

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: :

The banner features a dark blue background with a perspective view of a hallway made of binary code (0s and 1s) receding into the distance. A bright light source is at the end of the hallway. The text 'VIII Jornada Nacional de Seguridad Informática' is written in a bold, yellow, sans-serif font. To the right is the ACIS logo, which consists of a white square with a stylized arrow pointing right, followed by the letters 'ACIS' in a white, bold, sans-serif font.

VIII Jornada Nacional de Seguridad Informática



.... Objetivos

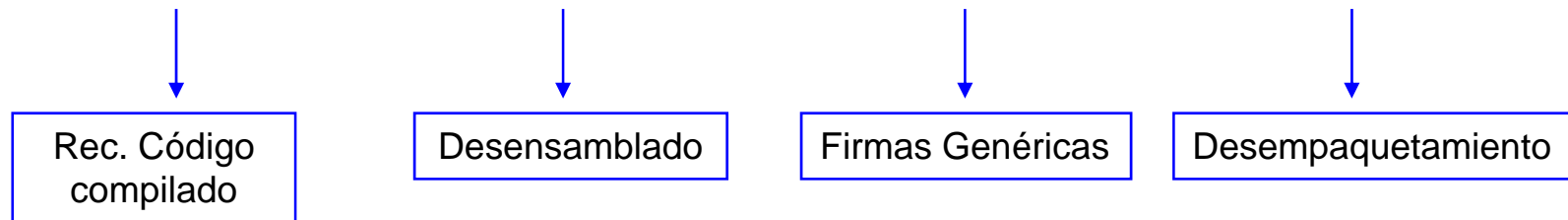
- Mostrar la debilidad de los antivirus, en base a la ejecución y resultados de una prueba de vulnerabilidad realizada a 27 de estos software.
- Evidenciar la necesidad de incluir en las evaluaciones y análisis de seguridad la plataforma antivirus.
- Demostrar la relevancia de las labores del hacker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

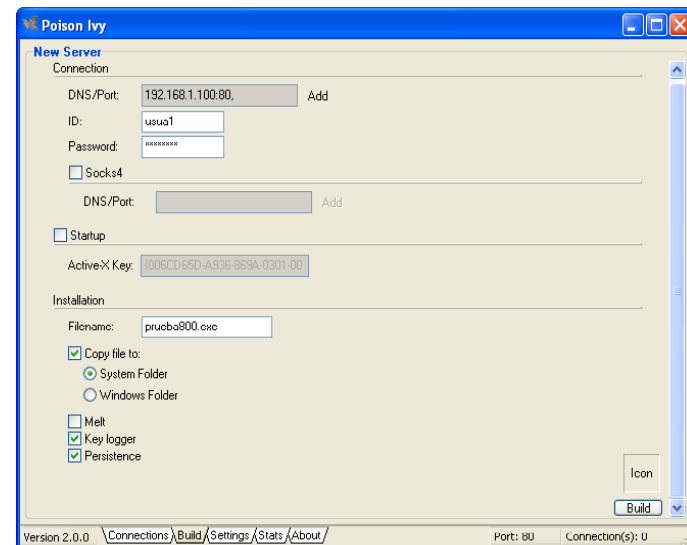
Archivo a encriptar:
 Examinar

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)

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.

```

Hex Workshop - TroyanoCifrado_Des
File Edit Disk Options Tools Window Help
B S L O F D
TroyanoCifrado_Des
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 .....

Virus
00000000 4D5A 0000 0100 0000 0200 0000 FFFF 0000 MZ.....
00000016 4000 0000 0000 0000 4000 0000 0001 0000 @.....
00000032 0E1F B409 BA0E 00CD 21B8 004C CD21 5045 !.L!PE
  
```

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 and ASCII data. An arrow points to the start of the encrypted data at offset 621. The 'Virus' window shows a list of offsets and their corresponding data, including file paths and process names.

Offset	Hex	ASCII
000006896	6739 6490 9494 5595 1646 701B 8D8C 2B31	g9d...U..Fp...+1
000006912	1108 58E4 4A28 4501 3150 879D 6DC2 5385	..X.J(E..1P..m.S.
000006928	545C 906D 6DC8 2090 5314 08B5 BDB1 CD21	T..mm. .S.....!
000006944	FDBC 0F8D 0CC8 78F7 B3A0 CDF7 2570 D16Ax.....%p..j
000006960	018D 950B 0823 6CA5 0CB1 FF7F F810 356C#1.....51
000006976	BEDD C82B 982A 09C0 0880 818D 6DCD D9F6	...+*.....m...
000006992	2051 2E00 75F4 6661 50D9 820D E1BE 6844	Q..u..faP....hD
000007008	2A70 2319 A8D3 F89F F595 9285 D77F 2885	*#.....(.
000007024	020F 8422 6A90 0699 6440 2E8C 8C8C 9041	...".j...d....A
000007040	8602 8888 0319 E480 8484 0DD7 1B90 0495b...;@..!%
000007056	0CF3 ADC3 8E62 C9EC 113B 4088 2182 2517	d .X...QH+...l.n.
000007072	4908 800B 33B2 9D5B B280 FDC4 6080 0A61	I...3...[.....a
000007088	8248 6060 2190 03F9 DE29 C45C 7C74 6C99	[2H'!.....)\ t1.
000007104	647C 8058 B78C 5148 2B84 94E4 21E4 6EC8xvxS...hu.d.p
000007120	6013 785C 7853 84C9 028F 6875 E664 1C70\$.tt..
000007136	211D B88C BAD3 0AC9 805C 2403 7474 830C2tpp.fc\$.X.+d
000007152	0532 7470 7090 6663 249F 8C58 932B E164	XX X...x).T1.G.d
000007168	5858 2058 9003 F978 299F 546C 0447 9B64	.S...0..e.6...
000007184	6CC4 539A 1F81 B030 B988 65A0 3698 86C4	{..Q.....p @...P.
000007200	7B88 5187 8289 848E 7020 400B D0C4 5004
000007216	6623 B71B 596A 2016 7811 0C17 64FB 3689	*#..I) ..x...d...
000007232	7CB8 35E8 0150 4598 7729 3276 F810 220D	..5...PE.w)2v..."
000007248	0545 983C 9873 87DB 1154 BC51 0768 8015	..E.(.s...T.Q.h...
000007264	5C68 76E6 26DD 1C48 0EB4 4866 53C9 76BB	\hv.&.H...HFS.v.
000007280	FB98 6683 C137 D12B C252 45BC B6B0 668B	..f..7.+RE...f.
000007296	BDB3 780F 8F4A 125C F9EB 3E48 2E48 854C	...x..J.N...>K.H.L
000007312	0502 1B55 BC52 8B6D E2E7 0445 D8EB 93D8	...U.R.m...E....
000007328	031D 0D9D C4DF 9B38 D83B 8D2F 0F8F F8328.../...2
000007344	1082 F52A 8D32 C80C C0C8 0DEE EEC6 F1BC	...*.2.....
000007360	2B2B 4814 4E8B 420C 327F D9BE 95D8 A475	++H.N.B.2.....u
000007376	BC2B 5611 7576 0C8A 1416 F6B6 611D FED2	..+V.uv.....a...
000007392	8A04 0832 C225 75CE 774C CBB2 0C66 2E45	...2.%u.wL...f.E
000007408	504D 415D 03EF 2F0C 10F6 D181 E12A 1D50	[PMA].../.....*P
000007424	2A52 6CC3 6227 8D72 3E1A 60E9 DE18 9C68	*R1'.b'.x>.....h
000007440	B385 285A 4019 6421 3614 BF28 C802 C9CB	...(2@.d16.../...

Diapositiva 6

75

Lo mismo, mucha letra....

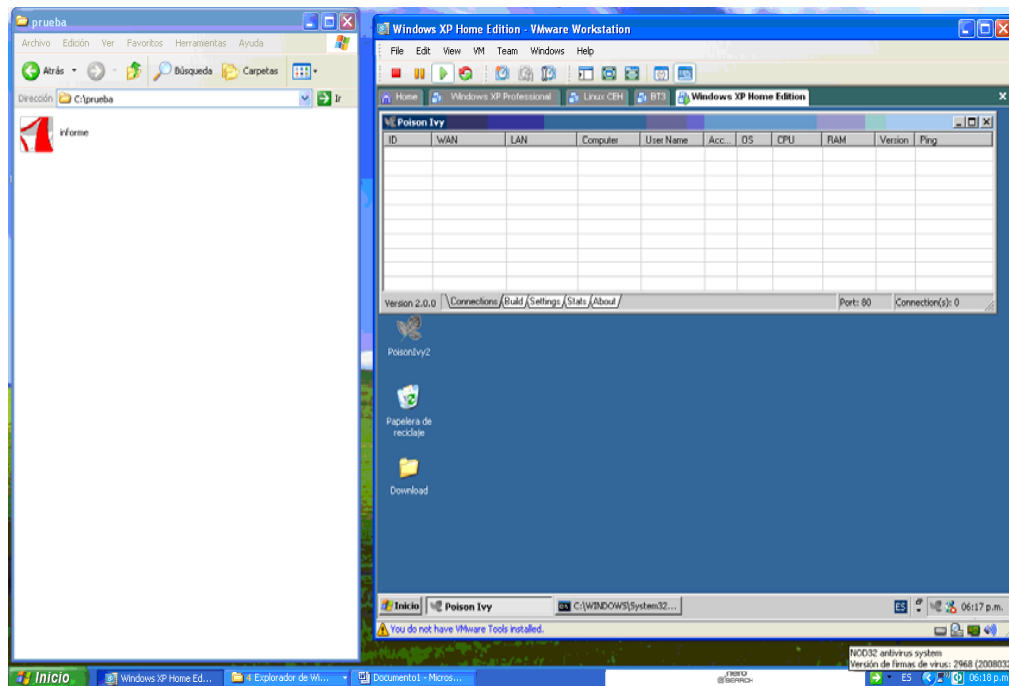
7141546, 05/06/2008

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

The screenshot displays a Windows XP Home Edition virtual machine running in VMware Workstation. The desktop environment includes a file explorer window showing a PDF document titled '1.pdf - Adobe Reader'. The document content is partially visible, showing a table with columns for ID, WAN, LAN, Computer, User Name, Acc, OS, CPU, RAM, Version, and Ping. The table lists an entry for 'admin' with IP addresses 192.168.200.1 and 192.168.200.1, and other details like 'HP-XP', 'LuisF', 'Admin', 'WinXP', '1729 MHz', '1.014.04...', '2.0.0', and '0'. A 'New Connection' dialog box is open, indicating a connection to 'admin' at IP 192.168.200.11. The taskbar shows the 'Inicio' button and several open applications, including 'Explorador de Windows', 'Documentos - Home...', and '1.pdf - Adobe Reader'. The system tray shows the time as 06:18 p.m. and a warning that VMware Tools are not installed.

Se ejecuta el archivo virus, vulnerando los patrones “heurísticos” del antivirus, generando la conexión remota a la consola de administración 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



.... 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?