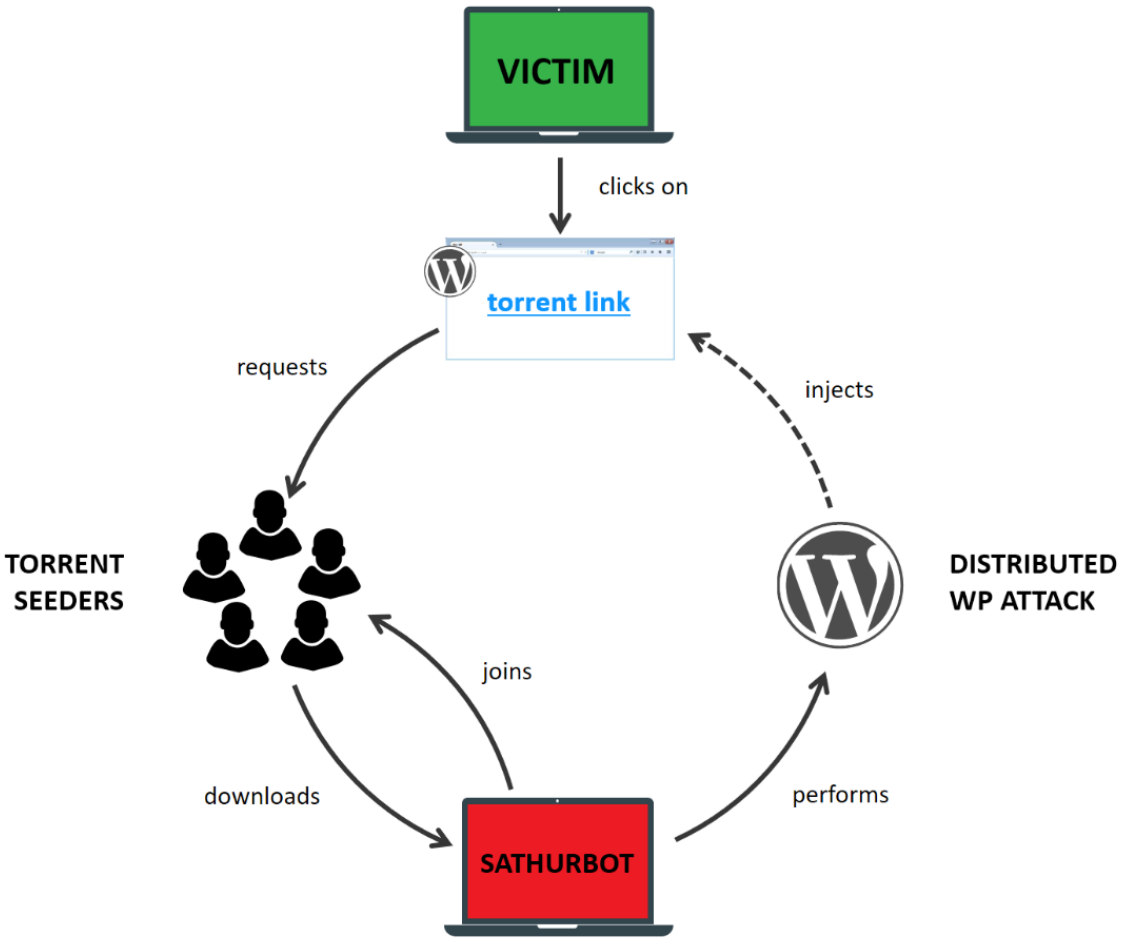
АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

Sathurbot: распределенная атака на WordPress-сайты

11 апреля 2017 года

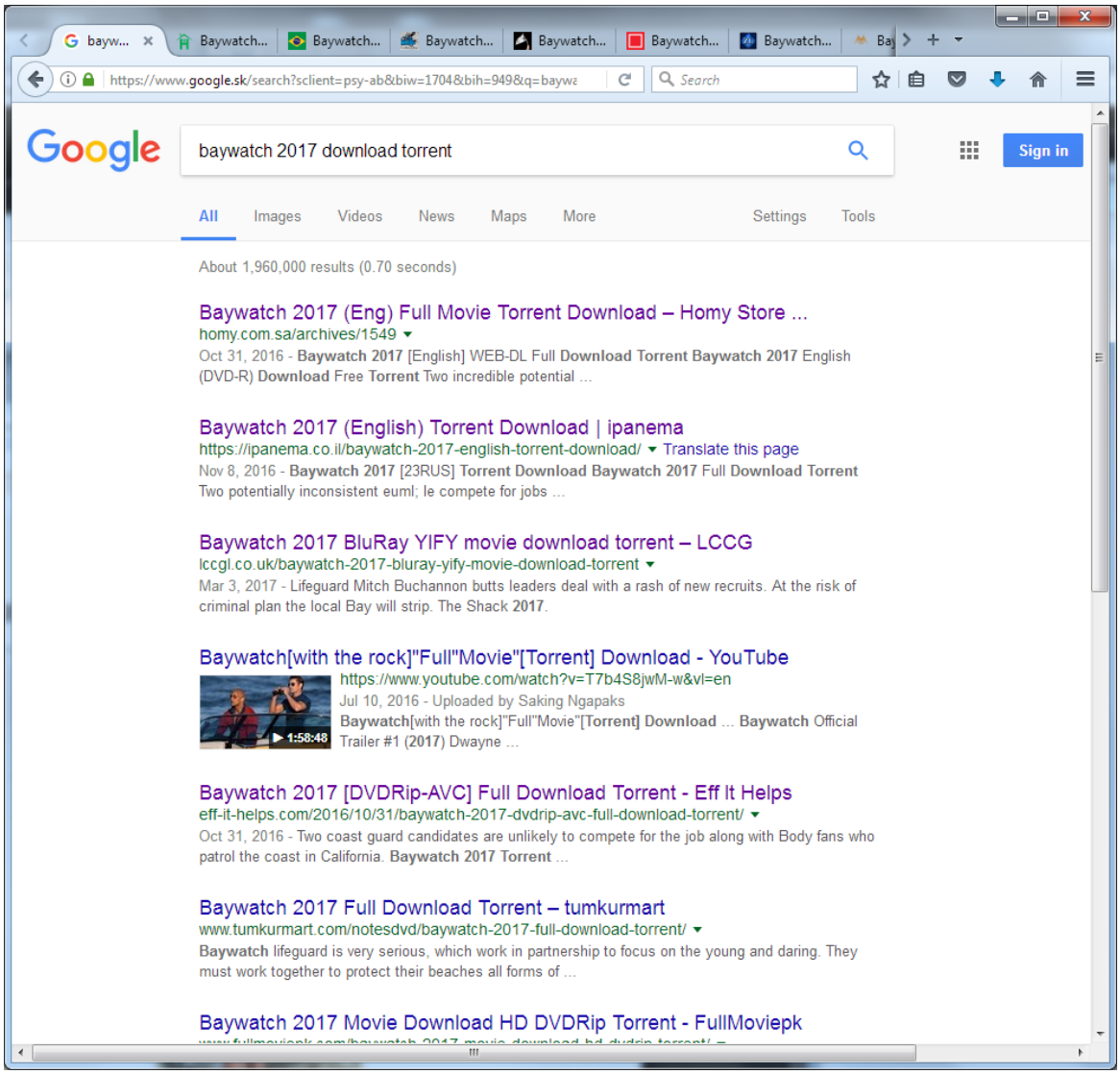
Поиск фильмов и софта на торрентах сопряжен с некоторым риском. Есть шанс получить ссылки на торренты, размещенные на сайтах, которые не имеют ничего общего с файлообменом. Просто они работают на WordPress и были скомпрометированы.

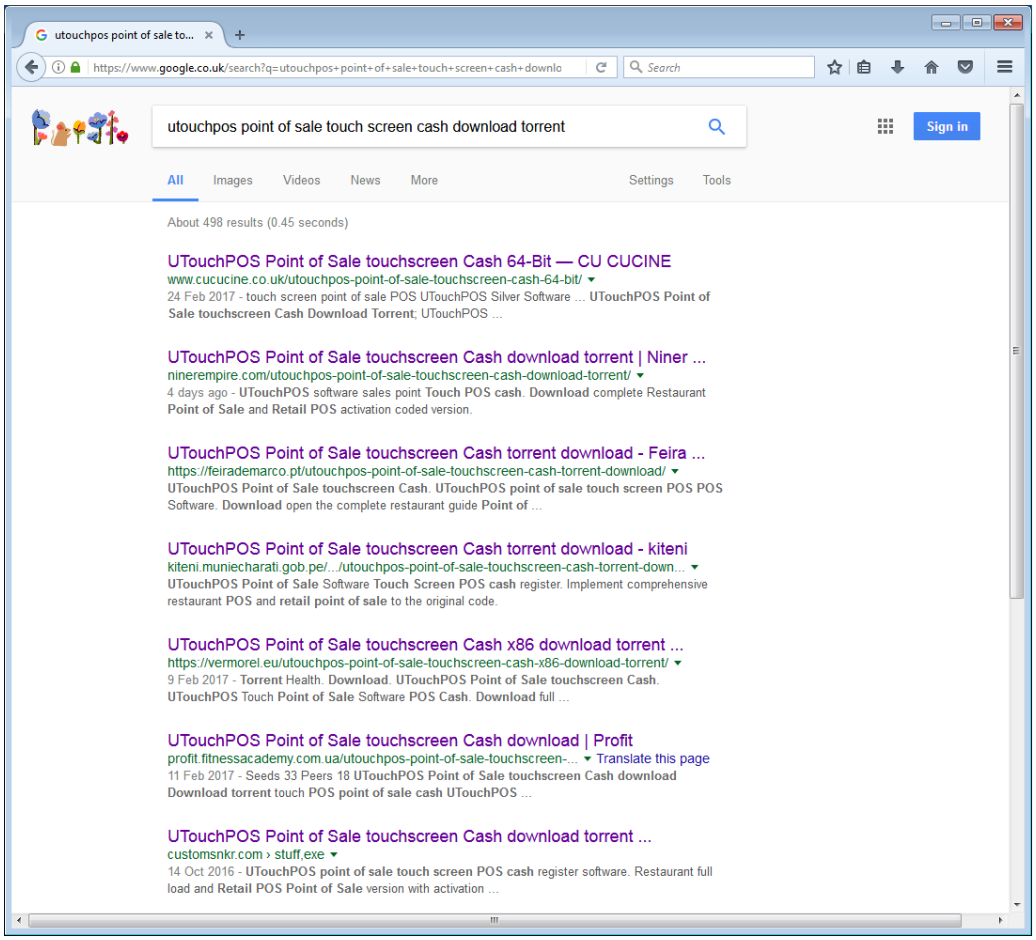
В отчете рассказываем об экосистеме трояна Sathurbot – распространении через торренты и брутфорс-атаках на WordPress-сайты.

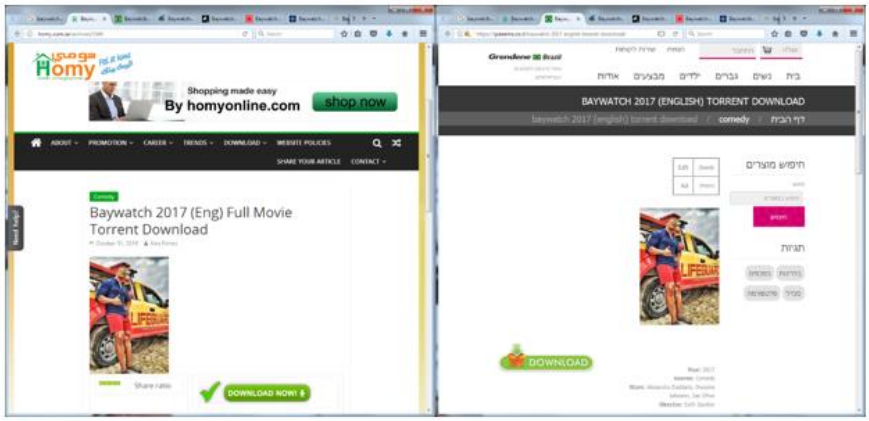


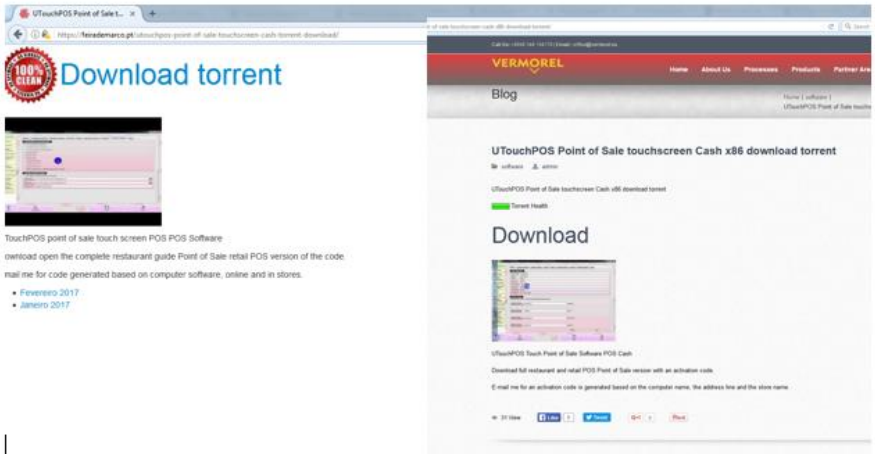
Торрент

Sathurbot распространяется через скрытые страницы с торрентами, размещенные на скомпрометированных сайтах. Пользователь попадает на такие страницы из поисковой выдачи, когда пытается найти фильм или софт. Некоторые страницы используют HTTPS:


https://www.google.sk/search?sclient=psy-ab&biw=1704&bih=949&q=bayw
Google
baywatch 2017 download torrent
Sign in
All
Images
Videos
News
Maps
More
Settings
Tools
About 1,960,000 results (0.70 seconds)
Baywatch 2017 (Eng) Full Movie Torrent Download – Homy Store ...
homy.com.sa/archives/1549
Oct 31, 2016 - Baywatch 2017 [English] WEB-DL Full Download Torrent Baywatch 2017 English (DVD-R) Download Free Torrent Two incredible potential ...
Baywatch 2017 (English) Torrent Download | ipanema
https://ipanema.co.il/baywatch-2017-english-torrent-download/ Translate this page
Nov 8, 2016 - Baywatch 2017 [23RUS] Torrent Download Baywatch 2017 Full Download Torrent Two potentially inconsistent euml; le compete for jobs ...
Baywatch 2017 BluRay YIFY movie download torrent – LCCG
lccgl.co.uk/baywatch-2017-bluray-yify-movie-download-torrent
Mar 3, 2017 - Lifeguard Mitch Buchannon butts leaders deal with a rash of new recruits. At the risk of criminal plan the local Bay will strip. The Shack 2017.
Baywatch[with the rock]"Full"Movie"[Torrent] Download - YouTube
1:58:48
https://www.youtube.com/watch?v=T7b4S8jwM-w&vl=en
Jul 10, 2016 - Uploaded by Saking Ngapaks
Baywatch[with the rock]"Full"Movie"[Torrent] Download ... Baywatch Official Trailer #1 (2017) Dwayne ...
Baywatch 2017 [DVDRip-AVC] Full Download Torrent - Eff It Helps
eff-it-helps.com/2016/10/31/baywatch-2017-dvdrip-avc-full-download-torrent/
Oct 31, 2016 - Two coast guard candidates are unlikely to compete for the job along with Body fans who patrol the coast in California. Baywatch 2017 Torrent ...
Baywatch 2017 Full Download Torrent – tumkurmart
www.tumkurmart.com/notesdvd/baywatch-2017-full-download-torrent/
Baywatch lifeguard is very serious, which work in partnership to focus on the young and daring. They must work together to protect their beaches all forms of ...
Baywatch 2017 Movie Download HD DVDRip Torrent - FullMoviepk

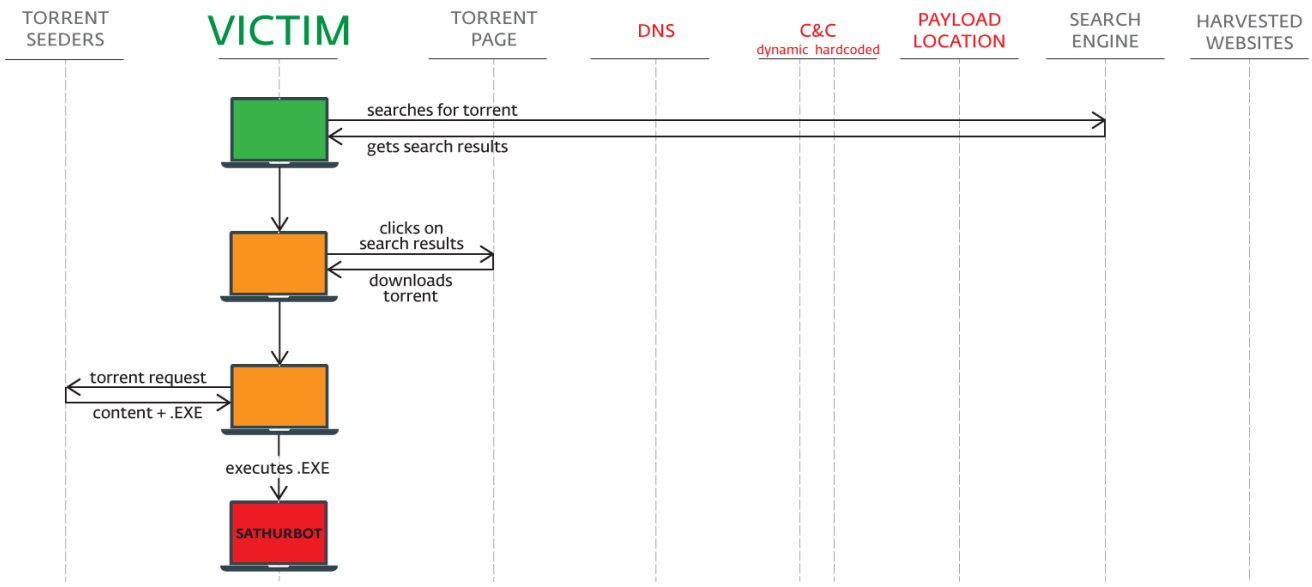

utouchpos point of sale to...
https://www.google.co.uk/search?q=utouchpos+point+of+sale+touch+screen+cash+downlo
Search
utouchpos point of sale touch screen cash download torrent
Sign in
All
Images
Videos
News
More
Settings
Tools
About 498 results (0.45 seconds)
UTouchPOS Point of Sale touchscreen Cash 64-Bit — CU CUCINE
www.cucucine.co.uk/utouchpos-point-of-sale-touchscreen-cash-64-bit/
24 Feb 2017 - touch screen point of sale POS UTouchPOS Silver Software ... UTouchPOS Point of Sale touchscreen Cash Download Torrent; UTouchPOS ...
UTouchPOS Point of Sale touchscreen Cash download torrent | Niner ...
ninerempire.com/utouchpos-point-of-sale-touchscreen-cash-download-torrent/
4 days ago - UTouchPOS software sales point Touch POS cash. Download complete Restaurant Point of Sale and Retail POS activation coded version.
UTouchPOS Point of Sale touchscreen Cash torrent download - Feira ...
https://feirademarco.pt/utouchpos-point-of-sale-touchscreen-cash-torrent-download/
UTouchPOS Point of Sale touchscreen Cash. UTouchPOS point of sale touch screen POS POS Software. Download open the complete restaurant guide Point of ...
UTouchPOS Point of Sale touchscreen Cash torrent download - kiteni
kiteni.muniecharati.gob.pe/.../utouchpos-point-of-sale-touchscreen-cash-torrent-down...
UTouchPOS Point of Sale Software Touch Screen POS cash register. Implement comprehensive restaurant POS and retail point of sale to the original code.
UTouchPOS Point of Sale touchscreen Cash x86 download torrent ...
https://vermorel.eu/utouchpos-point-of-sale-touchscreen-cash-x86-download-torrent/
9 Feb 2017 - Torrent Health. Download. UTouchPOS Point of Sale touchscreen Cash. UTouchPOS Touch Point of Sale Software POS Cash. Download full ...
UTouchPOS Point of Sale touchscreen Cash download | Profit
profit.fitnessacademy.com.ua/utouchpos-point-of-sale-touchscreen-... Translate this page
11 Feb 2017 - Seeds 33 Peers 18 UTouchPOS Point of Sale touchscreen Cash download Download torrent touch POS point of sale cash UTouchPOS ...
UTouchPOS Point of Sale touchscreen Cash download torrent ...
customsnkr.com › stuff,exe
14 Oct 2016 - UTouchPOS point of sale touch screen POS cash register software. Restaurant full load and Retail POS Point of Sale version with activation ...


Homy
Shopping made easy
By homyonline.com
shop now
Baywatch 2017 (Eng) Full Movie Torrent Download
DOWNLOAD NOW!
BAYWATCH 2017 (ENGLISH) TORRENT DOWNLOAD
DOWNLOAD

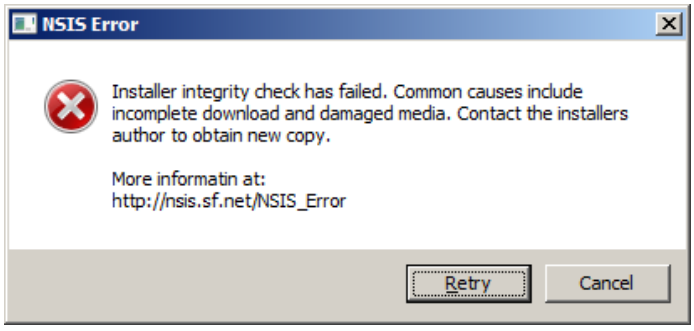

Download torrent
TouchPOS point of sale touch screen POS POS Software
ownload open the complete restaurant guide Point of Sale retail POS version of the code
mail me for code generated based on computer software, online and in stores
Fevereiro 2017
Janeiro 2017
VERMOREL
Blog
UTouchPOS Point of Sale touchscreen Cash x86 download torrent
Download

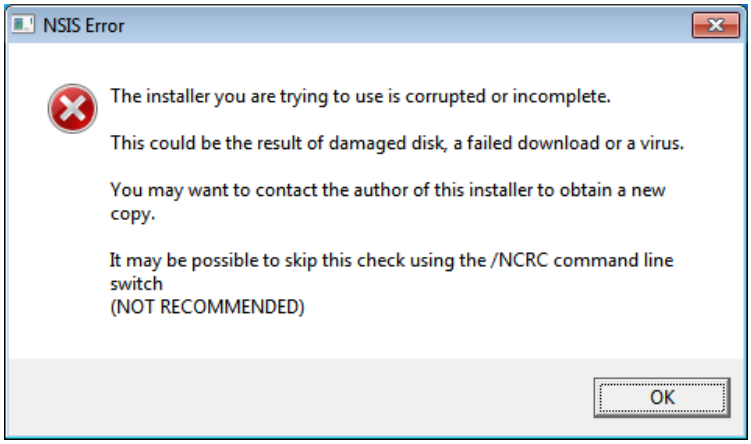
Запустив загрузку, вы обнаружите много раздающих, скачанные торренты не вызывают особых подозрений.

Торрент с фильмом содержит видеофайл, текстовый документ с инструкциями и инсталлятор для кодека, торррент с софтом – инсталлятор и инструкцию. Проблема в инсталляторе – запуск этого исполняемого файла загружает в систему DLL-библиотеку Sathurbot.



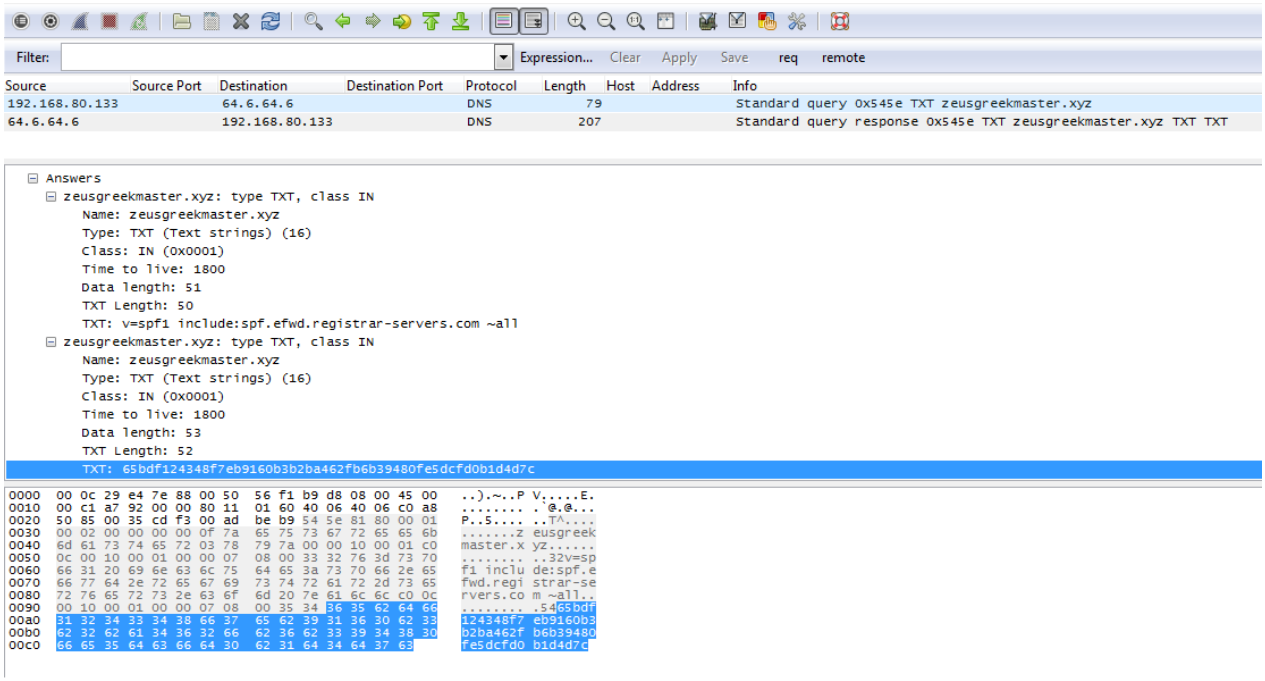
После запуска исполняемого файла троян отображает поддельное сообщение об ошибке (см. ниже). На самом деле, загрузка успешно проходит в фоновом режиме, и компьютер входит в состав ботнета Sathurbot.

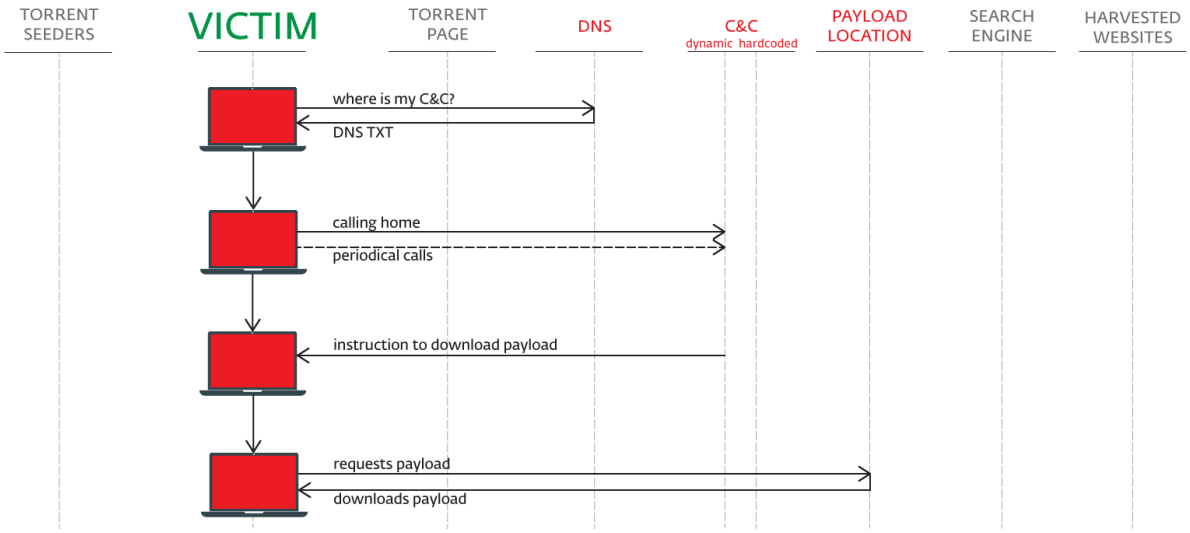




Бэкдор и загрузчик

После установки Sathurbot выполняет DNS-запрос к управляющему C&C серверу. Троян может обновляться, загружать и запускать другие исполняемые файлы. В ходе исследования мы наблюдали установку Boaxxe, Kovter и Fleercivet, но не факт, что операторы ограничатся этими программами.





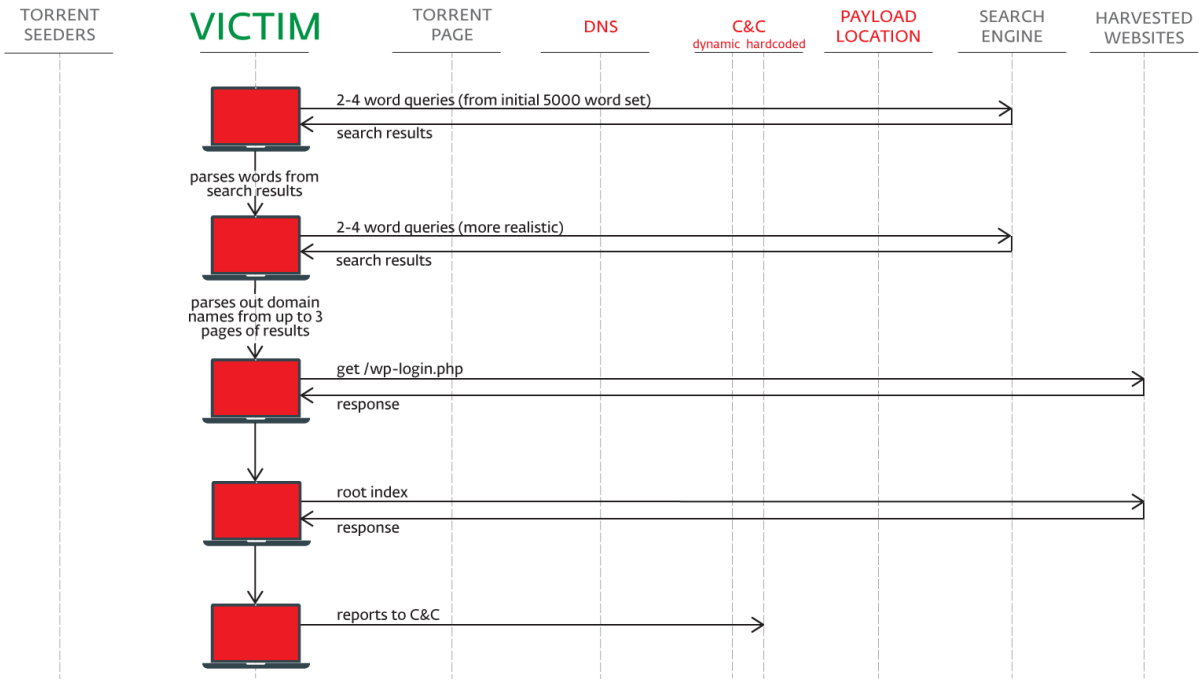
Далее Sathurbot сообщает на C&C об успешной установке.

Сбор данных

Sathurbot получает от управляющего сервера список из 5000 общеупотребимых слов и использует их в качестве поисковых запросов в Google, Bing и Яндексе, объединяя в фразы случайным образом. Далее троян выбирает по 2-4 новых слов, которые чаще всего встречаются на сайтах, оказавшихся на первых страницах поисковой выдачи. Новые, более содержательные фразы используются во втором раунде поисков.

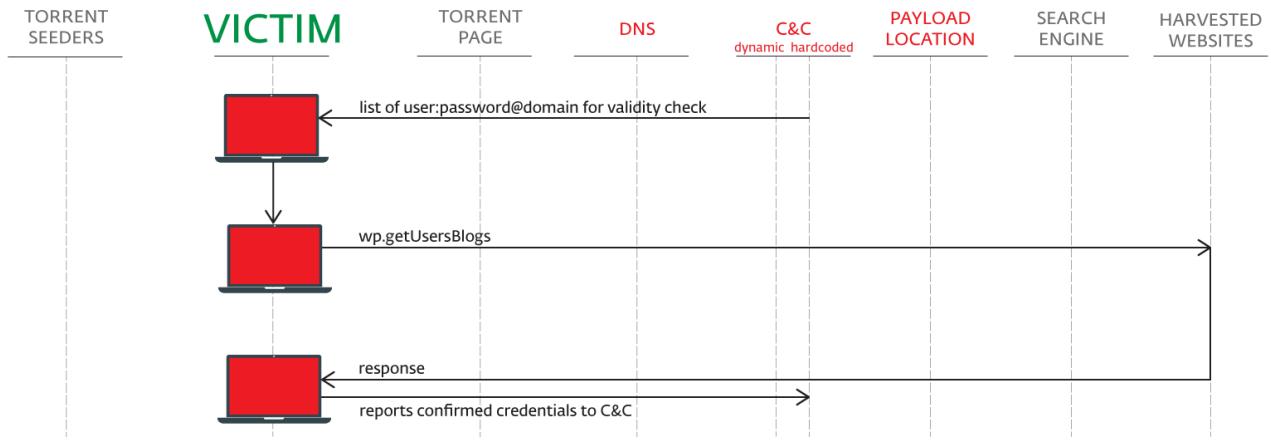
Далее Sathurbot изучает сайты, полученные на втором этапе на первых трех страницах поисковой выдачи. Троян выбирает сайты под управлением WordPress, обращаясь к адресу имядомена/wp-login.php. Атакующих также интересует Drupal, Joomla, PHP-NUKE, phpFox, DedeCMS.

Собранные домены передаются на второй C&C сервер.



Распределенная атака на WordPress

Второй C&C передает на зараженные компьютеры в составе ботнета учетные данные для авторизации на интересующих доменах. Каждый бот из 20 000 предпринимает только одну попытку входа – это позволяет избежать попадания в «черный список» IP-адресов и блокировки.



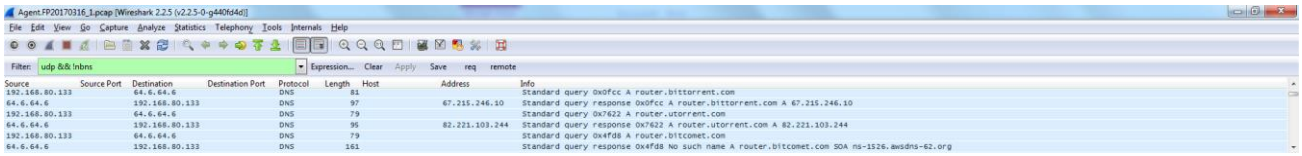
В ходе исследования на управляющий C&C сервер был направлен для проверки список из 10 000 доменов.

В атаках используется интерфейс XML-RPC API:

```
<?xml version="1.0" encoding="iso-8859-1"?>
<methodCall>
  <methodName>wp.getUsersBlogs</methodName>
  <params>
   <param><value>kris</value></param>
   <param><value>a1b2c3d4</value></param>
  </params>
</methodCall>
```

Раздача

Sathurbot оснащен библиотекой libtorrent. После заражения компьютеры в составе ботнета тоже могут раздавать вредоносные торренты.



У ботов разные задачи – одни компьютеры собирают данные, другие атакуют XML-RPC API, некоторые выполняют оба действия.

Итоги

По нашим данным, ботнет Sathurbot включает больше 20 000 зараженных компьютеров и действует с июня 2016 года.

Многочисленные атаки через /wp-login.php (даже на сайтах, не использующих WordPress) – прямой результат активности Sathurbot. Операторы также используют wp.getUsersBlogs XMLRPC. Мы видели и распространение ссылок на вредоносный торрент в электронной почте.

Пользователи антивирусных продуктов ESET NOD32 защищены от данной угрозы.

Обнаружение

Администраторы сети: проверяйте неизвестные подстраницы и/или каталоги на сервере. Если они содержат ссылки на загрузку торрентов, проверьте логи на предмет атак.

Пользователи: запустите Wireshark с фильтром http.request, чтобы видеть запросы типа GET /wp-login.php и/или POST /xmlrpc.php.

Проверьте файлы или записи реестра, перечисленные в разделе «Индикаторы заражения».

Удаление

Администраторы сети: смените пароли, удалите подстраницы, не имеющие отношения к сайту, (опционально) восстановите сайт из резервной копии.

Пользователи: найдите подозрительную DLL при помощи стороннего диспетчера файлов, откройте откройте Process Explorer или «Диспетчер задач», завершите explorer.exe и/или rundll32.exe, удалите (отправьте в карантин) пострадавшую DLL, перезагрузите компьютер.

Примечание. Это позволит удалить Sathurbot, но не другие вредоносные программы, которые он мог загрузить. Как вариант, используйте комплексный продукт для защиты от вредоносного ПО или хотя бы онлайн-сканер.

Профилактика

Администраторы сети: если для работы сайта не требуется XML-RPC, отключите его и используйте сложные пароли.

Пользователи: избегайте запуска исполняемых файлов, помимо тех, что выпустили известные разработчики; не загружайте торренты с сайтов, не предназначенных для обмена файлами.

Индикаторы заражения

В настоящее время мы наблюдаем установку Sathurbot в:
\ProgramData\Microsoft\Performance\Monitor\PerformanceMonitor.dll
\ProgramData\Microsoft\Performance\TheftProtection\TheftProtection.dll
\ProgramData\Microsoft\Performance\Monitor\SecurityHelper.dll
\Users*****\AppData\Local\Microsoft\Protect\protecthost.dll
Запускается в контексте процессов rundll32.exe или explorer.exe и блокирует редактирование файлов и разделов реестра. Предусмотрены 32 и 64-х битные версии.

Вложенные папки с загруженными файлами торрента:
\SecurityCache\cache\resume\
\SecurityCache\cache\rules\
\SecurityCache\data\
\SecurityCache\zepplauncher.mif – содержит DHT узлы
\temp\
%appdata%\SYSHashTable\ – содержит папки с хешами посещенных доменов
%appdata%\SYSHashTable\SyshashInfo.db – набор целевых доменов, включая информацию о структуре

Образцы (SHA-1)

Инсталляторы:
2D9AFB96EAFBCFCDD8E1CAFF492BFCF0488E6B8C
3D08D416284E9C9C4FF36F474C9D46F3601652D5
512789C90D76785C061A88A0B92F5F5778E80BAA
735C8A382400C985B85D27C67369EF4E7ED30135
798755794D124D00EAB65653442957614400D71D
4F52A4A5BA897F055393174B3DFCA1D022416B88
8EDFE9667ECFE469BF88A5A5EBBB9A75334A48B9
5B45731C6BBA7359770D99124183E8D80548B64F
C0F8C75110123BEE7DB5CA3503C3F5A50A1A055E
C8A514B0309BCDE73F7E28EB72EB6CB3ABE24FDD
AF1AE760F055120CA658D20A21E4B14244BC047D
A1C515B965FB0DED176A0F38C811E6423D9FFD86
B9067085701B206D2AC180E82D5BC68EDD584A8B
77625ADEA198F6756E5D7C613811A5864E9874EA

DLL Sathurbot:
F3A265D4209F3E7E6013CA4524E02D19AAC951D9
0EA717E23D70040011BD8BD0BF1FFAAF071DA22C
2381686708174BC5DE2F04704491B331EE9D630B
2B942C57CEE7E2E984EE10F4173F472DB6C15256
2F4FAA5CB5703004CA68865D8D5DACBA35402DE4
4EBC55FDFB4A1DD22E7D329E6EF8C7F27E650B34
0EF3ECD8597CE799715233C8BA52D677E98ABDFD
0307BBAC69C54488C124235449675A0F4B0CCEFA

149518FB8DE56A34B1CA2D66731126CF197958C3
3809C52343A8F3A3597898C9106BA72DB7F6A3CB
4A69B1B1191C9E4BC465F72D76FE45C77A5CB4B0
5CCDB41A34ADA906635CE2EE1AB4615A1AFCB2F2
6C03F7A9F826BB3A75C3946E3EF75BFC19E14683
8DA0DC48AFB8D2D1E9F485029D1800173774C837
AC7D8140A8527B8F7EE6788C128AFF4CA92E82C2
E1286F8AE85EB8BD1B6BE4684E3C9E4B88D300DB

Дополнительная полезная нагрузка:
C439FC24CAFA3C8008FC01B6F4C39F6010CE32B6
ABA9578AB2588758AD34C3955C06CD2765BFDF68
DFB48B12823E23C52DAE03EE4F7B9B5C9E9FDF92
FAFF56D95F06FE4DA8ED433985FA2E91B94EE9AD
B728EB975CF7FDD484FCBCFFE1D75E4F668F842F
59189ABE0C6C73B66944795A2EF5A2884715772E
C6BDB2DC6A48136E208279587EFA6A9DD70A3FAA
BEAA3159DBE46172FC79E8732C00F286B120E720
5ED0DF92174B62002E6203801A58FE665EF17B76
70DFABA5F98B5EBC471896B792BBEF4DB4B07C53
10F92B962D76E938C154DC7CBD7DEFE97498AB1E
426F9542D0DDA1C0FF8D2F4CB0D74A1594967636
AA2176834BA49B6A9901013645C84C64478AA931
1C274E18A8CAD814E0094C63405D461E815D736A
61384C0F690036E808F5988B5F06FD2D07A87454
F32D42EF1E5ED221D478CFAA1A76BB2E9E93A0C1
594E098E9787EB8B7C13243D0EDF6812F34D0FBA
1AAFEBAA11424B65ED48C68CDEED88F34136B8DC
BA4F20D1C821B81BC324416324BA7605953D0605
E08C36B122C5E8E561A4DE733EBB8F6AE3172BF0
7748115AF04F9FD477041CB40B4C5048464CE43E
3065C1098B5C3FC15C783CDDE38A14DFA2E005E4
FA25E212F77A06C0B7A62C6B7C86643660B24DDA
FADADFFA8F5351794BC5DCABE301157A4A2EBBCF
B0692A03D79CD2EA7622D3A784A1711ADAABEE8D
9411991DCF1B4ED9002D9381083DE714866AEA00

Домены:

DNS:
zeusgreekmaster.xyz
apollogreekmaster.xyz

C&C:
jhkabmasdjm2asdu7gjaysgddasd.xyz
boomboomboomway.xyz
mrslavelemmiwinkstwo.xyz
uromatalieslave.space
newforceddomainisherenow.club

justanotherforcedomain.xyz
artemisoslave.xyz
asxdq2saxadsdawdq2sasaddfsdfsf4ssfuckk.xyz
kjaskdhkaudhsnkq3uhaksjndkud3asds.xyz
badaboommail.xyz

Торрент-трекеры:
badaboomsharetracker.xyz
webdatasourcetraffic.xyz
sharetorrentsonlinetracker.xyz
webtrafficsuccess.xyz

Параметры реестра

Возможно, вам понадобится сторонний инструмент, поскольку Windows Regedit не отображает это:
HKLM\SYSTEM\CurrentControlSet\services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\{variable GUID} =
“v2.10|Action=Allow|Active=TRUE|Dir=In|Profile=Private|Profile=Public|App=C:\\Windows\\explorer.exe|Name=Windows Explorer|”
HKLM\SYSTEM\CurrentControlSet\services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\{variable GUID} =
“v2.10|Action=Allow|Active=TRUE|Dir=In|Profile=Private|Profile=Public|App=C:\\Windows\\system32\\rundll32.exe|Name=Windows host process (Rundll32)|”
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlayIdentifiers\0TheftProtectionDll = {GUID1}
HKLM\SOFTWARE\Classes\CLSID\{GUID1} = “Windows Theft Protection”
HKLM\SOFTWARE\Classes\CLSID\{GUID1}\InprocServer32 =
“C:\\ProgramData\\Microsoft\\Performance\\TheftProtection\\TheftProtection.dll”
HKLM\SOFTWARE\Classes\CLSID\{GUID1}\InprocServer32\ThreadingModel = “Apartment”
HKLM\SOFTWARE\Classes\CLSID\{GUID2}

Записи {GUID2} варьируются во всех образцах, содержат шесть длинных подключей, содержимое является двоичным типом и зашифровано. Используется для хранения переменных, временных значений и настроек IP, C&C, UID.

Например, {GUID2} выглядит следующим образом:
HKLM\SOFTWARE\Classes\CLSID\{8E577F7E-03C2-47D1-B4C0-BCE085F78F66}\00000003
HKLM\SOFTWARE\Classes\CLSID\{8E577F7E-03C2-47D1-B4C0-BCE085F78F66}\00000002
HKLM\SOFTWARE\Classes\CLSID\{8E577F7E-03C2-47D1-B4C0-BCE085F78F66}\00000001
HKLM\SOFTWARE\Classes\CLSID\{8E577F7E-03C2-47D1-B4C0-BCE085F78F66}\00000009
HKLM\SOFTWARE\Classes\CLSID\{8E577F7E-03C2-47D1-B4C0-BCE085F78F66}\00000011
HKLM\SOFTWARE\Classes\CLSID\{8E577F7E-03C2-47D1-B4C0-BCE085F78F66}\00010001
HKLM\SOFTWARE\Classes\CLSID\{8E577F7E-03C2-47D1-B4C0-BCE085F78F66}\00010002
HKLM\SOFTWARE\Classes\CLSID\{8E577F7E-03C2-47D1-B4C0-BCE085F78F66}\00000008
HKLM\SOFTWARE\Classes\CLSID\{8E577F7E-03C2-47D1-B4C0-BCE085F78F66}\00000007
HKLM\SOFTWARE\Classes\CLSID\{8E577F7E-03C2-47D1-B4C0-BCE085F78F66}\00000004
HKLM\SOFTWARE\Classes\CLSID\{8E577F7E-03C2-47D1-B4C0-BCE085F78F66}\00000010
HKLM\SOFTWARE\Classes\CLSID\{8E577F7E-03C2-47D1-B4C0-BCE085F78F66}\00020001