

VIII Jornada Nacional de Seguridad Informática



El orden de los bits sí altera el producto:

Talón de Aquiles de los Antivirus

VIII Jornada Nacional de Seguridad Informática

Bogotá – Colombia

:: 2008 ::



**Luis Fernando González V.
CEH
iQ Outsourcing S.A
lfgonzalez@iq-online.com**

...iQ: :



VIII Jornada Nacional de Seguridad Informática



.... Objetivos

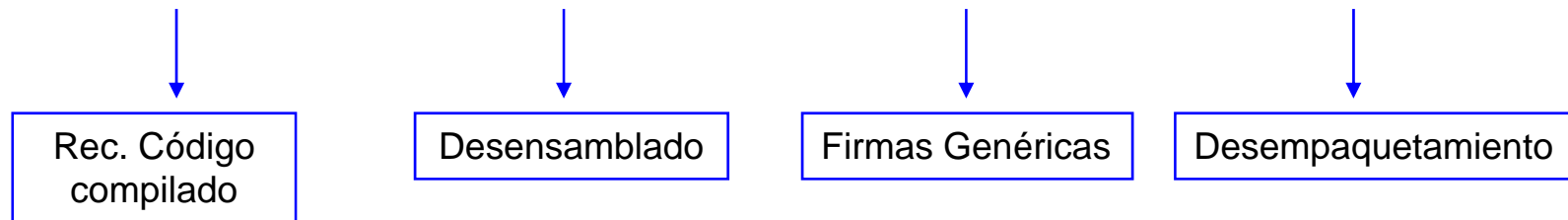
- Mostrar la debilidad de los antivirus, en base a la ejecución y resultados de una prueba de vulnerabilidad realizada a 27 de estos software.
- Evidenciar la necesidad de incluir en las evaluaciones y análisis de seguridad la plataforma antivirus.
- Demostrar la relevancia de las labores del hacker ético dentro de la organización (relación costo-beneficio).

.... Prueba de Vulnerabilidad

Surgió de la necesidad de evaluar el nivel de protección ofrecido por el software antivirus adquirido por la compañía.

Patrones Heurísticos

Técnicas que se emplean para reconocer códigos maliciosos (virus, gusanos, troyanos, etc.) que no se encuentren en la base de datos del antivirus (ya sea porque son nuevos, o por no ser muy divulgados).



Diapositiva 3

71 Viejo.

Mi consejo. Utiliza más imágenes que texto. Esto es lo que tu sabes. el hecho de poner tantas letras hace que el público se distraiga.

7141546, 05/06/2008

.... Herramientas

Herramienta Poison Ivy, orientada a prestar un servicio cliente servidor, su principal función es tomar el control total de la máquina víctima.

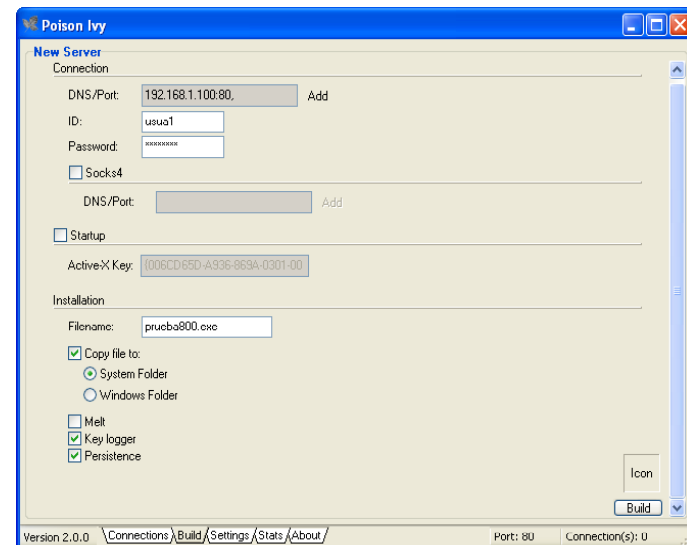
Archivo a encriptar:
 Examinar

Gardar como:
 Examinar

Tipo de encriptación

<input checked="" type="radio"/> Rijndael (AES)	<input type="radio"/> TEA
<input type="radio"/> Blowfish	<input type="radio"/> Twofish
<input type="radio"/> DES	<input type="radio"/> Xor
<input type="radio"/> Gost	<input type="radio"/> Eqv
<input type="radio"/> Skipjack	<input type="radio"/> Not

Archivo Ejecutable de 20KB



Archivo Ejecutable de 8KB

Herramienta "Crypter" que ofrece 10 distintos tipos de cifrado para evasión de antivirus.

Debe alterar el archivo virus dejándolo **funcional e indetectable**, de lo contrario "no sirve".

Diapositiva 4

72

Ser más claro. Mucha gente quedará lopca cuado le hables de conexión inversa remota. Entre más sencillo mejor.

7141546, 05/06/2008

VIII Jornada Nacional de Seguridad Informática



Se realizó un reemplazo del segmento en el archivo cifrado desde el offset 0 hasta el offset 25. (No se alteraron los dos primeros Offset (MZ) ni tampoco el 25 (@), de alterarse estos offset el archivo queda inservible)

Offset	Hex	ASCII
00000000	4D5A 9000 0300 0000 0400 0000 FFFF 0000	MZ.....
00000016	B800 0000 0000 0000 4000 0000 0000 0000@.....
00000032	0000 0000 0000 0000 0000 0000 0000 0000L!PE

Del offset 61 al offset 333 se realizó una inserción con datos predeterminados de otros archivos. Esta fracción hace parte de la firma genérica del Virus

Inserción de información empaquetada mediante UPX.

Diapositiva 5

74

Parte la gráfica y los pedazos los muestras, no toda la gráfica completa. Es decir tomas el primer pedazo y explicas, luego el segundo pedazo y luego el tercer. Si quieres ponle animación a la vaina pa que no se ve tan difícil de digerir.

7141546, 05/06/2008

VIII Jornada Nacional de Seguridad Informática



....Cifrado

El trabajo de cifrado se inicia desde el offset 621, dado que de hay en adelante se registra información primordial como la cadena de conexión del troyano, la ruta de alojamiento del mismo e información del proceso que obviamente hace parte de las características del virus y no debe ser detectado por el antivirus.

The screenshot shows the Hex Workshop interface with two windows: 'TroyanoCifrado_Des' and 'Virus'. The 'TroyanoCifrado_Des' window displays hex data in columns and ASCII data in a single column. The ASCII data starts at offset 621 and contains the following text:

```

g9d...U..Fp...+1
...X.J(E..IP..m.S.
T...mm...S.....!
.....x.....%p..j
.....#1.....51
...+*.....m...
Q..u..faP....hD
*#.....(.....)
...j...d@....A
...b...;@..l.%
I...3...[.....]a
2H'1.....)\t1.
d|.X...QH+...l.n.
.xvxS...hu.d.p
|.....$.tt...
2tpp.fc$.X.+d
XX X...x).T1.G.d
l.S...0...e.6...
{.Q.....p@...P.
*#...I) .x...d...
|.5...PE.w)2v...".
.E.(.s...T.Q.h...
\hv.&.H...HFS.v.
...f..7.+RE...f.
...x..J..N...>K.H.L
...U.R.m...E...
...8.../...2
...*.2.....
++H.N.B.2.....u
.+V.uv.....a...
...2.%u.wL...f.E
[PMA].../.....*P
*R1..b'.x>...h
...(2@.d16...f...
  
```

A red box highlights the ASCII data starting at offset 621, which contains the path 'prueba2.exe' and 'admin...admin'.

Diapositiva 6

75

Lo mismo, mucha letra....

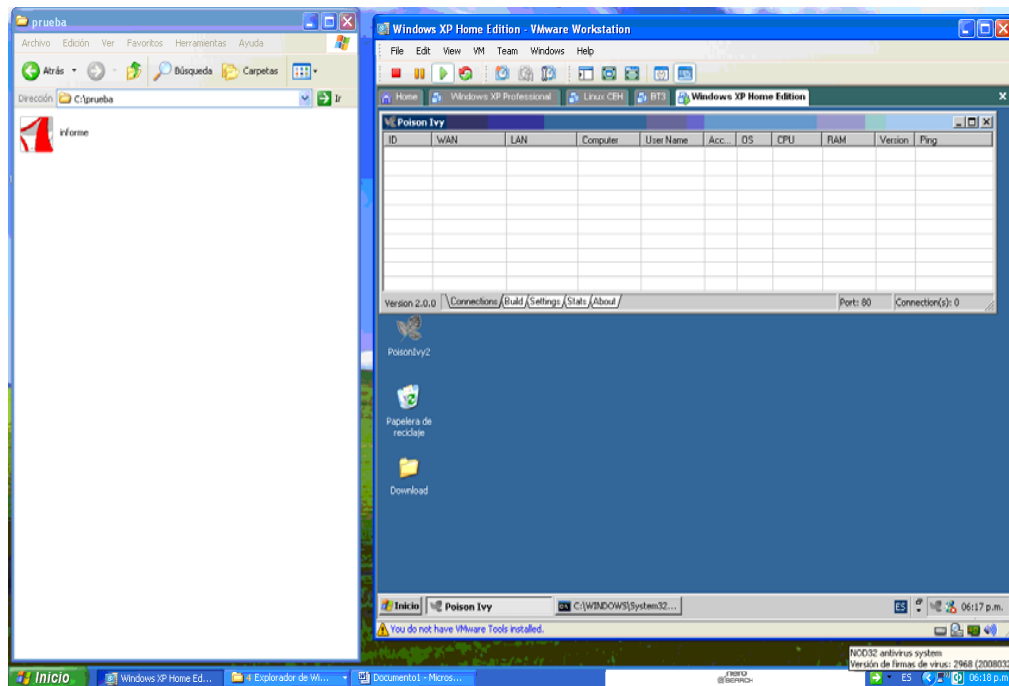
7141546, 05/06/2008

VIII Jornada Nacional de Seguridad Informática



.... Materialización del Riesgo

“De los 27 Software antivirus, solo 9 **NO** son vulnerables a estas amenazas, los 18 restantes por alguno de los 10 algoritmos de cifrado de virus pueden ser vulnerados”.

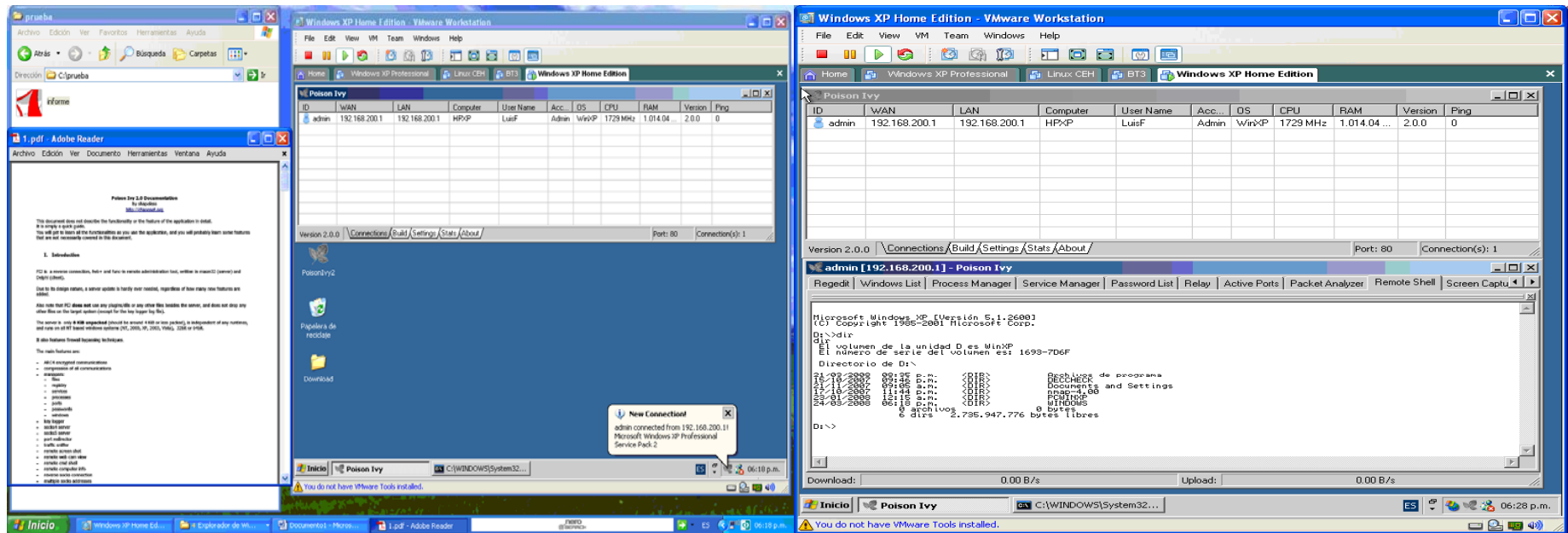


Archivo virus cifrado, enmascarado en un archivo PDF, al antivirus se esta ejecutando normalmente sin detectar la amenaza.

VIII Jornada Nacional de Seguridad Informática



.... Materialización del Riesgo



Se ejecuta el archivo virus, vulnerando los patrones "heurísticos" del antivirus, generando la conexi3n remota a la consola de administraci3n del troyano.

.... Conclusiones

Exigir al proveedor del antivirus alta calidad de servicio del producto adquirido.

78

✓ ¿Por qué tengo que actualizar la versión de mi antivirus para que me preste la funciones básicas?

✓ Lo ideal es actualizar únicamente los patrones de detección por firmas y heurísticos, sin importar la versión que se tenga.

Características Básicas: Análisis heurístico de alta capacidad, diversas técnicas de detección y análisis, actualización de firmas y patrones de detección en línea, protegido por contraseña, bajo consumo de recursos.

La plataforma Antivirus, un activo mas a involucrar en nuestras pruebas de vulnerabilidad.

✓ ¿Cómo?:

✓ Indagando ultimas vulnerabilidades en el mercado “underground”.

✓ Teniendo un área en la compañía que se encargue de evidenciar y explotar (en la medida de lo posible) la vulnerabilidad.

✓ Contando con personal éticamente calificado para desarrollar la función.

✓ Por un tercero.

Diapositiva 10

78

Mini checklist de que debe tener un antivirus. puntos más importantes.

7141546, 05/06/2008



VIII Jornada Nacional de Seguridad Informática

ACIS

.... Conclusiones

- ❑ Las pruebas de vulnerabilidad adquieren un valor comercial.
 - ✓ Vende la gestión de seguridad informática de la compañía ante los clientes.
 - ✓ Vende al área de seguridad Informática ante las demás áreas de la compañía.
 - ✓ Es un producto tangible, que tiene gran impacto dentro y fuera de la organización.
- ❑ El Hacker Ético toma importancia dentro la estructura de seguridad informática de la compañía.
 - ✓ Recurso dedicado que realiza las pruebas de vulnerabilidad y test de penetración en la compañía.
 - ✓ Es el encargado de monitorear la eficacia y eficiencia de los controles informáticos.
 - ✓ Realiza sus funciones desde tres enfoques:
 - ✓ Visión Técnica: Realizando evaluación de riesgos a la plataforma TI.
 - ✓ Visión de Seguridad: Realizando intrusión a los dispositivos.
 - ✓ Visión de Negocio: Realizando auditoria a los controles.
 - ✓ Replantea la seguridad como medida de mejoramiento en el proceso de gestión de la seguridad.

Ref: El valor del Hacker en la organización. Almanza Andres - VI JNSI

Diapositiva 11

77

Fuentes...

7141546, 05/06/2008



VIII Jornada Nacional de Seguridad Informática



.... Referencias

- ✓ “Pruebas de Vulnerabilidad”. Disponible en: <http://blownx.com/index.php/seguridad-informatica/44-seguridad-informatica/72-pruebas-de-vulnerabilidad>.
- ✓ Madantrax. “Cactus Methamorph”. Disponible en: <http://www.elhacker.net>
- ✓ BreakPoint Software. “Hex Workshop”. Disponible en: <http://www.bpsoft.com>.
- ✓ “The Anti-Virus or Anti-Malware Test File”. Disponible en: http://www.eicar.org/anti_virus_test_file.htm
- ✓ “Trece antivirus a examen”. Disponible en: <http://www.terra.es/tecnologia/articulo/html/tec6237.htm>
- ✓ Shapeless. “Poison Ivy”. Disponible en: <http://chasetnet.org>
- ✓ Nhaalckiemr. “Crypter”. Disponible en: <http://www.elhacker.net>
- ✓ Almanza Andrés. “El valor del hacker en la organización”. VI Jornada Nacional de Seguridad Informática.
- ✓ “Heurística en antivirus”. Disponible en: [http://es.wikipedia.org/wiki/Heur%C3%ADstica_\(antivirus\)](http://es.wikipedia.org/wiki/Heur%C3%ADstica_(antivirus))



VIII Jornada Nacional de
Seguridad Informática



Gracias
¿Preguntas?