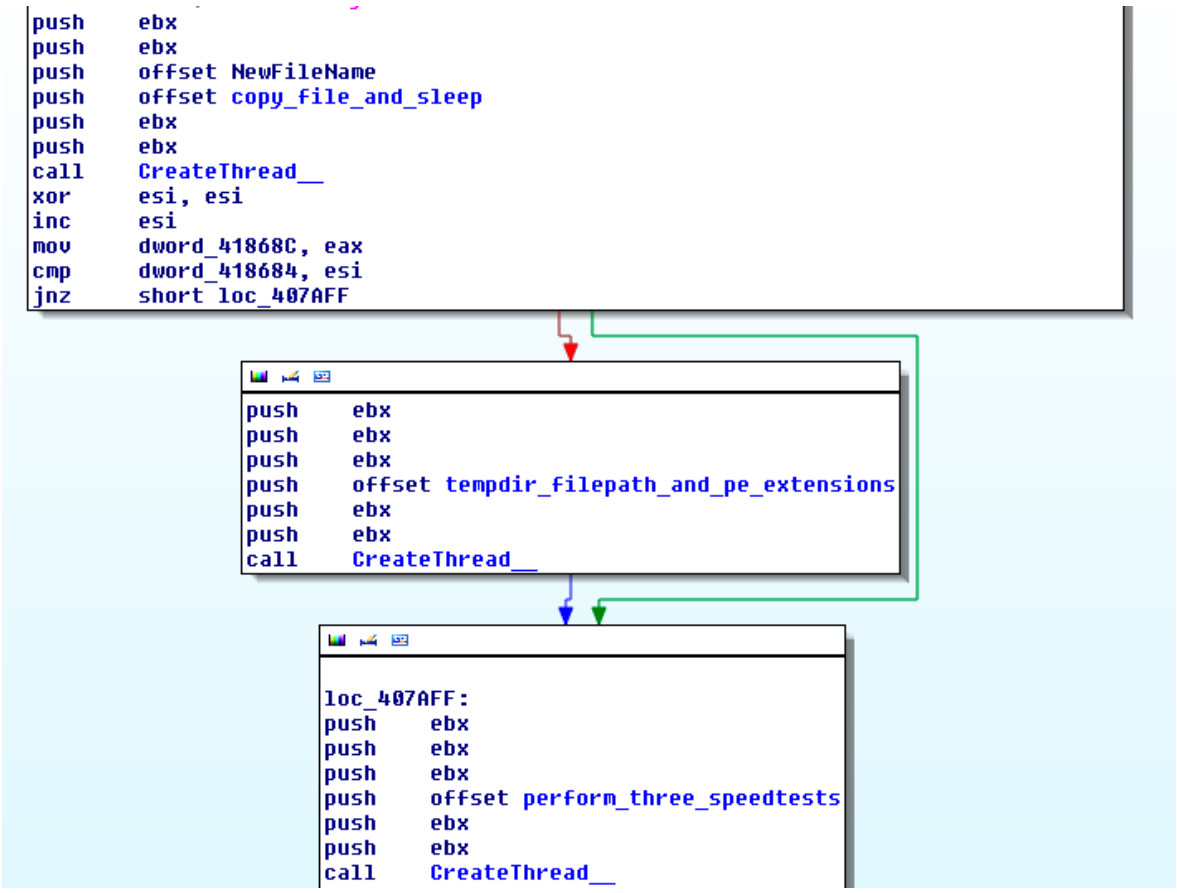
Артем Баранов
Ведущий вирусный аналитик ESET

Win32/DoS.OutFlare.A нацелен на обход anti-DDOS сервиса CloudFlare

CloudFlare представляет из себя популярный CDN-сервис поддержки веб-сайтов и включает в себя различные виды обслуживания, такие как, ускорение загрузки веб-страниц для конечного пользователя, функции обеспечения безопасности, например, anti-DDoS. Мы обнаружили вредоносную программу — Win32/DoS.OutFlare.A, которая нацелена на обход этого сервиса с целью осуществления DoS-атак на сайты, которые находятся под контролем CloudFlare. Наш анализ посвящен Win32/DoS.OutFlare.A.

Поведение вредоносного кода особенно ничем не примечательно. На старте он пытается создать мьютекс **Global\sad_day**, как свидетельство своего пребывания в системе. В случае успеха, он копирует себя в каталог %APPDATA%, добавляет себя в автозапуск и перезапускается. После этого OutFlare запускает копию процесса браузера Internet Explorer — iexplore.exe в приостановленном состоянии (suspend) и осуществляет внедрение в него своей полезной нагрузки.



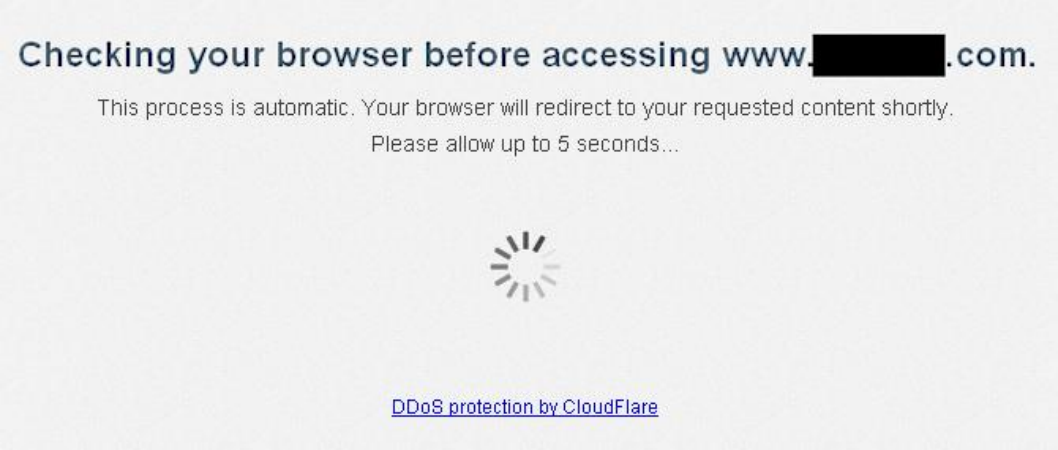
CloudFlare выполняет важные задачи в отдельных потоках.

Перед подключением к своему управляющему C&C серверу, вредоносный код выполняет три теста для измерения скорости исходящей загрузки, используя публичные сервисы www.speakeasy.net и сохраняет эти результаты в памяти. После этого, бот подключается к IRC-серверу, используя TCP-порт 9835 и канал #main. На этом этапе бот будет находится в состоянии Idle, ожидая команды со стороны сервера. Большинство из этих команд относятся к DoS-атакам. Одна из них — “cf”, особенно интересна. Эта команда отвечает за реализацию обхода anti-DDoS механизма CloudFlare на стороне клиента.

```
.rdata:0040EE77                         align 4
.rdata:0040EE78 ; char aDownload[]
.rdata:0040EE78 aDownload               db 'download',0
.rdata:0040EE81                         align 4
.rdata:0040EE84 ; char aUpdate[]
.rdata:0040EE84 aUpdate                 db 'update',0
.rdata:0040EE8B                         align 4
.rdata:0040EE8C ; char aArme[]
.rdata:0040EE8C aArme                   db 'arme',0
.rdata:0040EE91                         align 4
.rdata:0040EE94 ; char aGet[]
.rdata:0040EE94 aGet                    db 'get',0
.rdata:0040EE98 ; char aPost[]
.rdata:0040EE98 aPost                   db 'post',0
.rdata:0040EE9D                         align 10h
.rdata:0040EEA0 ; char aAny[]
.rdata:0040EEA0 aAny                    db 'any',0
.rdata:0040EEA4 ; char aSlow[]
.rdata:0040EEA4 aSlow                   db 'slow',0
.rdata:0040EEA9                         align 4
.rdata:0040EEAC ; char aSsyn[]
.rdata:0040EEAC aSsyn                   db 'ssyn',0
.rdata:0040EEB1                         align 4
.rdata:0040EEB4 ; char aUdp[]
.rdata:0040EEB4 aUdp                    db 'udp',0
.rdata:0040EEB8 ; char aL7[]
.rdata:0040EEB8 aL7                     db 'l7',0
.rdata:0040EEBB                         align 4
.rdata:0040EEBC ; char asc_40EEBC[]
.rdata:0040EEBC asc_40EEBC              db '/',0
.rdata:0040EEBC
.rdata:0040EEBE                         align 10h
.rdata:0040EEC0 ; char aHc[]
.rdata:0040EEC0 aHc                     db 'hc',0
.rdata:0040EEC3                         align 4
.rdata:0040EEC4 ; char aCf[]
.rdata:0040EEC4 aCf                     db 'cf',0
```

Список команд, поддерживаемых ботом.

Сервис CloudFlare использует специальный метод, направленный на предотвращение DDoS-атак. В такой системе клиент должен выполнить некоторые условия при доступе к сайту, находящемуся под контролем CloudFlare, который в свою очередь должен быть уверен, что запрос является легитимным и поступает именно от браузера пользователя. Сервис просит браузер выполнить специальный Java-скрипт, представляющий из себя математическое выражение, при этом визуально, проверка со стороны CloudFlare для пользователя выглядит как на рисунке ниже:



Страница содержит специальную форму POST-запроса, который будет использован для отправки ответа серверу. Сразу же под этой формой располагается фрагмент кода на Javascript, который подсчитывает математическое выражение и выполняет POST-запрос из предыдущей формы.

```
<div id="challenge" style="display:none;">
<p>This process is automatic. Your browser will redirect to your requested content shortly.</p>
<p>Please allow up to 5 seconds...</p>
<form id="ChallengeForm" action="http://www.[redacted].com/" method="POST">
<input type="hidden" name="act" value="jschl"/>
<input type="hidden" name="jschl_vc" value="3ce9a22a170ab1083cba4d94708eea94"/>
<input type="hidden" id="jschl_answer" name="jschl_answer"/>
</div>
```

Форма POST HTTP-запроса.

```
<script type="text/javascript">
        //<![CDATA[
        $('#challenge').show();
        $(function(){setTimeout(
            function(){
                $('#jschl_answer').val(41+33*1);
                $('#ChallengeForm').submit();
            },
            5850
        )});
        //]]>
    </script>
```

Подсчет математического выражения.

Веб-браузер пользователя будет исполнять этот Javascript и выполнит HTTP POST-запрос, который будет выглядеть как на скриншоте ниже. В этом отправленном серверу ответе, будет содержаться рассчитанное значение математического выражения.

```
POST / HTTP/1.1
Host: www.[redacted].com
Content-Type: application/x-www-form-urlencoded
Cookie: __cfduid=d0070009c4213dbefe31ccc9b0f74a6561360175321

act=jschl&jschl_vc=3ce9a22a170ab1083cba4d94708eea94&jschl_answer=74
```

Если выражение было рассчитано верно, сервис CloudFlare ответит установкой специальных cookie, подтверждающих подключение к серверу. Ссылки на этот cookie в дальнейших запросах, в течении этого открытого сеанса работы с сервером, приведут к тому, что CloudFlare будет отправлять запрос к серверу напрямую, минуя специальную проверку.

```
Set-Cookie: cf_clearance=72a1df3aa055166e219fea5b88d96139-1360175328-3600; expires=Wed, 06-Feb-2013 20:28:48
```

Win32/DoS.OutFlare.A содержит функционал, который направлен на обход этого защитного механизма. Он анализирует часть кода веб-страницы и ищет совпадения по необходимой части функционала JS CloudFlare. После того, как необходимые параметры были идентифицированы, вредоносный код рассчитывает математическое выражение и отправляет его на сервер для получения необходимого cookie, который необходим для проведения DDoS-атаки на реальный веб-сервер.

```
lea     eax, [ebp+74h+Str]
push    offset a_val     ; ".val("
push    eax              ; Str
mov     [ebp+74h+var_B0], bl
call    strstr
push    eax              ; Format
lea     eax, [ebp+74h+var_264]
push    0FFh             ; Count
push    eax              ; Dest
call    _snprintf
lea     eax, [ebp+74h+var_264]
push    offset asc_40B324 ; ");"
push    eax              ; Str
call    strstr
```

Извлечение выражения, которое необходимо вычислить.

```
lea     eax, [ebp+Str]
push    eax              ; Str
call    atoi
mov     esi, eax
lea     eax, [ebp+var_4]
push    eax              ; Str
call    atoi
imul    esi, eax
lea     eax, [ebp+Dest]
push    eax              ; Str
call    atoi
add     esp, 18h
add     eax, esi
```

Расчет выражения.