

Below is the text file opened as ANSI Cyrillic in Microsoft Word

Do not share this!
For Internal Use Only.

Руководство пользователя Zeus (ЧЕРНОВИК)

=====
= Содержание =
=====

1. Описание и возможности.
2. Настройка сервера.
 - 2.1. HTTP-сервер.
 - 2.2. Интерпретатор PHP.
 - 2.3. MySQL-сервер.
3. Настройка бота.
4. История версий.
5. TODO.
6. F.A.Q.
7. Мифы.

=====
= 1. Описание и возможности. =
=====

Zeus - программное обеспечение для кражи личных данных пользователей с удаленных систем Windows. На простом языке "Троян", "Бэкдор", "Вирус". Но автор не любит эти слова, поэтому далее в документации он будет называть это программное обеспечение "Бот".

Бот полностью основан на перехвате WinAPI в UserMode (Ring3), это значит, что бот не использует каких-либо драйверов и обращений в Ring0. Эта особенность дает возможность запускаться боту даже из Гостевых учетных записей Windows. Плюс это гарантирует повышенную стабильность, и адаптивность к последующим версиям Windows.

Бот разрабатывается на Visual C++ версии 9.0+, при этом не используются дополнительные библиотеки типа msvcrt, ATL, MFC, QT и т.д. Код бота пишется со следующими приоритетами (в порядке уменьшения):

1. стабильность (старательно проверяются все результаты вызова функций и т.д.),
2. размер (избегаются повторы алгоритмов, повторы вызовов функций и т.д.),
3. скорость (нет инструкций типа while(1){..}, for(int i = 0; i < strlen(str); i++){..}).

Функции и особенности бота:

1. Снифер трафика для протокола TCP.
 - 1.1. Перехват FTP логинов на любом порту.
 - 1.2. Перехват POP3 логинов на любом порту.
 - 1.3. Перехват любых данных из трафика (персональный заказ).

2. Перехват HTTP/HTTPS запросов для wininet.dll, т.е. всех программ работающих с этой библиотекой. Сюда входят Internet Explorer (любая версия), Maxton, и т.д.

2.1. Подмена ..

3. Функции сервера.

3.1 Socks4/4a/5.

3.2 Бэксонект для любого сервиса (RDP, Socks, FTP, и.т.д.) на зараженной машине. Вы можете получить доступ к компьютеру, который находится за NAT, или, например, к которому запрещены подключения из интернета.

3.3 Получение скриншота экрана в реальном времени.

=====
= 2. Настройка сервера. =
=====

Сервер является центральной точкой для управления ботнетом, он занимается сборкой отчетов ботов, и отдачей команд ботам. Крайне не рекомендуется использовать "Виртуальный Хостинг или VDS", т.к. при увеличении ботнета, нагрузка на сервер будет увеличиваться, и такой вид хостинга исчерпает довольно быстро свои ресурсы. Вам нужен "Выделенный сервер" (Дедик), рекомендуемая минимальная конфигурация:

1. 2Гб ОЗУ.
2. 2х процессор частотой 2Ггц,
3. SATA винчестер 7200rpm+

Для работы бота необходим HTTP-сервер с подключенным PHP + Zend Optimizer, и MySQL-сервер.

2.1 HTTP-сервер.

В качестве HTTP-сервера рекомендуется использовать: для nix-систем Apache версии 2.2+, для Windows-систем IIS версии 6+. Рекомендуется держать HTTP-сервер на 80 или 443 порту (это положительно влияет на отстук бота, поскольку провайдеры/прокси могут блокировать доступ на иные, нестандартные, порты).

=====
= 2. История версий. =
=====

Условные метки:

- [*] - изменение.
- [-] - исправление.
- [+] - добавление.

[Версия 1.2.0.0, 20.12.2008]

Общее:

[*] Более не будет документации в chm-файле, все будет писаться в этот файл.

[+] Теперь бот способен получать команды не только при отправке статуса, но и при отправки файлов/логов.

[+] Локальные данные, запросы к серверу, и файл конфигурации шифруются RC4 с ключом на ваш выбор.

[*] Полностью обновлен протокол бот <-> сервер. Возможно понизится нагрузка на сервер.

459905217 (15:47:57 5/03/2009)

Бот:

[-] Устранена ошибка, блокирующая бота на лимитированных учених записях Windows.

[*] Написан новый PE-криптор, теперь PE-файл получается очень аккуратным и максимально имитирует результат работы MS Linker 9.0.

[*] Обновлен процесс сборки бота в билдере.

[*] Оптимизировано сжатие файла конфигурации.

[*] Новый формат бинарного файла конфигурации.

[*] Переписан процесс сборки бинарного файла конфигурации.

[*] Socks и LC теперь работают на одном порту.

Панель управления:

[*] Статус панели управления переведен в BETA.

[*] Изменены все таблицы MySQL.

[*] Начет постепенный перевод Панели Управления на UTF-8 (возможны временные проблемы с отображением символов).

[*] Обновлена геобазы.

[Версия 1.2.1.0, 30.12.2008]

Бот:

[*] BOFA Answers теперь отсылается как BLT_GRABBED_HTTP (было BLT_HTTPS_REQUEST).

[-] Мелкая ошибка при отправке отчетов.

[-] Размер отчета не мог превышать ~550 символов.

[-] Ошибка существующая с начала существования бота: низкий таймаут для отсылки POST-запросов, в результате чего блокировалась отсылка длинных (более ~1 Мб) отчетов на медленных соединениях (не стабильных), как теоретическое последствие - бот вообще переставал слать отчеты.

Общее:

[+] В случаи записи отчета типа BLT_HTTP_REQUEST и BLT_HTTPS_REQUEST в поле SBCID_PATH_SOURCE (в таблице будет path_source) добавляется путь URL.

Панель управления:

[*] Обновлен redir.php.

=====
= 2. TODO. =
=====

1. Полноценная работа в Windows Vista/2008/Seven.
2. Изменение метода перехвата WinAPI.
3. Случайная генерация: имен файлов, настроек, и данных.
4. Консольный билдер.
5. x64 версия.

6. Поддержка IPv6.
7. Написание полноценной документации.
8. Сбор статистики используемого ПО (антивирусы, фаерволы и т.д.).
9. Перехват FireFox 3+.

=====
= 4. F.A.Q. =
=====

Q: Когда все началось?

A: Далеким летом 2006, когда в руки попал глючный "VisualBreeze e-Banca".
После этого возникло
желание написать что-то с такими же возможностями,

(05:11:25 23/01/2009)

но не с такой глючностью, и с не с такими
размерами. А вообще, dev, спасибо за образец ;)

Q: Что значат цифры в версии ZeuS?

A: a.b.c.d

a - полное изменение в устройстве бота.

b - крупные изменения, которые вызывают полную или частичную
несовместимость с предыдущими
версиями бота.

c - исправления ошибок, доработки, добавление возможностей.

d - номер чистки от AV для текущей версии a.b.c.

Q: Каким образом генерируется Bot ID?

A: Bot ID состоит из двух частей: %name%_%number%, где name - имя
компьютера (результат от
GetComputerName), а number - некое число, генерируемое на основе
некоторых уникальных данных ОС.

=====
= 5. Мифы =
=====

M: ZeuS использует DLL для своей работы.

A: Ложь. Существует только один исполняемый PE файл (exe). Dll, sys и
т.д. не когда не было и
врядли когда-либо будет. Этот миф пошел в результате того, что в
некоторых версия бота для
хранения настроек, используются файлы с такими расширениями.

M: ZeuS использует COM (BHO) для перехвата Internet Explorer.

A: Ложь. Всегда для этого использовался перехват WinAPI из wininet.dll.