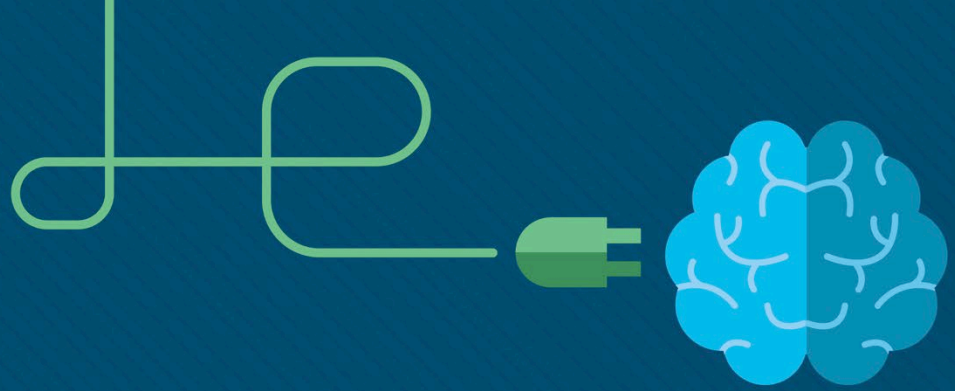


Seguridad informática Qué debemos conocer

Helber Leandro Baez Rodriguez
Especialista en Seguridad Informatica
hbaez@ucompensar.edu.co
SENA – CENIGRAF
25 de Julio del 2024

¿Quién ataca nuestra red?

Amenaza, vulnerabilidad y riesgo

- **Amenaza:** Peligro potencial de un recurso, como los datos o la red.

- **Vulnerabilidad y superficie de ataque:** **Debilidad** en un sistema o en su diseño que podría ser atacada por una amenaza.
  - La superficie de ataque describe diferentes puntos donde un atacante podría filtrarse en un sistema y obtener los datos (por ejemplo: sistema operativo sin parches de seguridad).

- **Explotar vulnerabilidades:** Mecanismo utilizado para aprovechar una vulnerabilidad con el fin de comprometer un recurso.

- **Riesgo:** Probabilidad de que una amenaza específica aproveche una vulnerabilidad de un activo y provoque una consecuencia indeseable.

¿Quién ataca nuestra red?

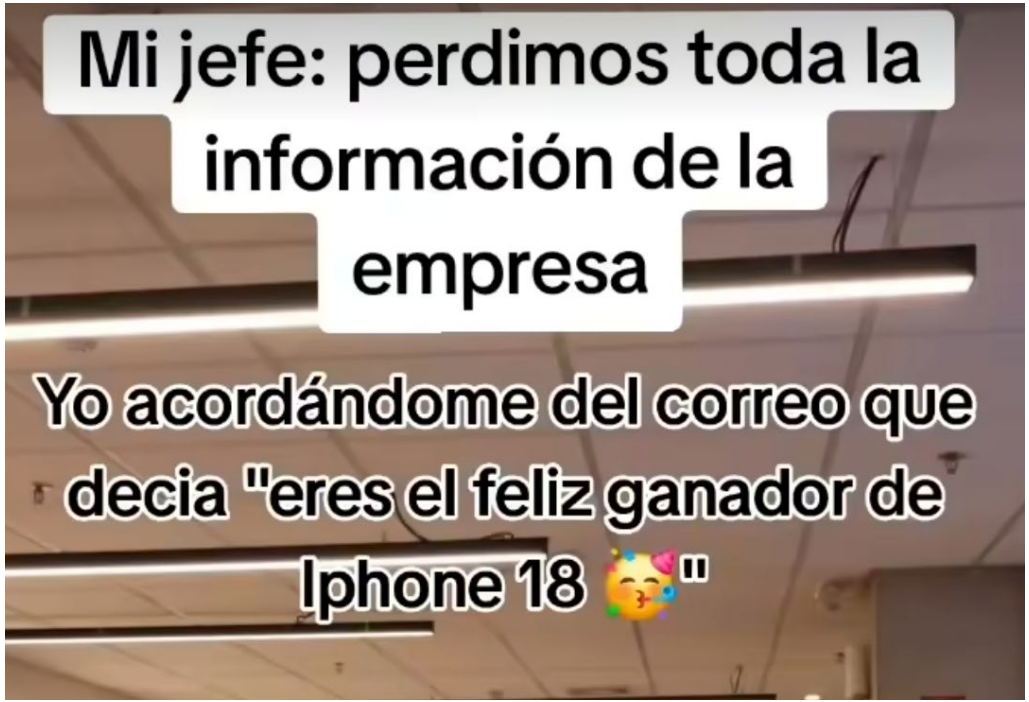
Hacker vs. actor de una amenaza

- **Hackers de sombrero blanco:** éticos utilizan sus habilidades de programación para fines buenos, éticos y legales. Realizan pruebas de penetración para descubrir vulnerabilidades y reportar a los desarrolladores antes de un ataque.
- **Hackers de sombrero gris:** Cometen delitos y hacen cosas probablemente poco éticas, pero no para beneficio personal o ni para causar daños. Puede comprometer la red, divulgar el problema para que la organización pueda solucionarlo.
- **Hackers de sombrero negro:** Delincuentes poco éticos que violan la seguridad para beneficio personal o por motivos maliciosos, como ataques a la red.

Actores de amenazas término empleado para describir hackers de sombrero gris o negro.

- https://cybermap.kaspersky.com/es
- https://threatmap.checkpoint.com/
- http://threatmap.fortiguard.com/
- https://www.fireeye.com/cyber-map/threat-map.html
- https://threatmap.bitdefender.com/
- https://livethreatmap.radware.com/

Responsabilidad como Usuarios



¿Quién ataca nuestra red?

Evolución de los actores de amenazas

- **Script kiddies**: Hackers inexpertos que ejecutan herramientas y ataques existentes para ocasionar daño, pero generalmente no para obtener ganancias.
- **Patrocinados por el estado:** De sombrero blanco o negro que roban secretos de gobierno, recopilan inteligencia y sabotean las redes. https://threatmap.checkpoint.com/
  - Sus objetivos son los gobiernos, los grupos terroristas y las corporaciones extranjeras.
- **Ciberdelincuentes:** sombrero negro robo de miles de millones de dólares en los consumidores y las empresas.
- **Hacktivistas:** sombrero gris que se reúnen y protestan contra ideas políticas y sociales.
  - Publicar artículos y vídeos pérdida de información confidencial.
- **Agentes de vulnerabilidad:** Descubren ataques y los reportan a proveedores, a veces por premios o recompensas.

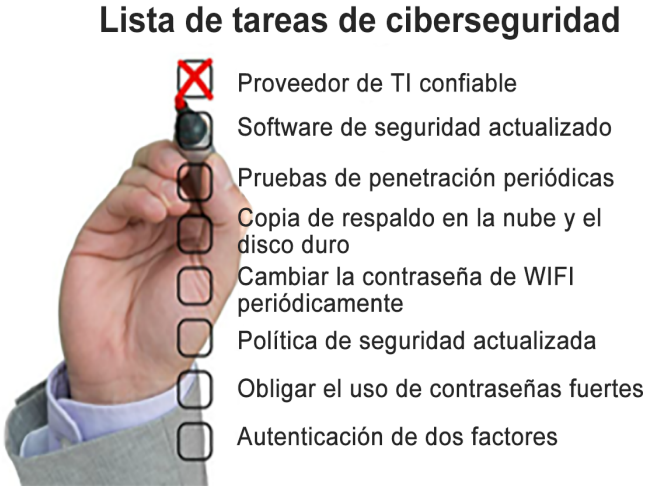
¿Quién ataca nuestra red?

Ciberdelincuentes

- Actores de amenazas motivados por dinero.
- Compran, venden e intercambian ataques, información privada y propiedad intelectual.
- Roban de consumidores, pequeñas empresas y grandes empresas e industrias.
- https://threatmap.fortiguard.com/

Tareas de ciberseguridad

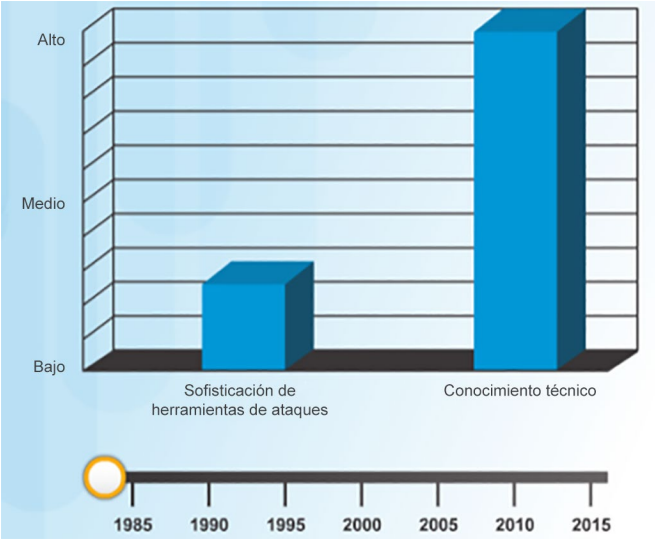
- Desarrolle conciencia sobre una buena ciberseguridad. El eslabón mas débil
- Informe la ciberdelincuencia a autoridades. CERT
- Tome conocimiento de posibles amenazas por E-mail y Web. Boletines internacionales
- Proteja información importante de robo.
- Las organizaciones deben tomar medidas y proteger sus activos, usuarios y clientes.
- Desarrollan tareas de ciberseguridad y las implementan de forma recurrente.

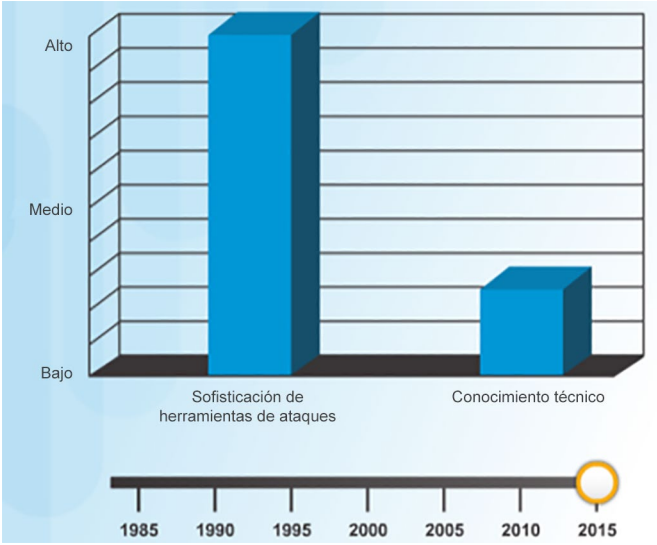


Introducción a las herramientas de ataque

- Los atacantes emplean herramientas para aprovecharse de las vulnerabilidades.

- La sofisticación de las herramientas de los ataques y el conocimiento técnico han avanzado mucho desde 1985.





Evolución de las herramientas de seguridad

- Herramientas de pruebas de penetración comunes
  - **Decodificadores de contraseñas**: hacen repetidos intentos por averiguar las contraseñas para decodificarlas y acceder al sistema.
  - **Herramientas de hacking inalámbrico**: hackean intencionalmente una red inalámbrica con el fin de detectar vulnerabilidades en la seguridad.
  - **Herramientas de hacking y análisis de la red**: sondean dispositivos, servidores y hosts de red en busca de puertos abiertos.
  - **Herramientas de fabricación de paquetes**: sondean y prueban la solidez de un firewall usando paquetes especialmente diseñados.
  - **Analizadores de protocolos de paquetes**: capturan y analizan paquetes en redes Ethernet LAN o WLAN tradicionales.
  - **Detectores de rootkits**: comprobador de integridad de archivos y directorios utilizado por hackers de sombrero blanco para detectar rootkits instalados.
  - **Fuzzers** : intentan descubrir las vulnerabilidades de seguridad de un sistema informático.
  - **Herramientas de informática forense**: detectan cualquier rastro de evidencia existente en un sistema informático. Costosas. cain
  - **Herramientas de depuración**: aplican ingeniería inversa en archivos binarios cuando programan ataques o analizan malware.
  - **Sistemas operativos de hacking**: sistemas operativos diseñados precargados con herramientas y tecnologías optimizadas para hacking.
  - **Herramientas de encriptación**: utilizan esquemas de algoritmo para codificar los datos a fin de prevenir el acceso no autorizado a los datos encriptados.
  - **Herramientas de ataque de vulnerabilidad**: determinan si un host remoto es vulnerable a un ataque a la seguridad.
  - **Escáneres de vulnerabilidad**: analizan una red o un sistema para identificar puertos abiertos.

Repositorios de herramientas de ataques

- http://www.yolinux.com/TUTORIALS/LinuxSecurityTools.html
- https://sectools.org/
- https://sectools.org/tag/pass-audit/
- https://resources.infosecinstitute.com/10-popular-password-cracking-tools/
- https://sectools.org/tag/sniffers/
- https://sectools.org/tag/forensics/
- https://sectools.org/tag/vuln-scanners/
- https://sectools.org/tag/web-scan
- https://sectools.org/tag/web-scanners/
- https://sectools.org/tag/wireless/
- https://sectools.org/tag/sploits/ https://sectools.org/tag/packet-crafters/

Categorías de ataques a redes

- **Interceptación**: captura y escuchar el tráfico de red.
- **Modificación de datos**: altera los datos en el paquete sin el conocimiento del remitente o del receptor.

- **Suplantación de direcciones IP**: crea un paquete IP que parece surgir de una dirección válida dentro de la intranet.
- **Basado en contraseñas**: usa esa cuenta válida robada para obtener listas de otros usuarios e información de la red.

- **Denegación de servicio**: impide el uso normal de un PC o red por parte de usuarios válidos. A servicios
- **Ataque man-in-the-middle**: se colocan entre un origen y un destino para monitorear, capturar y controlar la comunicación.

- **Clave comprometida**: se obtiene una clave secreta mediante el acceso a una comunicación asegurada sin que el emisor ni el receptor se enteren del ataque.
- **Analizador de protocolos**: una aplicación o un dispositivo que puede leer, monitorear y capturar intercambios de datos en la red y leer paquetes de red.

Tipos de malware

- **Malware:** Abreviatura de software malicioso o código malicioso. diseñado para dañar, alterar, robar o infligir acciones ilegítimas en los hosts o redes de datos.
- Cualquier software malicioso, para dañar sistemas

Malware
Virus

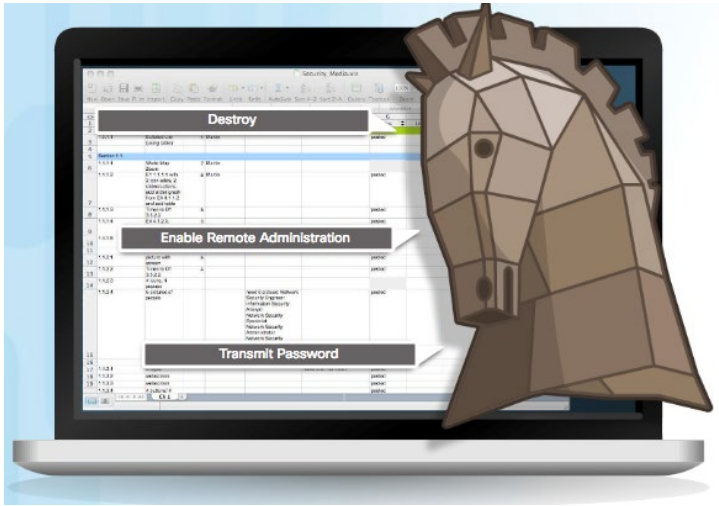
- **Malware que se propaga mediante la inserción de una copia de sí mismo en otro programa**.
- Se propaga de un PC a otro, infectándolas a todas.
- Se propaga mediante unidades de memoria USB, CD, DVD, recursos compartidos de red y correo electrónico.
- Puede permanecer inactivo y, luego, activarse en una fecha y hora determinadas.
- **Exige que un ser humano introduzca el código malicioso en otro programa**.
- Ejecuta una función no deseada específica y, generalmente, dañina en una computadora.

Malware

Caballo de Troya

- **Código malicioso que está diseñado para parecer legítimo**. Generadores de claves. Para piratería. O licenciar programas.
- A menudo se encuentran unidos a juegos en línea.
- **No se replica a sí mismo**.
- Ataca los privilegios de usuario que ejecutan el malware.
- Puede causar daños inmediatos, proporcionar acceso remoto al sistema o permitir el acceso mediante una puerta trasera

Clasificación de los caballos de Troya



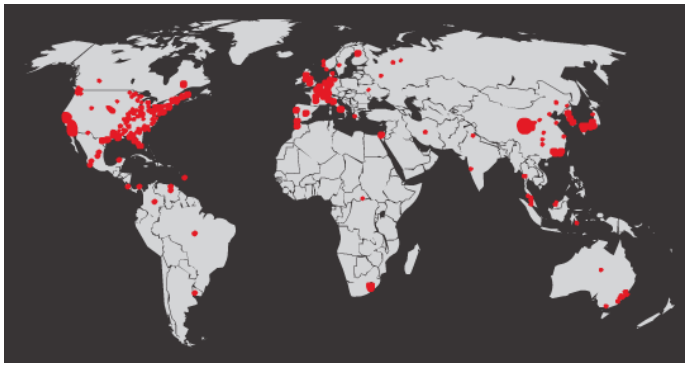
- **Caballo de Troya de acceso remoto**: permite el acceso remoto no autorizado.
- **Caballo de Troya de envío de datos**: proporciona al actor de amenaza datos confidenciales, como contraseñas. O hash
- **Caballo de Troya destructivo**: daña o elimina archivos.
- **Caballo de Troya de proxy**: utiliza la PC de la víctima como dispositivo de origen para lanzar ataques y realizar otras actividades ilegales.
- **Caballo de Troya de FTP**: habilita servicios no autorizados de transferencia de archivos en terminales. Servicio en desuso
- **Caballo de Troya habilitador del software de seguridad**: detiene el funcionamiento de programas antivirus o firewalls.
- **Caballo de Troya de DoS**: retarda o detiene la actividad de red.

Malware

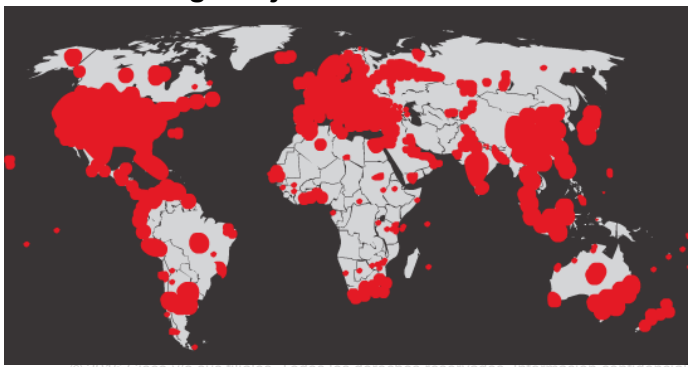
Gusanos

- **Ejecuta un código arbitrario y se instala a sí mismo en la memoria del dispositivo infectado**.
- **Se replica automáticamente y se esparce por la red de un sistema al otro**.
- Los ataques de gusanos consisten en el aprovechamiento de una vulnerabilidad, el envío de una carga útil maliciosa y la propagación automática.
- **Mientras que un virus requiere la ejecución de un programa del host, los gusanos pueden ejecutarse por sí mismos**.

Infección inicial del gusano Código Rojo: 658 servidores

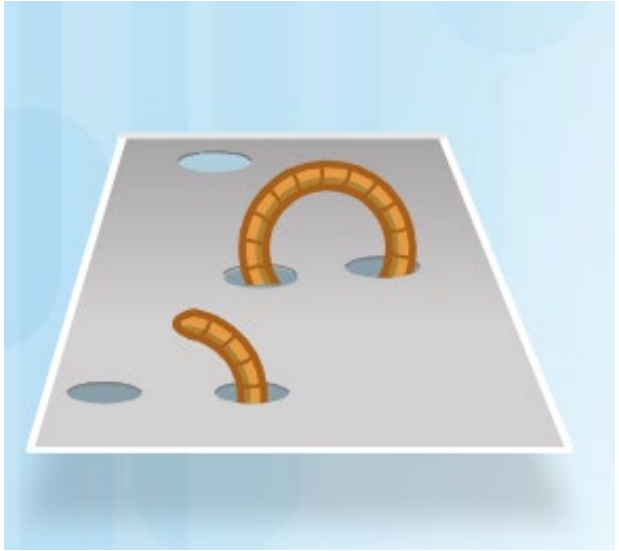


19 horas después de la infección del gusano Código Rojo 300.000 servidores



Componentes de un gusano

- Los ataques de gusanos consisten de tres componentes:
  - **Vulnerabilidad**: se instala a sí mismo en un sistema vulnerable utilizando un mecanismo de ataque, como un archivo adjunto de E-mail, un archivo ejecutable o un caballo de Troya.
  - **Mecanismo de propagación**: después de tener acceso a un dispositivo, se replica y localiza nuevos objetivos.
  - **Carga útil**: cualquier código malicioso que produce alguna acción que resulta ser una carga útil y se utiliza para crear una puerta posterior que permite que un agente de amenaza tenga acceso al host infectado o para crear un ataque de DoS.



Malware

Ransomware

- Niega el acceso al sistema informático infectado o a sus datos. https://www.youtube.com/watch?v=6BvvdrCk59c
- Exigen dinero para liberar el sistema informático.
- Suele utilizar un algoritmo de cifrado para encriptar datos y archivos de sistema, y no se puede descifrar fácilmente.
- La publicidad malintencionada y por E-mail constituye vectores para las campañas de ransomware.
- **También se utiliza ingeniería social**. Los ciberdelincuentes (que se identifican como técnicos de seguridad) llaman a los hogares y convencen a los usuarios para que se conecten a un sitio web que descarga el ransomware a un PC del usuario.
- https://www.youtube.com/watch?v=7RfLGngLsSs

Otros tipos de malware

- Malware moderno
  - **Spyware**: recolectar información sobre un usuario y enviar información a otra entidad, sin el consentimiento del usuario. Puede ser un monitor del sistema, caballo de Troya, Adware, las cookies de seguimiento y registradores. https://www.youtube.com/watch?v=6BvvdrCk59c&t=106s
  - **Adware**: muestra los elementos emergentes molestos para generar ingresos para sus autores. analizar intereses de un usuario al hacer un seguimiento de los sitios web que haya visitado y enviar publicidad pertinente a esos sitios.
  - **Scareware**: software de estafa utiliza ingeniería social para sorprender o generar ansiedad ante una percepción de una amenaza. dirigido a un usuario desprevenido e intenta convencerlo para infectar su PC adoptando medidas falsas que solucionan las supuestas amenazas.
  - **Suplantación de identidad (phishing)**: intenta convencer a las personas para que divulguen información sensible. Algunos ejemplos incluyen recibir un E-mail del banco en el que se solicita divulgar números de cuenta y códigos PIN, mensajes de texto.
  - **Rootkits**: se instala en un sistema en riesgo. permanece oculto y proporciona acceso privilegiado al agente de amenaza.

Comportamientos comunes del malware

- Con frecuencia, los PC infectadas con malware manifiestan uno o más de los siguientes:
  - Aparecen archivos, programas o iconos del escritorio extraños.
  - Los programas antivirus y firewall se apagan o sus ajustes se reconfiguran.
  - La pantalla de la computadora se detiene o el sistema deja de funcionar.
  - Se envían mensajes de correo electrónico espontáneos a su lista de contactos sin su conocimiento.
  - Se modifican o eliminan archivos.
  - Se intensifica el uso de la CPU o de la memoria.
  - Hay problemas para conectarse a redes.
  - Se reduce la velocidad de la computadora o el navegador web.
  - Se ejecutan procesos o servicios desconocidos.
  - Se abren puertos TCP o UDP desconocidos.
  - Se efectúan conexiones a hosts en Internet sin que el usuario las realice.
  - La computadora se comporta de manera extraña.

Ataques de ingeniería social

- Tipo de ataque de acceso busca manipular a los individuos para que hagan cosas o divulguen información confidencial necesaria para acceder a redes. Algunos ejemplos son los siguientes:
  - **Pretexto:** llama a una persona y le miente en un intento de obtener acceso a datos privilegiados. Finge necesitar datos personales o financieros para confirmar la identidad del destinatario.
  - **E-mail no deseado**: para engañar a un usuario a fin de que haga clic en un enlace infectado o descargue un archivo infectado.
  - **Suplantación de identidad**: envía E-mail no deseado personalizado con mensajes atractivos dirigido a personas con la meta de que el usuario objetivo haga clic en un enlace o descargue código malicioso.
  - **Algo por algo (quid pro quo)**: solicita información personal a cambio de algo, por ejemplo, un obsequio.
  - **Infiltración (tailgating)**: sigue rápidamente a una persona autorizada con una insignia corporativa mientras ingresa en un lugar que requiere autorización. https://www.youtube.com/watch?v=GIlS5eJHYNI
  - **Hostigamiento**: deja un dispositivo físico infectado con malware, como una unidad flash USB, en un lugar público, como el baño de una empresa. El buscador encuentra el dispositivo y lo inserta en su computadora.
  - **Hacking visual**: observa físicamente a la víctima introducir credenciales, tales como los datos para iniciar sesión en una estación de trabajo, un PIN de cajero automático o la combinación de una cerradura física. También conocido como "**espiar por encima del hombro**".

Ataques de ingeniería social

- **Suplantación de identidad**: utilizan para enviar E-mail que parecen provenir de una organización legítima (como un banco). Las variantes incluyen:
  - **Phishing dirigido (spear phishing)**: adaptado a un individuo u organización específicos, y es más probable que logre engañar al objetivo.
  - **Phishing dirigido especializado (whaling):** similar al dirigido, se centra en objetivos grandes, como los ejecutivos principales de una organización.
  - **Phishing en granja (pharming)**: pone en peligro los servicios de DNS al inyectar entradas en archivos de host local. incluye el envenenamiento del DNS al poner en riesgo los servidores DHCP que especifican los servidores DNS.
  - **Ataque "watering hole"**: determina los sitios web que un grupo de destino con regularidad visitas e intenta atacar esos sitios infectándolos con malware que pueda identificar y atacar solamente a miembros del grupo objetivo.
  - **Phishing por voz (Vishing)**: ataque de phishing utilizando la voz y el sistema telefónico en lugar del correo electrónico.
  - https://www.youtube.com/watch?v=Rpr9V-8QEoU
  - **Phishing por SMS (smishing)**: ataque de phishing mediante mensajes SMS en lugar de correo electrónico. https://www.youtube.com/watch?v=7iWF-DEfs-I

Fortalecimiento del eslabón más débil

- Por lo general, las personas son el eslabón más débil en ciberseguridad.
- Las organizaciones deben capacitar activamente al personal y fomentar una "cultura enfocada en la seguridad".

Métodos de evasión

- Los actores maliciosos entendieron hace mucho que el malware y los métodos de ataque de más eficacia son los que no se detectan.
- Métodos de evasión son **la encriptación, los túneles, el agotamiento de recursos, la fragmentación de tráfico, la interpretación errónea a nivel de protocolo, la sustitución de tráfico, la inserción de tráfico, el pivotaje y los rootkits**.
- Todo el tiempo se desarrollan nuevos métodos de ataque, se debe estar al tanto de los más recientes para poder detectarlos.
- https://www.youtube.com/watch?v=NPE7i8wuupk

Referentes e informes recientes de ciberseguridad

- https://securelist.lat/
- https://mx.norton.com/nortonlifelock-cyber-safety-report
- https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/3767-ccn-cert-ia-13-19-ciberamenazas-y-tendencias-resumen-ejecutivo-2019/file.html
- https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf revisar Colombia
- https://www.welivesecurity.com/wp-content/uploads/2020/08/ESET-Security-Report-LATAM_2020.pdf
- https://www.ccit.org.co/wp-content/uploads/informe-tendencias-abril-2020-final.pdf analizar todos.
- https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf
- https://pro-cdo-web-resources.s3.eu-west-1.amazonaws.com/elevenpaths/uploads/2020/2/elevenpaths-informe-tendencias-ciberseguridad-2020.pdf

Comportamientos comunes del malware

- Con frecuencia, los PC infectadas con malware manifiestan uno o más de los siguientes:
  - Aparecen archivos, programas o iconos del escritorio extraños.
  - Los programas antivirus y firewall se apagan o sus ajustes se reconfiguran.
  - La pantalla de la computadora se detiene o el sistema deja de funcionar.
  - Se envían mensajes de correo electrónico espontáneos a su lista de contactos sin su conocimiento.
  - Se modifican o eliminan archivos.
  - Se intensifica el uso de la CPU o de la memoria.
  - Hay problemas para conectarse a redes.
  - Se reduce la velocidad de la computadora o el navegador web.
  - Se ejecutan procesos o servicios desconocidos.
  - Se abren puertos TCP o UDP desconocidos.
  - Se efectúan conexiones a hosts en Internet sin que el usuario las realice.
  - La computadora se comporta de manera extraña.

Tips

tips

tips

tips

tips

tips

tips

Utilizar navegadores web actualizados

Recomendaciones finales para todos

- Mantener el software actualizado
- Utilizar protección antivirus y cortafuegos
- Crear distintas cuentas de usuario
- Tomar precauciones cuando se compartan datos personales
- Únicamente deben llevarse a casa los dispositivos y datos que sean absolutamente necesarios
- Utilizar navegadores web actualizados
- Utilizar distintas contraseñas, que pueden cambiarse si es necesario
- Autenticación con doble factor

Recomendaciones finales para todos

- **Proteger, mediante cifrado, los datos**
- **Descargar datos solo de fuentes de confianza**
- **Realizar periódicamente copias de seguridad**
- **Desactivar los dispositivos inteligentes activados por voz presentes en la oficina doméstica y tapar la webcam cuando no se utilice**
- **No mezclar los usos personal y laborales**
- **Cerrar la sesión cuando no se utilicen los dispositivos y mantener estos protegidos**
- **Ser especialmente cuidadoso ante correos o adjuntos sospechosos, sobre todo cuando el remitente sea un desconocido**


CISCO