Que Tipo De Virus Esconde Las Paginas De La Deep Web

CondarGuisbert Alison Paola
Universidad Mayor de San Andrés
Facultad de Ciencias Puras y Naturales
Carrera de Informática
Análisis y diseño de Sistemas de Información
alison_pao@hotmail.es

RESUMEN

En resumen un virus informático tiene como objetivo alterar el funcionamiento de una computadora, sin el permiso del usuario. Por lo general estos virus, suelen reemplazar archivos ejecutables del sistema por otros infectados con la intención de modificarlos para destruirlos de manera intencionada .Aunque no todos son dañinos existen algunos que son mas inofensivos ya que solamente son molestos.

En la Deep Web encontramos muchos tipos de virus la mayoria son muy dañinos ya que se encuentran los hackers y creadores de virus que solo por visitar su pagina tu computadora quedara destruida por la gran cantidad de virus infeccioso que lograra infiltrarse en tu computadora ya que ese es el plan que tienen tratar de controlar tu maquina o destruirla muchos de los que controlan son troyanos que logran hackear tu computadora controlando tus parlante, microfono, camara web y tus archivosos ademas de controlar tus paginas sociales como facebook y twitter logrando ver tus mensajes y contactos asi que debemos tener mucho cuidado en visitar la deep web.

Palabras Clave

Virus, hackers, Troyanos.

1. INTRODUCCION

Su origen se remonta a 1959 en los laboratorios de la Bell Computer donde tres jovenes programadores (Robert Thomas Morris, Douglas Mclory y Victor Vysottsky) desarrollaron un programa al que llamaron CoreWar el cual consisitia en un juego q ejecutaba una orden cadavez y el que llene primero la memoria del computador ganaba lo cual causaba un poco de desorden.

En 1980 la red ArpaNet emitio extraños mensajes que aparecian y desparecian en forma aleatoria. En el comienzo de 1986 empezo la gran epidemia donde se difundieron losvirus Brain, Bouncing Ball y Marihuana estos virus solo infectaban el sector de arranque de los disquetes posteriormente aparecen los virus con extension COM y EXE.

Ahora, los hackers profesionales pertenecen a bandas criminales o agencias de espionaje, para realizar robo de información o destrucción con un propósito, los daños son mayores y algunos de los malware son capaces de afectar la producción de industrias(aquí es donde los enemigos de las emprensas grandes que quieren ver destruida a tales mpresas deciden comprar virus infortaticos a las bandas delincuenciales formadas por hackers y lograr infiltrar un virus que destruya la informacion importante de la empresa lo que puede provocar q la empresa caiga en banca rota o lograr un daño irreparable) y el funcionamiento de bancos (logrando algunos hacker robar grandescantidades de dinero) y agencias gubernamentales(en este caso lograr tener informacion confidencial del gobierno).

Los virus informaticos son amenazas es un pequeño programa que puede instalarse en tu computadora sin que el usuario otorgue permiso alguno. Estos son programas parasito que elimina datos, robainformacion o en el peor delos casos malogra el ordenador (bios, placa, disco duro, etc.) o al sector de arranque otros logran replicarse (propagarse) mientras que otros pueden producir serios daños afectando al sistema. Algunos logran migrar infectando usb, discos,etc para infectar otros ordenadores. Algunos de los virus residen en la memoria de la pc para evitar ser eliminado por el antivirus o se auto- encapsula para burlarlos.

2. TIPOS DE VIRUS

2.1. EL GUSANO: ILOVEYOU(VBS/LOVELETTER O LOVE BUG WORM)

Es un virus de tipo gusano, muchas computadoras se han visto infectados por este gusano.

Su apariencia en forma de correo es un mensaje con el tema: “ILOVEYOU” y el fichero adjunto LOVE-LETTER-FOR-YOU.TXT.vbs aunque la extensión “vbs” (Visual Basic Script) puede quedar oculta en las configuraciones por defecto de Windows, por lo cual la apariencia del anexo es la de un simple fichero de texto.

Cuando se abre el archivo infectado el gusano infecta nuestra máquina y se intenta auto enviar a todo lo que tengamos en las agendas de OutLook (incluidas las agendas globales corporativas).

Su procedencia es Manila Filipinas y el autor se apoda Spyder.

2.2. EL VIRUS: MYDOOM (W32.MYDOOM@MM, NOVARG, MIMAIL.R O SHIMGAPI)

Este virus utiliza asuntos, textos y nombres de adjuntos variables en los correos en los que se envía, por lo que no es posible identificarlo o filtrarlo fácilmente, y utiliza como icono el de un fichero de texto plano para aparentar inocuidad.

Tiene capacidades de puerta trasera que podrían permitir a un usuario remoto controlar el ordenador infectado, dependiendo de la configuración de la red y del sistema.

2.3. EL GUSANO: BLASTER (LOVSAN O LOVESAN)

Se trata de un virus con una capacidad de propagación muy elevada.

Se trata de una vulnerabilidad para la que hay parche desde Junio de 2003, todos los usuarios que no hayan actualizado su sistema desde esa fecha deberían hacerlo inmediatamente. Por otra parte se propaga usando el puerto TCP 135, que no debería estar accesible en sistemas conectados a Internet con unos cortafuegos correctamente configurado.

Los efectos destructivos consisten en lanzar ataques de denegación de servicio con el web de Microsoft "Windows update" y quizás provocar inestabilidad en el sistema infectado.

2.4. EL GUSANO: SOBIG WORM

Gusano de envío masivo de correo cuya propagación se realiza a todas las direcciones electrónicas encontradas dentro de los ficheros de extensiones: .txt, .eml, .html, .htm, .dbx, y .wab. El correo en el que se propaga el gusano parece como si fuese enviado por "big@boss.com".

También realiza copias de sí mismo en máquinas remotas a través de recursos compartidos en red.

2.5. EL GUSANO: CODE RED

Este virus al atacar configuraciones más complejas, que no son implementadas por el usuario final, tuvo menor impacto que el Sircam. Cabe destacar las 2 mutaciones basadas en este virus que circulan por Internet,Codered.C y el Codered.D , que utilizan su misma técnica variando su carga destructiva.

2.6. EL VIRUS: CIH (CHERNOBYL O SPACEFILLER)

El código fuente del virus CIH (capaz de sobrescribir en determinadas circunstancias el BIOS y dejar la máquina absolutamente inoperante), los más diversos kits de creación de virus y otras tantas linduras están al alcance de todo mundo en Internet. Esta información alienta a otros programadores de virus a generar otros, e incluso a auténticos aficionados ("lamercillos" y crackers) a sentirse como niños en dulcería con el simple hecho de jugar con estas cosas.

2.7. EL GUSANO: KLEZ

Este virus explota una vulnerabilidad en el Internet Explorer por la cual es capaz de auto ejecutarse con solo visualizar el correo electrónico en el que llega como adjunto. El virus es capaz de impedir el arranque del sistema y de inutilizar ciertos programas.

2.8. EL GUSANO: MELISSA ("MAILISSA", "SIMPSONS", "KWYJIBO", O "KWEJEEBO")

El virus es conocido como W97M_Melissa o Macro.Word97.Melissa. Nos puede llegar en un archivo adjunto a un mensaje electrónico, enviado por alguien conocido (como el Happy99). Dicho mensaje, incluye en asunto (en inglés): "**Importantmessagefrom…**" (Mensaje importante de…) y en el cuerpo del mensaje: "**Hereisthatdocumentyouaskedfor …don't show anyoneelse ;)**", donde se indica que dicho documento fue solicitado por usted (y que no se lo muestre a nadie más).

Este virus infecta a MS Word y éste a todos los archivos que se abren, cambia ciertas configuraciones para facilitar la infección, se auto-envía por correo, como un mensaje proveniente del usuario a la primera 50 buzones de la libreta de direcciones de su correo.

2.9. EL GUSANO: SASSER (BIG ONE)

Gusano que para propagarse a otros equipos, aprovecha la vulnerabilidad en el proceso LSASS (Local Security AuthoritySubsystem). Sólo afecta a equipos Windows 2000/XP y Windows Server 2003 sin actualizar.

Los síntomas de la infección son: Aviso de reinicio del equipo en 1 minuto y tráfico en los puertos TCP 445, 5554 y 9996.

2.10. EL GUSANO: BAGLE (BEAGLE)

Gusano que se difunde mediante el envío masivo de correo electrónico a direcciones que captura de diversos ficheros en la máquina infectada. Utiliza un truco de ingeniería social muy simple pero efectiva, consistente en hacerse pasar por un mensaje de prueba con un fichero adjunto que usa el icono de la calculadora de Windows, lo que parece que hace pensar a las víctimas que es inofensivo.

Además de las molestias que causa la rutina de envío masivo de correo, lo que hace más peligroso a este gusano es su capacidad de puerta trasera. El gusano se queda residente en la máquina infectada y aguarda comandos de un usuario remoto no autorizado, que podría obtener control total del sistema infectado, dependiendo de la configuración del sistema y de la red.

Está programado para dejar de funcionar el día 28 de Enero de 2004. El gusano obtiene la fecha del PC infectado (que podría ser incorrecta) y termina su ejecución si ésta es posterior al 28 de Enero.

2.11. EL VIRUS: WIN32/SIMILE (ETAP)

Son los primeros virus híbridos que han aparecido, capaces de atacar tanto sistema Linux como Windows.

Frethem es un gusano muy engañoso que suele tener como asunto “Re: Yourpassword!”. Es muy fácil infectarse con él, ya que el virus se activa automáticamente con lapre visualización del mensaje en el Outlook Express.

2.12. EL GUSANO: NIMDA

Gusano troyano que emplea tres métodos de propagación diferentes: a través del correo electrónico, carpetas de red compartidas o servidores que tengan instalado IIS (empleando el “exploit” Web DirectoryTraversal). Descarga en el directorio C:\Windows\Temp un fichero (meXXXX.tmp.exe, un correo en el formato EML) que contiene el fichero que será enviado adjunto por el gusano.

3. LOS CINCO HACKERS NEGROS DE LA DEEP WEB

Internet está inundado de hackers conocidos como "crackers" o "blackhats" ("sombreros negro" que trabajan para explotar sistemas informáticos. Ellos son los que has visto en las noticias que son alejados de una computadora para evitar que incursionen nuevamente en ciber-crímenes. Algunos de ellos lo hacen por diversión y curiosidad, otros para beneficio económico personal.

3.1. JONATHAN JAMES.

James ganó notoriedad cuando se convirtió en el primer adolescente que era enviado a prisión acusado de Hacking. El fue sentenciado a seis meses cuando tenía solo 16 años de edad.

Las más importantes intrusiones de James tuvieron como objetivo organizaciones de alto grado, instaló un backdoor en un servidor de la Agencia de Reducción de Amenazas de la Defensa del Pentágono (DRTA).

El backdoor que él creó le permitió ver e-mails de asuntos delicados y capturar los nombres de usuario (username) y clave (passwords) de los empleados.

También crackeó las computadoras de la NASA robando software por un valor aproximado de 1.7 millones de dólares. Según el Departamento de Justicia, "entre elsoftware robado se encontraba un programa utilizado para controlar el medio ambiente -temperatura y humedad- de la Estación Espacial Internacional". La NASA se vio forzada a tener que paralizar 21 días sus computadoras.

3.2. ADRIAN LAMO.

Saltó a la fama por sus intrusiones a organizaciones mayores comoThe New York Times and Microsoft. Bajo el apodo de homeless hacker ("hacker sin hogar", el usó conexiones como Kinko (cafés Internet), tiendas café y librerías para hacer sus intrusiones.

Las acciones de Lamo mayormente consisten en "pruebas de penetración", en las que encuentra defectos de seguridad, los explota y luego envía un informe a las compañías de sus vulnerabilidades. Sus logros incluyen Yahoo!, Bank of America, Citigroup yCingular. Cuando los whitehat hackers son contratados por las compañías para hacer "pruebas de penetración" (penetration test) es legal.

Cuando Lamo rompió el sistema de seguridad de la Intranet de The New York Times las cosas se pusieron serias, se añadió a la lista de expertos que veía información personal de los contribuidores, incluyendo los números de Seguro Social. Lamo también hackeó las cuentas LexisNexis de The Times para la investigación de temas de interés.

Por su intrusión al New York Times, fue obligado a pagar 65 mil dólares de reparación. También fue sentenciado a seis meses de arresto domiciliario y dos años de libertad

condicional, que expiraron el 16 de enero del 2007. Actualmente trabaja como periodista y locutor público.

3.3. KEVIN MITNICK

El Ministerio de Justicia lo describe como "el criminal de PC más querido en la historia de los Estados Unidos." Sus proezas fueron detalladas en dos películas: FreedomDowntime y Takedown.

En realidad es un Phreaker considerado por muchos como "el mejor phreaker de la historia". Empezó explotando el sistema de tarjeta perforada de los autobuses de Los Ángeles para conseguir paseos libres (gratis).

Aunque hubieron numerosos delitos, Mitnick fue condenado en última instancia por hackear la red del ordenador de Digital Equipment y robar el software.

También, fue acusado de robo de software, fraude electrónico, daño a los ordenadores de la Universidad del Sur de California, robo de archivos e intercepción de mensajes de correo electrónico, por lo que pagó una condena de cinco años. Entre las compañías afectadas figuraban Nokia, Fujitsu, Nec, Novell, Sun Microsystems, Motorola, Apple.

En la actualidad, Mitnick, además de ser consultor de seguridad, se dedica a dar conferencias sobre protección de redes informáticas e ingeniería social.

3.4. KEVIN POULSEN.

También conocido como "Dark Dante", ganó reconocimiento cuando hackeó las líneas telefónicas de la radio de Los Ángeles "KISS FM", con lo cual obtuvo ganancias para comprarse un Porsche. Las fuerzas del orden lo apodaron "El HannibalLecter del crimen informático".

Las autoridades comenzaron a perseguir a Poulsen después que hackeara una base de datos de investigación federal. Otra hazaña fue cuando reactivó los números viejos deYellowPages (Páginas Amarillas). Después de que su foto saliera en el programa de "Misterios sin Resolver", las líneas 01-800 del programa quedaron inhabilitadas. Finalmente fue capturado en un supermercado y cumplió cinco años de condena.

Desde que fue liberado Poulsen ha trabajado como periodista, ahora es un redactor reconocido de Wired News.

3.5. ROBERT TAPPAN MORRIS.

Es hijo de un científico de la Agencia Nacional de Seguridad, y conocido como el creador del Gusano Morris, el primer gusano desencadenado en Internet.

Morris escribió el código del gusano cuando era estudiante de CornellUniversity. Su intención era usarlo para ver que tan largo era Internet, pero el gusano se replicaba excesivamente, haciendo las computadoras demasiado lentas.

Se habló de cientos de millones de dólares de pérdidas y de un 10% de Internet colapsado, Morris fue juzgado en enero de 1990 y condenado a 3 años en libertad condicional, una multa de 10 mil dólares y 400 horas de trabajo de servicio a la comunidad.

Actualmente trabaja como profesor de ciencias de la computación en el Instituto Tecnológico de Massachusetts (MIT) y en el laboratorio de Inteligencia Artificial.

4. LOS CINCO HACKERS BLANCOS DE LA DEEP WEB

Los hackers que usan sus habilidades para el bien son clasificados como White Hat. Estos "sombrero blanco" trabajan a menudo bajo la clasificación de "Hackers Éticos Certificados" y son contratados por las compañías para probar la seguridad de sus sistemas.

4.1. STEPHEN WOZNIAK.

"Woz" fundó Apple Computer junto con Steve Jobs en 1976 y creó los ordenadores Apple I y Apple II a mediados de los años setenta. Fue premiado con la Medalla Nacional de Tecnología así como doctorados honorarios de la KetteringUniversitiy y de la Nova SoutheasternUniversity, además fue nombrado para el Salón de la Fama de los Inventores del País, en Septiembre del año 2000.

Woz empezó a hackear haciendo cajas azules (blue boxes) las cuales lograban imitar los sonidos del teléfono de ésa época logrando así llamadas gratuitas de larga distancia. Después de leer un artículo de "phonepreaking", llamó a su amigo Steve Jobs, y los dos investigaron sobre frecuencias, luego construyeron y vendieron blue boxes a sus compañeros de clase.

Los dos amigos vendieron un prototipo de una calculadora científica para tener capital, y trabajaron en hacer prototipos en el garage de Steve Jobs. Wozniak diseñó el hardwarey casi todo el software. Y vendieron las primeras 100 Apple a un comprador local por 666 dólares cada una.

4.2. TIM BERNERS-LEE.

Sir Timothy "Tim" John Berners-Lee KBE (TimBL o TBL) es el creador de la Word Wide Web (WWW). Nacido el 8 de junio de 1955 en Londres Inglaterra, se licenció en Física en 1976 en el Queen'sCollege de la Universidad de Oxford. Trabajando como investigador en el Laboratorio Europeo de Física de Partículas (CERN) de Ginebra, concibió la idea de un proyecto de hipertexto global, que años más tarde se convertiría en la WWW.

Del 1991 al 1993 contribuyó al diseño de la Web: las especificaciones iniciales de "HTTP" y de "HTML", un "hipertexto" que permite la publicación de documentos. El año 2002 fue premiado con el Premio Príncipe de Asturias de Investigación Científica y Técnica. Mientras que en el año 2004 gana el primer Premio de Tecnología del Milenio.

4.3. LINUS TORVALDS.

Es el padre de Linux. Se llama a sí mismo "un ingeniero", y dice que aspira a algo simple, "solo quiero divertirme haciendo el mejor endemoniado sistema que pueda".

Creó el kernel/GNU de Linux en 1991, usando un sistema operativo llamado Minix como inspiración. Empezó con un "taskswitcher" en una Intel 80386 ensamblada y un periférico terminal.

Actualmente trabaja para el Open SourceDevelopmentLabs en Beaverton, Oregon. Sólo el 2% del código del Linux actual está escrito por él, pero en su persona sigue descansando la paternidad de este núcleo del sistema operativo.

4.4. RICHARD STALLMAN.

Su fama viene de la fundación del código abierto, es conocido como el padre del Software libre, en su biografía dice: "El software no libre mantiene a usuarios divididos y desamparados, prohibido para compartirlo e incapaz cambiarlo. Un sistema operativo libre es esencial para que la gente pueda utilizar las computadoras en la libertad".

Comenzó en hackeo en el MIT. Él criticaba el acceso restringido a las computadoras en el laboratorio. Cuando un sistema de passwords era instalado, Stallman lo rompía, y reseteaba los passwords como cadenas nulas, o "nullstrings", luego enviaba a los usuarios, informándoles que ya no había sistema de contra señas.

Actualmente trabaja en contra de movimientos como Digital Rights Management o como él lo llama Digital Restrictions Management, a través de organizaciones como Free Software Foundation y League forProgrammingFreedom.

4.5. TSUTOMU SHIMOMURA.

Fue un físico experto en seguridad conocido por colaborar con John Markoff y ayudar al FBI a arrestar a Kevin Mitnick. Shimomura buscó, encontró y desenmascaro a Kevin Mitnick, el cracker/phreaker más famoso de USA, a principios de 1994. Ha trabajado como consultor del FBI, la fuerza aérea y de la agencia de la seguridad nacional (NSA).

Figura1. El virus por la red

5. CONCLUSION

En conclusión podemos decir que muchas computadoras en todo el mundo a sufrido alguna vez el llenado de virus a su sistema por algún correo no identificado pero lo que aquí vemos es que muchas de las páginas de la DepWeeb tienen virus creados por algunos hackers por eso es recomendable no abrir paginas cifradas ya que esta contienen una gran cantidad de virus que podrían volver obsoleta a tu computadora.

6. BIBLIOGRAFIA

- http://jpmejarvis.blogspot.com/2013/10/virus-informaticos-los-mas-peligroso-y.html#!/2013/10/virus-informaticos-los-mas-peligroso-y.html
- http://surfeaweb.blogspot.com/2014_03_01_archive.html
- http://es.slideshare.net/farodin/presentacin-para-slideshare-36863026