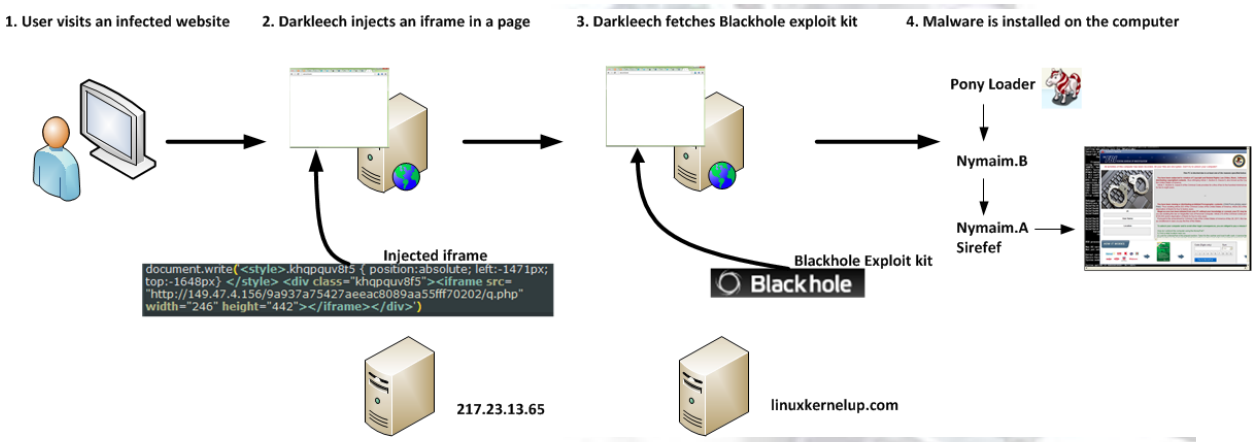
Вымогатель Win32/Nymaim – хроники обфускации кода

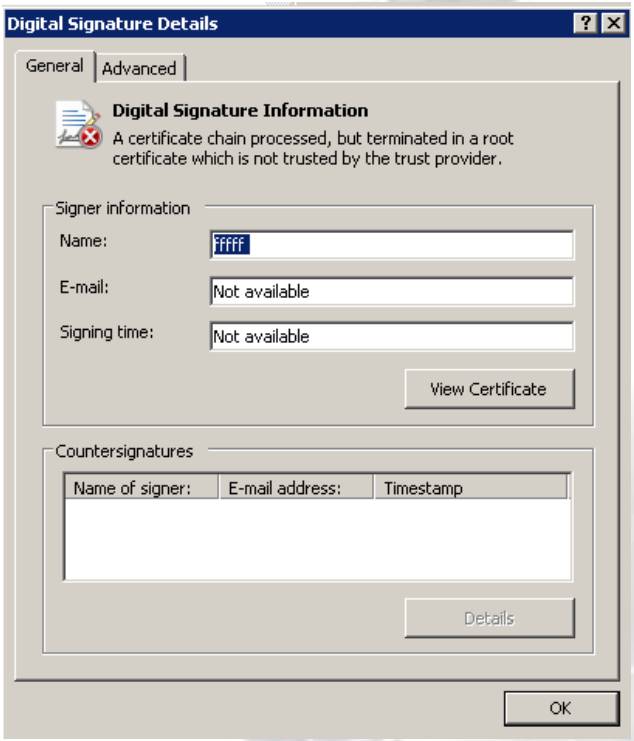
В прошлом месяце мы писали о кампании по распространению вредоносного ПО «Home Campaign». Злоумышленники на протяжении длительного времени компрометировали веб-серверы, работающие под управлением Apache Linux, используя при этом вредоносный модуль Apache известный как Darkeech (обнаруживается ESET как Linux/Chapro). Этот код использовался для перенаправления пользователей веб-сайтов на набор эксплойтов Blackhole Exploit Kit. В процессе анализа атаки выяснилось, что ее полезной нагрузкой было семейство вымогателей (ransomware) Win32/Nymaim. Данный анализ посвящен техническим особенностям этой вредоносной программы и способам ее установки на компьютеры пользователей.

Заражение

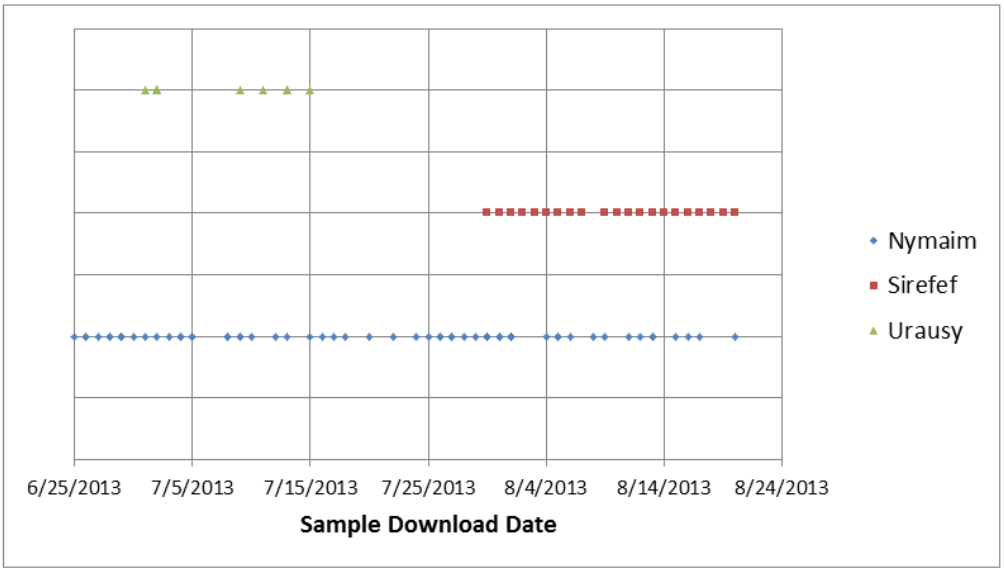
Метод, через который пользователи заражаются Nymaim, приведен ниже на рисунке. Как мы уже рассказывали ранее, он заключается в посещении пользователем скомпрометированного веб-сервера, через который доставляется веб-страница с вредоносным кодом. В случае с Nymaim результатом посещения такого ресурса становится заблокированный компьютер пользователя. Для загрузки основного кода Nymaim используется широко известный даунлоадер «Pony Loader» (обнаруживается ESET как Win32/Fareit).



Для поддержания видимой легитимности своего исполняемого файла, Fareit снабжен информацией о цифровой подписи.



Такой атрибут семплов Fareit дал нам возможность сгруппировать необходимые семплы для анализа. Анализируя их, мы выяснили, что домен catch-cdn.com был использован этим вредоносным кодом для извлечения дропперов Nymaim, который устанавливался затем на скомпрометированные компьютеры. Мы наблюдали загрузку файла с одним и тем же именем 6.exe, который в разные промежутки времени представлял из себя дроппер Win32/Sirefef (aka ZeroAccess), Win32/Urausy (Win32/LockScreen) и Win32/Nymaim. На следующем рисунке представлена временная шкала распределения вредоносных программ, которые загружались по этому статическому URL-адресу.



Алгоритм, по которому производилась смена этих семейств вредоносных программ на сервере, нам не совсем ясен. Мы отмечали, что семплы Urausy были доступны для загрузки первую половину июля. Sirefef появился в начале августа, а Nymaim появлялся регулярно на всем промежутке фиксируемого времени.

Технические характеристики

Процесс заражения Win32/Nymaim можно разбить на два этапа. На первом этапе даунлоадер пытается скачать основное тело Nymaim обращаясь к списку жестко зашитых IP-адресов. После того как закачка окончена, этот код переименовывает свой файл в произвольное имя. На каждом из этих этапов вымогатель использует несколько общих методов, чтобы помешать его анализу.

Один из таких методов – обфускация потока исполнения кода (control flow obfuscation). Вредоносный код вручную модифицирует стек вызовов для передачи управления на нужную функцию, скрывая таким образом истинные переходы между функциями при статическом анализе.

```
mov     [ebp+var_18], ecx
add     [ebp+var_34], ecx
xor     eax, eax
add     [ebp+var_24], 533D00h
sub     [ebp+var_34], ecx
mov     [ebp+var_14], eax
mov     [ebp+var_10], eax
mov     [ebp+var_C], eax
mov     [ebp+var_8], eax
mov     [ebp+var_4], eax
sub     [ebp+var_3C], edi
mov     [ebp+var_20], 0
lea     eax, [ebp+var_10]
push    33h
call    sub_4017A4
push    8
push    edi
push    341A7BFBh
push    341A5A68h
call    sub_4018C1
cmp     [ebp+var_3C], 0D7D500h
sub     [ebp+var_24], 0
push    eax
call    sub_40A99A
cmp     eax, 0
jz      loc_40A9D7
```

```
sub     [ebp+var_18], 0
```

На скриншоте выше выделены два метода обфускации. Первый заключается в вызове функции, которая модифицирует значение на стеке материнской функции в зависимости от передаваемого параметра. Более подробно такой способ представлен ниже.

```
mov     [esp+arg_0], eax
retn
sub_4017A4 endp
```

```
; START OF FUNCTION CHUNK FOR sub_4017A4

loc_406CFB:
cmp     [esp+arg_0], 34h
jnz     loc_4087A7
```

```
mov     [esp+arg_0], ecx
retn
; END OF FUNCTION CHUNK FOR sub_4017A4
```

```
; START OF FUNCTION CHUNK FOR sub_4017A4

loc_4087A7:
cmp     [esp+arg_0], 35h
jnz     loc_406363
```

```
; START OF FUNCTION CHUNK FOR sub_4017A4

loc_406363:
cmp     [esp+arg_0], 36h
jnz     loc_4046B1
```

```
mov     [esp+arg_0], edx
retn
; END OF FUNCTION CHUNK FOR sub_4017A4
```

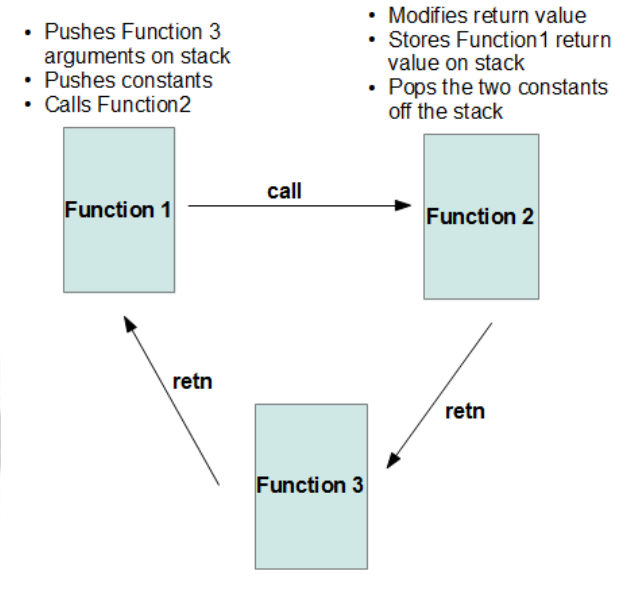
В зависимости от переданного в функцию аргумента (0x34, 0x35, 0x36), производится модификация содержимого на стеке одним из регистров, что равносильно простой команде push reg. Например в случае аргумента 0x34, получим push ecx.

Второй метод обфускации используется в функции ниже и предназначен для скрытия истинных адресов вызываемых функций. Ниже видно, что передаваемый в функцию аргумент будет использован как смещение при вызове другой функции, т. е. используется как константа для расчета требуемого адреса.

```
; Attributes: bp-based frame

sub_4018C1 proc near

arg_0= dword ptr  8
arg_4= dword ptr  0Ch
arg_8= dword ptr  10h

; FUNCTION CHUNK AT 00401A7A SIZE 00000008 BYTES

push    ebp
mov     ebp, esp
push    eax
mov     eax, [ebp+4]
mov     [ebp+arg_8], eax
mov     eax, [ebp+arg_4]
xor     eax, [ebp+arg_0]
jmp     loc_401A7A
sub_4018C1 endp
```

```
; START OF FUNCTION CHUNK FOR sub_4018C1

loc_401A7A:
add     [ebp+4], eax
pop     eax
leave
retn    8
; END OF FUNCTION CHUNK FOR sub_4018C1
```

Как видно по этому коду, функция использует две константы, передаваемые ей в качестве аргументов, для расчета необходимого смещения с применением операций XOR и ADD. Далее выполняется сохранение результата этой операции на стеке, причем модифицируется значение адреса, используемого функцией retn для передачи управления в вызывающую функцию. Таким образом будет вызвана новая функция.

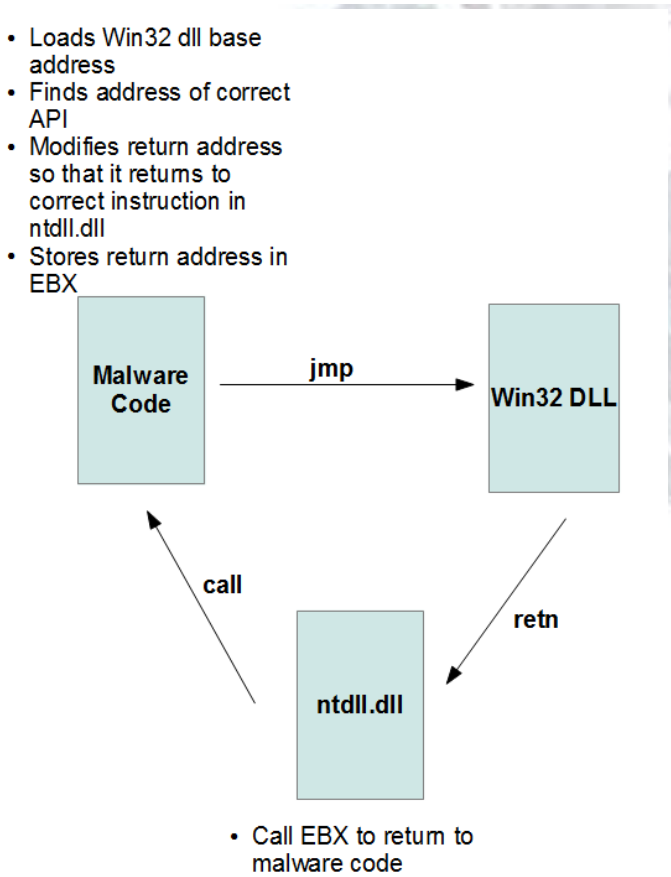


Еще один тип обфускации, используемый в Nymaim, относится к вызову Win32 API функций. Когда вредоносному коду необходимо вызвать нужную функцию из DLL, то он считывает

базовый адрес этой DLL из зашифрованной секции данных. Адрес функций вычисляется по заранее подготовленным хэшам имен этих функций. Ниже показан код функции, которая вычисляет хэш имени функции. Затем он используется для сравнения.

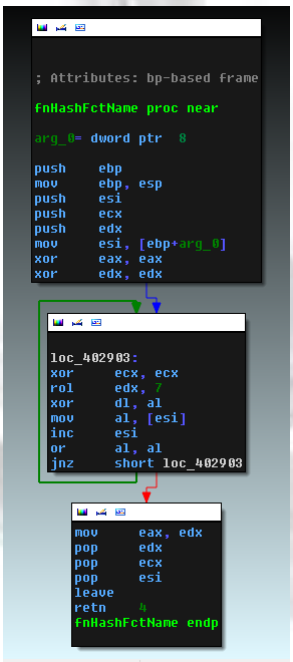
```
; Attributes: bp-based frame

fnHashFctName proc near

arg_0= dword ptr  8

push    ebp
mov     ebp, esp
push    esi
push    ecx
push    edx
mov     esi, [ebp+arg_0]
xor     eax, eax
xor     edx, edx

loc_402903:
xor     ecx, ecx
rol     edx, 7
xor     dl, al
mov     al, [esi]
inc     esi
or      al, al
jnz     short loc_402903

mov     eax, edx
pop     edx
pop     ecx
pop     esi
leave
retn    4
fnHashFctName endp
```

Когда адрес функции найден, он сохраняется в памяти и далее используется в различных местах кода с использованием инструкции перехода. Еще одной особенностью является тот факт, что при возврате из API, поток исполнения переходит не к вредоносному коду, а к инструкции в ntdll.dll call EBX. Непосредственно перед вызовом API, Nymaim выполняет модификацию стека таким образом, чтобы после выхода из API поток исполнения переключился бы на ntdll.dll, а EBX, в свою очередь, будет содержать настоящий адрес возврата. Более понятно этот процесс показан ниже на рисунке.



Подобные манипуляции позволяют Nymaim затруднить отладку, особенно, при пошаговом исполнении (трассировке). Корректируемый на стеке адрес возврата препятствует исполнить функцию в отладчике «до возвращения».

Nymaim использует шифрование строк. Функция расшифровки выглядит как показано ниже.



На втором этапе своего исполнения Win32/Nymaim использует схожие методы обфускации, но функциональность кода расширена для обеспечения выживаемости после перезагрузки и блокирования экрана. Вредоносный код использует обычную практику автозапуска прописывая себя в Software\Microsoft\Windows NT\CurrentVersion\Winlogon\shell.

Наш анализ показал, что в некоторых ситуациях Win32/Nymaim на второй стадии своего исполнения осуществляет установку на скомпрометированный компьютер другой угрозы, а именно Win32/Sirefef. Кроме этого, в дальнейшем, Nymaim может загрузить на компьютер и другие троянские программы.

Основной задачей Nymaim является блокирование компьютера. Для этого осуществляется загрузка HTML-страницы с информацией о блокировке. Такая гибкость позволяет злоумышленникам отображать различные запугивающие пользователя страницы, например, в зависимости от его расположения или установленного у него ПО (например, каких-либо медиа-файлов или торрент-клиента). В результате информация экрана блокировки становится очень правдоподобной для пользователя. Для этого в системе пользователя выполняется поиск следующих запущенных процессов.

- Azureus
- Utorrent
- Mediaget
- Bittorrent
- Bitcomet

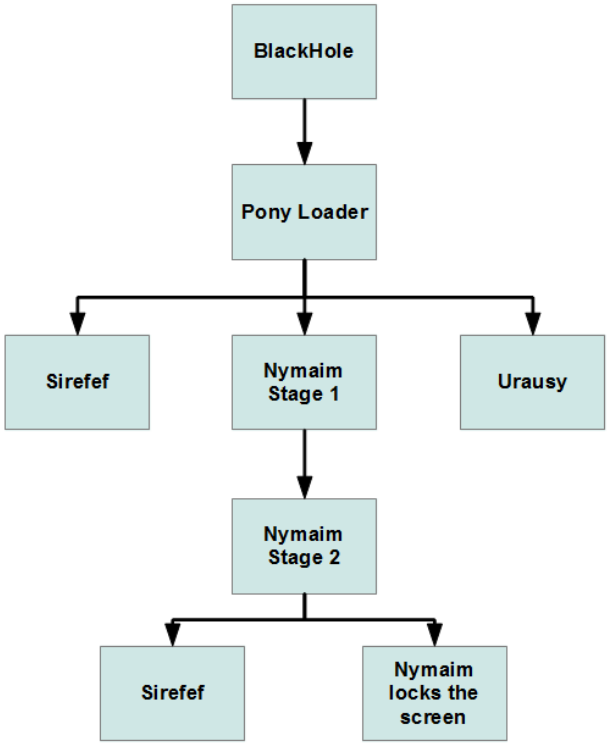
Кроме этого, Nymaim осуществляет поиск файлов со следующими расширениями: .doc, .xls, .psd, .bmp, .jpg, .mpg, .mov, .rtf, .fla и .mp3. Собранная информация будет храниться в файле compdata.js, который позднее будет включен в HTML-код блокировки. Пример такого файла приведен ниже.

```
compname="[redacted]";
var docfilesinfo = ["Blue hills.jpg","Sunset.jpg","Water lilies.
jpg","Winter.jpg","this_it_not_music.mp3","this_is_not_a_movie.m
pg","this_is_not_a_picture.jpg","upx.doc"]
docfiles=1;
var torclientinfo = ["Azureus.exe"];
torclient=1;
torfiles=0;
```

Вспомогательные файлы, которые используются для блокировки, а именно, HTML-код, скрипты и файлы изображений экрана хранятся в директории «Documents and Settings\[user_name]\Local Settings\Temp» (Windows XP). Для блокировки системы, вымогатель создает окно размером на весь экран и порождает два специальных потока. Один из которых будет отслеживать запущенные процессы и завершать стандартный диспетчер процессов taskmgr.exe в случае его запуска. Второй поток отслеживает появление новых рабочих столов, которые могли бы перекрыть активный «вредоносный» и выполняет переключение обратно в случае их появления. Подобное поведение похоже на поведение вымогателя Urausy, который был описан аналитиками AVAST. Ниже показан внешний вид обложки для пользователей, расположенных в США.

Вымогатель взаимодействует с удаленным сервером направляя ему bot ID. Сервер может прислать обратно некоторые инструкции по выполнению вспомогательных операций. Bot ID генерируется на основе значения HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\MachineGuid. Сервер может не отправить страницу блокировки боту, если бот с таким ID уже находится в базе сервера.

Заключение

Отслеживаемая нами «The home campaign» осуществляет доставку вымогателя Win32/Nymaim с марта 2013 года. Как мы указали в нашем исследовании, злоумышленники используют и другие семейства вредоносного кода для компрометации пользователей. Ниже

представлена схема, демонстрирующая этапы компрометации системы пользователя в такой кампании.