

• /var/www/.../docs/assets/snippets/.mandarin/class.phpmailer.php - RCE : CVE-2016-10045, CVE-2016-10031

**Эти файлы могут быть вредоносными или хакерскими скриптами (11)**

Отображать по  записей

Поиск:

Путь	Изменение свойств	Изменение содержимого	Размер
<p>/var/www/.../docs/client_side/page_company/css/favicon_f37c65.ico</p> <p>1 ...=isset(\$stsezmdb[\$rowxwzv[\$i]])?stsezmdb[\$rowxwzv[\$i]] :\$rowxwzv[\$i];\$ahhvcchyg["base64_decode";return\$ahhvcchyg(\$fspqminfyt);}\$ifnnofgi="rdbZinuPE62gGKL1miC</p>	04/12/2017 11:03:51	04/12/2017 11:03:51	28.43 Kb
<p>/var/www/.../docs/assets/galleries/33/thumbs/mnrerize.php</p> <p>2 ...q#x4Qe6{jp}&gt;h?vsUJPDg+LI_17&amp;-nw="EK";OR-}&lt;5 *CA/B,OcSd\$V^*3am-8HrWoT9KYGF";\$GLOBALS[\$GLOBALS["k8e447e69"]][93].\$GLOBALS["k8e447e69"] [83].\$GLOBALS["k8e447e</p>	01/12/2017 13:06:22	25/10/2017 22:06:31	12.20 Kb
<p>/var/www/.../docs/assets/modules/store/installer/index.php</p> <p>2 ...-WXV\$&gt;m+ale) C-FfZq5u6&amp;'gw_=-4-DHG,7NT%L}s#vY{2drU\tMnzIRocE3KbpA-iS}{.?!B'-'^!";\$i72d12d7[\$i72d12d7["b481"]][15].\$i72d12d7["b481"] [79].\$i72d12d7["b481"] [81].\$i</p>	01/12/2017 13:06:52	25/10/2017 22:05:55	13.48 Kb
<p>/var/www/.../docs/assets/snippets/phthumb/fexwmbty.php</p> <p>2 ...A'c#i7Z*=8akM+%Ro:Brw-Db93CV-{Qkdt-0egG/lm;5l_y]W^2hNp'4 sLH&lt;"E\uF{P&amp;vY-U{TO";\$GLOBALS[\$GLOBALS["ge3c9c022"]][75].\$GLOBALS["ge3c9c022"] [12].\$GLOBALS["ge3c9c0</p>	01/12/2017 13:06:32	25/10/2017 22:06:31	11.36 Kb
<p>/var/www/.../docs/assets/snippets/FormLister/config/nstyvgal.php</p> <p>2 ...G,Q8C=elmV&lt;_0U]o?r1gv' ]/3{S-yK+-T6FR}jH5A-Y#OZBb&amp;tdXE%I2hz;x^la@&gt;Wnw{]MN4"s";\$GLOBALS[\$GLOBALS["u01a0"]][8].\$GLOBALS["u01a0"] [13].\$GLOBALS["u01a0"] [62].\$GLO</p>	01/12/2017 13:06:45	25/10/2017 22:06:31	9.74 Kb
<p>/var/www/.../docs/assets/snippets/.mandarin/projectBanners.php</p>			

**serveradmin.ru**

На днях мне довелось впервые познакомиться с вирусом, который пытался майнить криптовалюту на одном из серверов, за которым я приглядывал. Сама история обнаружения и лечения веб сервера от этого вируса не представляет какого-то особенного интереса. Тем не менее я решил поделиться опытом

общения с новым для меня зловредом.

Содержание:

- 1 Симптомы заражения
- 2 Поиск криптомайнера
- 3 Удаление вируса майнера

## Симптомы заражения

Все началось как обычно — с сообщения от мониторинга zabbix о том, что на сервере повышенная нагрузка на CPU. Сразу скажу, что мониторинг — лучший друг в борьбе с вирусами. Без его помощи можно вообще не узнать, что у вас что-то случилось.

Кратенько расскажу о сервере. Этот веб сервер несет на себе очень старые сайты на популярных движках. Многие из этих сайтов давно не обновлены, в них есть уязвимости, которые периодически используют злоумышленники и заливают вирусы. То, что можно было и имело смысл обновить — обновили, но далеко не все. Это просто неоправданно дорого и бесполезно в данном случае. Я перенес в свое время все эти сайты на отдельный веб сервер, где все пакеты и сама система имеют свежие версии и оперативно обновляются. Тем не менее, это не сильно спасает от периодических проблем, которые я закрываю в ручном режиме.

В данном случае первой ласточкой был вирус, рассылающий спам. Я зашел на сервер и увидел огромную очередь писем на отправку. Почтовый лог был забит информацией. Я сразу же остановил и отключил postfix, так как он там по большому счету не нужен. Отправка писем ведется через внешний smtp.

Сразу же дам рекомендацию отключать почтовые сервера там, где на сервере они не нужны. Это избавит от лишних хлопот и проблем в будущем.

В разделе `/tmp` заметил левые файлы с владельцем apache. Удалил их. Времени подробно разбираться с сервером не было и я отложил это дело, но снизил метрики в мониторинге, чтобы сразу заметить малейшее увеличение нагрузки выше среднего.

В следующую ночь на сервере опять были странности, которые я сразу же заметил утром по мониторингу. Сервер — виртуальная машина с одним процессором. В стандартном шаблоне заббикс срабатывает триггер, если load average держится выше 5-ти, что для однопроцессорного сервера очень много. Я перед этим снизил порог срабатывания до 0.5, это и позволило мне своевременно среагировать. Нагрузка была примерно 1-1.5, что не позволило бы сработать стандартному триггеру.





Злоумышленники ведут себя очень грамотно. Выражается это в том, что они запускают свои вирусы глубокой ночью, когда администраторы спят. Ты реагируешь только утром, в итоге у вируса есть несколько часов, чтобы сделать то, что от него требуется. За это время можно разослать тысячи спамовых писем.

В общем, получилось такая история. Сервер был каким-то образом заражен. Сначала был запущен вирус, который рассылал спам. После того, как я его удалил, в дело пошла вторая очередь. Вторым вирусом, о котором я рассказываю, оказался криптомайнер. Ниже расскажу, почему я так решил.

## Поиск криптомайнера

Долго искать вирус мне не пришлось. По загрузке процессора в **htop** сразу же были найдены файлы опять же в директории `/tmp`, которые создавали нагрузку.



```

CPU[|||||100.0%] Tasks: 55, 115 thr; 2 running
Mem[|||||1565/1871MB] Load average: 1.07 1.12 1.12
Swp[||] 55/4031MB Uptime: 20:27:40

  PID CPU%  Mem  VSZ  RSS  %CPU  Mem%  CPU%  TIME  COMMAND
13623 apache 20 0 184M 18556 1616 R 97.7 1.0 6h18:17 /tmp/phpv65kNK_2xu3yzzrzlezbv6e -c /tmp/phpv65kNK.c
13622 apache 20 0 184M 18556 1616 S 97.7 1.0 6h18:17 /tmp/phpv65kNK_2xu3yzzrzlezbv6e -c /tmp/phpv65kNK.c
1658 root 20 0 3397M 1166M 6864 S 0.5 62.3 6:16.15 /root/youtrack/internal/java/linux-x64/jre/bin/java -Djl.service=YouTrack -Djl.home=/root/youtrack -ea -XX
1644 root 20 0 1951M 37304 6552 S 0.5 1.9 4:50.28 /root/youtrack/internal/java/linux-x64/jre/bin/java -Djl.service=YouTrack Launcher -Djl.home=/root/youtrack
2274 root 20 0 3397M 1166M 6864 S 0.5 62.3 0:01.58 /root/youtrack/internal/java/linux-x64/jre/bin/java -Djl.service=YouTrack -Djl.home=/root/youtrack -ea -XX
21573 root 20 0 111M 2944 1280 R 0.0 0.2 0:00.02 htop
2120 root 20 0 3397M 1166M 6864 S 0.0 62.3 0:32.74 /root/youtrack/internal/java/linux-x64/jre/bin/java -Djl.service=YouTrack -Djl.home=/root/youtrack -ea -XX
1447 mysql 20 0 889M 40572 4400 S 0.0 2.1 1:00.63 /usr/libexec/mysqld --basedir=/usr --datadir=/var/lib/mysql --plugin-dir=/usr/lib64/mysql/plugin --user=my
1662 root 20 0 1951M 37304 6552 S 0.0 1.9 2:06.29 /root/youtrack/internal/java/linux-x64/jre/bin/java -Djl.service=YouTrack Launcher -Djl.home=/root/youtrack
1661 root 20 0 1951M 37304 6552 S 0.0 1.9 2:09.05 /root/youtrack/internal/java/linux-x64/jre/bin/java -Djl.service=YouTrack Launcher -Djl.home=/root/youtrack
2118 root 20 0 3397M 1166M 6864 S 0.0 62.3 0:14.45 /root/youtrack/internal/java/linux-x64/jre/bin/java -Djl.service=YouTrack -Djl.home=/root/youtrack -ea -XX
1 root 20 0 19356 1056 888 S 0.0 0.1 0:01.09 /sbin/init
385 root 16 -4 10852 280 276 S 0.0 0.0 0:00.08 /sbin/udevd -d
926 root 16 -4 29764 704 608 S 0.0 0.0 0:00.00 auditd
925 root 16 -4 29764 704 608 S 0.0 0.0 0:00.04 auditd
948 root 20 0 243M 1136 912 S 0.0 0.1 0:00.00 /sbin/rsyslogd -i /var/run/syslogd.pid -c 5
949 root 20 0 243M 1136 912 S 0.0 0.1 0:00.00 /sbin/rsyslogd -i /var/run/syslogd.pid -c 5
950 root 20 0 243M 1136 912 S 0.0 0.1 0:00.00 /sbin/rsyslogd -i /var/run/syslogd.pid -c 5
947 root 20 0 243M 1136 912 S 0.0 0.1 0:00.02 /sbin/rsyslogd -i /var/run/syslogd.pid -c 5
969 rpc 20 0 18980 580 520 S 0.0 0.0 0:00.08 rpcbind
991 rpcuser 20 0 23352 724 720 S 0.0 0.0 0:00.00 rpc.statd
1012 root 20 0 11304 1380 1200 S 0.0 0.1 0:00.53 /bin/bash /usr/sbin/xm-daemon -p /var/run/xm-daemon.pid
1117 dbus 20 0 21432 376 372 S 0.0 0.0 0:00.00 dbus-daemon --system
1178 root 20 0 66256 564 464 S 0.0 0.0 0:00.00 /usr/sbin/sshd
  
```

serveradmin.ru





```
jetbrains-yotrack-workTimer2136280457115256281.tmp      6708 Apr  2 2015
phpv65kNK.c                                             160  Dec  5 01:27
*phpv65kNK_2xu3yzzrlezblv6e                          3876568 Jan 27 2017
remi-release-6.rpm                                    7615  Dec  9 2015
yum.log
```

Содержание одного из файлов навело на мысль о том, что эти файлы делают:

```
threads = 1

mine =
stratum+tcp://44FpmYtxaYgKSDCt8iuYTGLKfWdPDpi64a38SnfHunFXbkNbnsX473yGcrqhCL3NhZ2MZ9YNpGwPsbxaJULJrSSAFd3Yx8o:x@xmr.crypt
o-pool.fr:3333/xmr
```

Как я понял, тут указан один из пулов, куда отправлять намайненное. Я быстро позакрывал лишние процессы и удалил файлы.

Стало очевидно, что надо искать источник заражения и перекрывать его. Сервер явно попал в оборот какой-то ботнет сети. Изначально его использовали для рассылки спама. После того, как я перекрыл эту возможность, на нем стали майнить криптовалюту. И все это происходит ночью, когда я сплю :)

## Удаление вируса майнера

У меня каждый день делается бэкап всех сайтов. Я всегда рекомендую его делать не реже, чем раз в сутки. Беглое сравнение файлов на веб сервере и в архиве показало заражение как минимум двух сайтов. Кто из них в итоге был виновником, а может и оба сразу, неизвестно.

Я прогнал сайты антивирусом для веб хостинга **ai-bolit**. Он показал множество зараженных файлов. Более детальное изучение показало, что они вообще не имеют отношение к сайтам. В определенное время они были загружены на сервер и потом использовались.



• /var/www/.../docs/assets/snippets/.mandarin/class.phpmailer.php - RCE : CVE-2016-10045, CVE-2016-10031

**Эти файлы могут быть вредоносными или хакерскими скриптами (11)**

Отображать по  записей

Поиск:

Путь	Изменение свойств	Изменение содержимого	Размер
<p>/var/www/.../docs/client_side/page_company/css/favicon_f37c65.ico</p> <p> 1 ...=isset(\$tsezmdb[\$rowxwzv[\$i]])?\$tsezmdb[\$rowxwzv[\$i]] :\$rowxwzv[\$i];\$ahwccchyg="base64_decode";return\$ahwccchyg(\$fspqmlnfyt);\$ifnngfji="rdbZinuPE62gGKL1miC</p>	04/12/2017 11:03:51	04/12/2017 11:03:51	28.43 Kb
<p>/var/www/.../docs/assets/galleries/33/thumbs/mnrerize.php</p> <p> 2 ...q#x4Qe6(jjp)&gt;h?vsUJPDg+I-L1_17&amp;-nw=`EK';0R-;&lt;5*CA/B,OcSd\$)V^am-8HrWoT9KYGF-;\$GLOBALS[\$GLOBALS['k8e447e69']][93].\$GLOBALS['k8e447e69'] [83].\$GLOBALS['k8e447e</p>	01/12/2017 13:06:22	25/10/2017 22:06:31	12.20 Kb
<p>/var/www/.../docs/assets/modules/store/installer/index.php</p> <p> 2 ...WXV\$&gt;m+ale) C-FfZq5u6&amp;'gw_#=4-DHG,7NT%L)s#vY(2drU\tMnzIRocE3KbpA-iS{.?!B`-""^";\$i72d12d7[\$i72d12d7['b481']][15].\$i72d12d7['b481'] [79].\$i72d12d7['b481'] [81].\$i</p>	01/12/2017 13:06:52	25/10/2017 22:05:55	13.48 Kb
<p>/var/www/.../docs/assets/snippets/phpthumb/fexwmbty.php</p> <p> 2 ...A`c#i7Z*=8aKM+%Ro:Brw-Db93CV-f,Qkdt-0egG/lm;5I_y)W^2hNp'4 sLH&lt;"E\uf[P&amp;vY-U{TO";\$GLOBALS[\$GLOBALS['ge3c9c022']][75].\$GLOBALS['ge3c9c022'] [12].\$GLOBALS['ge3c9c0</p>	01/12/2017 13:06:32	25/10/2017 22:06:31	11.36 Kb
<p>/var/www/.../docs/assets/snippets/FormLister/config/nstyvgal.php</p> <p> 2 ...G,Q8C=eImV&lt;_0U}o?r1gv' /J/3{S-yK+T6FR}H5A-Y#OZBb&amp;tdXE%l2hz;x^la9&gt;Wnw{)MN4"s';\$GLOBALS[\$GLOBALS['u01a0']][8].\$GLOBALS['u01a0'] [13].\$GLOBALS['u01a0'] [62].\$GLO</p>	01/12/2017 13:06:45	25/10/2017 22:06:31	9.74 Kb
<p>/var/www/.../docs/assets/snippets/.mandarin/projectBanners.php</p>			

**serveradmin.ru**

Чтобы понять, через какой сайт идет заражение и управление вирусами — смотрите логи сервера. Явным признаком заражения — POST запросы к левым файлам.

```
5.9.31.30 - - [03/Dec/2017:11:17:57 +0300] "POST /ewcvqw HTTP/1.1" 200 36
```

Можно банить ip, с которых идут запросы. Но мне кажется, это не даст большого результата. Файлы время от времени меняются, как и ip адреса.

В итоге, я просто загрузил из бэкапа зараженные сайты месячной давности, где не было замечено подозрительных файлов. Если бы у меня не было этих бэкапов, не представляю, сколько бы времени и сил я потратил на вычищение сайтов.

По итогу принял решение разнести все эти сайты по отдельным **lxc** контейнерам, чтобы обезопасить сам сервер и соседние сайты от заражения. Так я смогу более точно определять источник заражения. К сожалению, более действенного способа по защите старых сайтов от заражения различными вирусами я не знаю.

Не понравилась статья и хочешь научить меня администрировать? Пожалуйста, я люблю учиться. Комментарии в твоём распоряжении. Расскажи, как сделать правильно!

Помогла статья? Есть возможность отблагодарить автора