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.

wp-login.php

```
/var/log/httpd/domains/mon-domaine.xxx.log:840:13.82.87.18 - -
[05/May/2020:06:38:39 +0200] "POST /wp-login.php HTTP/1.1" 200 2477 "-"
"Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:62.0) Gecko/20100101
Firefox/62.0"
/var/log/httpd/domains/mon-domaine.xxx.log:841:13.82.87.18 - -
[05/May/2020:06:38:41 +0200] "GET /wp-login.php HTTP/1.1" 200 2346 "-"
"Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:62.0) Gecko/20100101
Firefox/62.0"
/var/log/httpd/domains/mon-domaine.xxx.log:842:13.82.87.18 - -
```

```
[05/May/2020:06:38:43 +0200] "POST /wp-login.php HTTP/1.1" 200 2454 "-"
"Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:62.0) Gecko/20100101
Firefox/62.0"
/var/log/httpd/domains/mon-domaine.xxx.log:851:111.231.141.206 - -
[05/May/2020:06:45:18 +0200] "GET /wp-login.php HTTP/1.1" 200 2346 "-"
"Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:62.0) Gecko/20100101
Firefox/62.0"
/var/log/httpd/domains/mon-domaine.xxx.log:852:111.231.141.206 - -
[05/May/2020:06:45:20 +0200] "POST /wp-login.php HTTP/1.1" 200 2477 "-"
"Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:62.0) Gecko/20100101
Firefox/62.0"
/var/log/httpd/domains/mon-domaine.xxx.log:853:111.231.141.206 - -
[05/May/2020:06:45:21 +0200] "GET /wp-login.php HTTP/1.1" 200 2346 "-"
"Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:62.0) Gecko/20100101
Firefox/62.0"
/var/log/httpd/domains/mon-domaine.xxx.log:854:111.231.141.206 - -
[05/May/2020:06:45:25 +0200] "POST /wp-login.php HTTP/1.1" 200 2454 "-"
"Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:62.0) Gecko/20100101
Firefox/62.0"
/var/log/httpd/domains/mon-domaine.xxx.log:866:162.243.27.248 - -
[05/May/2020:06:54:46 +0200] "GET /wp-login.php HTTP/1.1" 200 2346 "-"
"Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:62.0) Gecko/20100101
Firefox/62.0"
/var/log/httpd/domains/mon-domaine.xxx.log:867:162.243.27.248 - -
[05/May/2020:06:54:52 +0200] "POST /wp-login.php HTTP/1.1" 200 2477 "-"
"Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:62.0) Gecko/20100101
Firefox/62.0"
/var/log/httpd/domains/mon-domaine.xxx.log:868:162.243.27.248 - -
[05/May/2020:06:54:58 +0200] "GET /wp-login.php HTTP/1.1" 200 2346 "-"
"Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:62.0) Gecko/20100101
Firefox/62.0"
/var/log/httpd/domains/mon-domaine.xxx.log:869:162.243.27.248 - -
[05/May/2020:06:55:03 +0200] "POST /wp-login.php HTTP/1.1" 200 2454 "-"
"Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:62.0) Gecko/20100101
Firefox/62.0"
/var/log/httpd/domains/mon-domaine.xxx.log:877:185.120.147.145 - -
[05/May/2020:07:05:26 +0200] "GET /wp-login.php HTTP/1.1" 200 2346 "-"
"Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:62.0) Gecko/20100101
Firefox/62.0"
/var/log/httpd/domains/mon-domaine.xxx.log:878:185.120.147.145 - -
[05/May/2020:07:05:28 +0200] "POST /wp-login.php HTTP/1.1" 200 2477 "-"
"Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:62.0) Gecko/20100101
Firefox/62.0"
/var/log/httpd/domains/mon-domaine.xxx.log:879:185.120.147.145 - -
[05/May/2020:07:05:28 +0200] "GET /wp-login.php HTTP/1.1" 200 2346 "-"
"Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:62.0) Gecko/20100101
Firefox/62.0"
/var/log/httpd/domains/mon-domaine.xxx.log:880:185.120.147.145 - -
[05/May/2020:07:05:29 +0200] "POST /wp-login.php HTTP/1.1" 200 2454 "-"
"Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:62.0) Gecko/20100101
Firefox/62.0"
```

```
/var/log/httpd/domains/mon-domaine.xxx.log:894:206.189.136.156 - -
[05/May/2020:07:15:21 +0200] "GET /wp-login.php HTTP/1.1" 200 2346 "-"
"Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:62.0) Gecko/20100101
Firefox/62.0"
/var/log/httpd/domains/mon-domaine.xxx.log:895:206.189.136.156 - -
[05/May/2020:07:15:23 +0200] "POST /wp-login.php HTTP/1.1" 200 2477 "-"
"Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:62.0) Gecko/20100101
Firefox/62.0"
/var/log/httpd/domains/mon-domaine.xxx.log:896:206.189.136.156 - -
[05/May/2020:07:15:23 +0200] "GET /wp-login.php HTTP/1.1" 200 2346 "-"
"Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:62.0) Gecko/20100101
Firefox/62.0"
/var/log/httpd/domains/mon-domaine.xxx.log:897:206.189.136.156 - -
[05/May/2020:07:15:24 +0200] "POST /wp-login.php HTTP/1.1" 200 2454 "-"
"Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:62.0) Gecko/20100101
Firefox/62.0"
```

Généralement effectués via plusieurs IPs (zombies) sur une période plus ou moins longue.

Pour résoudre le problème, vous pouvez:

- Bloquer l'accès au fichier wp-login.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 le/les adresses IPs avec le firewall du serveur.

Semrush / SemrushBot

```
/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)"
```

Vous pouvez le blocker à l'aide d'un fichier robots.txt placé à la racine de votre site avec le contenu suivant:

```
User-agent: SemrushBot
Disallow: /

User-agent: SemrushBot-SA
Disallow: /

User-agent: SemrushBot-BA
Disallow: /

User-agent: SemrushBot-SI
Disallow: /

User-agent: SemrushBot-SWA
Disallow: /

User-agent: SemrushBot-CT
Disallow: /

User-agent: SemrushBot-BM
Disallow: /
```

Il est aussi possible de bloquer les adresses IPs utilisés par Semrush via le Firewall. Parcontre, Semrush utilise une grande quantité d'adresses IPs. Comme dans notre exemple, plusieurs adresses IPs 46.229.168.XXX

Idéalement, vous pouvez bannir les plage entière de IPs pour régler le problème. Pour trouver la place, vous pouvez aller sur le site de BGP Toolkit de Hurricane Electric et y entrer une des adresse IP. La plage d'adresse IP sera incrite dans la colonne *Announcement* après votre recherche sur le site du BGP Toolkit (exemple: 46.229.168.0/24)