/May/2020:09:39:53 -0400] "POST /xmlrpc.php HTTP/1.1" 200 631 "-"  
"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like  
Gecko) Chrome/80.0.3987.149 Safari/537.36"  
/var/log/httpd/domains/mon_domaine.com.log:1264:54.36.38.246 - -  
[05/May/2020:09:39:54 -0400] "POST /xmlrpc.php HTTP/1.1" 200 631 "-"  
"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like  
Gecko) Chrome/80.0.3987.149 Safari/537.36"  
/var/log/httpd/domains/mon_domaine.com.log:1266:54.36.38.246 - -  
[05/May/2020:09:39:54 -0400] "POST /xmlrpc.php HTTP/1.1" 200 631 "-"  
"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like  
Gecko) Chrome/80.0.3987.149 Safari/537.36"  
/var/log/httpd/domains/mon_domaine.com.log:1267:54.36.38.246 - -  
[05/May/2020:09:39:55 -0400] "POST /xmlrpc.php HTTP/1.1" 200 631 "-"  
"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like  
Gecko) Chrome/80.0.3987.149 Safari/537.36"  
/var/log/httpd/domains/mon_domaine.com.log:1269:54.36.38.246 - -  
[05/May/2020:09:39:55 -0400] "POST /xmlrpc.php HTTP/1.1" 200 631 "-"  
"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like  
Gecko) Chrome/80.0.3987.149 Safari/537.36"  
/var/log/httpd/domains/mon_domaine.com.log:1272:54.36.38.246 - -  
[05/May/2020:09:39:55 -0400] "POST /xmlrpc.php HTTP/1.1" 200 631 "-"  
"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like  
Gecko) Chrome/80.0.3987.149 Safari/537.36"  
/var/log/httpd/domains/mon_domaine.com.log:1274:54.36.38.246 - -  
[05/May/2020:09:39:56 -0400] "POST /xmlrpc.php HTTP/1.1" 200 631 "-"  
"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like  
Gecko) Chrome/80.0.3987.149 Safari/537.36"
```

From: <https://wiki.proletaire.net/> - Wiki

Permanent link: https://wiki.proletaire.net/linux/debug_charge/exemple_grep_ip_serveur_web?rev=1588687034

Last update: **2020/05/05 13:57**

