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

```
grep -rnw '/var/log/httpd' -e '54.36.38.246'
```

Attaque Wordpress

Fichier xmlrpc.php

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

```
/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"
```

Pour résoudre le problème, vous pouvez:

- Bloquer l'accès au fichier xmlrpc.php à l'aide d'un fichier .htaccess. IMPORTANT DE RENVOYER LA REQUÊTE VERS UN AUTRE SITE QUI N'EST PAS SUR VOTRE SERVEUR...EX: google.com.
- Bloquer l'adresse IP (54.36.38.246 dans notre example) avec le firewall du serveur.

Semrush

```
/var/log/httpd/domains/mon-domaine.com.log:1224:46.229.168.129 - -
[05/May/2020:10:31:09 -0400] "GET /lapis-surabaya-ekonomis/ HTTP/1.1" 302
4327 "-" "Mozilla/5.0 (compatible; SemrushBot/6~bl;
+http://www.semrush.com/bot.html)"
/var/log/httpd/domains/mon-domaine.com.log:1225:46.229.168.137 - -
[05/May/2020:10:31:10 -0400] "GET / HTTP/1.1" 200 4681 "-" "Mozilla/5.0
(compatible; SemrushBot/6~bl; +http://www.semrush.com/bot.html)"
/var/log/httpd/domains/mon-domaine.com.log:1227:46.229.168.148 - -
[05/May/2020:10:31:54 -0400] "GET /pizza-gulung-pisang/ HTTP/1.1" 302 4327
```

```
"-" "Mozilla/5.0 (compatible; SemrushBot/6~bl;
+http://www.semrush.com/bot.html)"
/var/log/httpd/domains/mon-domaine.com.log:1228:46.229.168.135 - -
[05/May/2020:10:31:55 -0400] "GET / HTTP/1.1" 200 4681 "-" "Mozilla/5.0
(compatible; SemrushBot/6~bl; +http://www.semrush.com/bot.html)"
/var/log/httpd/domains/mon-domaine.com.log:1240:46.229.168.144 - -
[05/May/2020:10:35:51 -0400] "GET /tahu-bumbu-serai/ HTTP/1.1" 302 4327 "-"
"Mozilla/5.0 (compatible; SemrushBot/6~bl;
+http://www.semrush.com/bot.html)"
/var/log/httpd/domains/mon-domaine.com.log:1241:46.229.168.141 - -
[05/May/2020:10:35:53 -0400] "GET / HTTP/1.1" 200 4681 "-" "Mozilla/5.0
(compatible; SemrushBot/6~bl; +http://www.semrush.com/bot.html)"
/var/log/httpd/domains/mon-domaine.com.log:1248:46.229.168.154 - -
[05/May/2020:10:39:15 -0400] "GET /siomay-goreng/ HTTP/1.1" 302 4327 "-"
"Mozilla/5.0 (compatible; SemrushBot/6~bl;
+http://www.semrush.com/bot.html)"
/var/log/httpd/domains/mon-domaine.com.log:1249:46.229.168.161 - -
[05/May/2020:10:39:16 -0400] "GET / HTTP/1.1" 200 4681 "-" "Mozilla/5.0
(compatible; SemrushBot/6~bl; +http://www.semrush.com/bot.html)"
/var/log/httpd/domains/mon-domaine.com.log:1259:46.229.168.146 - -
[05/May/2020:10:46:19 -0400] "GET /opor-tahu-tempe/ HTTP/1.1" 302 4327 "-"
"Mozilla/5.0 (compatible; SemrushBot/6~bl;
+http://www.semrush.com/bot.html)"
/var/log/httpd/domains/mon-domaine.com.log:1260:46.229.168.136 - -
[05/May/2020:10:46:21 -0400] "GET / HTTP/1.1" 200 4681 "-" "Mozilla/5.0
(compatible; SemrushBot/6~bl; +http://www.semrush.com/bot.html)"
/var/log/httpd/domains/mon-domaine.com.log:1265:46.229.168.163 - -
[05/May/2020:10:47:57 -0400] "GET /tag/soun-goreng/ HTTP/1.1" 302 4327 "-"
"Mozilla/5.0 (compatible; SemrushBot/6~bl;
+http://www.semrush.com/bot.html)"
/var/log/httpd/domains/mon-domaine.com.log:1266:46.229.168.149 - -
[05/May/2020:10:47:58 -0400] "GET / HTTP/1.1" 200 4681 "-" "Mozilla/5.0
(compatible; SemrushBot/6~bl; +http://www.semrush.com/bot.html)"
/var/log/httpd/domains/mon-domaine.com.log:1293:46.229.168.129 - -
[05/May/2020:11:06:23 -0400] "GET /crackers-lapis-tape/ HTTP/1.1" 302 4327
"-" "Mozilla/5.0 (compatible; SemrushBot/6~bl;
+http://www.semrush.com/bot.html)"
/var/log/httpd/domains/mon-domaine.com.log:1294:46.229.168.151 - -
[05/May/2020:11:06:24 -0400] "GET / HTTP/1.1" 200 4681 "-" "Mozilla/5.0
(compatible; SemrushBot/6~bl; +http://www.semrush.com/bot.html)"
/var/log/httpd/domains/mon-domaine.com.log:1314:46.229.168.140 - -
[05/May/2020:11:09:39 -0400] "GET /telur-pindang/ HTTP/1.1" 302 4327 "-"
"Mozilla/5.0 (compatible; SemrushBot/6~bl;
+http://www.semrush.com/bot.html)"
/var/log/httpd/domains/mon-domaine.com.log:1315:46.229.168.163 - -
[05/May/2020:11:09:40 -0400] "GET / HTTP/1.1" 200 4681 "-" "Mozilla/5.0
(compatible; SemrushBot/6~bl; +http://www.semrush.com/bot.html)"
/var/log/httpd/domains/mon-domaine.com.log:1316:46.229.168.131 - -
[05/May/2020:11:09:53 -0400] "GET /fu-yung-hai-ayam/ HTTP/1.1" 302 4327 "-"
"Mozilla/5.0 (compatible; SemrushBot/6~bl;
+http://www.semrush.com/bot.html)"
```

```
/var/log/httpd/domains/mon-domaine.com.log:1317:46.229.168.144 - -
[05/May/2020:11:09:55 -0400] "GET / HTTP/1.1" 200 4681 "-" "Mozilla/5.0
(compatible; SemrushBot/6~bl; +http://www.semrush.com/bot.html)"
/var/log/httpd/domains/mon-domaine.com.log:1329:46.229.168.151 - -
[05/May/2020:11:14:39 -0400] "GET /tag/buah-tropis/ HTTP/1.1" 302 4327 "-"
"Mozilla/5.0 (compatible; SemrushBot/6~bl;
+http://www.semrush.com/bot.html)"
/var/log/httpd/domains/mon-domaine.com.log:1330:46.229.168.146 - -
[05/May/2020:11:14:40 -0400] "GET / HTTP/1.1" 200 4681 "-" "Mozilla/5.0
(compatible; SemrushBot/6~bl; +http://www.semrush.com/bot.html)"
/var/log/httpd/domains/mon-domaine.com.log:1340:46.229.168.133 - -
[05/May/2020:11:20:28 -0400] "GET /robots.txt HTTP/1.1" 200 4235 "-"
"Mozilla/5.0 (compatible; SemrushBot/6~bl;
+http://www.semrush.com/bot.html)"
/var/log/httpd/domains/mon-domaine.com.log:1341:46.229.168.129 - -
[05/May/2020:11:20:29 -0400] "GET /tag/variasi-resep-brokoli/ HTTP/1.1" 302
4327 "-" "Mozilla/5.0 (compatible; SemrushBot/6~bl;
+http://www.semrush.com/bot.html)"
```