

Leveraging ZeuS to send spam through social networks

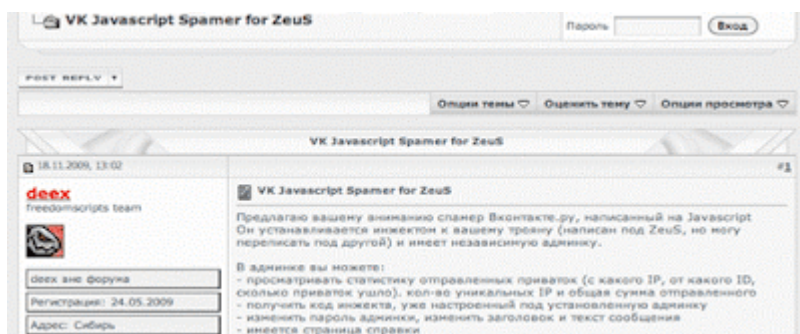
Archived: 2026-04-05 15:58:55 UTC

MalwareIntelligence is a site dedicated to research on all matters relating to anti-malware security, criminology computing and information security in general, always from a perspective closely related to the field of intelligence.

[Leveraging ZeuS to send spam through social networks](#)

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).

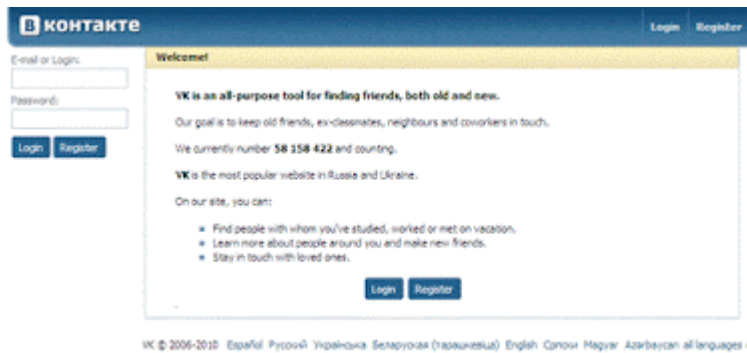


The pack includes several configuration files, which make it:

- **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.



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/sites.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=H0H0H0H0H0H0" "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?i=0.770993946307197B
HTTP/1.1" 200 81 "http://vkontakte.ru/mail.php?autosend=1&act=write&to=BBBBBBBBBB" "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=0.4629986281027114&myid=XXXXXXXXXX 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=XXXXXXXXXX" "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=AAAAAAAAA" "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?i=0.08157689112485272
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=0.07626892995503542&myid=XXXXXXXXXX HTTP/1.1" 200 20
"http://vkontakte.ru/mail.php?autosend=1&act=write&to=AAAAAAAAA" "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]"

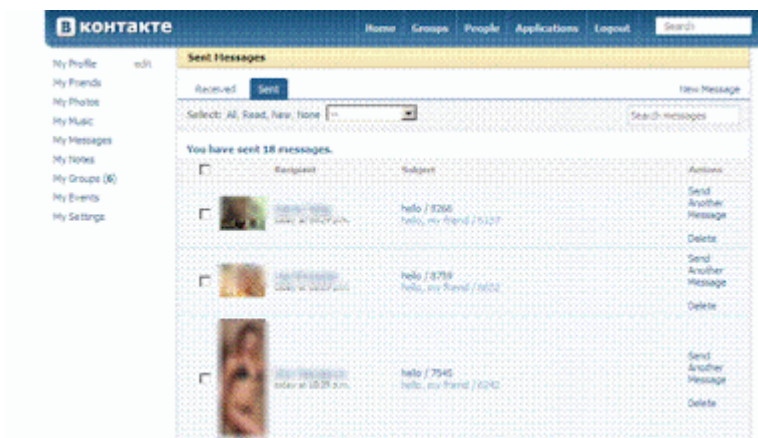
192.168.72.131 -- [21/Jan/2010:22:29:46 +0100] "GET /spam/vk/js.php?i=0.8682432031277047
HTTP/1.1" 200 80 "http://vkontakte.ru/mail.php?autosend=1&act=write&to=H0H0H0H0H0H0" "Mozilla/4.0
[compatible; MSIE 7.0; Windows NT 5.1]"

192.168.72.131 -- [21/Jan/2010:22:29:46 +0100] "GET
/spam/vk/success.php?nocache=0.11933687238992235&myid=XXXXXXXXXX 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:



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:

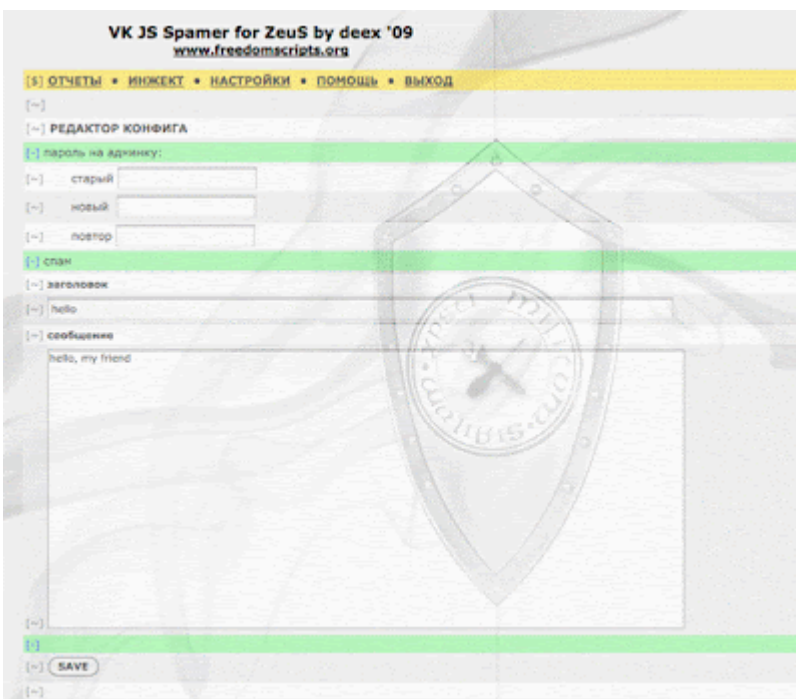
- **Reports:** shows the result of sending spam. In our example, the ID has sent 20 messages from the specified IP.



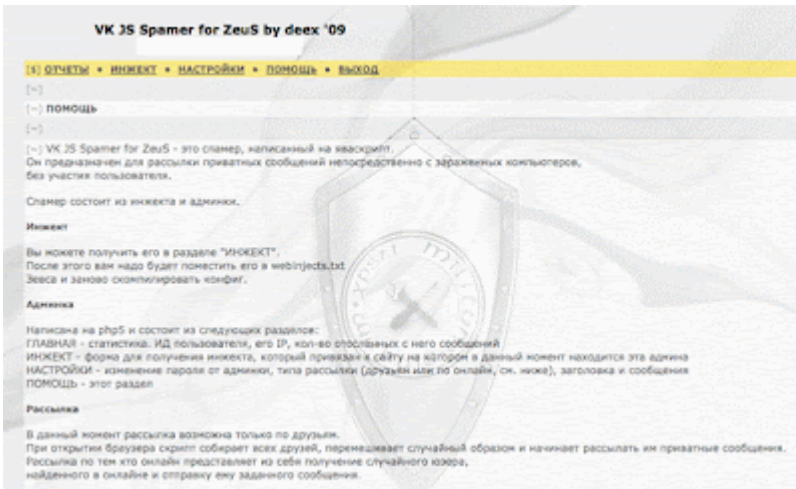
- **Inject:** shows the code injection (webinjects.txt) and links to three pages responsible for performing tasks involving the shipment.



- **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.



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



- **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