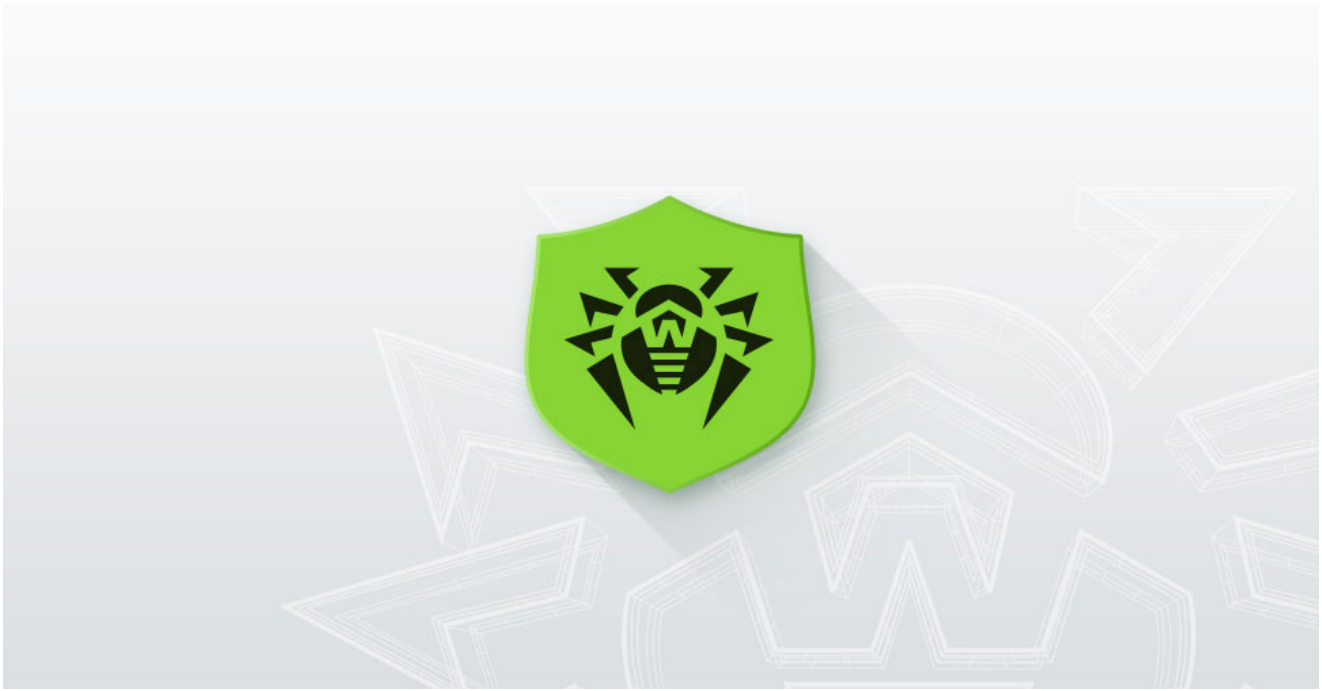
Trojan.Mutabaha.1

vms.drweb.ru/virus/



SHA1:

```
8a56002732c57e90eb482f7fd3aa75d400b6ba7f
```

Вредоносная программа, устанавливающая на зараженный компьютер собственную сборку браузера Chrome с названием Outfire. Этот браузер подменяет уже установленную копию Chrome, модифицирует имеющиеся ярлыки (или удаляет их и создает новые), а также копирует в новый браузер существующий профиль пользователя Chrome. В браузере Outfire невозможно изменить установленную по умолчанию стартовую страницу, также он содержит неотключаемую надстройку, предназначенную для подмены рекламы на веб-страницах.

В первую очередь на атакуемом компьютере запускается дроппер, который повышает свои привилегии посредством модификации ветви системного реестра HKCU\Software\Classes\mscfile\shell\open\command.

Дроппер сохраняет на диск и запускает приложение setup_52.3.2743.82_1471853250.exe, также сохраняются и запускаются .bat-файлы, предназначенные для удаления самого дроппера. Для реализации задержки используется следующая команда:

```
"C:\Windows\system32\cmd.exe" /c choice /t 20 /d y /n >nul & del "
<fullpath> \<dropper>.exe" >> NUL
```

Где <fullpath> — полный путь к месту расположения дроппера, <dropper> — имя файла дроппера.

Программа-установщик связывается с принадлежащим злоумышленникам управляющим сервером, получает оттуда конфигурационный файл, в котором указан адрес для скачивания браузера. Браузер устанавливается в папку C:\Program Files\Outfire и регистрируется в системном реестре:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Outfire]
"path"="C:\\Program Files\\Outfire\\"
"publicdirectroy_du"="C:\\Program Files\\Outfire\\Reports\\Dump"
"channel"="ince"
"userid"="harddisk_123"
"version"="52.3.2743.82"
```

Троянец запускает несколько системных служб и создает задачи в Планировщике заданий с целью загрузки и инсталляции собственных обновлений.

Вредоносная программа проверяет наличие в системе других поддельных браузеров, генерируя их имена с помощью комбинации значений из двух списков-словарей:

```
"apple", "bag", "cat", "boy", "pear", "ball", "fish", "bird", "egg", "fan",
"jam", "cup", "book", "bed", "gun", "jar", "leg", "hip", "boob", "pen",
"kit", "tool", "map", "nose", "ant", "box", "big", "zoo", "hot", "to",
"in", "out", "red", "on", "set", "bang", "sea", "go", "for", "shut",
"boss", "mon", "sys", "east", "left", "cold", "foot", "ever", "hi", "yeah",
"yes", "no", "do", "june", "day", "be", "we", "stan", "that", "her",
"all", "will", "can", "year", "new", "Gold"  "fly", "old", "has", "per",
"fun", "ship", "duck", "pat", "eat", "look",
"my", "glad", "one", "hair", "lamp", "face", "suck", "lose", "job", "kiss",
"ass", "leaf", "blue", "hat", "fat", "bear", "rice", "bean", "anna", "tony,
"bob", "mike", "larry", "ben", "jane", "bin", "sarah", "ness", "son",
"dear","eye", "arm", "toe", "car", "boat", "pig", "dog", "tie", "door",
"flat", "cine", "rain", "seed", "fire", "may"
```

Таким образом формируются имена и номера версий браузеров, полный список которых приведен ниже:

```
50.17.2661.78 Weness
50.19.2661.78 Eastness
50.21.2661.78 Footblue
50.22.2661.78 Bangone
50.25.2661.78 Legpat
50.26.2661.78 Yestony
50.27.2661.78 Nosemay
51.5.2704.63 Cupblue
51.6.2704.63 Birdkiss
51.7.2704.63 Hipbear
```

```
51.8.2704.63 Juneper
51.9.2704.63 Hisarah
51.10.2704.63 Mapcar
51.12.2704.63 Docine
51.13.2704.63 Noanna
51.14.2704.63 Wefat
51.15.2704.63 Seaness
51.16.2704.63 Allold
51.17.2704.63 Gunship
51.18.2704.63 Footship
51.19.2704.63 Nobean
51.20.2704.63 Jamsarah
51.21.2704.63 Birdsarah
51.23.2704.63 Doold
51.24.2704.63 Junedoor
51.25.2704.63 Toolrain
51.26.2704.63 Lefttoe
51.27.2704.63 Zooface
51.28.2704.63 Hipfat
51.29.2704.63 Yesdear
51.30.2704.63 Fishlamp
51.31.2704.63 Outlose
51.32.2704.63 Nosejane
51.33.2704.63 Hiprain
51.34.2704.63 Eastfat
51.35.2704.63 Goldlarry
51.36.2704.63 Bigjane
52.1.2743.82 Birddear
52.2.2743.82 Boobseed
52.3.2743.82 Outfire
52.4.2743.82 Allhair
52.5.2743.82 Outboat
52.6.2743.82 Bookfat
52.7.2743.82 Zootony
52.8.2743.82 Birdeye
50.2.2661.78 Sysblue
50.3.2661.78 Eggsuck
50.4.2661.78 Jarsarah
50.7.2661.78 Thatrice
50.8.2661.78 Pearbob
50.10.2661.78 Herness
50.11.2661.78 Redpig
50.13.2661.78 Toolduck
50.14.2661.78 Guntony
50.15.2661.78 Seablue
50.20.2661.78 Monold
```

Полученные имена троянец сравнивает со значением «Outfire» (с целью исключить самоудаление), после чего удаляет соответствующие записи из системного реестра, останавливает процессы обнаруженных браузеров и удаляет их записи из Планировщика заданий (пример для браузера с именем Bangone):

```
 TASKKILL /F /IM protect.exe
TASKKILL /F /IM Bangone.exe
TASKKILL /F /IM Bangone_server.exe
TASKKILL /F /IM BangoneUpdate.exe
"C:\Windows\System32\cmd.exe" /c chcp 437 & schtasks /Delete /TN
"BangoneCheckTask" /F
"C:\Windows\System32\cmd.exe" /c chcp 437 & schtasks /Query /TN
"BangoneCheckTask"
"C:\Windows\System32\cmd.exe" /c chcp 437 & schtasks /Delete /TN
"BangoneBrowserUpdateUA" /F
"C:\Windows\System32\cmd.exe" /c chcp 437 & schtasks /Query /TN
"BangoneBrowserUpdateUA"
"C:\Windows\System32\cmd.exe" /c chcp 437 & schtasks /Delete /TN
"BangoneUpdateTaskMachineUA" /F
"C:\Windows\System32\cmd.exe" /c chcp 437 & schtasks /Query /TN
"BangoneUpdateTaskMachineUA"
"C:\Windows\System32\cmd.exe" /c chcp 437 & schtasks /Delete /TN
"BangoneBrowserUpdateCore" /F
```

Новость о троянце