ZeuS Version scheme by the trojan author

contagiodump.blogspot.com/2010/07/zeus-version-scheme-by-trojan-author.html

List of all official existing Zeus versions and the scheme description made by the author in his mother tongue. The source is Damagelab.org but I can't find the original post, sorry - it was from this winter 2010. Many other versions like 1.3.1.1 and other random numbers are fakes - hex'd , slightly modified older versions. There is an English translation below, it is not perfect but *not* Google machine. Email me if you have any questions.

Read more about ZeuS here - **Zeus Trojan Research Links**

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: What do the numbers in the version of ZeuS mean?
A: a.b.c.d
a - a complete change in the bot design
b - the major changes that cause complete or partial incompatibility with the previous versions of the bot.
c - correction of bugs, errors, refining, additional features.
d - number of cleaning for protection against AV for the current version abc

SCROLL DOWN TO SEE ENGLISH TRANSLATION
========== = 5. 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 отправки 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.
Бот:
[-] Устранена ошибка, блокирующая бота на лимитированных ученых 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 геобаза.

[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.

[Версия 1.2.2.0, 11.03.2009]
Бот:
[-] Устранена ошибка в HTTP-инжектах существующая на протяжении ВСЕХ версий бота. При использовании в программе асинхронного режима wininet.dll, был упущен момент синхронизации потоков создаваемых wininet.dll, в результате чего, при

некоторых условиях происходило исключение.
[+] При срабатывании HTTP-инжекта, теперь также изменяются файлы в локальном кэше. Отсутствие этой доработки, позволяло не всегда срабатывать HTTP-инжектам.
[+] Уменьшен размер PE-файла.

[Версия 1.2.3.0, 28.03.2009]
Бот:
[-] Мелкие ошибки в крипторе, спасибо доблестным говноаналитикам из Avira.
Общее:
[*] Изменен протокол раздачи команд ботам.
Панель управления:
[*] Полностью переписана панель управления.
[*] Дизайн переписан на XHTML 1.0 Strict (под IE не работает).
[*] Бот теперь опять способен получать команды только при отправке отчета об онлайн-статусе (слишком высокая нагрузка).
[*] Обновлена геобаза.

[Версия 1.2.4.0, 02.04.2009]
Бот:
[+] При работе с HTTP, заголовок User-Agent теперь читается от Internet Explorer, а не является константой как раньше. Теоретически из-за постоянного User-Agent'a, запросы могли блокироваться провайдерами, или попадать под подозрение. Панель управления:
[-] Исправлена ошибка отображения отчетов, содержащих символы 0-31 и 127-159.

[Версия 1.2.5.0, 27.05.2009]
Бот:
[+] Незначительная оптимизация кода. Панель управления:
[-] Устранена уязвимость в gate.php, позволяющая записывать файлы в родительские директории.
[+] Добавлены запрещенные расширения в массив $bad_exts.
[+] В модуле botnet_bots, при изменение фильтра сохраняется текущая сортировка.

[Версия 1.2.6.0, 04.06.2009]
Бот:
[+] Перехват библиотеки nspr4.dll.

[Версия 1.2.7.0, 22.06.2009]
Общее:
[+] В отчеты добавляется имя пользователя, которому принадлежит процесс. Бот:
[+] Отключение фишинг-фильтра в IE7, IE8.

Версия 1.2.8.0, 05.10.2009]

Бот:
[+] За счет включения опции TCP_NODELAY, увеличена скорость работы Socks-сервера, и прочих встроенных протоколов. Это будет особенно заметно для протоколов, обменивающихся мелкими TCP-пакетами.
[+] При соединении с сервером через Wininet, не добавлялся HTTP-заголовок "Connection: close", когда это было необходимо. Из-за особенностей Wininet, это могло создать лишнею нагрузку на сервер (вероятно). Панель управления:
[*] Обновлена геобаза.

[Версия 1.2.9.0, 10.10.2009]
Бот:
[+] Добавлен граббер паролей для следующих FTP-клиентов: FlashFXP, Total Commander, WS_FTP FileZilla, FAR Manager, WinSCP, FTP Commander, Core FTP, SmartFTP.
[Версия 1.2.10.0, 17.10.2009] Панель управления:
[+] Полная интеграция "Jabber notifier".

Версия 1.3.0.0, 22.11.2009]
Бот:
[*] Перехват WinAPI методом сплайсинга.
[+] Полноценная работа в Windows Vista/7.
[*] Временно отключено скрытие файлов бота.
[*] Убран TAN-граббер.
[-] Исправлена ошибка дублирования отчетов в nspr4.dll.
[*] Сграбленные сертификаты теперь пишутся с именем grabbed_dd_mm_yyyy.pfx, и паролем в UTF-8. [*] Команда getcerts, получается сертификаты только из MY-хранилища, а не из всех. Т.к. получение сертификатов из всех хранилищ не имеет смысла.
[*] Изменено поведение граббера сертификатов.
[*] Переписан FTP/POP3 снифер, улучшено обнаружение логинов, сделана поддержка IPv6-адресов.
[*] Переписан перехват ввода клавиатуры, исправлен метод работы с интернациональными символами. [-] Исправлена ошибка в HTTP-фейках, которая могла привести к deadlock.
[*] Изменен способ генерации BotID.

[Версия 1.3.1.0, 29.11.2009]
Бот:
[-] Устранена серьезная ошибка, которая могла возникнуть при работе с файлом конфигурации.

[Версия 1.3.2.0, 11.01.2010]
Бот:
[-] Устранена серьезная ошибка, которая могла привести к deadlock в любом процессе

(актуально только для билдов с поддержкой nspr4.dll).

[Версия 1.4.*]
[*] Полная несовместимость с предыдущими версиями.
[*] Поскольку ядро бота нацелено на Windows Vista+, в боте никогда не будут использоваться сплойты повышения привелегий и т.д. Бот работает в переделах одного пользователя. Тем неменее элементарные попытки заразить прочих пользователей Windows совершаются (обычно эффективно в случаях отключения UAC или запуск с из-под LocalSystem).
[+] Возможна работа с "Roaming User Accounts".
[*] Произвольные имена файлов, мютексов.
[*] Пайпы более не используются.
[*] Полностю переписано ядро бота, от процесса установки в систему до отсука в админку.
[+] При инсталяции, перекриптовывает свое тело, таким оброзом сохраняется уникальная копия exe-файла на каждом компьютере.
[+] Привязка бота к компьютеру, путем модификации/удаления некоторых данные в exe-файле. [+] Полноценная работа с x32 приложениями в Windows x64.
[+] Удаление исходного файла бота, после исполнения.
[+] Полноценная работа в "Terminal Services".
[+] При запуске из под пользователя LocalSystem, происходит попытка заражения всех пользовталей системы.
[*] Убрана опция StaticConfig.blacklist_languages.
[+] Имя ботнета ограничено 20 сиволами, и может содержать любые интернациональные символы.
[+] Файл Конфигурации читается как UTF8 ---------- НЕ СДЕЛАНО ЕЩЕ. нет поддержки в buildcfg.cpp
[*] Убрана опция StaticConfig.url_compip.
[+] Нельзя обновить новую версию на старую.
[+] При обновлении бота происходит полное обновление немедленно, не дожидаясь перезагрузки.
[*] В данный момент из-за некторых соображений скрытие файлов бота не будет производиться вообще.
[*] Убран граббер Protected Storage, покольку начинася с IE7 он более не испольузуется им.
[*] С связи с не надежностью старой системы подсчета Инсталлов, бот имеет метку Инсталла при добавлении в базу.

Q: Каким оброзом генерируется Bot ID?
A: Bot ID состоит из двух частей: %name%_%number%, где name - имя компьютера (результат от GetComputerName), a number - некое число, генерируемое на основе некотрых 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 врятли 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 (БХО) для перехвата Internet Explorer.
A: Ложь. Всегда для этого использовался перехват WinAPI из wininet.dll.

Machine translation - it is quite bad, I am planning to make a better one later.

Q: How Bot ID is generated ?
A: Bot ID consists of two parts:% name% _% number%, where the name - the name of the computer (the result of GetComputerName), and the number - a certain number generated on the basis of unique data of the OS.
==========
= 5. Myths =
========== M: ZeuS uses a DLL to their work. A: False. There is only one executable PE file (exe). Dll, sys, etc. not when there was no vryatli ever will. This myth came from the fact that in some version of the bot to store the settings used files with extensions.

M: ZeuS uses COM (BHO) to intercept Internet Explorer.
A: False. Always used WinAPI from wininet.dll. for this interception

========== 5. Version History (dates are in DD/MM/YY format). = ==========
Tags: [*] - change. [-] - A correction. [+] - Add.

[Version 1.2.0.0, 20.12.2008]
Overall:
[*] There will be no more documentation in the chm-file, everything will be written to this file.
[+] Now the bot is able to receive commands not only when sending its status, but also when sending files / logs.
[+] Local data, server requests, and the configuration file are RC4 encrypted with the key of your choice.
[*] Completely updated bot <-> server protocol. Perhaps it will diminish the server load.
Bot:
[-] Fixed a bug that blocks the bot on limited Windows accounts.
[*] Written a new PE-cryptor, now PE-file is very neat and simulates the working result of MS

Linker 9.0.
[*] Updated build process of the bot.
[*] Optimized compression of the configuration file.
[*] Introduced a new format of the binary configuration file.
[*] The build process of the binary configuration file is re-written.
[*] Socks and LC are now working on the same port.
Control Panel:
[*] Control panel status is now beta
[*] Changed all tables in MySQL.
[*] Started a gradual transfer of the Control Panel to UTF-8 (there may be temporary problems with some displaying characters).
[*] Updated geobase.

[Version 1.2.1.0, 30.12.2008]
Bot:
[*] BOFA Answers are now being sent as BLT_GRABBED_HTTP (was BLT_HTTPS_REQUEST).
[-] Small error when sending reports.
[-] The size of the report could not exceed about 550 characters.
[-] Error in existence since the bot introduction: a low timeout for sending POST-requests resulting in blocked long (more than ~ 1 Mb) reports on slow connections (unstable conections) and, as the theoretical implication, the bot would stop sending reports altogether.
Overall:
[+] When entering reports like BLT_HTTP_REQUEST and BLT_HTTPS_REQUEST into the field SBCID_PATH_SOURCE (would be path_source in the table) URL is now added.
Control Panel:
[*] Updated redir.php.

[Version 1.2.2.0, 11.03.2009]
Bot:
[-] Fixed a bug in HTTP-injections for all versions of the bot. When using asynchronous mode wininet.dll, it would miss the moment of the thread synchronization, which under certain conditions could cause an an exception. (ok, this is iffy and may need a better translation)
[+] when HTTP-injection occurs, the files in the local cache change too. Without this feature the HTTP-injections was not always triggered.
[+] Reduce the size of PE-file
[Version 1.2.3.0, 28.03.2009]
Bot:
[-] Minor errors in the cryptor, thanks to the shit analysts from Avira.
Overall
[*] Changed the protocol of bot control commands.
Control Panel:

[*] Completely re-written Control Panel.
[*] Design rewritten to XHTML 1.0 Strict (does not work in IE).
[*] Bot again receives commands only when sending online status reports (utilization too high).
[*] Updated geobase.

Version 1.2.4.0, 02.04.2009]
Bot:
[+] When you work with HTTP, User-Agent string now shows as Internet Explorer and is not a constant value as before. Theoretically, never changing User-Agent queries could be blocked by providers or cause suspicions in the past.'
Control Panel:
[-] Fixed a bug in the display of reports containing characters 0-31 and 127-159

[Version 1.2.5.0, 27.05.2009]
Bot:
[+] Minor code optimization.
Control Panel:
[-] Fixed a vulnerability in gate.php allowing adding files to parent directories.
[+] Added new forbidden file extensions in the array $bad_exts.
[+] Changing filter in the botnet_bots module does not prevent from keeping the current sorting

[Version 1.2.6.0, 04.06.2009]
Bot:
[+] interception of nspr4.dll library.

[Version 1.2.7.0, 22.06.2009]
Overall:
[+] Added the name of the user- process owner into the reports
Bot:
[+] Ability to disable the phishing filter in IE7, IE8.

[Version 1.2.8.0, 05.10.2009]
Bot:
[+] By including option TCP_NODELAY, increased speed of the Socks-server, and other built-in protocols. This is particularly noticeable for the protocols, exchanging small TCP-packets.
[+] When connecting to the server via Wininet, HTTP-header "Connection: close" was not added when needed. This could possibly create an unnecessary load on the server.
Control Panel:
[*] Updated geobase.

Version 1.2.9.0, 10.10.2009]
Bot:
[+] Added grabber passwords for the following FTP-Client: FlashFXP, Total Commander, WS_FTP FileZilla, FAR Manager, WinSCP, FTP Commander, Core FTP, SmartFTP.

[Version 1.2.10.0, 17.10.2009]
The control panel:
[+] Full integration of "Jabber notifier".
Version 1.3.0.0, 22.11.2009]
Bot:
[*] Intercept of WinAPI by means of splicing
[+] Fully functional in Windows Vista /windows 7.
[*] Temporarily disabled hiding of bot files.
[*] Removed TAN-grabber.
[-] Fixed duplicate records in nspr4.dll.
[*] Intercepted certificates are now entered as grabbed_dd_mm_yyyy.pfx, and password in UTF-8.
[*] Command "getcerts" allows to get certificates only from MY-store, not from all locations because obtaining certificates from all the stores does not make sense.
[*] Changed behavior of the certificates grabbers.
[*] Rewrote FTP/POP3 sniffer, improved detection of logins, introduced support for IPv6-addresses.
[*] Rewrote keyboard input interception feature, fixed methods of working with international symbols.
[-] Fixed bug in HTTP-fakes, which could lead to deadlock.
[*] Changed the way of generating BotID.

[Version 1.3.1.0, 29.11.2009]
Bot:
[-] Fixed a bug that could occur with the configuration file.

Version 1.3.2.0, 11.01.2010]
Bot:
[-] Fixed a serious bug, which could lead to a deadlock in any process (relevant only for builders with nspr4.dll support).

[Version 1.4 .*]
[*] Full incompatibility with all the previous versions.
[*] Since the core of the bot is targeted to Windows Vista+, the bot will never use exploits for increasing privileges, etc. The bot works within one user account, however it will attempt to infect other Windows users (usually effective if you disable UAC or start it as LocalSystem).
[+] Ability to work with "Roaming User Accounts".

[*] Random file names, mutexes
[*] Pipe no longer used.
[*] The core of the bot has been completely changed. Everything - from the installation to the callback process.
[+] As it installs itself, it re-encrypt itself so every computer has a unique copy of the exe file
[+] Binding bot to a computer by modifying / deleting some data in the exe file.
[+] Fully functional work with x32 applications in Windows x64.
[+] Delete the original file after the execution.
[+] Fully functionalin the "Terminal Services".
[+] When running as LocalSystem, it tries to infect all windows users
[*] Removed StaticConfig.blacklist_languages option.
[+] Name of the botnet is limited to 20 of characters, and may contain any international characters
[+] Configuration File is read as UTF8 ---------- NOT DONE YET. no support in buildcfg.cpp
[*] Removed staticConfig.url_compip option.
[+] Can not be used to upgrade an older version
[+] the bot update happens instantly, not need to wait for a reboot.
[*] At the moment, after condidering some aspects, decided not to hide the bot files
[*] Removed the Protected Storage grabber because IE7+ is not using it
[*] Since the old system had reliability issues with the way installs were counted, the bot will now have an install marker when added to the database.