

Seguridad y Privacidad en redes

Lic. Paula Venosa



Presentación de la materia

- Plantel docente
- Objetivos
- Contenido
- Cronograma
- Forma de aprobación
- Bibliografía
- Herramientas



Motivación de la materia

- Resulta importante entender la razón por la cual es importante tener en cuenta la seguridad cuando se diseña y se administra redes, cuando se desarrollan sistemas y cuando se gestiona una organización.
- Es necesario:
 - Examinar las amenazas de seguridad existentes en las redes, servicios y sistemas.
 - Saber de qué manera incorporar medidas y mecanismos de seguridad frente a las amenazas existentes.



Qué rol juega nuestra materia

- En primer lugar comprender algunos conceptos/terminología básica relacionada con la seguridad. (Amenaza, ataque, vulnerabilidad....).
- Analizar distintas herramientas a fin de entender: riesgos existentes, cómo descubrir vulnerabilidades y cómo analizar la seguridad de la red, de sus servicios y de las aplicaciones.
- Estudiar normas, mecanismos, protocolos y herramientas que pueden ayudar a proteger a la organización, a sus redes, servicios y las aplicaciones que en ellas residen .



Contenidos de la materia

- Conceptos básicos y terminología relacionada
- Amenazas: con acceso a las personas, con acceso físico a dispositivos de la organización, con acceso a la organización a través de Internet, con acceso a algún segmento de la LAN de la organización.
- Tendencias actuales
- Mecanismos de protección:
 - Criptografía y sus aplicaciones (Firma digital, PGP, Esteganografía)
 - Firewalls, IDS y honeypots
- Seguridad de aplicaciones WEB
- Gestión de seguridad de la información: Serie ISO 27000



Clase 1

- Terminología: Información, seguridad, privacidad, confidencialidad, integridad, disponibilidad, autenticidad, no repudio y trazabilidad.
Vulnerabilidades. Amenazas. Incidentes
- Amenazas con acceso a las personas:
 - Definiciones
 - Ejemplos
 - Contramedidas
- Amenazas con acceso físico a las instalaciones y/o dispositivos de la organización.



Definiciones

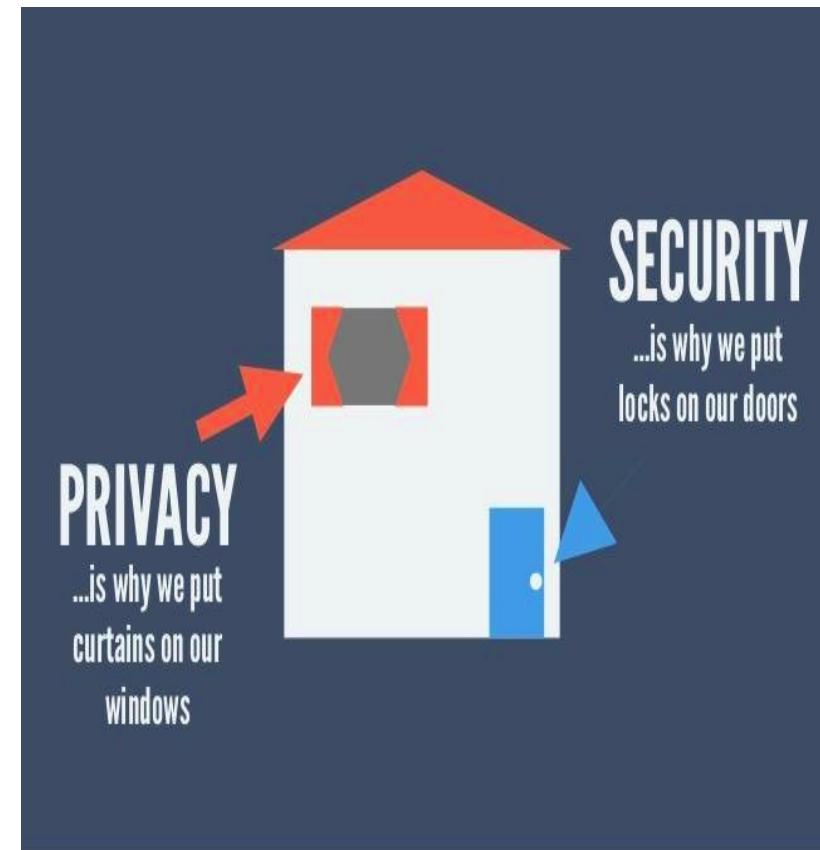
- ¿Qué se debe asegurar?
 - Los activos de una organización
- ¿Cuál es el lugar que ocupa la información?
 - La información constituye un activo muy importante para la organización, ya que tiene un rol fundamental a la hora de cumplir sus objetivos

Debemos proteger la información adecuadamente garantizando su seguridad y privacidad



Seguridad y privacidad de la información

- ¿Qué significa garantizar la seguridad de la información?
 - Significa proteger la información y los sistemas de información del acceso, uso, divulgación, interrupción, modificación o destrucción **no autorizados**.
- ¿Qué es garantizar la privacidad de la información?
 - Significa **no revelar** la información o revelarla selectivamente de manera de protegerla de cualquier intromisión



Privacidad de la información - Desafío

- ¿Tenés un celu con Android?
- ¿Te acordás donde estuviste hace un mes?
- Verificalo en <https://maps.google.com/locationhistory>
(con sesión iniciada en tu cuenta de Google)



¿Qué significa seguridad de la información?



Seguridad de la información

¿Qué se debe garantizar? Atributos

- Confidencialidad: Garantiza que la información sólo sea accesible por las personas autorizadas.
- Integridad: Garantiza que la información sólo pueda ser modificada por quien está autorizado a hacerlo
- Disponibilidad: Garantiza que los usuarios autorizados tienen acceso a la información y recursos relacionados cuando lo necesiten.



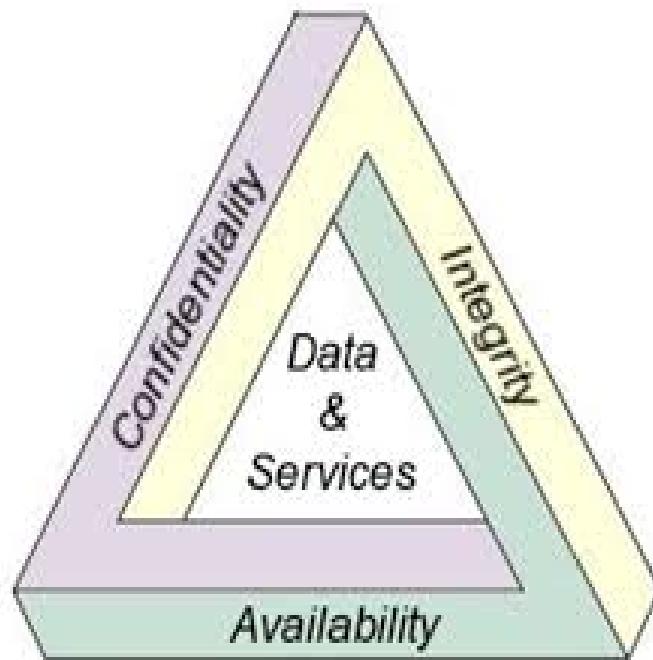
Seguridad de la información

¿Qué se debe garantizar? Atributos

- Autenticidad: Garantiza que la persona que origina o recibe el mensaje es quien dice ser.
- No repudio: Garantiza que la persona que envió o recibió el mensaje no pueda negar haberlo hecho
- Trazabilidad: Garantiza que toda acción puede ser reproducida



Atributos de seguridad de la información



La implementación de la seguridad

Seguridad en capas



*"Seguridad no es "hacking", así como un militar que conoce tanto de operaciones ofensivas como defensivas a la hora de decidirse por una defensa, aplica herramientas, tácticas y metodologías defensivas; en la defensa de un sistema informático se deben respetar esas mismas ideas, y no nos sirve con conocer únicamente técnicas de escaneo, intrusión, evasión, exploits, crack, etc... debemos saber implantar una adecuada **estrategia defensiva** justamente contra estos acciones".*

Alejandro Corletti



Principios Universales de Seguridad:

- **Mínimo privilegio:** Los permisos otorgados a un sujeto deben estar basados en la necesidad de saber.
- **Valores por omisión seguros:** A menos que se otorgue explícitamente a un sujeto un objeto, éste debe ser denegado.
- **Economía de mecanismos:** Los mecanismos de seguridad deben ser lo más simples posibles.
- **Mediación completa:** Todos los accesos a objetos deben poder auditarse.



Vulnerabilidades y Amenazas

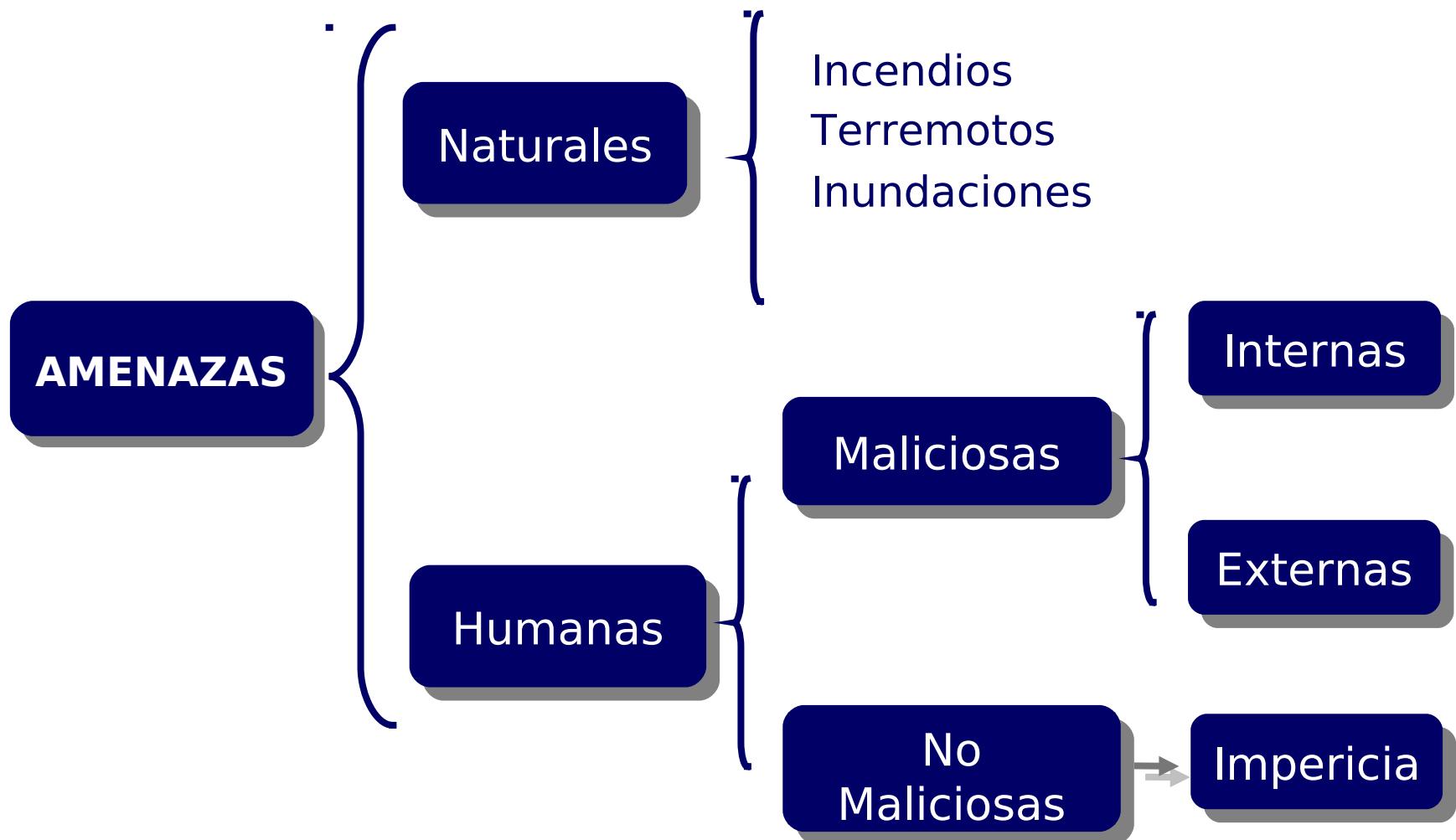
- Una **vulnerabilidad** es una debilidad en un activo.
- Una **amenaza** es una violación potencial de la seguridad.



Las amenazas sacan ventaja de las vulnerabilidades.



Tipos de amenazas



Amenazas - Conceptos Generales

Las amenazas **atentan contra**:

- La confidencialidad de la información
- La integridad de la información
- La disponibilidad de la información

Están **son causadas por** (de ahí su clasificación mencionada previamente):

- fallas humanas
- ataques malintencionados
- catástrofes naturales



Amenazas - Conceptos Generales

La materialización de una amenaza puede causar:

- el acceso, robo, modificación o eliminación de información no autorizada
- la interrupción de un servicio o el procesamiento de un sistema;
- daños físicos o robo del equipamiento y medios de almacenamiento de información.



Incidente de seguridad

Un incidente de seguridad, es un evento adverso que afecta los activos de la organización.

Se produce cuando una amenaza se concreta.

Todo incidente detectado debe ser reportado ante quien corresponda



Ejemplos de incidentes

- Defacement
- Acceso no autorizado.
- Robo de contraseñas.
- Ataque de DDOS
- Robo de información.
- Abuso y/o mal uso de los servicios informáticos internos o externos de una organización.
- Introducción de código malicioso en la infraestructura tecnológica de una organización.



Amenazas a la Organización

Una clasificación (¡Enfoque propio!):

- Amenazas teniendo acceso a las personas de la organización.
- Amenazas teniendo acceso físico a recursos de la organización (hosts, servidores, routers...o a las instalaciones).
- Amenazas teniendo acceso a distintos segmentos de la red de la organización.
- Amenazas teniendo acceso a la organización a través de Internet



Amenazas teniendo acceso a las personas – Ejemplos

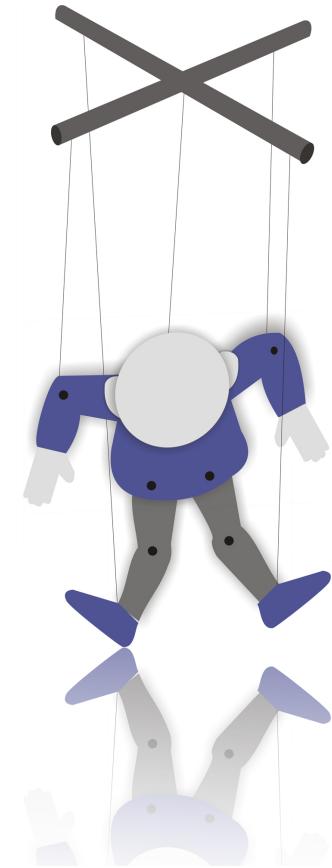
- Ingeniería Social
- Phishing
- SPAM
- Malware
 - Ramsomware
 - Keylogger
 - Botnets
- Acceso no autorizado





Ingeniería social

La ingeniería social es un conjunto de trucos, engaños o artimañas que permiten confundir a una persona para que entregue información confidencial



La principal defensa contra la ingeniería social es concientizarnos en el uso de políticas de seguridad



Ingeniería social

Según Kevin Mitnick, uno de los ingenieros sociales más famosos de los últimos tiempos, la ingeniería social se basa en estos cuatro principios:

- Todos queremos ayudar.
- El primer movimiento es siempre de confianza hacia el otro.
- No nos gusta decir “No”.



A todos nos gusta que nos alaben.

No nos gusta decir No.

El primer movimiento es siempre de confianza hacia el otro.

Todos queremos ayudar.

Ingeniería social



“La Seguridad muchas veces es una mera Ilusión. Una compañía puede tener la mejor tecnología, firewalls, sistemas de detección de intrusos, dispositivos de autenticación avanzados como tarjetas biométricas, etc y creen que están asegurados 100%. Viven una Ilusión. Sólo se necesita un llamado telefónico y listo. Ya son vulnerables a un ataque. La Seguridad no es un producto, es un Proceso”

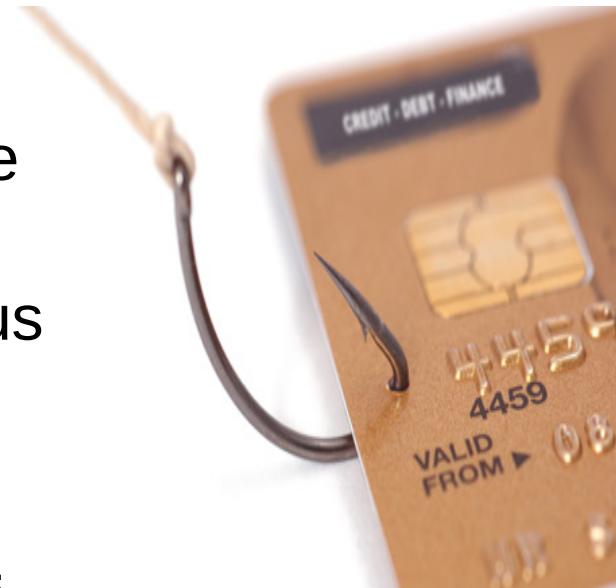
Kevin Mitnik



Phishing

El Phishing es una combinación de ingeniería social y elementos técnicos para engañar a un usuario y lograr que éste entregue involuntariamente información confidencial o acceso a sus activos, a usuarios malintencionados.

La forma más común es mediante el envío de mails falsos, escritos como si hubieran sido enviados por la auténtica organización



Phishing

Estimado cliente de Banco BBVA! - Message (HTML)

File Edit View Insert Format Tools Actions Help

Type a question for help

Reply | Reply to All | Forward | Print | Save | X | ? | ▲ ▾ ▶ ▷ ▷ ▷

You forwarded this message on 16/08/2005 19:12. Click here to find all related messages.

From: BBVA S.A. [bbva@bbvanet.com] Sent: martes 16/08/2005 11:06
To: [REDACTED]
Cc:
Subject: Estimado cliente de Banco BBVA!

BBVA net

Estimado cliente de Banco BBVA!

Por favor, lea atentamente este aviso de seguridad.
Estamos trabajando para proteger a nuestros usuarios contra fraude.
Su cuenta ha sido seleccionada para verificación, necesitamos confirmar que Ud. es el verdadero dueño de esta cuenta.
Por favor tenga en cuenta que si no confirma sus datos en 24 horas, nos veremos obligados a bloquear su cuenta para su protección.

Gracias.
<http://www.bbvacom.net>

© BBVA S.A. 2005

Phishing
Mail falso



Phishing

*Phishing
Sitio
verdadero*

The image shows two side-by-side web pages. On the left is the official website for BBVA Francés, featuring a blue header with links to Contacto, Seguridad, Cajeros, Sucursales, and Mapa. It includes a search bar and a Google search button. The main content area features the BBVA Francés logo and navigation tabs for INDIVIDUOS (blue), COMERCIOS Y NEGOCIO, and BBVA. A sidebar offers links to Francés Net, Francés Net VIP, Francés Net Empresa, BBVA Cash, and sections for Productos and Servicios. Below this is a 'Noticias' section with a story about an airplane fire in Madrid. At the bottom are links for 'Más noticias' and 'Mercados'. On the right is a Mozilla Firefox browser window displaying a phishing page with a similar layout. The title bar says '- Mozilla Firefox' and the address bar shows the URL https://hb.bbv.com.ar/hbbf/login_popup.jsp?nra=937. The page itself is titled 'Francés net Opere sus Cuentas Personales'. It contains fields for 'DNI' and 'Clave', with the 'DNI' field highlighted with a red oval. A warning box is overlaid on the right, containing the text 'Protéjase del fraude electrónico' and 'No responda e-mails ni llamados telefónicos en los que se le solicite claves y datos personales.' A red circle highlights this warning box. The bottom of the browser window shows the URL hb.bbv.com.ar, a certificate icon labeled 'Certificate OK', and a note about 'Tarjetas de Crédito.'

Phishing

**2017-Un
ejemplo más
actual**

Carrefour

Estimado cliente,

La tarjeta Pass (Carrefour) es un servicio ofrecido por la cadena de hipermercados Carrefour, con el cual, podrá optar a realizar sus pagos en la cadena de supermercados cómodamente, en más de 28 millones de establecimientos adheridos, en sus más de 800.000 cajeros con el distintivo VISA, así como beneficiarse de ofertas exclusivas dirigidas a los titulares de la tarjeta Pass (Carrefour).

Tu tarjeta esta desactivada por las nuevas normas de seguridad. Para activar la tarjeta nº .

5499 *****

tiene que seguir 2 pasos.

1. Hacer click en el siguiente link
2. Responder al cuestionario

Activar servicios

Saludos,
Carmen Maria Marchal Basalo.



Phishing

Entre las principales técnicas utilizadas en ataques de phishing, podemos citar:

- Mails basados en HTML, utilizando ofuscación de información de la URL;
- Uso de acortadores de URL;
- Mensajes falsos utilizando encabezados de los mensajes modificados (From).

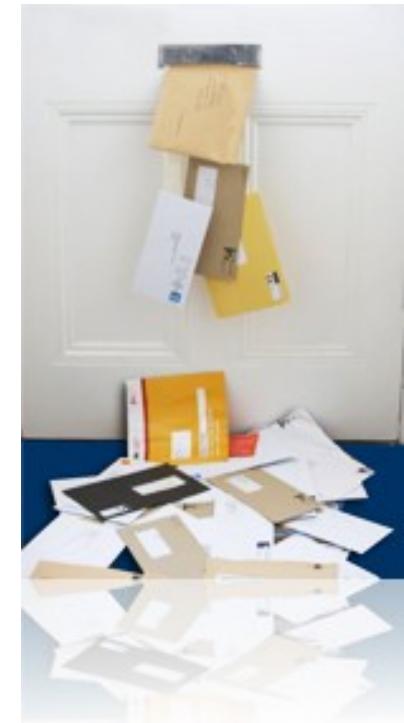


SPAM

También llamado “Correo Basura”. Es uno de los principales medios para hacer llegar todo tipo de problemas a los usuarios del correo electrónico y de otros servicios de mensajería como SMS o WhatsApp

Los problemas pueden ser:

- Publicidad no deseada
- Phishing
- Transmisión de código malicioso



Malware



El malware es software malicioso que puede:

- Infectar otras PCs
- Permitir el acceso remoto a la información de la PC
- Destruir información
- Robar información personal
- Hacer que nuestra PC ejecute acciones ordenadas por un tercero: enviar SPAM, saturar comunicaciones, etc.

Consideramos malware a cualquiera de los siguientes: Virus, Gusano, Troyano, Spyware, Keylogger, Backdoor, Ransomware



Malware



El malware puede llegar **con o sin** nuestro consentimiento.

Sin nuestro consentimiento, infectando nuestro dispositivo:

- Al visitar un sitio web malicioso
- Al utilizar un pendrive infectando
- A través de la red a la que está conectada nuestro dispositivo

Con nuestro consentimiento:

- Instalando software pirata. (juegos, cracks, keygens)
- Siendo víctimas de ingeniería social.



Malware



A veces, que un dispositivo esté infectado con un malware es como tener a alguien observando qué hacemos.

El malware puede saber: qué sitios visitamos, qué teclas presionamos, donde hacemos click,... todo.

Es por esto que debemos ser cuidadosos con el dispositivo utilizado para acceder a los sistemas críticos para nosotros o para la organización: Homebanking, Paypal, Webmail.

- Evitar usar PCs no confiables (ubicadas en lugares públicos, PCs en las que se instaló software pirata)





Ransomware

El ransomware es malware usado por cibercriminales para secuestrar un dispositivo o la información almacenada en estos.

Dependiendo del tipo de ransomware:

- Encripta archivos importantes y pide el pago de un rescate a cambio de la clave de desencripción utilizada. Amenaza con borrar la clave luego de una fecha límite.
- Se hace pasar por la policía y extorsiona al usuario diciendo que se encontró pornografía y software pirata.
- Altera el arranque de la PC evitando que pueda encender.



Malware

El poder de acción de un ransomware que cifra la información no está limitado solamente a la PC infectada, también puede:

- Cifrar la información alojada en carpetas compartidas en otra PC a las que el usuario tiene acceso.
- Cifrar la información alojada en dispositivos USB u otros conectados a la PC (pendrives, discos externos, memorias flash).

Están diseñados para buscar archivos importantes para las organizaciones y encriptarlos.



Keyloggers

Software o hardware que tiene la capacidad de almacenar lo que se tipea.



Los keyloggers por software también permiten, por ejemplo, capturar pantallas cuando el usuario “cliquea”..



Botnets

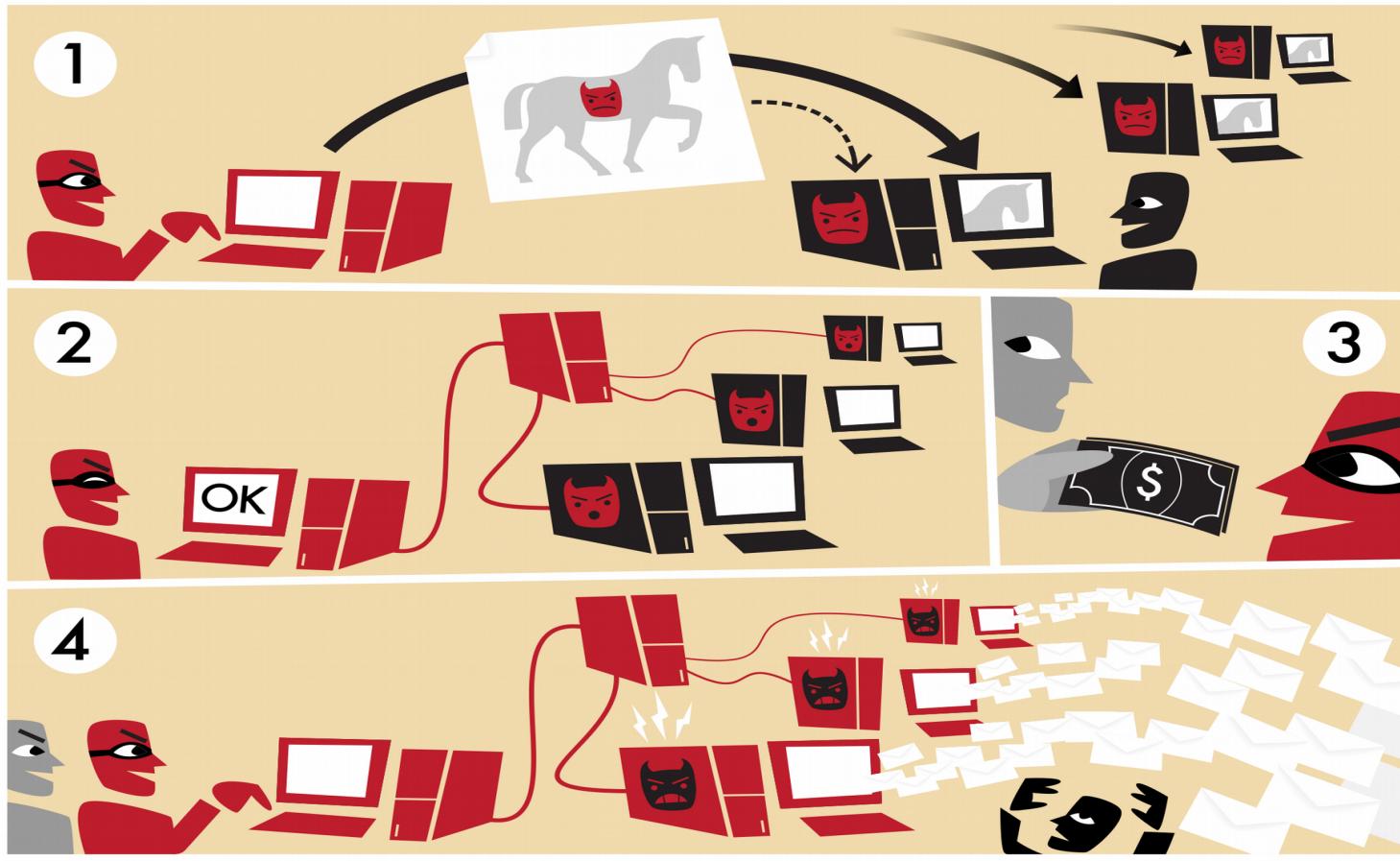
¿Qué es una botnet?

- Es una red de bots, que son hosts infectados (combinan aspectos de virus, troyanos, gusanos y rootkits: control remoto, propagación, etc)
- Hay una entidad de control conocido como Servidor “Command & Control” manejado por “bot master/herder” (una persona o grupo)
- Realizan actividades maliciosas, como por ej:
 - Robo de credenciales
 - Envío de SPAM
 - DDOS



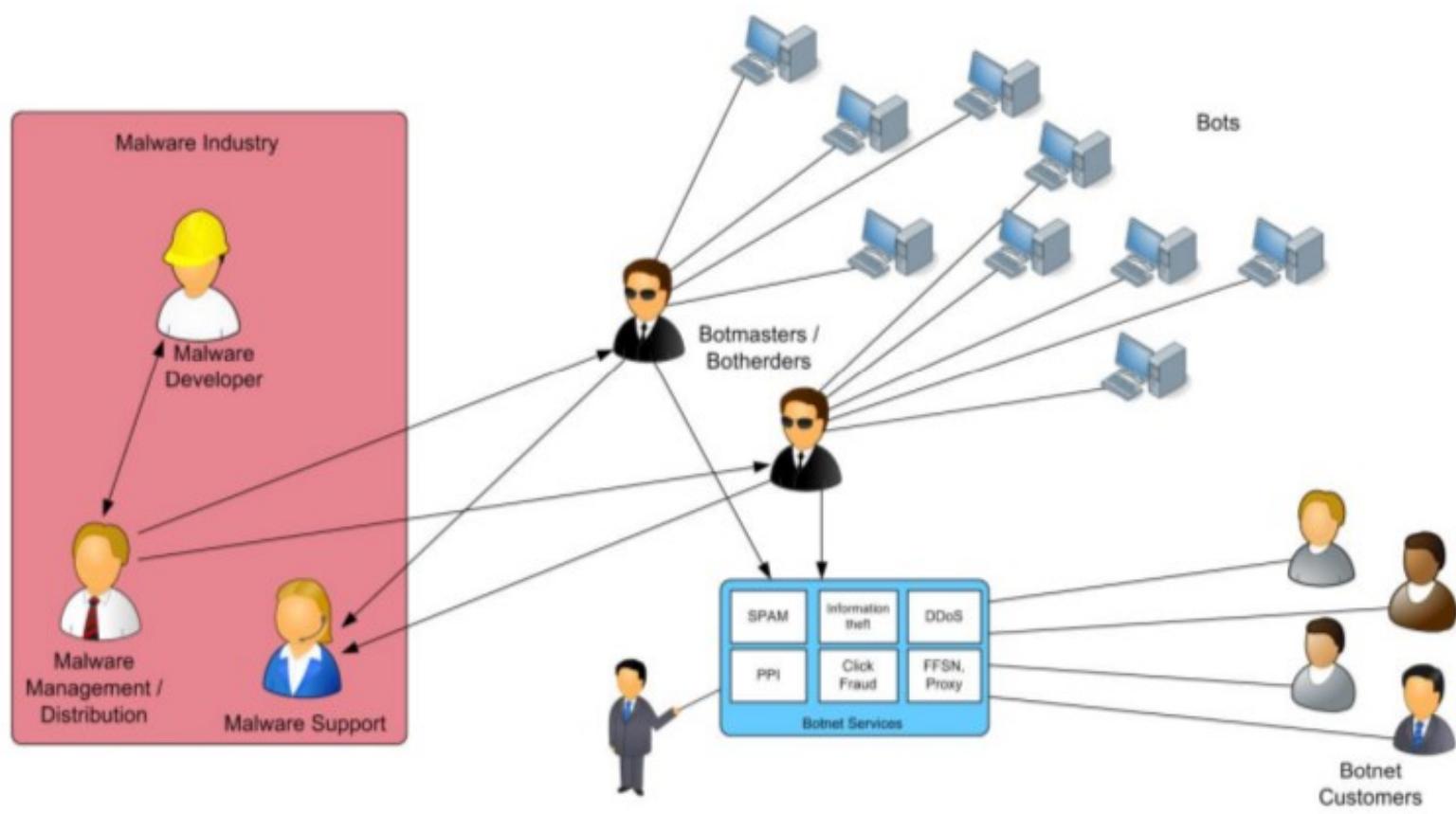
Botnets

¿Cómo funcionan?



Botnets

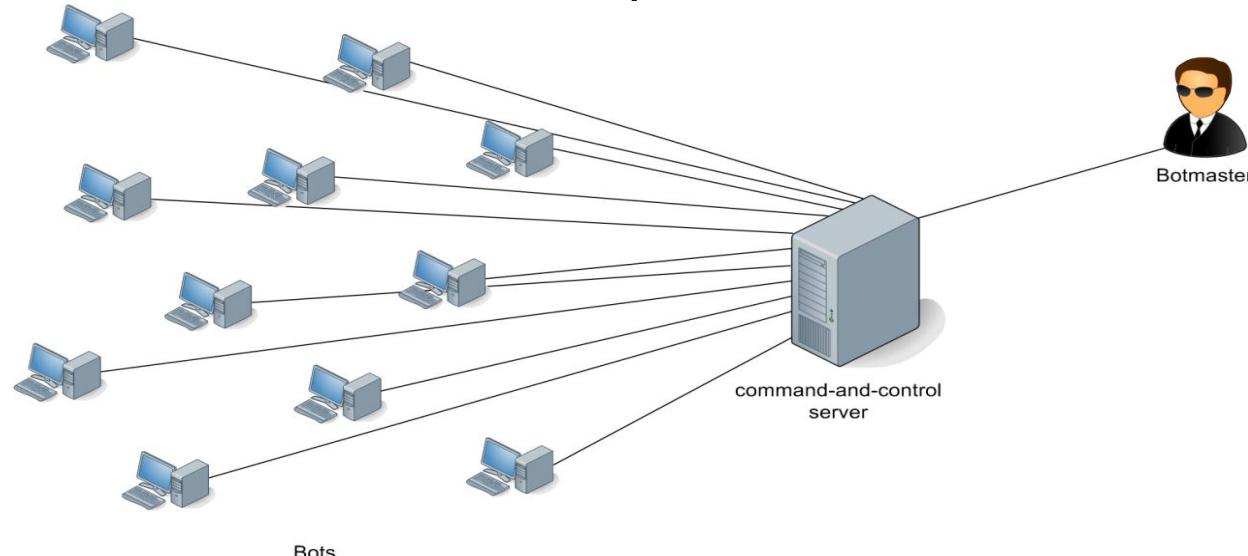
Economía del MW - Modelo de roles simplificado



Botnets

Arquitectura centralizada

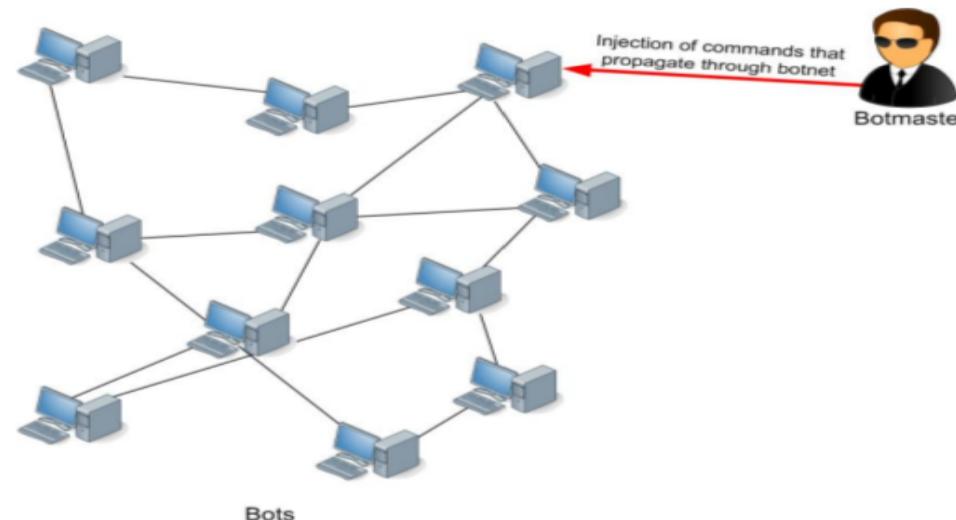
- Los bots establecen comunicación con un único servidor (o jerarquía de servidores) (C&C)
- En sus inicios, basadas en el funcionamiento del protocolo IRC
- Es simple coordinar y monitorear la botnet
- El protocolo de comunicación puede ser IRC, HTTP, HTTPS



Botnets

Arquitectura descentralizada

- También conocidas como botnets P2P
- El botmaster inyecta los comandos a un bot (usando el protocolo de comunicación de la botnet o a través de una actualización (los bots intercambian su número de versión y en caso de ser necesario se actualizan a partir del más nuevo))
- Es difícil localizar al botmaster → alto grado de anonimato



Acceso no autorizado

Ataques a contraseñas:

Consiste en la prueba metódica de contraseñas para lograr el acceso a un sistema, siempre y cuando la cuenta no presente control de intentos fallidos de logueo.

Este tipo de ataque puede ser realizado:

- Por diccionario: existiendo un diccionario de palabras, una herramienta intentará acceder al sistema probando una a una las palabras incluidas en el mismo.
- Por fuerza bruta: una herramienta generará combinaciones de letras, números y símbolos formando posibles contraseñas y probando una a una en el login del sistema.



Cómo enfrentamos las amenazas

- Como usuarios/administradores/desarrolladores:
 - Siguiendo buenas prácticas
- Como responsables de seguridad en nuestra organización:
 - Concientización de los usuarios/personal de la organización.
 - Especialización en temas relacionados a seguridad de la Información
 - Implementación de controles adecuados



Buenas prácticas como usuarios

- Ante algunas amenazas vistas en esta clase:
 - Elegir una clave segura.
 - Proteger adecuadamente la clave.
 - Descargar aplicaciones sólo desde sitios confiables.
 - Utilizar antivirus y firewalls personales.
 - Mantener el sistema actualizado (SO, aplicaciones, antivirus!!)
 - No abrir adjuntos que provienen de orígenes no confiables o conectarse directamente a urls contenidas en los mails.



Buenas prácticas como desarrolladores

- Como administradores/desarrolladores:
 - Siguiendo las buenas prácticas de seguridad que indican los estándares/normas nacionales e internacionales.

A lo largo de la cursada estudiaremos mecanismos, herramientas, protocolos etc que nos formarán al respecto...

