Tipos de virus

1. Worm

Un gusano es un malicioso, y autorreplicante programa que puede extenderse a través de una red sin ayuda humana.

Los gusanos causan daños similares a los virus normales, explotando agujeros en el software de seguridad y potencialmente robando información confidencial, corrompiendo archivos e instalando una puerta trasera para acceso remoto al sistema, entre otros problemas.

A menudo utilizan grandes cantidades de memoria y ancho de banda, por lo que los servidores, redes y sistemas individuales afectados a menudo se sobrecargan y dejan de responder; pero los gusanos no son virus. Los virus necesitan una computadora host o sistema operativo. El programa de gusanos funciona solo.

El gusano a menudo se transmite a través de redes de intercambio de archivos, funciones de transporte de información, archivos adjuntos de correo electrónico o haciendo clic en enlaces a sitios web maliciosos. Una vez descargado, el gusano aprovecha una debilidad en su sistema de destino o engaña a un usuario para que lo ejecute.

Las clasificaciones y nombres de gusanos incluyen:
- Gusano de e-mail
- Gusano IM
- Gusano IRC
- Gusano Neto
- Gusano P2P

El gusano más famoso según un articulo del 2019, escrito por Mark Bowden para el diario New York Times, cuenta como el **Conficker,** afecto a 10 millones de computadoras. Dicho gusano explota una vulnerabilidad en el servicio Windows Server en los sistemas Windows 2000, Windows XP, Windows Vista, Windows Server 2003 y Windows Server 2008.

El sistema de operación de **Conficker** empieza al propagarse el gusano a sí mismo principalmente a través de una vulnerabilidad del desbordamiento de búfer del servicio Server de Windows. Usa una solicitud RPC especialmente desarrollada para ejecutar su código en el computador objetivo.

Cuando ha infectado un computador, Conficker desactiva varios servicios, como Windows Automatic Update, Windows Security Center, Windows Defender y Windows Error Reporting. Luego se contacta con un servidor, donde recibe instrucciones posteriores sobre propagarse, recolectar información personal o descargar malware adicional en el computador víctima. El gusano también se une a sí mismo a ciertos procesos tales como svchost.exe, explorer.exe y services.exe.

2. Ransomware

Un ransomware 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.
Normalmente un ransomware se transmite como un troyano o como un gusano, infectando el sistema operativo, por ejemplo, con un archivo descargado o explotando una vulnerabilidad de software. En

este punto, el ransomware se iniciará, cifrará los archivos del usuario con una determinada clave, que solo el creador del ransomware conoce, e instará al usuario a que la reclame a cambio de un pago.

El más famoso de los ransomware es **WannaCry** o también conocido como **WanaCrypt0r**, que apareció el 12 de mayo de 2017 con origen en el arsenal estadounidense de malware Vault 7 revelado por Wikileaks pocas semanas antes, el código malicioso ataca una vulnerabilidad descrita en el boletín MS17-010 en sistemas Windows que no estén actualizados de una manera adecuada.

Provocó el cifrado de datos en más de 75 mil ordenadores por todo el mundo afectando, entre otros, a:

- Rusia: red semafórica, metro e incluso el Ministerio del Interior;
- Reino Unido: gran parte de los centros hospitalarios;
- España: empresas tales como Telefónica, Gas Natural e Iberdrola.

El ransomware cifra los datos que, para poder recuperarse, pide que se pague una cantidad determinada, en un tiempo determinado. Si el pago no se hace en el tiempo determinado, el usuario no podrá tener acceso a los datos cifrados por la infección. WannaCry se ha ido expandiendo por Estados Unidos, China, Rusia, Italia, Taiwán, Reino Unido y España, al igual de que se señala que los sistemas operativos más vulnerables ante el ransomware son Windows Vista, Windows 7, Windows Server 2012, Windows 10 y Windows Server 2016.

Un ordenador infectado que se conecte a una red puede contagiar el ransomware a otros dispositivos conectados a la misma, pudiendo infectar a dispositivos móviles. A su inicio, WanaCrypt0r comienza a cifrar los archivos de la víctima de una manera muy rápida.

3. Timebomb

Un programa malicioso que está programado para "detonar" en un momento específico y liberar un virus en el sistema informático o la red.

El mayor representante de este tipo de virus es **Michelangelo**, ya que este tiene como día de activación el 6 de marzo, coincidentemente con la conmemoración del cumpleaños del famoso artista italiano Miguel Ángel, el 6 de marzo de 1475. De ahí el nombre del virus.

El método de infección de **Michelangelo** sigue este patrón:

- Se transmite al ordenador cuando éste se arranca con un disquete contaminado por el virus.
- Desde el disquete infectado, Michelangelo se coloca como residente en la memoria del ordenador. Concretamente, el virus ocupa 2048 Bytes en la TOM (Top of memory o memoria alta).
- Desde la memoria, Michelangelo infecta todos los disquetes que se utilicen. Para ello intercepta las interrupciones de acceso a disquetes.
- Michelangelo mueve el sector de arranque original del disco duro (del sector 0, cara 1, cilindro 0 al sector 7, cara 0, cilindro 0).

Los efectos de **Michelangelo** son:

- Infecta el sector de arranque de los disquetes (Boot) y el de los discos duros (Master Boot Record o MBR).
- Sustituye el sector de arranque original del disco duro por otro infectado. Esto lo consigue moviendo el sector de arranque original a otra sección del disco duro. Esta técnica se conoce como Stealth.

- Infecta todos los disquetes que se utilicen en el ordenador afectado, siempre que no estén protegidos contra escritura.
- Cuando se activa, el 6 de marzo, sobreescribe la información incluida en parte del disco duro.
- De hecho, destruye toda la información contenida en la pista 0, más concretamente los primeros 17 sectores de las cuatro primeras caras en los 250 primeros cilindros del disco infectado. Esto supone una pérdida de la información contenida en 8 MB, aproximadamente.
- En esta sección se encuentra la Tabla de Asignación de Ficheros (FAT) y la información del directorio raíz, por lo que tras la infección, el disco será inaccesible.

https://www.infobae.com/america/tecno/2018/05/12/como-surgio-y-se-propago-wannacry-uno-de-los-ciberataques-mas-grandes-de-la-historia/
https://www.vipre.com/resource/what-is-a-worm-virus/
https://www.nytimes.com/2019/06/29/opinion/sunday/conficker-worm-ukraine.html
https://es.wikipedia.org/wiki/Conficker