TIPOS DE MALWARE

Acrónimo para el software malicioso, malware es cualquier código que pueda utilizarse para robar datos, evitar los controles de acceso, ocasionar daños o comprometer un sistema. A continuación, se encuentran algunos tipos comunes de malware:

- **Spyware:** este malware está diseñado para rastrear y espiar al usuario. El spyware a menudo incluye rastreadores de actividades, recopilación de pulsaciones de teclas y captura de datos. En el intento por superar las medidas de seguridad, el spyware a menudo modifica las configuraciones de seguridad. El spyware con frecuencia se agrupa con el software legítimo o con caballos troyanos.

- **Adware:** el software de publicidad está diseñado para brindar anuncios automáticamente. El adware a veces se instala con algunas

versiones de software. Algunos adwares están diseñados para brindar solamente anuncios, pero también es común que el adware incluya spyware.

- **Bot:** de la palabra robot, un bot es un malware diseñado para realizar acciones automáticamente, generalmente en línea. Si bien la mayoría de los bots son inofensivos, un uso cada vez más frecuente de bots maliciosos es el de los botnets. Varias computadoras pueden infectarse con bots programados para esperar silenciosamente los comandos provistos por el atacante.

- **Ransomware:** este malware está diseñado para mantener captivo un sistema de computación o los datos que contiene hasta que se realice un pago. El ransomware trabaja generalmente encriptando los datos de la computadora con una clave desconocida para el usuario. Algunas otras versiones de ransomware pueden aprovechar vulnerabilidades específicas del sistema para bloquearlo. El ransomware se esparce por un archivo descargado o alguna vulnerabilidad de software.

- **Scareware:** este tipo de malware está diseñado para persuadir al usuario de realizar acciones específicas en función del temor. El scareware falsifica ventanas emergentes que se asemejan a las ventanas de diálogo del sistema operativo. Estas ventanas muestran mensajes falsificados que indican que el sistema está en riesgo o necesita la ejecución de un programa específico para volver al funcionamiento normal. En realidad, no se evaluó ni detectó ningún problema y, si el usuario acepta y autoriza la ejecución del programa mencionado, el sistema se infecta con malware.

- **Rootkit:** este malware está diseñado para modificar el sistema operativo a fin de crear una puerta trasera. Los atacantes luego utilizan la puerta trasera para acceder a la computadora de forma remota. La mayoría de los rootkits aprovecha las vulnerabilidades de software para realizar el escalamiento de privilegios y modificar los archivos del sistema. También es común que los rootkits modifiquen las herramientas forenses de supervisión del sistema, por lo que es muy difícil detectarlos. A menudo, una computadora infectada por un rootkit debe limpiarse y reinstalarse.

- **Virus:** un virus es un código ejecutable malintencionado que se adjunta a otros archivos ejecutables, generalmente programas legítimos. La mayoría de los virus requiere la activación del usuario final y puede activarse en una fecha o un momento específico. Los virus pueden ser inofensivos y simplemente mostrar una imagen o pueden ser destructivos, como los que modifican o borran datos. Los virus también pueden programarse para mutar a fin de evitar la detección. La mayoría de los virus ahora se esparcen por unidades USB, discos ópticos, recursos de red compartidos o correo electrónico

- **Troyano:** un troyano es malware que ejecuta operaciones maliciosas bajo la apariencia de una operación deseada. Este código malicioso ataca los privilegios de usuario que lo ejecutan. A menudo, los troyanos se encuentran en archivos de imagen, archivos de audio o juegos. Un troyano se diferencia de un virus en que se adjunta a archivos no ejecutables.

- **Gusanos:** los gusanos son códigos maliciosos que se replican mediante la explotación independiente de las vulnerabilidades en las redes. Los gusanos, por lo general, ralentizan las redes. Mientras que un virus requiere la ejecución de un programa del host, los gusanos pueden ejecutarse por sí mismos. A excepción de la infección inicial, ya no requieren la participación del usuario. Una vez infectado el host, el gusano puede propagarse rápidamente por la red. Los gusanos comparten patrones similares. Todos tienen una vulnerabilidad de activación, una manera de propagarse y contienen una carga útil.

Los gusanos son responsables de algunos de los ataques más devastadores en Internet. En 2001 el gusano Código Rojo infectó 658 servidores. En el plazo de 19 horas, el gusano infectó más de 300 000 servidores.

- **Hombre en el medio (MitM):** el MitM permite que el atacante tome el control de un dispositivo sin el conocimiento del usuario. Con ese nivel de acceso, el atacante puede interceptar y capturar información sobre el usuario antes de retransmitirla a su destino. Los ataques MitM se usan ampliamente para robar información financiera. Existen muchas técnicas y malware para proporcionar capacidades de MitM a los atacantes.

- **Hombre en el móvil (MitMo):** una variación del hombre en el medio, el MitMo es un tipo de ataque utilizado para tomar el control de un dispositivo móvil. Cuando está infectado, puede ordenarse al dispositivo móvil que exfiltre información confidencial del usuario y la envíe a los atacantes. ZeuS, un ejemplo de ataque con capacidades de MitMo, permite que los atacantes capturen silenciosamente SMS de verificación de 2 pasos enviados a los usuarios.

SÍNTOMAS DE MALWARE

Independientemente del tipo de malware con el que se ha infectado un sistema, estos son síntomas frecuentes de malware:

- Aumento del uso de la CPU.
- Disminución de la velocidad de la computadora.
- La computadora se congela o falla con frecuencia.
- Hay una disminución en la velocidad de navegación web.
- Existen problemas inexplicables con las conexiones de red.
- Se modifican los archivos.
- Se eliminan archivos.
- Hay una presencia de archivos, programas e iconos de escritorio desconocidos.
- Se ejecutan procesos desconocidos.
- Los programas se cierran o reconfiguran solos.

- Se envían correos electrónicos sin el conocimiento o el consentimiento del usuario.

¿QUÉ HACER SI TENGO UN MALWARE?

Si se cree que el equipo se encuentra infectado con algún tipo de malware, se pueden seguir ciertos consejos para no comprometer la información disponible en dicho sistema, así como tampoco sufrir del robo de datos de origen crítico:

1. **Desconectar el equipo de Internet:** Esto impedirá que el malware que infectó el equipo continúe propagándose por la red, así como también una posible reinfección online luego de la limpieza.

2. **Si no se posee un programa antivirus, instalar alguno en esta instancia:** Siempre es recomendable algún software con capacidad de detección proactiva

de amenazas. Descargar y actualizar la base de firmas del antivirus instalado previamente para contar con la última actualización y así poder realizar un análisis del equipo más eficiente.

3. **Realizar un análisis completo del sistema:** Efectuar un análisis completo de los discos del equipo en busca de amenazas.

4. **Modificar las contraseñas de los correos, cuentas de redes sociales y cualquier servicio que requiera autenticación:** Este procedimiento debe efectuarse para eliminar toda posibilidad de robo de credenciales por parte del cibercriminal detrás del malware.

5. **En caso de ser necesario, realizar una limpieza manual:** Muchas veces luego de una infección no es suficiente escanear el sistema y realizar una limpieza automatizada. Es por esto que en ciertas ocasiones se debe efectuar una limpieza manual. Para poder llevar a cabo esta tarea, es recomendable identificar de qué tipo de malware se trata para luego buscar el método correcto de desinfección.

Estos pasos son un buen punto de partida en el caso que se sospeche que el equipo ha sido infectado por malware. Además, esto debe complementarse con la serenidad por parte del usuario, es decir, no entrar en pánico, ya que muchas veces esto puede derivar en acciones que comprometan aún más el sistema. Finalmente, se le recomienda al usuario leer la guía de consejos completa sobre qué hacer en el caso de que se confirme la infección.