Citadel 1.1 - FF/IE/Chrome Grabber/Video Recording, AntiTracker Protection & CRM
Citadel 1.1 - FF/IE/Chrome Grabber + Video Recording & AntiTracker Protection

Предлагаем вам достойное решение для создания и обновления вашего ботнета.
Мы не пытались изобрести велосипед или создать революционный продукт. Всего лишь доработали уже хорошо зарекомендовавший себя в работе Zeus, значительно расширив его функционал и адаптировав под современные условия выживания под новым именем. Софт писали для себя, в процессе родилась идея о создании "социального круга поддержки", об этом читайте ниже.

We proudly offer a solution for creation and updating your botnet. We have not tried to re-invent the wheel. We have improved a well-respected Zeus, by enhancing its functionality and by adapting it to the modern requirements of resiliency, and gave it a new name. We developed tis software for usselves. The idea of creating a community for support was born during the process of development. Read below about it.

Изменения коснулись как непосредственно самого бота, так и веб-составляющей.
Никаких "красивых иконок" вы у нас не найдете. Вы платите исключительно за новый приведенный ниже функционал и мотивацию кодеров для выполнения поддержки продукта.

The changes were done to the bot software itself and to the web-enabled management subsystem. You will not find “pretty icons”. You pay only for the new functions listed below and to motivate the developers to do product maintenance.

Список нововведений для бота:

The list of improvements:

[+] Фикс VNC бага на Vista/Windows 7. Теперь можно полноценно работать с Internet Explorer (напомню, была проблема с рендерингом IE)

Fix of VNC bug on Vista/Windows 7. Now it is possible to fully work with Internet Explorer (reminder, there was a problem to render IE)

[+] Поддержка Mozilla Firefox 7.0 (решена проблема, при которой не слались отчеты в последних версиях браузера)

Mozilla Firefox 7.0 is now supported (there was a problem with reporting in last versions of FF browser)

[+] Крипто-защита (расшифровывающая тело в памяти).

Encryption (the software gets decrypted in memory)

[+] Редиректы DNS (не через hosts). Можно блокировать/редиректить любые URL'ы, не опасаясь, что их заметит эвристика. Например заблокировать AV-сервера или редиректить банк-пагу на другой хост.
!BONUS! Список URL'ов популярных антивирусных программ для блокирования идет в комплекте.

DNS redirections (not via hosts). It is possible to block/redirect any URL without fear that it is going to be detected by heuristics. For example, to block AV-servers and redirect banking application to a different host.
!BONUS! The list of URL's of popular AV programs to be blocked is included with the software.

[+] Информация о версии сотфа в репорте. Высылает вам подробную версию браузера холдера вместе с отчетом. Помогает, при имитации настроек холдера.

Information about software version is sent in report. The full version description of the browser is being sent together with the report. It is helpful to imitate hosts settings.

[+] Дополнительный уровень защиты сервера от трекеров - Login Key.

Additional level of server defense from trackers – Login Key.

[+] Механизм аутинтефикации при загрузке конфигов (нет прямых урлов). Дает полноценную защиту от устоявшихся трекеров.

Mechanism of authentication during the load of configuration (no direct URLs). It gives full defense against known trackers.

[+] Поддержка граббера Google Chrome. [Проверено на последней версии 15.x/16.x].

Support of Google Chrome grabber. [Checked on the last version 15.x/16.x]

[+] Поддержка инжектов Google Chrome. [Проверено на последней версии 15.x/16.x].

Support of injects into Google Chrome. [Checked on the last version 15.x/16.x]

[+} Добавлено кеширование поиска функций, что ускоряет установку хуков Chrome.

Cashing of search function has bee added. It speeds up installation of hooks into Chrome.

[+] Добавлена возможность выполнения системных CMD команд при старте бота (секция CMDList) с отправкой репорта на сервер. К примеру, нужно вам чтобы при инсталле, отправлялся результат команды "ipconfig /all", или список всех доступных шар. Полезно, при анализе внутренней структуры компаний. (например, часто попадаются боты в локалке с именами ACCOUNTANT_PC, POS_SERV, DATABASE...)

System command (CMD) execution during the start of the bot (section of CMDList) with delivering a report to the server. For example, it is useful if you need to send yourself a result of command “ipconfig /all” or for the analysis of internal structure of companies (it is common to find internal hosts like ACCOUNTANT_PC, POS_SERV, DATABASE ...)

[+] Добавлен механизм проверки сохранности хуков на некоторых Windows.

Added a mechanism of checking the resiliency of hooks on some versions of Windows.

[+] Эвристический анализатор окружения со стоп листом для нежелательного ПО (значительно повышает скрытность),включены все популярные антивирусы.

Heuristics analyzer of the environment with the “stop list” for unwanted software (it improves stealth ability), all popular anti-virus programs are included.

[+] Исправлены мелкие баги.

Small bugs have been fixed

[+] Видео граббер. Уникальная возможность следить за работой ваших инжектов "глазами холдерами", в конфиге указываются список сайтов и длина записи видео в секундах, при заходе на заданный линк, активируется видео-запись в формате .mkv. Рекомендуется настроить свой сервер для приема файлов 10-60МБ.

Video grabber. It is a unique opportunity to check on the works of the software “through the eyes of the victim”. Configuration options: are the length of the recording in seconds, the list of URLs, link which triggers the recording. Video recording is in .mkv format. It is recommended to configure server to accept files with the size of 10-60 MB.

[+] Убрано удаление кукисов при инсталле, т.к это сбивает "fingerprint" холдера при работе с заливами.

Deletion of cookies during installation has been removed, since it destroys “fingerprint” of the host.

[+] добавлена поддержка HTTP 1.0 и расширенных хидеров (например респонз не всегда выглядит как "HTTP/1.1 200 OK", бывает "HTTP/1.1 200 follow document", в данном случае после кода 200 идет несколько слов) применимо к браузерам Firexfox & Chrome

Support of HTTP 1.0 was added along with enhancing the hiders (for example, response does not always look like “HTTP/1.1 200 OK”, it can be “HTTP/1.1 200 follow document”, in this case after code 200 there are several words). It is useful for browsers Firefox and Chrome.

[+] Добавлен гейт генератор (на случай, если вы хотите разместить файлы на промежуточном хосте для редиректа).

Gateway generator has bee added (for the case if you need to place files on some intermediate host)

[+] Весь базовый функционал, оставшийся от зевса присутствует. Думаю, не стоит его писать здесь снова.

The basic functionality of Zeus was left intact. There is no reason to mention it here.

[+] Полностью измененый интерфейс веб-админки, user-friendly.

The interface of web-enabled administration program has been totally changed. It is more user-friendly.

Рис 1. Главное окно билдера (Full Screen# hxxp://img405.imageshack.us/img405/2131/2812.png)

Pic 1. Main window of the builder (Full Screen# hxxp://img405.imageshack.us/img405/2131/2812.png)

Рис 2. Главное окно веб-панели. (Full Screen# hxxp://img851.imageshack.us/img851/4718/cpscreen.png)
Pic 2. Main window of web-panel. (Full Screen# hxxp://img851.imageshack.us/img851/4718/cpscreen.png)

Про живучесть ботов ничего не скажем, увидите все сами. Благодарность принимаем в виде LR-знаков
We will not mention the resiliency of the bots. See for yourself. We accept gratitude.

Это базовая комплектация сборки. Стоимость $2399.00
This is base system. The price is $2,399.00

Важное замечание:
Наш софт НЕ работает на русскоязычных системах, если обнаруживается русская или украинская раскладка - софт дает отказ в работе. Данное введение сделано в целях борьбы с СНГ загрузками. Относитесь к этому как хотите, для нас это табу.
Если хотите протестировать работу и разрабатывать инжекты - ставьте англоязычную систему, ссылки на образ + VMWare мы даем, чтобы сэкономить ваше время на поиск.

Very important note:
Our software does not function on Russian-based systems. If Russian or Ukrainian versions of Windows are detected software stops functioning. It is done to fight against infections in CIS. You can have different opinions about it. For us it is a taboo.
If you want to test the software, install English-based version of the system. We are giving a link to the image + VMWare, to save your time for doing search.

ДОПОЛНИТЕЛЬНЫЕ МОДУЛИ:

ADDITIONAL MODULES:

Список нововведений для веб-админки (отдельные модули):

List of new features for web-based administration (separate modules)

[+] Реализована полноценная VNC-админка для работы с ботами.
Developed full-featured VNC-based administration module to work with bots.

Теперь вы можете:
Now you can:

- Собирать нужные вам конторы и акки в отдельную БД, в отдельный скрипт. В нем есть удобный просмотр записей, можно смотреть список онлайн-ботов и данные по пришедшим аккам.

Group specific companies and accounts into separate database and into separate script. There is a convenient way of browsing records. Now you can see the list of on-line bots and information on accounts.

- Создавать VNC-соединения в 2 клика с любым ботом.
Create VNC connections with any bot in 2 clicks

- Просмотр статистики по живым/мертвым аккам(по ботам).
List statistics on alive/dead accounts (on bots)

- Редактирования/изменений примечаний к пришедшим аккаунтам.
Editing notes on accounts

- Автоматические jabber-уведомления о новых поступлениях, либо, если бот появился в онлайне. Вам приходит уже готовый IP:PORT в жаббер, для соединения по ВНЦ протоколу.
Automatic jabber-alerts on new bots or when bot appears on-line. You receive Jabber message containing IP:Port for VNC connection.

- Возможность сортировки ботов по online/used/unused статусу.
Possibility to sort bots by on-line/used/unused status.

- Указать BotID и VNC-соединение автоматически установится, как только бот появится в онлайне.
Configure automatic VNC connection by BotID as soon as bot is on-line

Стоимость $495.00
Price: $495.00

Рис 3. Панель управления VNC (Full Screen# hxxp://img259.imageshack.us/img259/8664/vnc.png)
Pic 3. VNC administration panel (Full Screen# hxxp://img259.imageshack.us/img259/8664/vnc.png)

[+] Модуль качественной проверки Socks на валидность.
Возможность указать несколько БД разных ботнетов. Выдает 99,9% валидность соксов, засчет проверки через веб-серфинг.
Стоимость: $49.00

Module to check quality of Socks. Possibility to configure several databases of different botnets. Outputs 99.9% of valid socks by checking via web-surfing
Price: $49.00

[+] Модуль авто-крипта exe-файлов.
Как много рутины создает постоянная ручная криптовка файлов и долгие ожидания криптовщиков в онлайне? Автоматизируйте ваш труд, был разработан замечательный модуль авто-крипта, который позволяет самообновлять exe-файлы ваших ботнетов. Скрипт работает через jabber-сервис Death'a, который именуется как cbot, стоимость 1 крипта - 15$. Ответственность за качество крипта мы не несем. Скрипт запускается по крону и позволяет криптовать файлы нужное количество раз.

Стоимость: $395.00

Module to auto-encrypt executables.
How much of routine work is encrypting files by hand and long waiting time of on-line cyphers? To automate your work, there is a auto-encryption module, which allows to update executables of your botnets. Script works over jabber-service Death'a which is called as cbot. The price of 1 encryption is $15. We are not responsible for the quality of encryption. Script is triggered by cron and allows to encrypt files necessary number of times.
Price: $395.00

[+] Модуль парсера логов.
Наверное, многие сталкивались с проблемой, когда ботнетов становилось много, а логов еще больше. С текущим уровнем поиска данных по БД - это отнимает очень много времени.
Мы разработали скрипт, который позволяет включить в список несколько БД сразу и вывести вам список всех встречающихся http/https линков, а также данных по ним.
Присутствует возможность кеширования, а также заметок, для вашего удобства.
Стоимость: $295.00

Module to parse logs.
Many people, probably, faced the problem, when there were too many botnets and there were even more logs. Searching through the database takes too much time. We developed a script, which allows working with several databases at once, which outputs list of all http/https links and metadata regarding them. There is a possibility of caching and creating notes for convenience.

Все модули можно приобрести только при покупке базовой комплектации, отдельно они не продаются. С покупкой модуля, вы получаете право на дальнейшие обновления и поддержку данного модуля с нашей стороны.
All modules are available only together with the purchase of the base system. They are not sold separately. When you buy a module, you receive a right for updates and for technical support.

В РАЗРАБОТКЕ:[*] Полноценный поиск & отсылка файлов по жесткому диску, список масок задается в конфиге. Например "passwords*.txt"[*] Загрузка модуля видео-граббинга с удаленного хоста, в целях снижения веса билда.
IN WORKS:
[*] Full search and copying of files from the hard drive, the list of file masks is configurable. Example “passwords*.txt”
[*]. Remote load and configuration of video-grabbing module to lower the “weight” of the build.

СЕРВИС & СОЦИАЛЬНЫЙ КРУГ:
SERVICE and COMMUNITY

Не секрет, что продукты в нашей нише, без поддержки со стороны разработчиков - это кусок хлама на жестком диске.
Поэтому продукт должен развиваться с учетом пожеланий наших клиентов, одна проблема - вы наверное сталкивались с игнором разработчиков в IM, потому что клиентов много, а разработчик один
It it's no secret, that without support by developers, products in our field is nothing but garbage on hard disk.
Therefore, the product has to be improved taking in consideration of our clients. One problem is that

many of you faced problem with ignore on IM, because there are a lot of clients, but there is only one developer.

Время - деньги, мы сделали для вас специальную систему, подобную социальной сети для наших клиентов.
Time is money, we made a special system for our clients similar to social network,

Citadel CRM Store позволяет вам принимать участие в развитие продукта, а именно:
Citadel CRM Store gives you an opportunity to influence the product in the following:

- Сообщать о баг-репортах и найденых ошибках в софте, все тикеты рассматриваются тех.поддержкой и вы своевременно получите ответ по возникшему вопросу, не надо больше доставать автора в icq/jabber'e.
- Notify us on bugs and other errors in software. All tickets are looked at by technical support and you will timely get an answer regarding your questions. You do not need to bother the author in ICQ/Jabber.

- Каждый клиент имеет право создавать неограниченое количество заявок внутри системы, в которой он может выдвинуть предложение на создание нового модуля/доработки, который ему необходим в функционале софта. Каждая такая заявка, может быть как публичной так и приватной(доступной только вам)
- Every client has a right to create an unlimited number of requests inside the system. Requests can contain suggestions on new module or improvements of existing module. Such requests can be public or private.

- Каждый клиент имеет право голосовать за выдвинутую другим мембером идею и предлагать свою цену за реализацую данной доработки/модуля. По окончанию голосования, принимается решение разработчиками: делать данный модуль или нет, в зависимости от результата голосования среди клиентов.
- Each client has a right to vote on new ideas suggested by other members and offer his/her price for development of the enhancement/module. The decision is made by the developers on whether to go forward with certain enhancement or new module depending on the voting results.

- Каждый клиент имеет право комментировать любые заявки и общаться с другими мемберами, теперь вам будет интересно найти партнеров и единомышленников, а также принимать активное участие в дискуссии совместно с разработчиками.
- Each client has a right to comment on any request and talk to any member. Now it is going to be interesting for you to find partners and like-minded people and also take active parts in discussions with the developers

- Вы можете видеть все стадии процесса создания модуля, если он утвержден мемберами. Мы своевременно обновляем статус и сроки у заявки.
- You can see all the stages of module development, if it is approved by the members. We update the status and time to completion.

- Вы можете вносить предоплату, если модуль был утвержден (50%), после вноса предоплаты мемберами, данный проект начинает двигаться вперед, т.к сумма выплачивается напрямую кодерам и никакой лени или бездействия вы с нами не найдете. Все прозрачно: каждый этап разработки подробно отображается.

- You may pay a deposit, if module is approved (50%). After the deposit is paid by the members, the project starts moving forward, so that the money is paid directly to coders and there will be no laziness or inaction. Everything is clear: every stage of development is thoroughly shown.

- Удобные уведомления в jabber о новых комментариях или новых созданных заявках.
Вы по достоинству оцените новый формат работы!
- Convenient notifications are sent over jabber regarding new comments or new requests. You will deservedly like new format of work!

Покупая базовую комплектацию, ежемесячно взымается арендная плата $125(можно оплатить на несколько месяцев вперед), что входит в эту плату:
Buying the base system, you will be paying rental fee of $125 (you can pay them several months in advance). Here is what's included in this price

- Нам интересно работать с нашими клиентами. На форумах часто старательно пишут что "мы поддерживаем продукт... блабла" а в итоге получается что обновления выходят раз в три месяца или вообще автор пропадает с концами. Проблема в мотивации авторов. Вы поддерживаете нас - мы поддерживаем вас. Все просто.
- It's very interesting for us to work with our clients. A lot of authors write in forums that they “support the product”, but at the end the updates only come out once per 3 months or the author disappears forever. Problem is in author's motivation. You support us, we support you. It is easy.

- Вы получаете ежемесячное обновление билдера (в 20 числах), которое включает обновленную защиту от антивирусов (шифрование тела бота, эвристический анализ перед инжектом в процессы).
- You get monthly update to the builder (in 20th of every month), which includes updated AV defense (encryption of the body of the bot, heuristics analysis before the injection of the process).

- Вы получаете доступ в CRM: право инициативы на создания новых доработок, улучшений, право голоса за другие проекты и возможность общаться с другими мемберами в Citadel CRM Store.
- You receive access to CRM: right to initiate updates, enhancements, improvements, right to vote for or against other projects and possibility to communicate with other members of Citadel CRM.

- Поддержку с нашей стороны: ответы на ваши вопросы(через тикеты), помощь в установке и рекомендации к использованию. Запрещено передавать ваш персональный аккаунт в CRM кому-либо еще.
- Our technical support: responses to your questions (via tickets), help in installation and recommendations on how to use the system. It is prohibited to give access to your CRM account to anyone.

- В ближайших планах подключить к CRM системе веб-программистов, занимающихся исключительно инжектами (в т.ч написание АЗ). Наши клиенты смогут создавать ТЗ внутри системы, объявлять сроки и стоимость - а кодеры браться за выполнение поставленной задачи. Если вы качественно пишите инжекты - обращайтесь к нам, обсудим.
- It is in immediate plans to connect CRM to the system of web-programmers, working specifically on injectors. Our clients can create technical tasks inside the system, announce time-frames and the price. The coders can than work on those tasks. If you write quality injectors – contact us.

Рис 4. Citadel CRM Store (Full Screen#
hxxp://img819.imageshack.us/img819/2624/democrmscreen.png)

Демо-доступ по запросу (выдается в течении 24 часов).
Билдер идет с привязкой к вашему ПК, можете создавать неограниченое количество доменов.
Оплата исключительно (Быстро обменять WM-LR можно на форумах типа mmgp.ru). Webmoney не принимаем.

Demo-access is upon request (given out within 24 hours).
Builder is given to you with consideration of your configuration. You can create an unlimited number of domains. Payment is over LR. We do not take WebMoney.

Чтобы сэкономить ваше и наше время, не надо писать "ты тут?" и т.п
Скидывайте ваш запрос в формате:
"Хочу приобрести базовую комплектацию, а также модули VNC, автокрипт и сокс. Сколько будет стоить со скидкой ? "

To save your and our time, do not write “are you here?” and so forth.
Send us your questions in the format:
“I want to purchase base system, and the modules: VNC, autoscript, and socks. How much is it going to cost with the discount?”

Jabber: aquabox@jabber.jp (время работы с 12 до 04.00 - переодическое присутствие, пишите сразу вопросы)

Jabber aquabox@jabber.jp (from 12:00 to 04:00 – sporadically on-line, write direct questions)