CAPÍTULO 6

SEGURIDAD INFORMÁTICA

6.1 DEFINICIONES

SEGURIDAD INFORMÁTICA

Podemos definir la **seguridad informática** o **ciberseguridad** como el proceso de prevenir y detectar el uso no autorizado de un sistema informático. Implica las actividades de proteger contra intrusos el uso de nuestros recursos informáticos, especialmente la información contenida en una computadora o circulante a través de las redes de computadoras, con intenciones maliciosas, con intención de obtener ganancias o incluso la posibilidad de acceder a ellos por accidente.

La seguridad informática abarca una serie de medidas de seguridad, tales como programas de software de antivirus, firewalls y otras medidas que dependen del usuario, tales como la activación de la desactivación de ciertas funciones de software, como scripts de Java, ActiveX, cuidar del uso adecuado de la computadora, los recursos de red o de Internet.

MALWARE

El malware (una contracción para soft**ware mal**icioso) es cualquier software diseñado intencionalmente para causar daños a una computadora, servidor, cliente o red informática. Por el contrario, el software que causa daños involuntarios debido a alguna deficiencia se describe típicamente como un error de software (bug). Existe una amplia variedad de tipos de malware, incluyendo virus informáticos, gusanos, troyanos, ransomware, spyware, adware, wiper y scareware, entre otros.

VIRUS INFORMÁTICO

Un **virus informático** es un tipo de programa informático que, cuando se ejecuta, se replica modificando otros programas informáticos e insertando su propio código. Si esta replicación tiene éxito, se dice que las áreas afectadas están "infectadas" con un virus informático, una analogía derivada de los virus biológicos.

Los virus informáticos generalmente requieren un programa host. El virus escribe su propio código en el programa anfitrión. Cuando se ejecuta el programa, el programa de virus escrito se ejecuta primero, causando infección y daños. Un gusano informático no necesita un programa host, ya que es un programa independiente o fragmento de código. Por lo tanto, no está restringido por el programa anfitrión, pero puede ejecutarse de forma independiente y llevar a cabo ataques de forma activa.

6.2 ASPECTOS QUE ATAÑEN A LA SEGURIDAD INFORMÁTICA

Las cuatro áreas principales que cubre la seguridad informática son:

1. **Confidencialidad**: Sólo los usuarios autorizados pueden acceder a nuestros recursos, datos e información.
2. **Integridad**: Sólo los usuarios autorizados deben ser capaces de modificar los datos cuando sea necesario.

3. **Disponibilidad**: Los datos deben estar disponibles para los usuarios cuando sea necesario.
4. **Autenticación**: Estás realmente comunicándote con los que piensas que te estás comunicando.

6.2.1 Medidas de mantenimiento y prevención de intrusiones

Los ataques más utilizados en contra de un sistema informático son los troyanos, los gusanos y la suplantación y espionaje a través de redes sociales. También son populares los ataques DoS/DDoS, que pueden ser usados para interrumpir los servicios. A menudo algunos usuarios autorizados pueden también estar directamente involucrados en el robo de datos o en su mal uso. Pero si se toman las medidas adecuadas, la gran mayoría de este tipo de ataques pueden prevenirse, por ejemplo, a través de la creación de diferentes niveles de acceso, o incluso limitando el acceso físico. Las medidas de **seguridad informática** que se pueden tomar incluyen:

1. Asegurar la instalación de software legalmente adquirido: por lo general el software legal está libre de troyanos o virus.
2. Actualizar el software y el sistema operativo: esto significa que aprovechará las últimas revisiones de seguridad.
3. Utilizar software antivirus: las soluciones de seguridad detectarán y eliminarán las amenazas. Mantenga su software actualizado para obtener el mejor nivel de protección, con las reglas de configuración y del sistema adecuadamente definidos.
4. Hardware y software cortafuegos: los firewalls ayudan con el bloqueo de usuarios no autorizados que intentan acceder a tu computadora o tu red.
5. Uso de contraseñas complejas y grandes: las contraseñas deben constar de varios caracteres especiales, números y letras. Esto ayuda en gran medida a que un hacker no pueda romperla fácilmente.
6. Cuidado con la ingeniería social: a través de las redes sociales los ciberdelincuentes pueden intentar obtener datos e información que pueden utilizar para realizar ataques.
7. No abrir archivos adjuntos de correos electrónicos de remitentes desconocidos: podrían estar infectados con malware. No hacer clic en los vínculos de los correos electrónicos de remitentes o sitios web desconocidos.
8. Criptografía, especialmente la encriptación: juega un papel importante en mantener nuestra información sensible, segura y secreta.
9. Evitar el uso de redes Wi-Fi no seguras en lugares públicos: las redes no seguras lo dejan vulnerable a ataques del tipo “Man-in-the-middle”.
10. Tapar la webcam. En general, los distintos sensores de un dispositivo como GPS, micrófono, acelerómetro, etc. podrían ser hackeados y utilizados para fines ilícitos.

Referencias: https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/brocker

6.3 VIRUS

6.3.1 Virus – dificultades que generan

¿Si un virus no hace más que copiarse a sí mismo y nada más, por qué trabajan las personas tanto cuando tienen uno?. Por ejemplo: un virus emite pitidos cada vez usted le da a una tecla con su teclado, el 18 de cada mes, ¿por qué hace que todos quienes nos infectemos queramos librarnos de él?. Hay varias razones para esto. Si usted no se libra del virus, hay una probabilidad fuerte que en el futuro usted se lo pasará a un proveedor o cliente que serán perturbados. Más de 99% de los virus que realmente se extendieron es residente en memoria. Hay la posibilidad de incompatibilidades entre el virus y algún otro programa que usted está corriendo [por ejemplo, Jerusalem intenta usar uno de los recursos que Novell NetWare usa, así que usted no puede ejecutar Novell NetWare y Jerusalem en el mismo sistema]. Además, aunque nosotros hemos analizado y hemos documentado el virus, el usuario podría permanecer nervioso pensando que el virus hace más de lo que se ha documentado, o que él tiene una versión diferente del virus. Así en casi todos los casos que nosotros hemos visto, las personas realmente quieren librarse del virus [a excepción, a veces, por guardar un espécimen para un “zoológico”].

Si usted desea realmente librarse del virus, esto le va a tomar tiempo, y tiempo es dinero. Cada PC tomará varios minutos por lo menos, y cada disco flexible tomará varios segundos por lo menos [y puede haber muchos discos flexibles]. Sería bueno si usted sólo tuviera que preocuparse por esas computadoras y discos flexibles que se infectan, pero por supuesto usted no sabe cuáles son éstos hasta que haya hecho la búsqueda de virus, así que tiene que verificar todo.

6.3.2 Cosas que no son virus

ERRORES DE PROGRAMA. (BUGS)

Los Bugs no son virus, y los virus no son "Bugs". Yo estoy usando un procesador de textos que sé que tiene un "Bug" serio. Si usted trabaja durante mucho tiempo con un archivo grande, entonces en el futuro algo sale mal dentro del programa, y se niega a permitirle guardar el archivo al disco, de manera que usted perderá todo el trabajo que ha hecho desde la última vez que salvó. Este programa viene de una casa de software importante, y ellos no hicieron esto a propósito, así que no es un troyano. Los programadores cometieron un error. Los programadores son humanos, y los humanos cometen errores. Los programadores, como otros humanos, tienen orgullo, y no les gusta admitir que cometen errores, así que ellos los llaman "bugs", como si el bicho (bug) hubiese entrado volando a través de la ventana y se hubiese establecido en el programa. Todos los programas suficientemente complejos tienen "bugs".

El software anti-virus no descubre "bugs". Si lo hiciera, informaría "bugs" en casi todo. El término inglés bug, que significa insecto o, más genéricamente bicho, tiene su origen en los primeros días de la informática, cuando se descubrió que un problema de hardware en un ordenador electromecánico de la Universidad de Harvard (EEUU) se debía a una polilla atrapada entre los contactos de un relé de la máquina.

ALARMAS FALSAS

Las alarmas falsas no son virus. Una alarma falsa es cuando usted piensa que tiene un virus, pero está equivocado. A veces, las personas tienen alguna falla del hardware o del software, y después de ejecutar algunos diagnósticos, eliminada la posibilidad de hardware o problemas del software, concluye que es por consiguiente un virus, y procede en esa asunción. Más a menudo, una alarma falsa es el resultado de la ejecución de software anti-virus.

El software anti-virus, igual que otro software, no es infalible. Los dos errores principales que un programa anti-virus puede cometer son: no encontrar un virus que está allí [yo probé una vez un programa que no encontró ningún virus de sector de arranque, y éstos se consideran causa de más de dos tercios de las infecciones] o indicar que un virus está presente cuando no hay ninguno, y eso se llama una alarma falsa.

Cuando un programa anti-virus da una alarma falsa, se parece bastante mucho a la realidad.

Hay varias cosas que podrían indicar que la alarma es falsa:

- Sólo un archivo está dando la alarma [o quizás cuatro archivos, pero ellos son copias del mismo archivo].
- Sólo un producto da la alarma; otros productos dicen que el sistema está limpio.
- Usted recibe la alarma después de ejecutar productos múltiples, pero no al arrancar en frío y ejecutar un producto.
- El virus que se descubre está en la lista de virus reconocidos [por supuesto, esta lista cambia todo el tiempo].

No hay ninguna regla fija que puede aplicarse, desgraciadamente. Usted no puede decir que es una alarma falsa si uno de los cuatro casos indicados arriba es verdad, o incluso si los cuatro son verdad. La única manera de realmente descartar una alarma falsa es enviarle el archivo sospechoso al vendedor del producto que da la alarma, pidiéndole que verifique que es un virus, analizándolo en su laboratorio de virus. Y esta determinación tarda algún tiempo.

Entretanto, una alarma falsa puede ser tanta molestia como un virus real, o más aún. Si tiene un disco flexible que se infecta con el virus Stoned, usted puede copiar los datos simplemente fuera del disco y puede destruir el disco flexible infectado, o usted puede librarse del virus con su programa de anti-virus, o exigir un disco de reemplazo. En cualquier caso, el costo es sólo unos segundos. Pero si usted consigue una actualización de su programa de anti-virus favorito, y le dice que usted tiene el virus Stoned en los archivos en su servidor de archivos, entonces resolver la situación tomará mucho más tiempo. Usted sabe y yo sé que Stoned no puede infectar archivos. Pero simplemente quizá alguien ha escrito un virus de archivo y ha decidido llamarlo Stoned [por ejemplo, hay dos virus no relacionados, uno llamado Parity y el otro Parity.b]. Así que, usted le envía el archivo a su vendedor del producto para el análisis y comentario. Entretanto, para estar seguro, usted quita el archivo del servidor [o posiblemente el producto está obstruyendo el acceso a ese archivo]. Esta situación significa que algún sistema importante no trabajará más, cuando necesite ese archivo.

No es sorprendente que algunas personas hayan cambiado su software anti-virus después de demasiadas alarmas falsas.

El software anti-virus no descubre alarmas falsas. ¿Si lo hiciera, no informaría la alarma falsa?

CHISTES (Jokes)

Un chiste es algo cómico. Por supuesto, que lo que una persona encuentra cómico no es igual que lo que otra persona encuentra cómico. Depende de su sentido del humor. Considere un programa que pretende formatear su disco duro, y luego revela que no tiene formato. ¿Es eso cómico?. Depende de su sentido de humor.

Algunas personas aman hacer bromas, y en ciertas fechas uno debe aplicar un poco de escepticismo a los informes de virus. Algún software anti-virus descubre chistes, y le dice "Usted tiene un chiste llamado. . . ". La razón para esto es que algunos chistes están bastante extendidos,

y se conciben para causar preocupación, así que el programa anti-virus está intentando tranquilizar las cosas, diciendo "Si, yo sé sobre esto, y es inofensivo".

TROYANOS

Un troyano es un programa que hace algo más de lo que el usuario estaba esperando; y esa función adicional es perjudicial. Esto conlleva a un problema en la detección de troyanos. Suponga que yo escribí un programa que podría descubrir infaliblemente si otro programa formateó el disco duro. ¿Entonces, puede decir que este programa es un troyano? Obviamente no si se supusiera que el otro programa formateaba el disco duro [como el FORMAT hace, por ejemplo], entonces no es un troyano. Pero si el usuario no estuviera esperando el formateo, entonces es un troyano. El problema es comparar lo que el programa hace con las expectativas del usuario. Usted no puede determinar las expectativas del usuario para un programa.

Es así que nosotros tenemos que hacer algunas consideraciones. Generalmente se considera que el Diskette de Información del SIDA es un troyano. Aproximadamente 20.000 copias de éste se mandaron por correo a los usuarios en 1989, pretendiendo ser un programa que le enseña sobre el virus del SIDA. De hecho, era un troyano; después de que usted arrancaba su computadora 90 veces, él encriptaba y escondía todos los nombres de archivo de su disco duro, y demandaba que usted pagase por su licencia para usarlo. Aunque la documentación que vino con él le decía que era probable que algo malo pasara, generalmente se considera que es un troyano. El FORMAT no es un troyano.

Como regla, usted no ve muy a menudo troyanos. Ellos no se copian, y no se extienden de la manera que los virus hacen. Los troyanos no son una amenaza real, excepto en una de las circunstancias siguientes.

- Cuando ellos se diseminan ampliamente, como el Diskette de Información de SIDA.
- Ellos son focalizados en una organización, en este caso es un "trabajo interno", hecho por un empleado.

Algunos productos anti-virus descubren unos troyanos [como SIDA], pero la mayoría de los productos no descubren troyanos en absoluto.

PROGRAMAS ADULTERADOS

Algunos archivos simplemente se adulteran [quizás por un problema del hardware], y cuelgan a la computadora cuando corren. Por alguna razón, éstos a veces terminan en colecciones de virus, a menos que la colección sea mantenida cuidadosamente.

INTENCION DE HACER VIRUS

Algunos autores de virus son menos habilidosos de lo que les gustaría ser, y escriben lo que se piensa claramente que es un virus, pero por alguna razón hay semejante error de programación que el virus no trabaja en absoluto. Ellos sueltan éstos, sin embargo, en la creencia aficionada que nadie los probará [o quizás ellos no los probaron]. Un error típico es confundir el decimal con el hexadecimal, y así que su código fuente dice probablemente `int 21' para la función interrupción del DOS, pero debería haber dicho `int 21h ' [que es 33 en decimal].

CUENTAGOTAS (DROPPERS)

Un cuentagotas es un programa que no es un virus, ni se infecta con un virus, pero cuando corre instala un virus en la memoria, en al disco, o en un archivo. A veces se han escrito cuentagotas como un portador conveniente para un virus, y a veces como un acto de sabotaje. Algunos programas anti-virus intentan descubrir cuentagotas.

GÉRMENES

Un germen es un caso de virus de generación cero, y en semejante forma que la infección no pudiera pasar naturalmente. Por ejemplo, un virus que sólo infecta archivos más grandes que 5Kb, pero ha infectado un archivo diminuto de 10 b. Alternativamente, podría ser un caso de virus sin ningún archivo anfitrión. Si usted quita el virus, usted queda con un archivo de cero-byte. Éste es el archivo original creado por el autor del virus.

GUSANOS

Los Gusanos (Worms) son programas que realizan copias de sí mismos, alojándolas en diferentes ubicaciones del ordenador. El objetivo de este malware suele ser colapsar las computadoras y las redes informáticas, impidiendo así el trabajo a los usuarios. A diferencia de los virus, los gusanos no infectan archivos.

6.3.3 Tipos diferentes de virus

VIRUS DEL SECTOR DE ARRANQUE (BSVs)

Los tipos mas comunes de virus son virus de sector de arranque [BSVs], como Form o Stoned. Éstos infectan los sectores de arranque de discos flexibles, y/o el sector de la partición [Registro Maestro de Arranque, MBR] o el sector de arranque del DOS [Registro de Arranque del DOS, DBR] de discos duros. He aquí como un BSV se disemina.

Un disco flexible recién ha llegado, con algunos datos en él [algunos archivos de procesador de textos y una hoja de cálculo, quizás]. Ésta es parte de un proyecto que usted está haciendo juntamente con un colega. Lo que su colega no sabe es que su computadora está infectada con un BSV, y por consiguiente lo está también el disco que él le envió. Usted puso el disco en la unidad A y comenzó a usar estos archivos. Hasta ahora, el virus no ha hecho nada. Pero cuando usted termina por ese día, usted apaga a la computadora y va a casa. El próximo día, usted entra y enciende. El disco flexible todavía está en la unidad A, así que la computadora intenta arrancar de este disco. Carga el primer sector en la memoria y lo ejecuta [normalmente, esto es un pequeño programa escrito por Microsoft para cargar el DOS; o si no puede encontrar DOS en el disco, para decirle así: No hay disco de sistema o error de disco. Reemplácelo y oprima una tecla cuando esté listo (Non-System disk, or disk error. Replace and press any key when ready)]. Todos hemos visto este mensaje numerosas veces, así que usted abre la puerta de la unidad A y aprieta una tecla.

Pero este disco está infectado con Stoned, así que lo que ejecutó no era exactamente el programa de Microsoft, sino el virus Stoned, escrito en 1987 en Nueva Zelanda [y a veces llamado el virus de Nueva Zelanda]. El virus se instala en el disco duro, reemplazando el MBR, y copiando el MBR original un poco más adelante en el disco.

Cuando usted pone en marcha el disco duro, el MBR corre, pero esto es el virus Stoned. El virus Stoned queda residente de memoria, capturando la interrupción 13h, de lectura/escritura del disco, y entonces carga el MBR original, y el proceso arranque continúa normalmente. Pero, como la interrupción de read/write de disco fue capturada, cada vez que haya un acceso de escritura o lectura [usted piensa que está haciendo una lectura, pero el virus, en cambio, decide escribir] a la unidad A, el disco flexible se examina, y si todavía no está infectado, el virus Stoned se instala en el sector de arranque. Así, su computadora está infectando cada disco puesto en la unidad A, y más pronto o más tarde de éstos se enviarán a un colega, y el ciclo continuará.

El detalle de varios BSVs es diferente, pero el principio es el mismo. Ellos son llevados por los sectores de arranque de discos infectados, y sólo de esa manera [un BSV no puede

extender por una red, por ejemplo]. Y la única manera a infectarse es intentar arrancar de un disco infectado, aún cuando el arranque falle.

Los BSVs infectan PCs. Ellos no tienen en cuenta que sistema operativo está corriendo, o qué software de seguridad se instala, porque en el momento en que el BSV se instala el sistema operativo o el programa de seguridad no está corriendo todavía. Sin embargo, con algunos sistemas operativos no-DOS por ejemplo, Windows NT, u OS/2], aunque el PC es infectado, el virus no puede copiarse a si mismo hacia otros discos y no se puede difundir. Puede, sin embargo, todavía hacer daño, como fue descubierto a través de un sorprendido usuario de UNIX cuando Michelángelo se activó el 6 de Marzo.

A la mayoría de las personas, el hecho que los virus pueden infectar de esta manera les sorprende, lo cual da cuenta porqué los BSVs son tan comunes.

VIRUS DE MACRO

Los virus de Macro [como el WM.Concept], el último desarrollo de virus, parece volverse una amenaza significante, por varias razones.

Macros, escritos en WordBasic, y accesible a muchos usuarios de computadora, son más fáciles de escribir que los "tradicionales" virus de archivo [escritos, en su mayoría, en código assembly].

Ellos fueron los primeros virus en infectar archivos de datos, en lugar de ejecutables. Los archivos de datos, a los cuales se atan macros, proporcionan un método de replicación más eficaz a los virus que los archivos ejecutables. Frecuentemente se intercambian archivos de datos mucho más que archivos ejecutables. Si usted agrega el incremento del uso de e-mail [y la habilidad de atar archivos al e-mail], y el acceso masivo a Internet [y servicios en-línea como CompuServe y América Online], es probable que esto haga a los virus de macro una amenaza mucho mayor para los usuarios de computadora que los virus de archivo tradicionales.

Los virus de macro no son de una plataforma específica. Hay versiones de Microsoft Word para Windows 3.x, Windows 95, Windows NT y Macintosh. Esto hace a todos estos sistemas operativos susceptible a los virus de macro [aunque algo en un macro que produce llamadas a un sistema operativo específico [como con el WM.FormatC macro trojan] se restringirá a ese sistema operativo en particular].

Los virus de macro ya han tenido un marcado efecto. WM.Concept actualmente contabiliza alrededor de 50% de todos los informes de virus a nuestra sección de asistencia técnica. Y aunque WM.Concept no causa daño a los datos, nosotros ya hemos visto el primero de los pasos [aunque vacilante] hacia un virus de macro que amenaza datos.

Los virus de macro no están restringidos a Word de Microsoft para Windows. En Enero de 1996, aparecía el primer virus de macro para infectar archivos Lotus AmiPro [APM.GreenStripe]. Al contrario de lo que ocurre en Word para Windows en el que se unen macros directamente a DOC [y DOT] los archivos, los macros de AmiPro están contenidos en un archivo separado [con la extensión SMM]; esto hace posible intercambiar documentos AmiPro [por ejemplo, vía e-mail] sin intercambiar macros infectados. Y XM.Laroux que aparecía en Julio de 1996, es el primer virus de macro para infectar las hojas de cálculo Microsoft Excel para de Windows.

VIRUS DE ARCHIVO TSR

Los virus de archivos TSR son ahora poco comunes. Como el nombre lo sugiere, éstos infectan archivos. Éstos normalmente son COM y EXE, pero hay algunos virus de drivers de

dispositivos, y algunos virus infectan archivos overlay (OVL); los programas ejecutables no siempre tienen la extensión COM o EXE, aunque así sea en más de 99% de ellos.

Para que un virus de TSR se disemine, alguien tiene que ejecutar un programa infectado. El virus queda residente en memoria, y típicamente mira cada ejecución del programa después de lo cual lo infecta, si es que ya no lo estaba. Algunos virus se llaman “fast infectors” (que infectan inmediatamente) y ellos infectan apenas usted abre el archivo [por ejemplo, un backup podría abrir cada archivo en el drive]. El Dark Avenger fue el primer “fast infector”. En el caso de Green Caterpillar, el disparador de infección es algo que determina que archivos están presentes [como DIR]. Se han usado otros disparadores, pero el más común es infectar cada programa que usted está a punto de correr.

VIRUS DE ARCHIVO NO-TSR

Es mucho mas fácil escribir un virus NO-TSR, y así lo hacen tantos de los autores de virus principiantes. Pero es bastante raro encontrar semejante virus en la actualidad; menos del 1% de eventos informados es un virus NO-TSR. Con este tipo de virus, ejecutando un programa infectado se ejecuta el virus, que busca otro archivo para infectar, y lo infecta. Vienna es el mas común de los virus NO-TSR. Vienna fue el primer virus de archivo, pero ahora tiene el estado de “raro”.

Hay muchos virus basados en Viena, porque en 1987 se publicó en un libro un desensamblado [que es casi equivalente al código de la fuente].

VIRUS COMPAÑEROS

Si usted tiene un archivo de COM y un archivo de EXE con el mismo nombre de archivo y teclea ese nombre, DOS corre los archivos COM preferentemente a los archivos EXE. Los virus compañeros usan este rasgo de DOS. Cada archivo de EXE que usted tiene adquiere a un compañero COM con el mismo nombre. Entonces, cuando usted intenta ejecutar su programa EXE, realmente corren los programas COM, y ése es el virus. Cuando el virus ha terminado haciendo lo que quiere hacer [como crear a otro compañero para otro archivo], corre entonces los programas EXE, para que todo parezca trabajar normalmente.

Ha habido unos virus compañeros exitosos, pero no muchos. La ventaja principal para el autor del virus es que debido a que el archivo EXE no cambia, algún software que busque cambios no podría detectar que un virus está extendiendo.

Otro tipo de compañero es el compañero de PATH (camino, ruta de directorios). Esta clase de virus pone un programa en un directorio que está antes en el PATH de DOS del que está la víctima. Cuando usted ejecuta un programa que no está en un sub-directorio actual, DOS busca el programa en varios sub-directorios, tal como lo especifica el orden de la directiva PATH en el archivo de AUTOEXEC.BAT. Los compañeros de PATH son más difíciles de escribir que los compañeros ordinarios y no hay muchos de ellos.

VIRUS DE SOBRESCRITURA

Un virus de sobrescritura borra cada archivo que infecta, reemplazándolo con sí mismo simplemente, y el programa ya no funciona. Debido a que esto es tan obvio, estos virus nunca han sido exitosos para distribuirse.

VIRUS MULTIPLES

Algunos virus, como Tequila, infectan objetos múltiples. Cuando usted ejecuta un EXE infectado por Tequila, Tequila se instala en el MBR. Cuando usted arranca la computadora, Tequila se ejecuta en el MBR, y va residente a memoria. Mientras Tequila está residente en la

memoria, infecta archivos EXE. Otros virus, como algunas de las versiones de Anticad, infectan COM, EXE y MBRs indistintamente. Algunos virus infectan COM, EXE, MBRs y drivers de dispositivo.

OBJETOS MISCELANEOS DE INFECCION

Hay un virus que infecta archivos OBJ. Hay un virus [Starship] que infecta creando un nuevo DBR, dejando el viejo intacto, dejando el código en el MBR intacto, y cambiando el puntero en el MBR para que el DBR de Starship se ejecute ante el DBR original.

Hay otros virus [DIR II y Dir.Byway] que infectan archivos del sistema cambiando la FAT y directorios para que los archivos en el disco duro queden con enlaces cruzados al virus.

6.3.4 Características de los virus

RAPIDO

Como explicó anteriormente, un "fast infector" se extiende rápidamente dentro de una computadora infectando todo lo que se accede. Un infector rápido no es tan malo como parece; es tan fácil limpiar una computadora con 1.000 archivos infectados como una con 10, con tal de que usted tenga un programa de anti-virus que haga un trabajo de limpieza bueno. Sin embargo, la mayoría los productos anti-virus verifican la memoria buscando virus, y la posibilidad de que un infector rápido esté en memoria es una de las razones de hacerlo. Si hay un infector rápido en memoria y el producto abre todos sus archivos, usted infectaría cada archivo en la computadora infectada.

LENTO

El opuesto de un "fast infector" es un "show infector" (infector lento). La idea aquí es que si el virus se extiende despacio, usted tiene menos probabilidades de notarlo y matarlo. Hay varias maneras que un infector lento pueda trabajar, pero el infector lento clásico trabaja sólo infectando esos archivos que usted ya había pensado cambiar. Esto significa que si usted está ejecutando un detector de cambios como una medida anti-virus, el detector de cambios avisará cada vez que hay una infección, pero como usted había pensado modificar el archivo, le dirá que acepte el cambio.

Starship es otra manera de hacer un infector lento. Sólo infecta archivos cuando usted los copia a su disco duro. Así que ningún archivo en el disco duro cambia, y el detector de cambios está contento. Pero cuando usted copia un archivo a un disco flexible, la copia se infecta, y cuando usted lleva esto a otra computadora protegida por el detector de cambios, el detector de cambios lo advierte de la existencia del nuevo archivo. Usted tranquilizará al detector de cambios indicándole que usted sabe que es un nuevo archivo, el descubridor de cambio estará contento, y otro sistema se habrá infectado.

OCULTO (STEALTH)

Si un virus es residente en memoria [como es más de 99% de los virus], entonces él ha enganchado una de las interrupciones, por lo menos. Si es un BSV, entonces ha enganchado la interrupción 13h, de lectura/escritura en disco. Si es un virus oculto y cualquier programa intenta leer el sector de arranque, entonces el virus dice "Aha, alguien quiere ver el sector de arranque; yo leeré entonces el sector de arranque original de donde yo lo puse, y presentaré ese en su lugar". Así que el software no ve nada excepcional. Brain, cosecha 1986, fue el primer virus que usó este truco. Los virus de archivo pueden usar un truco similar para enmascarar su presencia, para que cualquier software que sólo lee el archivo vea que los bytes que estaban allí antes de

que el virus llegara. Frodo es un ejemplo de esto. Es mas común ver virus ocultos en BSVs que en virus de archivo, ya que mas fácil para un autor de virus realizar ocultamiento en un BSV.

POLIMORFISMO

El tipo mas común de programa anti-virus que usan las personas en el escáner, buscando por un repertorio de virus. Así para la mayoría de autores de virus éste es el tipo de producto que mas le gusta derrotar. Un virus polimórfico tal que si usted toma dos instancias del virus, no hay ningún byte en común entre ellas, así que usted no puede anotar una sucesión de bytes y luego buscarlos en ese orden para descubrir el virus. Usted tiene que hacer algo mucho más complejo y difícil.

6.3.5 Daño hecho por los virus

Nosotros podemos categorizar el daño hecho por virus en seis grupos, según la severidad del daño. Algunas autoridades en la materia postulan la posibilidad de un virus que realmente hace algo bueno, pero nadie ha demostrado semejante virus todavía.

Nosotros definimos daño como: el virus hace algo que yo lo preferiría que no haya hecho. Y nosotros cuantificamos daño midiendo cuánto tiempo toma para volver a poner las cosas de la manera que debe ser.

No incluimos el daño “consecuente” en esta categorización [daño hecho por el usuario en un esfuerzo equivocado por librarse del virus]. Es notable cuantas personas darán formato al disco duro para librarse de Stoned, por ejemplo. Todo esto sólo ha conseguido que pierda todos sus datos. El virus está intacto, ya que reside en el MBR que no está afectado por FORMAT. Ni podemos incluir el daño hecho por incompatibilidades oscuras entre el virus y el sistema. Por ejemplo, si una computadora que estaba originalmente preparada para DOS 2 [pero está ejecutando una versión posterior de DOS ahora] se infecta por Stoned, entonces un número grande de archivos se adulterará porque el diseño del virus no había anticipado esta situación.

DAÑO TRIVIAL

Esto es hecho por un virus como Form [una vez fue el virus mas común en el mundo]. En el 18 de todos los meses, cada tecla que usted oprima hace al parlante emitir una señal sonora. Todos que usted necesita es librarse del virus. Esto normalmente tomará segundos o minutos [por cada computadora].

DAÑO MENOR

Un buen ejemplo de daño menor es la manera que el virus de Jerusalén borra cualquier programa que usted intenta correr después de que el virus ha ido de residente en memoria, los viernes 13. En el peor de los casos, usted tendrá que re-instalar algunos programas, así que recuperar el daño demandará unos 30 minutos por computadora.

DAÑO MODERADO

Si un virus da formato al disco duro, mezcla la FAT o borra el disco duro, éste es daño moderado. El daño es sólo moderado porque usted sabe que ha pasado, y usted puede re-instalar DOS y recargar el backup de ayer, porque usted hace un backup todos los días. Así que, usted perderá en mitad del promedio el trabajo de un día, más quizá una hora que para reinstalar y restaurar. El virus más famoso de daño moderado es Michelángelo.

DAÑO MAYOR

Este ocurre cuando un virus ataca tanto sus backups como su disco duro. Cada 16ava vez que un archivo infectado con Dark Avenger se ejecuta, sobrescribe un sector al azar en el disco duro con "Eddie lives . . . somewhere in time". Esto podría haber estado ocurriendo durante varias semanas. Usted descubre al Dark Avenger, se libra del virus, y halla "Eddie lives . . . somewhere in time" en varios archivos. Usted restaura el backup de ayer, y halla "Eddie lives . . . somewhere in time" en aquéllos también. Usted podría tener que remontarse unas semanas atrás, antes de que pueda encontrar archivos de datos limpios, y cuando usted ha restaurado con un backup de seis semanas de antigüedad, encontrará que no tiene ninguna manera de rehacer el trabajo, porque no tiene los documentos originales con los que trabajó.

DAÑO SEVERO

Daño severo ocurre cuando un virus hace cambios graduales y progresivos [para que también se adulteren backups], pero los cambios no son obvios [no hay "Eddie lives . . . somewhere in time" para buscar]. Usted termina simplemente no sabiendo si sus datos son correctos o cambiaron.

DAÑO ILIMITADO

Algunos virus [como Cheeba, Vacsina.44.login y GP1] apuntan a conseguir la contraseña del administrador del sistema y pasarlo a una tercera persona. Por ejemplo, en el caso de Cheeba, crea a un nuevo usuario con máximo privilegio, con un nombre de usuario fijo y contraseña. El daño es hecho entonces por esa tercera persona, que puede ingresar (log-in) al sistema y hacer lo que desee.

6.3.6 Como se difunden los virus

Parece ser una creencia común que los virus son difundidos por juegos, por shareware o por BBS (Bulletin Board System). La verdad es más compleja. Primero, recuerde como trabaja la clase más común de virus, los virus de sector de arranque. Un disco flexible físico tiene que estar involucrado y no necesita que haya software en él. Usted no puede conseguir un BSV usando un BBS.

Las rutas más probables por las que un virus entra en una organización son los ingenieros y los padres.

Los ingenieros de hardware visitan un número grande de computadoras, y como la pequeña abeja ocupada, podría recoger un poco de polen aquí, y depositarlo allí. Los ingenieros de hardware deberían tener todos sus discos de software permanentemente protegidos contra escritura, pero no lo hacen. Los ingenieros de hardware frecuentemente deberían verificar cualquier disco con escritura habilitada para ver si tiene virus, pero no lo hacen. Por supuesto, la mayoría de los ingenieros de hardware está limpia y bien educada, pero hay algunos que requieren reeducación.

Los padres tienen niños, y si hay un PC en casa, y los niños son adolescentes jóvenes, entonces ellos posiblemente intercambien software en la escuela. Los discos que ellos traen casa bien podrían estar infectados, y si el padre está llevando y trayendo discos del trabajo, ellos podrían tomar un virus fácilmente y llevarlo al trabajo con ellos.

Un virus de sector de arranque podría llegar en un disco de datos de un colega.

Otras maneras de conseguir un virus incluyen:

- en software empaquetado [algunas de las compañías más grandes han enviado un virus accidentalmente en software empaquetado];
- junto con el hardware comprado [la mayoría el hardware viene con discos que contienen utilidades o drivers];
- los vendedores que ejecutan demostraciones podrían instalar el virus que ellos recogieron inconscientemente del último lugar donde ejecutaron su demostración.

6.4 MEDIDAS DE PREVENCION

Nosotros recomendamos que todo sea verificado antes de que se use. Esto incluye discos, memorias SD, pen drives, etc. Esto podría hacerse con un escáner como AVG, el cual podría instalarse en cada computadora [si es conveniente, porque si no lo es, no se hará] o podría instalarse en determinadas computadoras dedicadas, lo que es más conveniente para las personas de soporte, para mantenerlo actualizado, pero menos conveniente para los usuarios.

Alternativamente, usted puede hacer todo esto tan transparente y sin dificultad instalando un escáner residente. Windows incorpora el antivirus Windows defender por defecto y también un firewall. Esto significa que todo se examina automáticamente sin que el usuario sea consciente de ello [a menos que sea encontrado un virus, por supuesto]. El escáner residente es la ruta que la mayoría de las personas escogen, junto con algunas máquinas dedicadas.

6.4.1 Reglas, procedimientos, educación y herramientas

Linda había trabajado en su trabajo durante algunos años. Ella tomó trabajo de vez en cuando para hacer en la PC de su casa, con el conocimiento y aprobación de su supervisor. Un día, la sección de soporte de PC encontró un virus en la PC de su oficina. El mismo día, un poco mas tarde, Linda fue despedida por introducir un virus a la empresa.

Linda estaba muy disgustada por lo que ella vio como despido injusto y demandó a la compañía. Ella ganó, porque la compañía para la que ella trabajó no tenía ninguna regla para decirles a los empleados qué hacer [así que ella no había roto ninguna regla]. Aunque ellos tenían software anti-virus, no había ningún procedimiento para verificar los discos que ingresaban [es así que ella no faltó a procedimientos de la compañía].

En la investigación, parecía probable que la sección de soporte de PC había infectado su máquina accidentalmente, y sólo lo descubrió cuando enviaron discos, copiados en la máquina de Linda, a otra compañía que verificó la presencia de virus y encontró uno en esos discos.

Si tales procedimientos hubieran existido y Linda los hubiese ignorado, entonces la compañía habría tenido una buena razón para despedirla. Por supuesto, con reglas apropiadas y procedimientos, probablemente no habrían sido infectados por un virus desde el primer momento.

Pero usted tiene que reconocer el hecho de que las personas se comportan la manera que lo hacen. Si usted hace sus procedimientos anti-virus onerosos y difíciles, probablemente se ignorarán en los sitios donde los virus son muy raros, y el costo y molestia de los procedimientos es demasiado grande.

Un buen conjunto de reglas podría ser como sigue:

- Cualquier unidad extraíble entrante debe verificarse.
- Si su software anti-virus encuentra un virus, avise al soporte de PC.

Nótese que las reglas son muy simples. De esa manera es más probable que, las personas las recuerden y respeten. La próxima cosa que usted necesita son procedimientos. El procedimiento les dice a los usuarios cómo obedecer las reglas. El procedimiento para verificar discos debe redactarse con detalles [' Ponga el disco/unidad USB en el drive, y tipee. . . ']. Si usted tiene una computadora que actúa como servidor, ponga el procedimiento en la pared, cerca de ella.

La educación también es importante. Usted no puede decirles a adultos que hagan algo y esperar simplemente que ellos le obedezcan sin preguntar; tiene que explicarles las razones. Puede hacer esto con charlas, o consiguiendo el vídeo sobre virus de Dr Solomon y permitiéndoles mirarlo.

Usted también tiene que proporcionar herramientas. No puede descubrir un virus con sus manos desnudas. Cualquier estrategia de anti-virus sensata debe tomar cuenta del hecho que incluso un usuario capacitado es falible; y que ellos transgredirán incluso las mejores reglas y procedimientos [consciente o inconscientemente. . . recuerde que la seguridad no es la preocupación primaria de personal que trabajo en Ventas, Comercialización y otras secciones dentro de una organización]. La base de cualquier estrategia de anti-virus coherente, por consiguiente, deben ser herramientas de anti-virus que eficazmente deberán descubrir, quitar y prevenir infecciones de virus. . . incluso cuando no se han seguido las reglas y procedimientos.

6.4.2 Herramientas anti-virus

ESCÁNERES

Un escáner es un programa que sabe encontrar un repertorio particular de virus. Los escáneres se actualizan en forma mensual o trimestral.

Los escáneres pueden ejecutarse a pedido (on-demand) o en cada acceso a los archivos (on-access). FindVirus es un escáner que se ejecuta a pedido, y debe ser corrido por el usuario [aunque esto podría hacerse automáticamente, al arrancar, indicándolo en el AUTOEXEC.BAT; o usando un programador de tareas (scheduler)].

WinGuard [Windows 3.x, Windows 95 y Windows NT] y AVG [Windows 7 hasta 10] son escáneres que trabajan continuamente, cuando se accede a los archivos. Cada vez que algún disco se accede, se verifica que no tenga virus el sector de arranque; y cuando se usa cualquier archivo, se verifica que el mismo no tenga virus.

Ambos programas pueden ser [opcionalmente] configurados para verificar archivos cuando se escriben al disco duro [útil si están transmitiéndose archivos de un sitio remoto, como un BBS, o Internet]. VirusGuard ocupa aproximadamente 9 kB de memoria convencional [DOS]; WinGuard, que es un programa específico para Windows no usa memoria convencional. Cualquier tiempo adicional involucrado para verificar el disco o el archivo es improbable que sea percibido en la mayoría de los casos. VirusGuard, un programa residente DOS, no tiene toda la capacidad de FindVirus [para economizar en consumo de memoria y tiempo]; específicamente, VirusGuard no puede encontrar virus de macro [que no trabajan, sin embargo, bajo DOS] y un porcentaje sumamente pequeño de los virus polimórficos [VirusGuard encontrará virus polimórficos en memoria, si se ejecutó un programa infectado]. WinGuard que no tiene los condicionamientos de un programa residente DOS, tiene la misma capacidad de detección que FindVirus.

Nota: Si en su PC está instalado un antivirus que monitorea todos los ejecutables, en caso de detectarse un archivo que contenga virus aparecerá una pantalla similar a la anterior.

CHECKSUMMERS

Un checksummer es un descubridor de cambios. Los archivos ejecutables no deben cambiar, salvo por una buena razón, como una actualización de software. Un checksummer intenta descubrir cambios. La ventaja de los checksummers es que no descubren un repertorio de virus, así que no necesitan actualización. El aspecto negativo de los checksummers, es que son más molestia que los escáneres [los archivos en su computadora cambian más a menudo de lo que usted podría haber pensado, por razones buenas y válidas], y no descubren todos los virus. Por ejemplo, los checksummers no descubren los infectores lentos; no descubren todos los virus de sector de arranque [si el código del disco duro queda inalterado]; y tienen problemas con virus ocultos. Algunas personas usan checksummers, pero son una minoría.

Los checksummers pueden ejecutarse a pedido [como ViVerify], o en cada acceso a los archivos.

SOLUCIÓN COMPLETA DE SEGURIDAD

AVG Internet Security

- Antivirus avanzado: Analiza su PC en busca de virus, ransomware, spyware y otros tipos de malware.
- Escudo de comportamiento: Envía alertas si detecta un comportamiento sospechoso del software de su PC.
- Detección de IA: Identifica de forma proactiva muestras de malware para protegerle contras las amenazas nuevas.
- CyberCapture: Bloquea las amenazas nuevas haciendo que nuestro software antivirus las envíe para su análisis.
- Análisis de PUA: Identifica las aplicaciones potencialmente no deseadas que pueda haber descargado de forma inadvertida.
- Análisis turbo: Reduce el tiempo de análisis omitiendo los archivos que ya sabe que son seguros
- Actualizaciones en tiempo real: Asegura que siempre esté protegido, con actualizaciones automáticas de seguridad, resolución de errores y nuevas funciones.

- Modo de «no molestar»: Detiene automáticamente todas las ventanas emergentes y las notificaciones de la aplicación, para que pueda concentrarse en lo que está haciendo.
- Modo silencioso: Pospone los análisis, las actualizaciones y las ventanas emergentes para evitar las interrupciones mientras trabaja.

Referencias: https://www.avg.com/

6.4.3 Redes y virus

Una red es un grupo de computadoras conectadas para hacer más fácil compartir datos. Esto da oportunidades interesantes a los virus, y para tratar con ellos.

Hay una percepción común que una vez que un virus ingresa a una red, de algún modo infecta muy rápidamente la red entera. La verdad, por supuesto, es más compleja. Primeramente, los BSVs no puede viajar por las redes. Si se infectan varias máquinas en una red, que es porque el virus se extendió vía los discos flexibles de la manera usual. Así es como un virus de archivo se extiende en una red.

1. La computadora del usuario 1 se ve infectada, quizás por un disco de demostración de un vendedor. El virus queda residente en memoria (TSR).

2. El usuario 1 ejecuta otros programas en su disco duro. Ellos se infectan.

3. El usuario 1 ejecuta algunos programas en la red. Ellos se infectan. Una red emula un dispositivo de DOS; cuando se leen o escriben archivos en el servidor se hace exactamente de la misma manera como si fuera localmente. El virus no tiene que porqué comportarse de manera diferente para infectar archivos en el servidor.

4. El usuario 2 ingresa en el servidor, y ejecuta un archivo infectado. El virus es ahora TSR en la máquina del usuario 2.

5. El usuario 2 ejecuta otros programas, en su disco duro local, y en el servidor. Cada archivo se infecta.

6. Los usuarios 3, 4 y 5 ingresan al servidor y al ejecutar infectan archivos.

7. Y así sucesivamente.

PROTECCION DE REDES

Muchas redes usaban Novell NetWare, así que lo usaremos como ejemplo, pero usted puede adaptar los mismos principios para otros sistemas operativos de red.

1. Usted puede hacer directorios de sólo-lectura. Si usted hace archivos de sólo-lectura en el disco duro local, usted está perdiendo su tiempo, porque casi todos los virus de archivo les harán lectura-escritura, los infectarán, y los harán de nuevo de sólo-lectura. Esto es porque el usuario tiene el privilegio para hacer lectura-escritura los archivos en su disco duro local. Pero en un servidor de archivos, usted no tiene que darle ese privilegio al usuario, y el virus tiene el mismo privilegio que el usuario. De hecho, el virus es el usuario, y puede hacer nada más de lo que el usuario pueda. No hay magia sobre los virus; ellos están sujetos a los mismos condicionamientos que cualquier otro programa.

Desgraciadamente, algunos paquetes no pueden ejecutarse en subdirectorios de sólo-lectura, porque requieren escribir la configuración o archivos temporales, en el mismo directorio.

2. Usted puede hacer que un programa sea sólo-ejecutar. Esto significa que, aunque el directorio sea lectura-escritura, los ejecutables no pueden ni escribirse ni leerse. Ellos sólo pueden ejecutarse. Sea precavido, ya que en Novell NetWare ésta es un camino en un solo

sentido. Una vez que usted ha hecho un archivo sólo-ejecutar, no puede regresar. Todo lo que puede hacer es borrarlo, aun siendo Supervisor. Algunos programas no se ejecutarán son sólo-ejecutar, porque tienen archivos complementarios (OVL) que se encadenan en el extremo del archivo EXE. Así, si el archivo EXE no puede leerse, los complementos no pueden cargarse.

3. Usted puede hacer sólo-lectura archivos individuales usando el atributo de DOS, de esa manera se niega al usuario el privilegio de modificar atributos en ese directorio.

Usando una combinación de las tres técnicas mencionadas, usted debe poder hacer no-infectables un porcentaje grande de los archivos del servidor [de hecho, no-modificables sin la intervención del Supervisor]. Esto detiene virus que infectan la mayoría de los ejecutables en el servidor. El usuario tiene acceso de lectura-escritura a los datos [lo necesita para hacer su trabajo], y así es que el virus también tiene acceso de lectura-escritura a los datos. El borrado de archivos es lo que menos nos debe preocupar. Considere que en algunos virus la rutina de daño consiste en alterar archivos. Así, ¿cómo protegemos efectivamente los datos en el servidor?. La única respuesta es mantener los virus también fuera de las estaciones de trabajo.

La próxima cosa que usted puede hacer, si su servidor está ejecutando Novell NetWare, es ejecutar un anti-virus NLM [NetWare Loadable Module] en el servidor. Éste puede programarse para inspeccionar los archivos del servidor. El uso de un escáner de acceso basado en el servidor [como el File Access Monitor en el anti-virus Toolkit de Dr Solomon para NetWare] proporciona una defensa de niveles múltiples contra infecciones de virus, verificando los archivos cuando pasan a y desde las estaciones de trabajo. Además, puede negarse el acceso a los usuarios al servidor a menos que su estación de trabajo esté protegida.

Una protección similar está disponible para Windows NT. El anti-virus Toolkit de Dr Solomon para Windows NT ofrece protección completa, tanto para las estaciones de trabajo como para los servidores. FindVirus proporciona un escáner a pedido; y un programador de tareas, para verificar el sistema en momentos pre-definidos. Winguard para Windows NT proporciona protección constante, verificando archivos y discos antes de que se accedan.

Referencias: https://www.pandasecurity.com/es/security-info/malware/

6.5 AMENAZAS ACTUALES

En la actualidad se considera "**MALWARE**" tanto a virus, gusanos, troyanos, spyware, rootkits, exploits, adware, botnets, ransomware, etc. En tanto que los hoax basan su efecto en la ingeniería social.

6.5.1 Spyware

Cualquier aplicación que recopila la información sobre la actividad en el PC de una persona u organización tanto en línea como fuera de ésta y que es capaz de guardar los datos recopilados localmente o enviarlos a terceros sin que el objeto de espionaje se entere de ello. El spyware puede recopilar la información sobre los correos electrónicos y hasta sobre contraseñas y números de tarjetas de crédito.

6.5.2 Adware

Un programa que puede mostrar anuncios mientras se esté ejecutado o mediante otros mecanismos se llama adware. A menudo estos sistemas publicitarios se integran en los programas gratuitos ayudando a los desarrolladores a cubrir los gastos o les rinden ganancias. No obstante, con el tiempo el adware empezó a gozar de mala fama, ya que muchas veces estos programas no sólo descargan y muestran los anuncios, sino que envían información sobre el usuario sin consentimiento expreso de éste.

6.5.3 Rootkits

Se trata de programas diseñados para ocultar objetos como procesos, archivos o entradas del Registro de Windows. Este tipo de software no es malicioso en sí mismo, pero es utilizado por los creadores de malware para esconder evidencias y utilidades en los sistemas infectados. Existen ejemplares de malware que emplean rootkits con la finalidad de ocultar su presencia en el sistema en el que se instalan.

6.5.4 Exploits

Es una técnica o un programa que aprovecha un fallo o hueco de seguridad -una vulnerabilidad- existente en un determinado protocolo de comunicaciones, sistema operativo, o herramienta informática.

Dicho error se refiere a operaciones que provocan un funcionamiento anormal de la aplicación, y que pueden ser producidas intencionadamente por una persona con fines maliciosos, como la ejecución de código remoto, denegación de servicio, revelación de información o elevación de privilegios.

6.5.5 Gusanos

Los gusanos son en realidad una subclase de virus, por lo que comparten características. Son programas que realizan copias de sí mismos, alojándolas en diferentes ubicaciones de la computadora.

El objetivo de este malware suele ser colapsar las computadoras y las redes informáticas, impidiendo así el trabajo a los usuarios. A diferencia de los virus, los gusanos no infectan archivos.

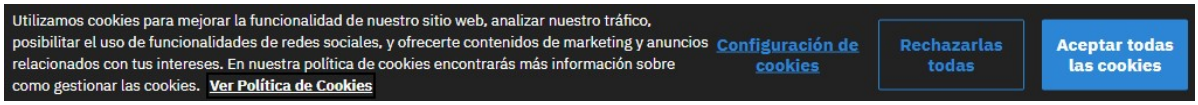
Los gusanos suelen utilizar técnicas de ingeniería social para conseguir mayor efectividad. Para ello, los creadores de malware seleccionan un tema o un nombre atractivo con el que camuflar el archivo malicioso. Los temas más recurrentes son los relacionados con el sexo, famosos, temas de actualidad o software pirata.

6.5.6 Cookies

Las cookies son pequeños archivos de texto que el navegador de Internet guarda en el ordenador del usuario cuando se visitan páginas web. La información que guardan las cookies se utiliza con distintos fines: para personalizar la navegación por la página, para recoger información demográfica sobre cuántos usuarios visitan la página y el tiempo que permanecen en ella, para realizar un seguimiento de los banners mostrados a cada usuario, entre otras cosas.

Por ejemplo, si un usuario visita una página web con cierta frecuencia, la cookie recuerda información sobre esa página, como nombre de usuario o contraseña de acceso facilitando así la navegación por la misma.

Aunque las cookies no son maliciosas como tal, un uso malintencionado de las mismas puede derivar en una amenaza para la privacidad del usuario, ya que pueden utilizarse para crear un perfil del usuario, con información que el usuario no controla y que puede ser enviada posteriormente a terceros.



Actualmente, las páginas Web que utilizan cookies deben solicitar la aprobación del visitante para hacer uso de ellas.

6.5.7 Hoax

Los “virus” HOAX se difunden por la llamada “ingeniería social”. En general a través de un mensaje de texto se le solicita que lo reenvíe a cuantas personas conozca con motivos más o menos verosímiles. En realidad, el virus es el mensaje, que de cumplir su cometido saturará los servidores de correo y generará tráfico innecesario en la red. Algunos mensajes son más directos en su objetivo de hacer daño y solicitan borrar archivos de sistema aduciendo que son virus, nuevamente aprovechando el desconocimiento de los usuarios y nombres de archivos “sospechosos”. Otras veces se usan para obtener direcciones de correo válidas que luego se podrán usar para enviar publicidad u otros fines. Lo recomendable es no reenviar este tipo de correos.

6.5.8 Virus de ejecución especulativa

Los virus Meltdown y Spectre se aprovechan de las características de ejecución especulativa de los procesadores, pero especialmente del procesador Intel, usando código que no debería haberse ejecutado pero que el procesador realiza como una de sus propiedades de mejora de la performance. Esto permite al virus acceder a memoria de kernel, a la que en modo usuario no debería hacerlo. Con la actualización del microcódigo se puede subsanar esta debilidad.

6.5.9 Ransomware

Un ransomware (del inglés ransom, «rescate» y ware, contracción de software), o «secuestro de datos» en español, es un tipo de programa dañino que restringe el acceso a determinadas partes o archivos del sistema operativo infectado y pide un rescate a cambio de quitar esta restricción.

Algunos tipos de ransomware cifran los archivos del sistema operativo inutilizando el dispositivo y coaccionando al usuario a pagar el rescate. Se han propuesto algunas alternativas en español al término en inglés, como "programa de secuestro", "secuestrador", «programa de chantaje» o «chantajista». En los primeros tiempos el pago se hacía a través de cuentas bancarias de países opacos, pero como el rastreo al delincuente era posible, se pasó al uso de monedas virtuales no rastreables.

6.5.10 Botnets

Son redes de computadoras con infección de malware que los cibercriminales utilizan para realizar tareas en línea sin el permiso del usuario. La palabra botnet es una combinación de robot y red (Net en inglés). Una botnet es un número de dispositivos conectados a Internet, cada uno de los cuales está ejecutando uno o más bots. El término se utiliza generalmente con una connotación negativa o maliciosa, derivada de usos criminales que se hacen de estas redes.

Un botnet no es un virus en sí mismo, sino una es una colección de dispositivos automáticos conectados. Si estos han sido infectados con un malware, los cibercriminales pueden utilizarlos para obtener el control y distribuir programas nocivos.

Los atacantes suelen utilizar sus botnets para lanzar ataques DDoS, así como para enviar SPAM en forma de correos electrónicos no deseados, detectar contraseñas confidenciales o distribuir ransomware.

6.5.11 Phishing

El phishing es cuando los cibercriminales atacan a sus víctimas con correos electrónicos que parecen ser de una empresa legítima que solicita información confidencial. Los ataques de

phishing se utilizan a menudo para inducir a que las personas entreguen sus datos de tarjetas de crédito y otra información personal.

6.5.12 Inyección de código SQL

Una inyección de código SQL (por sus siglas en inglés Structured Query Language) es un tipo de ciberataque utilizado para tomar el control y robar datos de una base de datos. Los cibercriminales aprovechan las vulnerabilidades de las aplicaciones basadas en datos para insertar código malicioso en una base de datos mediante una instrucción SQL maliciosa. Esto le brinda acceso a la información confidencial contenida en la base de datos.

6.5.13 “Man-in-the-middle”

Un ataque de tipo “Man-in-the-middle” es un tipo de ciberamenaza en la que un cibercriminal intercepta la comunicación entre dos individuos para robar datos. Por ejemplo, en una red Wi-Fi no segura, un atacante podría interceptar los datos que se transmiten desde el dispositivo de la víctima y la red.

6.5.14 Denegación de servicio

Un ataque de denegación de servicio es cuando los cibercriminales impiden que un sistema informático satisfaga solicitudes legítimas sobrecargando las redes y los servidores con tráfico. Esto hace que el sistema sea inutilizable e impide que una organización realice funciones vitales.

6.5.15 Backdoor

Los virus de puerta trasera son aquellos en los que los hackers acceden a funciones de la computadora de manera oculta y trabajan en segundo plano. Este tipo de virus son, en realidad, una combinación de diferentes amenazas de seguridad y algunos funcionan automáticamente y no necesitan ser controlados de manera remota.

A menudo, las puertas traseras se introducen en el sistema gracias a otros programas nocivos como troyanos, virus o incluso spyware. Consiguen acceso sin que el administrador se dé cuenta y luego infectan las sesiones a cada uno de los usuarios conectados a la red comprometida. Es posible que algunas amenazas puedan ser colocadas con carácter previo por usuarios que tienen los privilegios adecuados, para ganar acceso más tarde.

6.5.16 Keylogger

El término keylogger se refiere a un programa informático malicioso que registra en secreto todas las pulsaciones sobre el teclado realizadas por el usuario de un ordenador. Los Keyloggers se utilizan para obtener acceso ilegal a información confidencial, como por ejemplo datos personales, datos de tarjetas de crédito, credenciales de acceso, etc.

6.5.17 Malvertising

El malvertising (publicidad maliciosa) consiste en el uso de publicidad en línea para difundir e instalar malware o redirigir su tráfico. Los ciberdelincuentes inyectan anuncios infectados en redes publicitarias legítimas que muestran anuncios en sitios web en los que confía. Luego, cuando visita un sitio, el anuncio malicioso infecta su dispositivo con malware, incluso sin hacer clic en él. Mas información en: https://www.avg.com/es/signal/what-is-malvertising

6.6 AMENAZAS INFORMATICAS DEL FUTURO

Si en un momento el objetivo de los ataques fue cambiar las plataformas tecnológicas, ahora las tendencias **cibercriminales** indican que la nueva modalidad es manipular los certificados que contienen la información digital. El área semántica, era reservada para los humanos, se convirtió ahora en el núcleo de los ataques debido a la evolución de la Web 2.0 y las redes sociales, factores que llevaron al nacimiento de la generación 3.0.

- Se puede afirmar que "la Web 3.0 otorga contenidos y significados de manera tal que pueden ser comprendidos por las computadoras, las cuales -por medio de técnicas de inteligencia artificial- son capaces de emular y mejorar la obtención de conocimiento, hasta el momento reservada a las personas".
- Es decir, se trata de dotar de significado a las páginas web, y de ahí el nombre de Web semántica o Sociedad del Conocimiento, como evolución de la ya pasada Sociedad de la Información.

En este sentido, las amenazas informáticas que viene en el futuro ya no son con la inclusión de troyanos en los sistemas o softwares espías, sino con el hecho de que los ataques se han profesionalizado y manipulan el significado del contenido virtual.

- "La Web 3.0, basada en conceptos como elaborar, compartir y significar, está representando un desafío para los **hackers** que ya no utilizan las plataformas convencionales de ataque, sino que optan por modificar los significados del contenido digital, provocando así la confusión lógica del usuario y permitiendo de este modo la intrusión en los sistemas", La amenaza ya no solicita la clave de homebanking del desprevenido usuario, sino que directamente modifica el balance de la cuenta, asustando al internauta y, a partir de allí, sí efectuar el robo del capital".
- Obtención de perfiles de los usuarios por medios, en un principio, lícitos: seguimiento de las búsquedas realizadas, históricos de navegación, seguimiento con geoposicionamiento de los móviles, análisis de las imágenes digitales subidas a Internet, etc.

Referencias: https://en.wikipedia.org/wiki/Computer_security, https://www.universidadviu.com/que-es-la-seguridad-informatica; https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

6.7 CIFRADO DE LA INFORMACIÓN O CRIPTOGRAFÍA

La criptografía es la técnica de escribir de manera secreta u oculta, buscando proteger la información.

Para que un mensaje que, desde que es generado por el emisor, deba atravesar un medio de comunicación inseguro para luego llegar al receptor, desde hace muchos años se emplean métodos para mantenerlo oculto.

6.7.1 Cifrado simétrico

El cifrado simétrico consiste en la codificación mediante una regla (clave) que sólo conocen el emisor y el receptor.

Una vez de acuerdo, el remitente cifra un mensaje usando la clave, lo envía al destinatario, y éste lo descifra usando la misma clave.

El inconveniente de este método es que se debe enviar al receptor la clave de cifrado con algún método seguro y si el receptor se encuentra lejos esto puede ser costoso.

Como ejemplo de sistema simétrico está «Enigma»; Éste fue un sistema usado por Alemania en la segunda guerra mundial, en el que las claves se distribuían a diario en forma de libros de códigos. Cada día, un operador de radio, receptor o transmisor consultaba su copia del libro de códigos para encontrar la clave del día. Todo el tráfico enviado por ondas de radio durante aquel día era cifrado y descifrado usando las claves del día.

En la Web de TDIII hay dos videos muy interesantes sobre el código Enigma, que recomendamos ver.

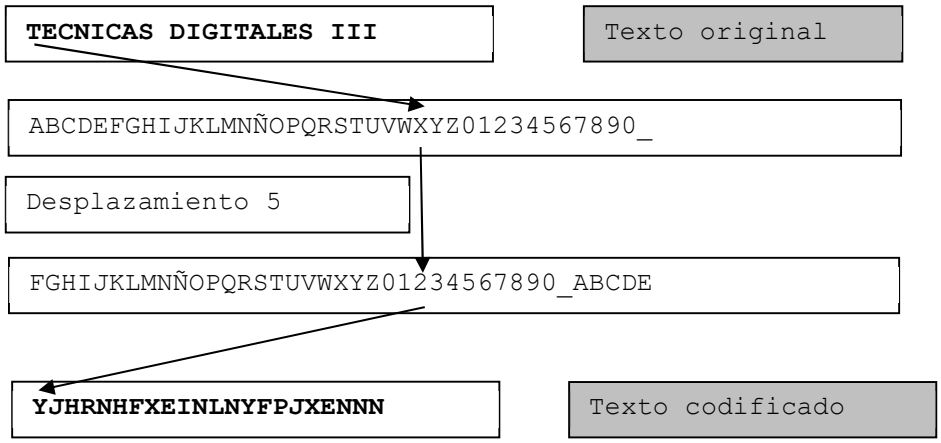


Figura 6.7.1 – Cifrado simétrico

Se analizará un ejemplo de codificación simple:

El texto original es "**TECNICAS DIGITALES III**" y el método de cifrado es incrementar en 5 la posición de cada letra. Disponemos de una lista de letras ordenadas y luego la misma lista, pero desplazada 5 posiciones. Para la primera letra (T) corresponde (Y), luego para la segunda letra (E) corresponde (J) y así sucesivamente.

Se obtiene entonces el texto codificado "**YJHRNHFXEINLNYFPJXENNN**", el que por supuesto es incomprensible.

Con el proceso inverso, conocido por el receptor, se puede reconstruir el texto original.

6.7.2 Cifrado asimétrico

Este método se atribuye a Diffie y Hellman, investigadores de la universidad de Stanford.

El sistema se basa en la idea de que dos interlocutores pueden generar conjuntamente una clave compartida sin que un intruso, que esté escuchando las comunicaciones, pueda llegar a obtenerla.

Para ello se eligen dos números públicos y cada interlocutor, un número secreto propio. Usando una fórmula matemática ($A=g^a \bmod(p)$, cada interlocutor hace una serie de operaciones con los dos números públicos y su número secreto. A continuación, los interlocutores se intercambian los resultados de forma pública. En teoría, revertir esta función es tan difícil como calcular un logaritmo discreto (un sextillón de veces más costosa que la exponenciación usada para transformar los números). Luego, ambos interlocutores utilizan por separado una fórmula matemática que combina los dos números transformados con su número secreto y al final los dos

llegan al mismo número resultado (K), que será la clave compartida, pero que nunca esa clave fue enviada por el canal inseguro.

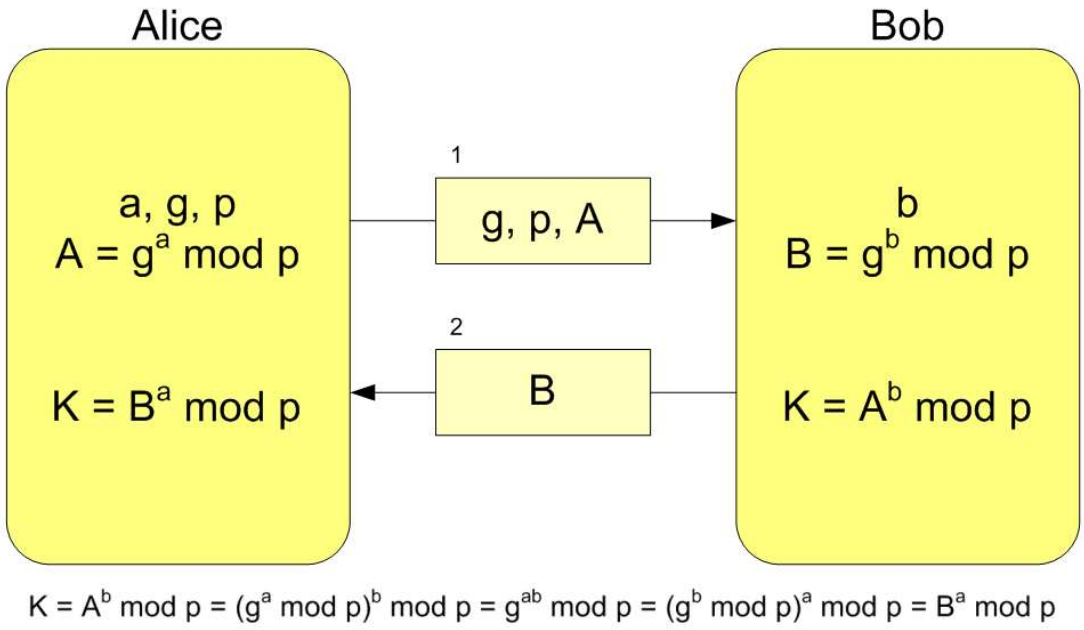


Figura 6.7.2 – Codificación asimétrica – generación de claves y envío de mensajes

Referencias: https://es.wikipedia.org/wiki/Intercambio_de_claves_de_Diffie-Hellman
Referencias (video): https://www.youtube.com/watch?v=bMO59atm8yc

6.7.3 Cifrado híbrido

Un sistema de cifrado híbrido usa tanto el cifrado simétrico como el asimétrico. Funciona mediante el uso de una clave pública para compartir una clave privada para el cifrado simétrico. El mensaje que se esté enviando en el momento, se cifra usando la clave y enviándolo al destinatario. Ya que compartir una clave simétrica no es seguro, la clave usada es diferente para cada sesión. La clave de sesión es cifrada con la clave pública, y el mensaje saliente es cifrado con la clave simétrica, todo combinado automáticamente en un sólo paquete. El destinatario usa su clave privada para descifrar la clave de sesión y acto seguido usa la clave de sesión para descifrar el mensaje.

Nota: El tema criptografía tiene una complejidad que excede el alcance de nuestra asignatura y de este apunte. Si desea más información, se cita un excelente trabajo de tesis en: https://repository.unad.edu.co/bitstream/handle/10596/40365/rtorrescar.pdf?sequence=3&isAllowed=y.

También se puede consultar el artículo “GNU privacy guard” en https://www.gnupg.org/gph/es/manual/c190.html

6.8 MÓDULO DE PLATAFORMA CONFIABLE

Trusted Platform Module (TPM, también conocido como ISO /IEC 11889) es un estándar internacional para un criptoprocesador seguro, un microcontrolador dedicado, diseñado para

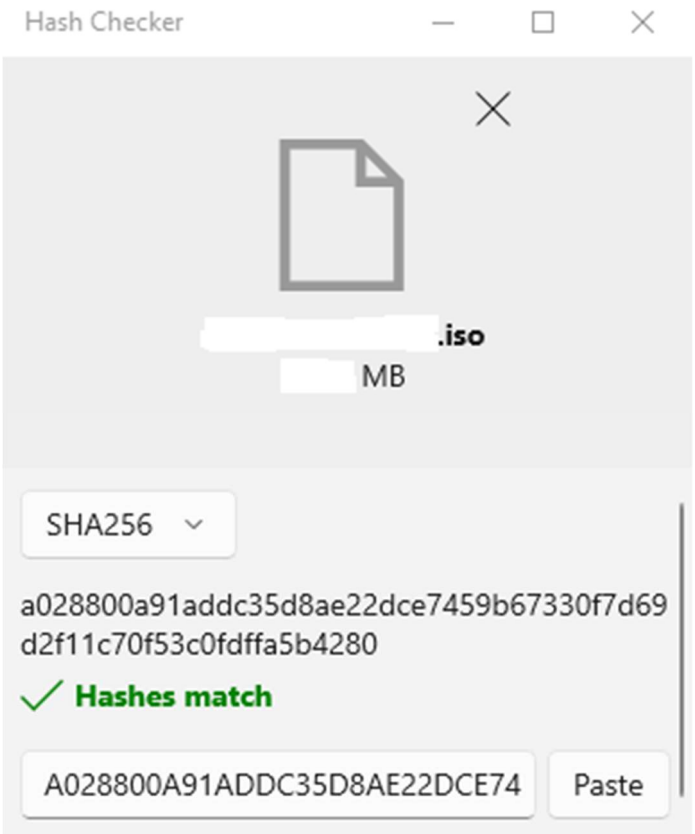
proteger el hardware a través de claves criptográficas integradas. El término también puede referirse a un chip que cumple con el estándar.

Trusted Platform Module proporciona:

- Un generador de números aleatorios por hardware
- Facilidades para la generación segura de claves criptográficas para usos limitados.
- Atestación remota: crea un resumen de clave hash casi indescifrable de la configuración de hardware y software. El software encargado de "hashear" los datos de configuración determina el alcance del resumen. Esto permite a un tercero verificar que el software no se ha cambiado. Los archivos que se descargan de Internet suelen suministrarse con un texto que contiene el valor calculado de hash y el algoritmo, por ejemplo, hash256.

  En la Store de Windows hay programas para verificar este chequeo, por ejemplo, Hash Checker, del que se muestra una imagen en la figura 6.7.3.

  También se puede realizar la verificación on line, pero esto conlleva "subir" el archivo en cuestión a una página web.
- Enlace: Cifra los datos utilizando la clave de enlace TPM, una clave RSA única descendiente de una clave de almacenamiento.
- Sellado: Similar al enlace, pero, además especifica el estado TPM para los datos que se descifrará.
- Otras funciones de Trusted Computing (Computación confiable) para que los datos se descifren.



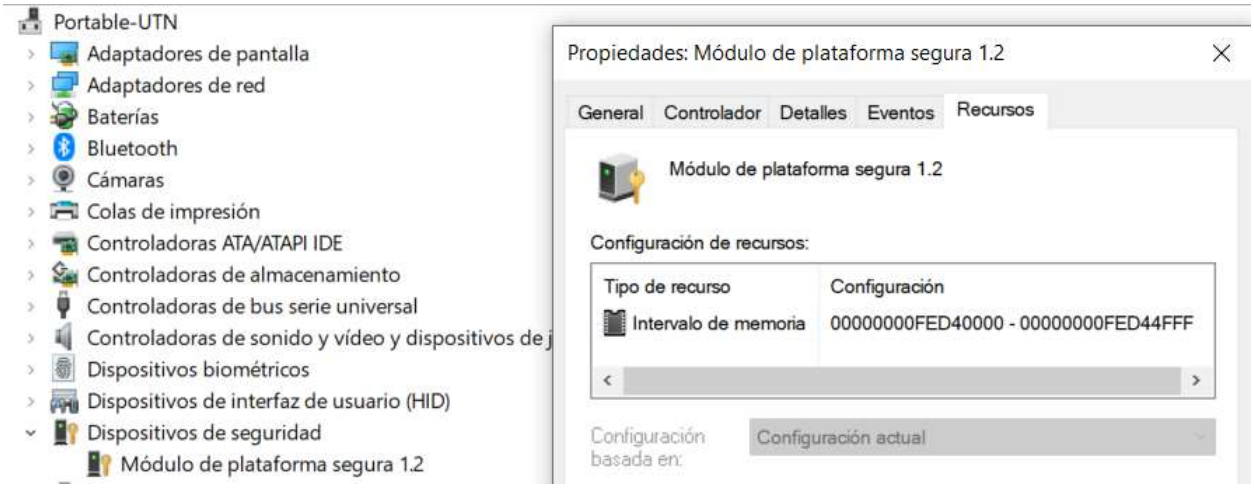
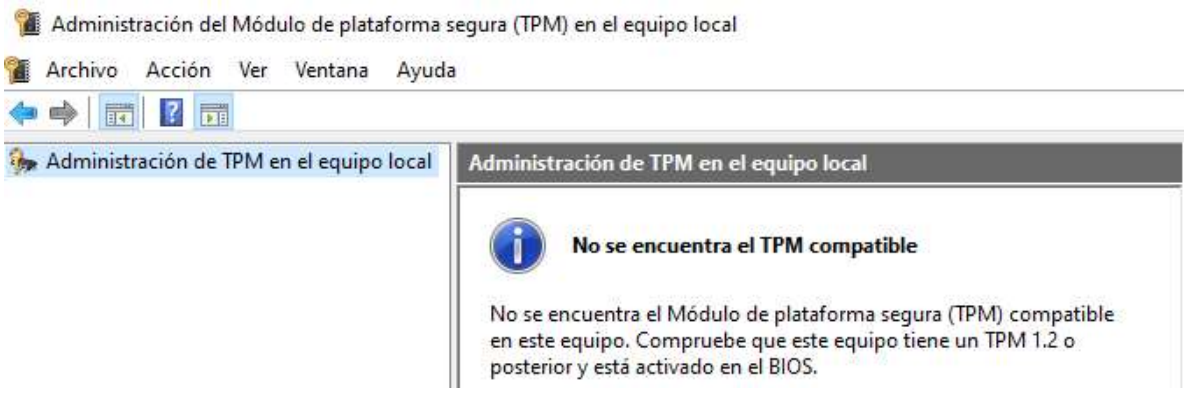
- **Figura 6.8.1 – Programa Hash Checker**

Los programas informáticos pueden usar un TPM para autenticar dispositivos de hardware, ya que cada chip TPM tiene una clave de aprobación (EK) única y secreta que se graba a medida que se produce. La seguridad integrada en el hardware proporciona más protección que una solución solo de software.

El Departamento de Defensa de los Estados Unidos (DoD) especifica que "los nuevos activos informáticos (por ejemplo, servidor, computadora de escritorio, computadora portátil, cliente ligero, tableta, teléfono inteligente, asistente digital personal, teléfono móvil) adquiridos para admitir el DoD incluirán una versión 1.2 o superior de TPM cuando lo requieran las Guías de Implementación Técnica de Seguridad (SURG) de la Agencia de Sistemas de Información de Defensa (DISA) y donde dicha tecnología esté disponible". El Departamento de Seguridad anticipa que TPM se utilizará para la identificación, autenticación, cifrado y verificación de la integridad del dispositivo.

La última versión de Windows, Windows 11, exige que el dispositivo donde será instalado posea al menos TPM 2.

En una PC con esta característica, el administrador de dispositivos de Windows muestra un aspecto similar al de la figura siguiente.



Para verificar si su PC tiene habilitado el módulo TPM, se debe ejecutar el comando de consola tpm.msc. En este caso, TPM está deshabilitado o no existe.