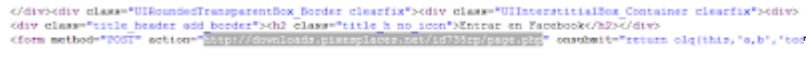
New phishing campaign against Facebook led by Zeus

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.

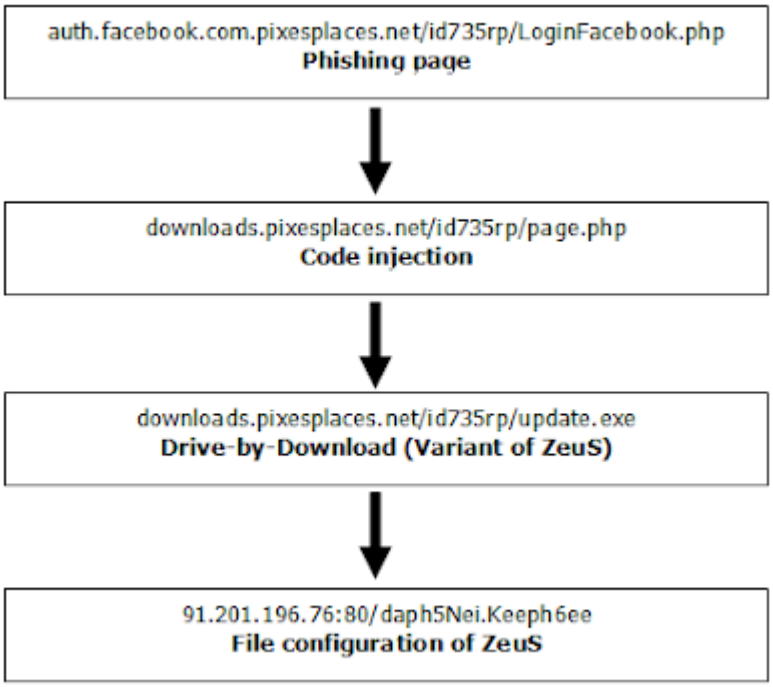
New phishing campaign against Facebook led by Zeus

Updated 15.03.2010
New domains have been released and has multi-stage attack whereby you chain multiple websites with malicious content.



The last download a binary called update.exe (19d9cc4d9d512e60f61746ef4c741f09) which is a variant of the trojan ZeuS, which has a high detection rate.

The sequence is as follows:



Original 14.03.2010
At this point the "circus", no doubt, as I always say, that ZeuS is the "creme de la creme" current on crimeware.

Some time ago we warned about different campaigns where the employer, in all cases without exception, is the exploitation of social engineering to execute a fraudulent component, and the goal is the theft of sensitive information.

Cases like the previous campaign by using the image of ZeuS Facebook and phishing attacks using popular services such as primary coverage, including IRS, VISA, Google and Blogger, among many others, are concrete examples that demonstrate what is the magnitude of the business ZeuS offers computer criminals.

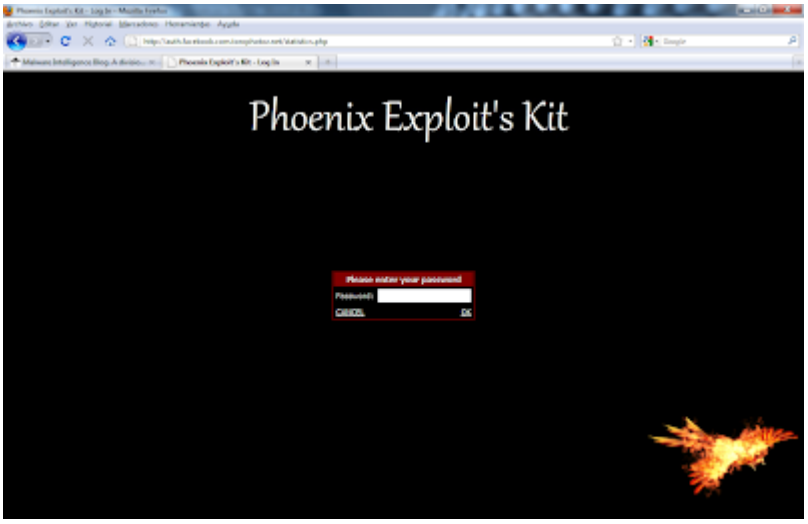
A few days ago, a new campaign to materialize from the hand of ZeuS, involving a large battery of malicious domains. Among them:

downloads.legomay.com/id735rp/LoginFacebook.php
downloads.legomay.net/id735rp/LoginFacebook.php
downloads.legomay.org/id735rp/LoginFacebook.php
downloads.megavids.org/id735rp/LoginFacebook.php
downloads.migpix.com/id735rp/LoginFacebook.php
downloads.migpix.net/id735rp/LoginFacebook.php
downloads.migpix.org/id735rp/LoginFacebook.php
downloads.modavedis.com/id735rp/LoginFacebook.php
downloads.modavedis.net/id735rp/LoginFacebook.php
downloads.modavedis.org/id735rp/LoginFacebook.php
downloads.portodrive.org/id735rp/LoginFacebook.php
downloads.reggiepix.com/id735rp/LoginFacebook.php
downloads.reggiepix.net/id735rp/LoginFacebook.php
downloads.reggiepix.org/id735rp/LoginFacebook.php
downloads.regzapix.com/id735rp/LoginFacebook.php
downloads.regzapix.net/id735rp/LoginFacebook.php
downloads.regzapix.org/id735rp/LoginFacebook.php
downloads.regzavids.com/id735rp/LoginFacebook.php
downloads.regzavids.net/id735rp/LoginFacebook.php
downloads.regzavids.org/id735rp/LoginFacebook.php
downloads.restopix.org/id735rp/LoginFacebook.php
downloads.restpictures.com/id735rp/LoginFacebook.php
downloads.restpictures.net/id735rp/LoginFacebook.php
downloads.restpictures.org/id735rp/LoginFacebook.php
downloads.restway.net/id735rp/LoginFacebook.php
downloads.restway.org/id735rp/LoginFacebook.php
downloads.tastyfiles.net/id735rp/LoginFacebook.php
downloads.vedivids.com/id735rp/LoginFacebook.php
downloads.vedivids.net/id735rp/LoginFacebook.php
downloads.vedivids.org/id735rp/LoginFacebook.php
downloads.vediway.com/id735rp/LoginFacebook.php

downloads.vediway.net/id735rp/LoginFacebook.php
downloads.vediway.org/id735rp/LoginFacebook.php

auth.facebook.com.legomay.com/id735rp/LoginFacebook.php
auth.facebook.com.legomay.net/id735rp/LoginFacebook.php
auth.facebook.com.legomay.org/id735rp/LoginFacebook.php
auth.facebook.com.megavids.org/id735rp/LoginFacebook.php
auth.facebook.com.migpix.com/id735rp/LoginFacebook.php
auth.facebook.com.migpix.net/id735rp/LoginFacebook.php
auth.facebook.com.migpix.org/id735rp/LoginFacebook.php
auth.facebook.com.modavedis.com/id735rp/LoginFacebook.php
auth.facebook.com.modavedis.net/id735rp/LoginFacebook.php
auth.facebook.com.modavedis.org/id735rp/LoginFacebook.php
auth.facebook.com.portodrive.org/id735rp/LoginFacebook.php
auth.facebook.com.reggiepix.com/id735rp/LoginFacebook.php
auth.facebook.com.reggiepix.net/id735rp/LoginFacebook.php
auth.facebook.com.reggiepix.org/id735rp/LoginFacebook.php
auth.facebook.com.regzapix.com/id735rp/LoginFacebook.php
auth.facebook.com.regzapix.net/id735rp/LoginFacebook.php
auth.facebook.com.regzapix.org/id735rp/LoginFacebook.php
auth.facebook.com.regzavids.com/id735rp/LoginFacebook.php
auth.facebook.com.regzavids.net/id735rp/LoginFacebook.php
auth.facebook.com.regzavids.org/id735rp/LoginFacebook.php
auth.facebook.com.restopix.org/id735rp/LoginFacebook.php
auth.facebook.com.restpictures.com/id735rp/LoginFacebook.php
auth.facebook.com.restpictures.net/id735rp/LoginFacebook.php
auth.facebook.com.restpictures.org/id735rp/LoginFacebook.php
auth.facebook.com.restway.net/id735rp/LoginFacebook.php
auth.facebook.com.restway.org/id735rp/LoginFacebook.php
auth.facebook.com.tastyfiles.net/id735rp/LoginFacebook.php
auth.facebook.com.vedivids.com/id735rp/LoginFacebook.php
auth.facebook.com.vedivids.net/id735rp/LoginFacebook.php
auth.facebook.com.vedivids.org/id735rp/LoginFacebook.php
auth.facebook.com.vediway.com/id735rp/LoginFacebook.php
auth.facebook.com.vediway.net/id735rp/LoginFacebook.php
auth.facebook.com.vediway.org/id735rp/LoginFacebook.php

Even in the same URL format strategy is being used by another known crimeware: Phoenix Exploit Pack.



Related information

[Zeus and the theft of sensitive information]

[Facebook & VISA phishing campaign proposed by ZeuS]

[New ZeuS phishing campaign against Google and Blogger]

[ZeuS on IRS Scam remains actively exploited]

[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
