malware/windows/gozi-isfb at master · gbrindisi/malware

By gbrindisi

Archived: 2026-04-05 15:09:24 UTC

```
ISFB - программа-бот предназначенная для анализа и модификации HTTP траффика на компьютер

Поддерживает все 32х и 64х битные Windows, начиная с Windows XP.
Поддерживает все 32х и 64х битные версии Internet Explorer, начиная с 6.0.
Поддерживает все 32х и 64х битные версии Mozilla Firefox.
ПОддерживает все 32х битные версии Google Chrome.

Программа способна устанавливаться и работать без привелегий администратора.
Обрабатывает весь HTTP траффик браузера в том числе и шифрованый HTTPS.

Бот управляется с удаленного сервера, с помощью файлов конфигурации и команд.
Файлы конфигурации и команд подписываются посредством RSA. При получении файлов, бот про
 и, в случае несоответвия подписи, файл игнорируется.

При первом запуске бот инициирует таймер. В дальнейшем, по таймеру, бот обращается на упр

Поддерживается 2 способа поиска управляющего сервера:
- перебор заданного списка доменных имен и выбор активного;
- генерациия динамического списка доменных имен в зависимости от текущей даты и конфигура

Анализ траффика производится на основе специально сформированного файла конфигурации, ко
Такой файл может содержать следующие инструкции:
- подмена HTML страницы целиком
- замена фрагмента HTML страницы
- скопировать фрагмент страницы и отправить на сервер
- найти файл по маске и оправить на сервер
- сделать скриншот экрана и отправить на сервер

Кроме файла конфигурации бот получает с сервера команды:
GET_CERTS       - экспортировать и выслать сертификаты, установленные в системном хранилище
                      Для XP выгружает, также, неэкспортируемые сертификаты.
GET_COOKIES     - собрать cookie FF и IE, SOL-файлы Flash, упаковать их с сохранением структуры
                      каталогов и выслать на сервер.
CLR_COOKIES     - удалить cookie FF и IE, SOL-файлы Flash.
GET_SYSINFO     - собрать системную информацию: тип процессора, версию ОС, список процесс
                      драйверов, список установленных программ.
KILL            - убить ОС (работает только с правами администратора)
REBOOT          - перезагрузить ОС
GROUP=n         - сменить ID группы бота на n
```

```
LOAD_EXE=URL    - загрузить файл с указанного URL и запустить его
LOAD_REG_EXE=URL- загрузить файл с указанного URL, зарегистрировать его в autirun и запустить
LOAD_UPDATE=URL - загрузить апдейт программы и запустить
GET_LOG         - отправить внутренний лог на сервер
GET_FILES=*     - найти все файлы, соответствующие заданной маске, и отправить на сервер
SLEEP=n         - остановить обработку очереди команд на n миллисекунд. (используется при дол
SEND_ALL        - отправить все данные из очереди на отправку немедленно. В противном случае
                  по таймеру.
LOAD_DLL=URL[,URL] - загрузить по указанному URL DLL и инжектить её в процесс explorer.exe.
                  первый URL для 32х-битной DLL, второй - для 64х-битной.

SOCKS_START=IP:PORT     - запустить сокс4\5 сервер (при его наличии)
SOCKS_STOP              - остановить сокс4\5 сервер

GET_KEYLOG      - отправить данные кейлоггера (при его наличии)
GET_MAIL        - активировать граббер E-Mail (при наличии) и отправить, полученные от него, д
GET_FTP         - активировать граббер FTP (при наличии) и отправить, полученные от него, данн

SELF_DELETE - удалить софт из системы, включая все файлы и ключи реестра

URL_BLOCK=URL   - заблокировать доступ ко всем URL удовлетворяющим заданной маске
URL_UNBLOCK=URL - разблокировать доступ к URL, удовлетворяющим заданной маске, ранее заблоки
FORMS_ON                - включить граббер HTTP форм (если есть дефайн _ALWAYS_HTTPS, то граббе
FORMS_OFF               - отключить граббер HTTP форм
KEYLOG_ON[= list]       - включить кейлог, для заданного списка процессов
KEYLOG_OFF              - отключить кейлог
LOAD_INI=URL    - загрузить упакованный INI-файл с указанного URL, сохранить его в рееестре и и
                                  прикреплённого к софту с помощью билдера. INI-файл до

LOAD_REG_DLL = name, URL[,URL] - загрузить DLL по указанному URL, сохранить её под заданным име
                                  автоматической загрузки после каждого запуска системы
UNREG_DLL = name        - удалить из автоматической загрузки DLL с заданным именем

Технические детали

Дропер - программа установки.
Дропер представляет собой исполняемый файл Windows (PE32). В файле, в виде бинарного ресур
две упакованые DLL: 32х битный и 64х-битный бот.
При старте дропер распаковывает DLL и регистрирует их для автозапуска.
DLL распаковываются и регистрируются таким образом, чтобы иметь возможность выполняться пр
 как при администраторе, так и при пользователе.

DLL - бот.
Бот представляет собой динамически загружаемую библиотеку (DLL). Для каждой архитектуры со
DLL-бот загружается во все запускаемые процессы.
Бот состоит из 2х логических компонентов: парсер и сервер. Парсер активируется в контексте пр
Сервер активируется в контексте процесса оболочки (как правило explorer.exe).
```

Парсер выполняет следующие функции:
- отправка/получение данных (получение команд, конфигов; отправка форм, файлов)
- непосредственный перехват, анализ, и модификация HTTP траффика

Сервер (в контексте explorer.exe) выполняет:
- файловые операции (поиск, создание и удаление файлов)
- запуск программ, обновление
- системные функции (перезагрузка, блокировка ОС)

Таким образом, все операции, требующие привелегий, выполняются сервером в контексте explo
а все операции с сетью исключительно из браузера.

Сборка и настройка

Проект собирается при помощи Microsoft Visual Studio 2005, либо более поздней версии.
В проект интегрирован криптор, который используется по-умолчанию.
В результате сборки и криптовки получаются следующие файлы:
Release\crm_p.exe
Release\client_p.dll
x64\Release\client_p.dll
это упакованные и криптованые версии бота и дропера, причем дропер (файл crm_p.exe) содерж
Некриптованные версии бота лежат там же:
Release\crm.exe
Release\client.dll
x64\Release\client.dll

Кроме бота, проект включает в себя:
Release\dname.exe - утилита для генерации псевдо-случайных доменных имен;
Release\rsakey.exe - утилита для подписывания файлов команд и конфига;
config.exe - программа конфигуратор.

Основные настройки программы находятся в файлах id.h и config.h.
id.h содержит номер группы бота.
config.h содержит такие параметры как: список управляющих серверов, названия URL-ов для пол
и для отсылки данных, а также различные ключи и параметры влияющие на настройку програм

Сборка с билдером

Существует возможность собрать ISFB так, чтобы в дальнейшем прикреплять к DLL ключи и файл
не пересобирая проект.

1. Собрать ISFB в конфигурации Release(Builder) под x86 и x64.
2. Отредактировать файлы: \public.key и \client.ini, содержащие RSA-ключ и настройки програм
3. В консольном окне выполнить build.bat из папки \Builder

4. Забрать готовый installer.exe из папки \Builder\Release

Батник build.bat запускает билдер, который прикрепляет к каджой DLL (для x86 и x64) файлы:
public.key и client.ini.
В последствии обе DLL прикрепляются к инсталлеру.
Готовый инсталлер сохраняется в файл \Release\install.exe

Сборка с BK

Существует возможность собрать ISFB вместе BK в один исполняемый файл-установщик, так, чтоб
ошибки при установке BK, устанофщик извлекал DLL и устанавливал их отдельно.
Примечание: папка, содержащая солюшен с BK2 должена находиться в той же директории, что и

1. Собрать BK в конфигурации Release под x86 и x64.
2. Собрать ISFB в конфигурации Release(Builder) под x86 и x64.
3. Отредактировать файлы: \public.key и \client.ini.
4. В консольном окне запустить bkbuild.bat из папки \Builder
5. Забрать собраный bksetup.exe, содержащий BK, ISFB-DLL и ISFB-инсталлер, из \Builder\Release

Работа в режиме инжекта из памяти

Для работы в режиме инжекта из памяти необходимо установить значение флага _INJECT_AS_IMAGE
TRUE, и пересобрать проект. В этом случае инсталлер не создает DLL на диске, а копирует себя
и регистрируется в Windows AutoRun.
При запуске инсталлер инжектит образ DLL, соответствующей архитектуры, в Explorer.exe, откуда
сооответствующий образ DLL инектится во все пораждаемые процессы, разных архитектур.

Плагины

ISFB поддерживает плагины: специально собраные, DLL, экпортирующие функцию PluginRegisterCa
внутренние функции софта (например, функции отправки данных).
Для загрузки плагина используется команда:
LOAD_PLUGIN=URL[,URL] - где первый URL для 32х-битной версии DLL, второй - 64х-битной.
Софт скачивает DLL соответствующей архитектуры и инжектит её в explorer.exe, затем вызывается
PluginRegisterCallbacks, в которую передаётся указатель на список коллбэков (функций), реализ
внутри софта, которые может использовать плагин.
Описание структур и прототипов функций для создания плагинов находится в файле \common\plug

Состав проекта

\AcDLL - библиотека инжектов. Реализует механизм инжекта DLL во все пораждаемые процессы,
        Поддерживает два режима работы: инжект, непосредственно DLL и инжект образа DLL из
\ApDepack - библиотека на основе APLIB, релизующая функции распаковки.

```
\BcClient - библиотека клиента для бэкконект сервера.
\Client - основная DLL приложения
\Common - библоиотека, реализующая общие функции, используемые в разных частях проекта. Та
        операции с потоками данных, со строками, с XML, хуки и т.п.
\Crypto - библиотека криптографических функций. Реализует следующие алгоритмы: CRC32, BASE6
        Используется для подписи конфиг-файлов и файлов команд, а также, для саршифровки
\Dname  - программа генерации доменных имён на основе номера группы софта и текущей даты.
\Ftp    - библиотека FTP-грабберов.
\Handle - библиотека, реализующая хэш таблицу. Используется для привязки хэндлов HTTP запрос
        Также, используется кейлоггером, для группировки клавиатурных логов по PID-ам и HWND
\IM             - DLL-плагин, реализующая граббер Instant Messangers.
\Install - программа-установщик ISFB.
\KeyLog - библиотека кейлоггер.
\Mail   - библиотека E-mail грабберов.
\RsaKey - программа для шифрования и цифровой подписи конфиг-файлов и файлов команд.
\SocksLib - библиотека, реализующая SOCKS4\5-сервер.
\Sqlite3 - библиотека для работы с БД SQLLite. Используется IM-грабберами.
\ZConv  - программа-конвертер конфигов Zeus в конфиг-файлы ISFB.
```

Source: https://github.com/gbrindisi/malware/tree/master/windows/gozi-isfb