UNIVERSIDAD DE GUADALAJARA

CENTRO UNIVERSITARIO DE CIENCIAS EXACTAS E INGENIERIAS
DEPARTAMENTO DE CIENCIAS COMPUTACIONALES

MATERIA:
SEGURIDAD DE LA INFORMACION

MAESTRO:
FRANCO LOPEZ VELARDE, EMMANUEL

TITULO DE INVESTIGACIÓN:
ACTIVIDAD 1: INVESTIGACIÓN DEL CASO ISRAEL O VIERNES 13

FECHA ENTREGA:
LUNES 20 DE AGOSTO 2018

ALUMNO:
FELIPE DE JESUS RUIZ GARCIA

CODIGO:
214522077

CARRERA: INGENIERIA INFORMATICA (INNI)

SECCION: D02

CALIFICACIÓN Y OBSERVACIONES:

Indice

[INVESTIGACION] Caso Israel o viernes 13.

Es el virus más conocido dentro y fuera del mundo de la informática, debido a su gran difusión y al protagonismo que adquiere en los medios informativos cada vez que se acerca un viernes con la fecha trece. Su gran expansión se debe a que respeta las funciones habituales de los programas que lo albergan. La primera versión fue descubierta en diciembre de 1987 en las computadoras de la Universidad Hebrea de Jerusalén.

El descubrimiento se debió a lo que se supone un fallo en el diseño del programa. El virus no detectaba los programas .EXE contaminados y, por tanto, volvía a infectarlos. Cada vez, su tamaño crecía unos 2 Kb, hasta que estos alcanzaban un tamaño imposible de manejar por el sistema operativo DOS. El resto de los programas ejecutables sólo se infectaban una vez. Si un programa contaminado se ejecutaba, el virus pasaba a la memoria de trabajo de la computadora y, a partir de ese momento, se contaminaba cualquier programa que se ejecutase.

El virus, totalmente desconocido, se extendió por Israel rápidamente, debido principalmente a que este país dispone de extensas y potentes redes de computadoras. Las computadoras personales mostraban claros síntomas de un mal funcionamiento, manifestaban lentitud y largo tiempo de respuesta. Debido a su tamaño, algunos programas no podían ejecutarse por falta de espacio suficiente en la memoria de trabajo. Estos síntomas llevaron a los expertos, pertenecientes a la Universidad Hebrea, a investigar el fenómeno, hasta que a finales de diciembre de 1987, dieron con el virus. Pudieron así, desactivar la pequeña bomba de relojería cuya detonación estaba preparada para el 13 de mayo de 1988. Su objetivo era borrar programas militares y científicos, así como innumerables programas pertenecientes a los usuarios de computadoras personales. La vacuna preparada por los expertos de la Universidad Hebrea redujo considerablemente sus efectos.

Existen dos teorías sobre el origen y el objetivo principal del virus. Ambas hacen referencia a su fecha de activación. La primera de ellas, y más convincente, se deduce de las instrucciones relativas a la obtención de la fecha de la computadora para su comparación con la fecha de activación. El programa ignora todos los posibles viernes con fecha trece que pudieran existir en 1987, año en que se dedicaría únicamente a la multiplicación y propagación. Esta teoría, atribuida a un origen político, juega con la posibilidad de que el virus fuese un nuevo tipo de arma lógica creada contra el pueblo judío, posiblemente por seguidores palestinos. El l primer viernes trece del año 1988 fue en el mes de mayo y coincidió con el cuadragésimo aniversario del final de la guerra de Yom Kippur. Las consecuencias de dicha guerra fueron la desaparición de Palestina y la constitución del estado de Israel el 14 de mayo. Por tanto, el 13 de mayo de 1988 se celebraba el cuadragésimo aniversario del último día de la existencia de Palestina.

La segunda de las teorías, menos difundida, asegura que las especulaciones de la anterior son pura coincidencia. Basa la existencia del Viernes13, tanto en Israel como en Estados Unidos, en que ellos son países con extensas redes de telecomunicaciones, y no a consecuencia de un objetivo político. Se ampara en que esta fecha es símbolo de la mala suerte para la cultura anglosajona, como lo es en España, el martes13.

La razón de que el virus no se activase durante el año 1987 se debe a la necesidad de una etapa de incubación. Si el virus hubiera actuado en el mismo momento en que infectó un programa, su efecto sería mínimo. Además, al detectarse con rapidez, pudiera haberse descubierto a su creador. Por eso, su programador extendió el período de incubación a un año en espera de que su alcance fuera el mayor posible.

Y asi aparecieron los antivirus...

1988, este año será recordado siempre entre los expertos en seguridad informática como "el año en el que empezó el baile". De hecho, fue el año en el que comenzaron a aparecer los fabricantes de anti-virus, creando una moda de lo que en principio sólo era un problema potencial. Los vendedores de software anti-virus eran pequeñas compañías, que ofrecían sus productos a muy bajo precio, en algunos casos gratuitamente. Fue en este año cuando la compañía IBM se dio cuenta de que tenía que tomarse el asunto de los virus completamente en serio. Esta conclusión no la tomaron debido a la incidencia del popular 'gusano del árbol de Navidad', de amplia difusión, sino porque IBM sufrió un brote del virus 'Cascade', y se encontró en la embarazosa necesidad de tener que comunicar a sus clientes que ellos

también habían sido infectados. Desde este momento, el 'High Integrity Laboratory' de IBM fue el encargado del área virus.

En 1988 aparecieron, desde luego, múltiples rebrotes de 'Brain', 'Italian', 'Stoned', 'Cascade' y 'Jerusalem'. Esto representó la prueba definitiva de la existencia real de los virus. Peter Norton, en una entrevista, había comentado que eran una leyenda urbana, como los cocodrilos de las alcantarillas de Nueva York, y un experto informático del Reino Unido llegó a proclamar que tenía la prueba de que los virus eran un producto de la imaginación de mentes calenturientas...

En aquel momento, cada nueva aparición de virus provocaba la aplicación de un análisis paso-a-paso. El software existente era utilizado para detectar virus de sector de arranque, y solamente fue escrito un programa anti-virus, de manera excepcional, para afrontar los rebrotes de 'Cascade' y 'Jerusalem'. Entonces apareció el virus "B", el cual no se alojaba en memoria residente, y resultó ser una modificación de aquel que borraba los archivos todos los viernes y 13. Cuando 'Virus-B' se ponía en funcionamiento, desplegaba el siguiente mensaje:

"Warning! This program is infected with Virus-B! It will infect every .COM file in the current sub directory!".

Un virus que se manifiesta de una manera tan obvia, obviamente no puede ser tan pernicioso: evidentemente, se trata de la demostración de la forma de actuación de un virus, de ahí el mensaje.

A finales de 1988 se dieron varios sucesos importantes. En primer lugar, se produjo la aparatosa intrusión del virus 'Jerusalem' en una importante institución financiera, que durante varios días se vio en la necesidad de 'limpiar' a conciencia sus bases de datos. Por otro lado, la compañía S&S; impartió el primer 'Seminario sobre Virus', en el cual se explicó pormenorizadamente lo que era un virus y de qué forma actuaba. Por último, en enero del año siguiente rebrotó otra vez 'Jerusalem', como todos los viernes y 13, y se difundió ampliamente en diversas empresas e instituciones... Estaba clara la necesidad de una herramienta que permitiera limpiar masivamente los sistemas de cualquier virus en activo. El doctor Alan Solomon, consciente de esta necesidad, desarrolló un anti-virus, le añadió algunas herramientas que, según su experiencia, podían ser útiles, y creó de esta forma la primera herramienta anti-virus, 'Dr. Solomon's Anti-Virus Toolkit'.

A finales de 1988, 'Jerusalem' se había difundido de forma espectacular por España y Reino Unido.Debido al comportamiento destructivo de este virus, los expertos llegaron a la conclusión de que era necesario habilitar algún tipo de alarma para alertar a los usuarios. Pero los medios de comunicación también entraron en el juego: la posibilidad de predecir la aparición de un virus cautivó su imaginación, y de esta forma la actividad de los virus informáticos traspasó las fronteras de las universidades y empresas de informática y llegó al usuario habitual de PCs.

Y se reduce el tiempo de incubacion del virus.

El mismo Viernes 13 fue una de esas versiones mejoradas que cada día 13 del mes eliminaba todos los archivos infectados, lo que producía el terror para muchos usuarios esperando a que el siguiente mes su equipo no hubiera sido afectado. Además, aumentó el ataque a las extensiones.
La primera version de Viernes 13 solo infectaba .EXE y .COM y en su siguiente version se extendio a infectar tambien archivos .OVL, .SYS, .BIN y .PIF.

Viernes 13 fue también de alguna manera el primer virus “famoso”, con él entraron en juego los medios de comunicación, ávidos de noticias en el sector y fascinados por la naturaleza y poder de un virus.

[CONCLUSION] Seguridad hoy es.

En esta noticia, viernes 13, podemos contemplar la seguridad como un **todo**: la evolucion de la informatica cambio con la introduccion del internet, donde el principal objetivo de las aplicaciones era la funcionalidad, dejando de lado la proteccion y seguridad de la informacion y fue asi como se introdujeron los primeros hackeos en el mundo conectado.
Actualmente todo esta conectado, la evolucion del hardware llevo al software a procesar grandes cantidades de informacion, informacion disponible a todos : por ejemplo, yo estudiante, tengo un codigo de estudiante, mediante el cual, con ese simple codigo se podria obtener toda la informacion sobre mi, quien soy ? Donde vivo ? Cuantos años tengo ?. Todo!
La evolucion fue del hardware y software tambien marco la evolucion de la seguridad y claro, como en todo lo que no se planea, **se aprendio a la mala, en todos los ambitos, Desde sql Injection hasta aplicar algoritmos de fuerza bruta.**

Seguridad hoy es la vida: Esta presente en todos los ambitos de nuestra vida, y dependemos de ella:
Desde los autos autonomos, robots en el sector de salud, telefonia movil, cuentas bancarias... Todo esta en bases de datos.
Es por ello que el dia de hoy han cobrado un papel tan pero tan necesario en el mundo de la tecnologia.

[NOTICIA: 29 de junio, 2018]
Vulnerabilidad en repo de Gentoo.

Gentoo es una de las distribuciones Linux (aunque también hay una implementación con FreeBSD) con más historia, y destaca por la instalación de una gran cantidad de paquetes y aplicaciones mediante la compilación del código fuente a través de una gestión de los paquetes realizada por Portage, cuya implementación para línea de comandos se llama Emerge

Según informan nuestros compañeros de MuyLinux, la comunidad que está detrás de esta distribución anunció ayer que una cuenta de uno de los encargados del repositorio de GitHub fue hackeada. Esto fue utilizado por parte de los ciberdelincuentes para comprometer el código alojado ahí, modificando los árboles de Portage y musl-dev con versiones maliciosas de los ebuilds en un intento de eliminar todos los ficheros de los usuarios.

Ebuild es un conjunto de scripts en Bash creados por los desarrolladores de Gentoo que se encarga de automatizar los procesos de compilación e instalación de los paquetes de software, siendo un componente fundamental junto con Portage. Si bien se sabe exactamente qué componentes terminaron comprometidos, los encargados de Gentoo han preferido marcar el repositorio de GitHub como totalmente comprometido.

Sin embargo, parece que los atacantes no fueron muy listos si querían provocar un gran perjuicio a los usuarios de esta distribución Linux, ya que el repositorio de GitHub no es más que un espejo (mirror) y no el repositorio principal. La mayoría de los usuarios utilizan el repositorio alojado en el sitio web oficial y otros espejos, así que el impacto de este ataque ha terminado siendo mínimo.

Como medida de precaución y tras recuperar el control sobre la cuenta hackeada, los encargados de Gentoo han decidido borrar o inhabilitar el

repositorio en GitHub, que ahora da un código 404 cuando es visitado mediante un navegador web.

En caso de haber obtenido Gentoo desde GitHub, lo recomendable es hacer una copia de seguridad de los datos, a ser posible utilizando otra distribución que funcione en live, para reinstalar el mismo Gentoo descargado desde el sitio web oficial.

[CONCLUSION] Mi conclusion: Aprende del error.

No es dificil darse cuenta que los hackers “nomas estan viendo ”, que aplicación se puede vulnerar, esperando cazar la oportunidad de lucrar o darle un mal rato a un usuario o empresa que expuso su falta de proteccion en aplicaciones. Una mala configuracion, una falta de vision, un escenario no estudiado puede significar la perdida o divulgacion de informacion… dinero, las bases de datos son dinero… Y es en este punto donde uno se vuelve paranoico, desde contraseñas de 24 caracteres hasta desactivar Javascript porque “no me da confianza”.
Cuando se habla de seguridad nada “esta de mas”,claro está, Nada es seguro, y si todo puede ser vulnerado… para que arriesgar ?
Gentoo pudo evitar este dolor de cabeza agregando un “two-factor authentication” en su cuenta de github.

Fuentes

Caso Israel o viernes 13

- http://bvs.sld.cu/revistas/aci/vol11_5_03/aci04503.htm
- https://web.archive.org/web/20071005233501/http://alerta-antivirus.red.es/virus/ver_pag.html?tema=V&articulo=4&pagina=3
- https://es.gizmodo.com/historia-del-virus-jerusalem-o-como-un-viernes-13-se-i-1742971725

Vulnerabilidad en repo de Gentoo

- https://www.gentoo.org/news/2018/06/28/Github-gentoo-org-hacked.html
- https://www.muyseguridad.net/2018/06/29/hackean-repositorio-gentoo-linux-github/
- https://thehackernews.com/2018/07/github-hacking-gentoo-linux.html
- https://thehackernews.com/2018/06/gentoo-linux-github.html