U4 – Malware

Mg. Ing. Bruno Roberti

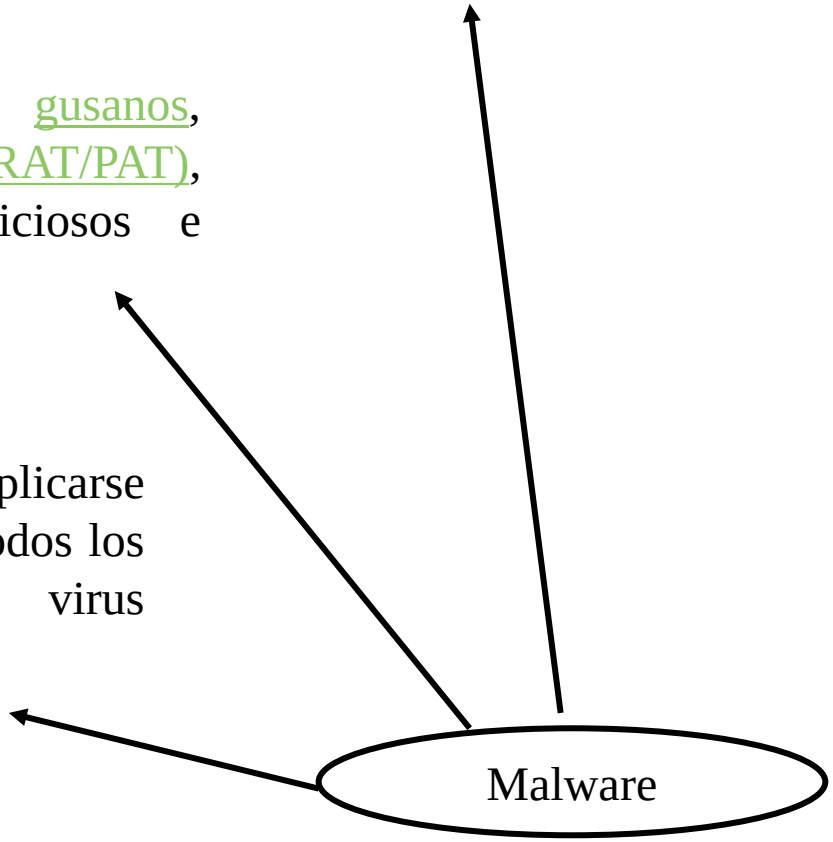
2.023

Malware

Malware (del inglés ***mal****icious* ***software***), **software malicioso**, es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora sin el consentimiento de su propietario. El término *malware* es muy utilizado para referirse a una variedad de software hostil, intrusivo o molesto.

El término *malware* incluye virus, gusanos, troyanos, spyware, adware, y rootkits (RAT/PAT), ramsonware, y otros softwares maliciosos e indeseables.

El término virus informático suele aplicarse de forma incorrecta para referirse a todos los tipos de malware, incluidos los virus verdaderos.



Historia

Inicios (años 90)	Eran elaborados como experimentos o bromas. A veces causaban daño en forma no intencional (Melissa)
Segunda Etapa (2000 – 2009)	Se populariza el concepto de Vandalismo, aparecen los primeros gusanos
Cambio metas (2010-2019)	El software malicioso se diseña con el propósito de obtener beneficios. El crimen organizado entra en escena
Actualidad	Inicio del modelo de negocios del MaaS. “Democratización” del malware

Malware con mayor actividad

Virus: Es un programa que puede replicarse a si mismo, y utilizan diversos métodos para evitar la detección: técnicas Stealth, Encriptación y Polimorfismo. Además necesita un vector.

Gusano: Es un programa standalone que puede replicarse solo, para infectar otros equipos. Además de las acciones programadas en el payload, suele traer problemas de congestión de ancho de banda en la redes.

Troyanos: Es un programa diseñado para entregar el control de una PC a otro equipo. Además puede disfrazarse como un programa legítimo o útil

Rootkit: Es un malware diseñado para esconder la existencia de ciertos procesos o programas y brindar acceso con privilegios a una computadora. Su detección es extremadamente difícil, y su eliminación casi imposible si esta bien construido.

Ramsonware: En esta categoría entran programas que luego de infectar un equipo encriptan los archivos del usuario, solicitando un rescate para volverlos a su estado normal.

Otros malware

Spyware: Es un programa que recolecta información sobre el usuario sin su conocimiento. Generalmente no se replica por si solo

Adware: Es un software que automáticamente muestra publicidad, la mayoría de la veces en la forma de una ventana pop up.

Características malware

Persistencia

- Se puede definir como la cualidad que tiene un malware de permanecer en el equipo infectado, sin ser descubierto, para poder ampliar todo lo posible en el tiempo sus acciones sobre él.

Ofuscación

- Se encarga de ocultar todo lo posible el código del software para hacerlo pasar por un programa inocuo, de modo que los antivirus no sean capaces de detectarlo como un malware cuando va a entrar en el sistema.

Otras características

Backdoor: Es uno o varios programas que un hacker instala en un sistema para permitirle acceder en cualquier momento. La mayoría de los troyanos y rootkits implementan esto.

Canal Abierto: es la forma legitima en que los programas se comunican dentro de un equipo o red

Ej. Comunicación entre el cliente DNS y el servidor DNS en el puerto TCP 53

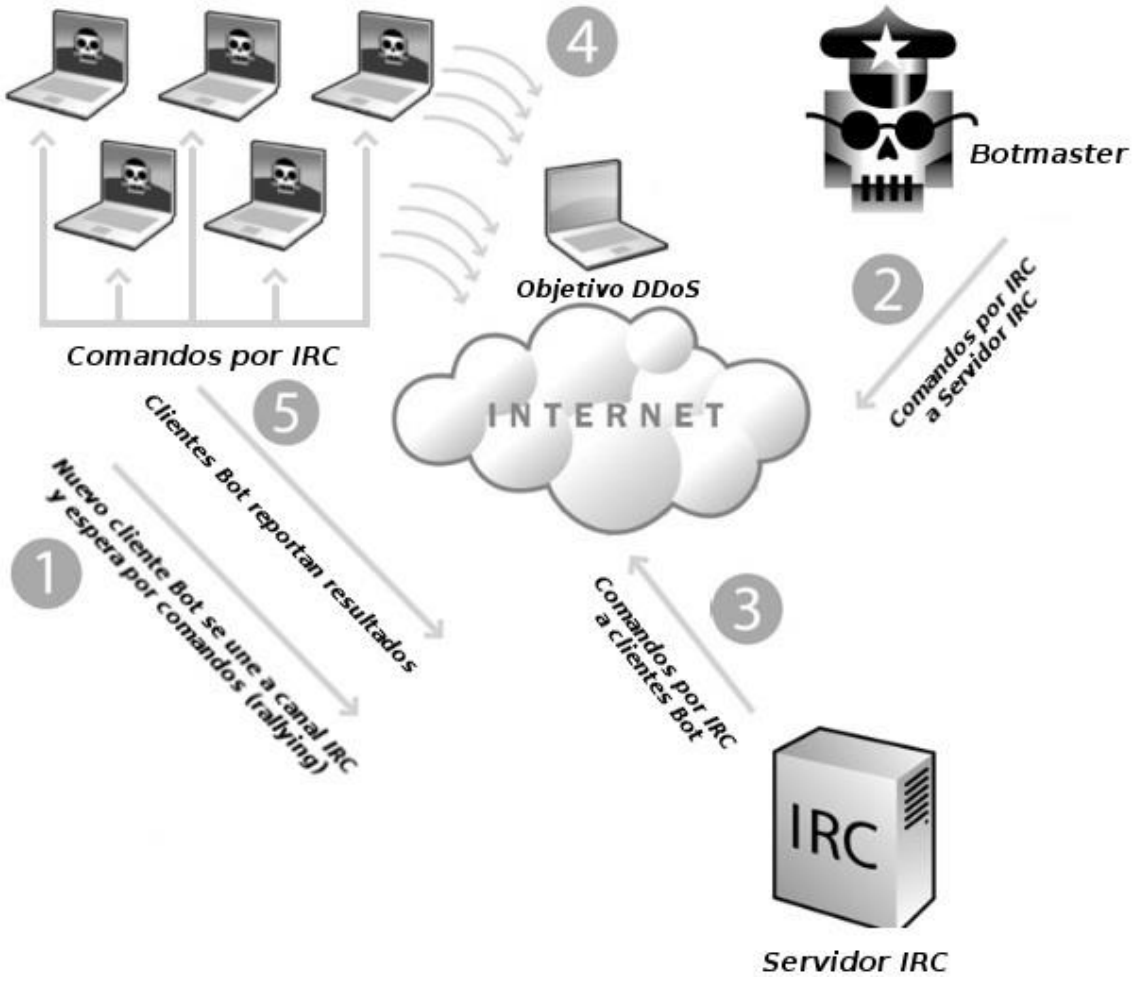
Canal Encubierto: es la utilización de canales de información de formas en las que no fueron diseñados, generalmente para enviar información

Ej. Utilización de puertos poco comunes: Net Bus (UDP 12345/12346); Back Orifice (31337/31338)

Compresión y Encriptación: es la utilización de técnicas de compresión o de encriptación para evitar la detección mediante técnicas estáticas de escaneo

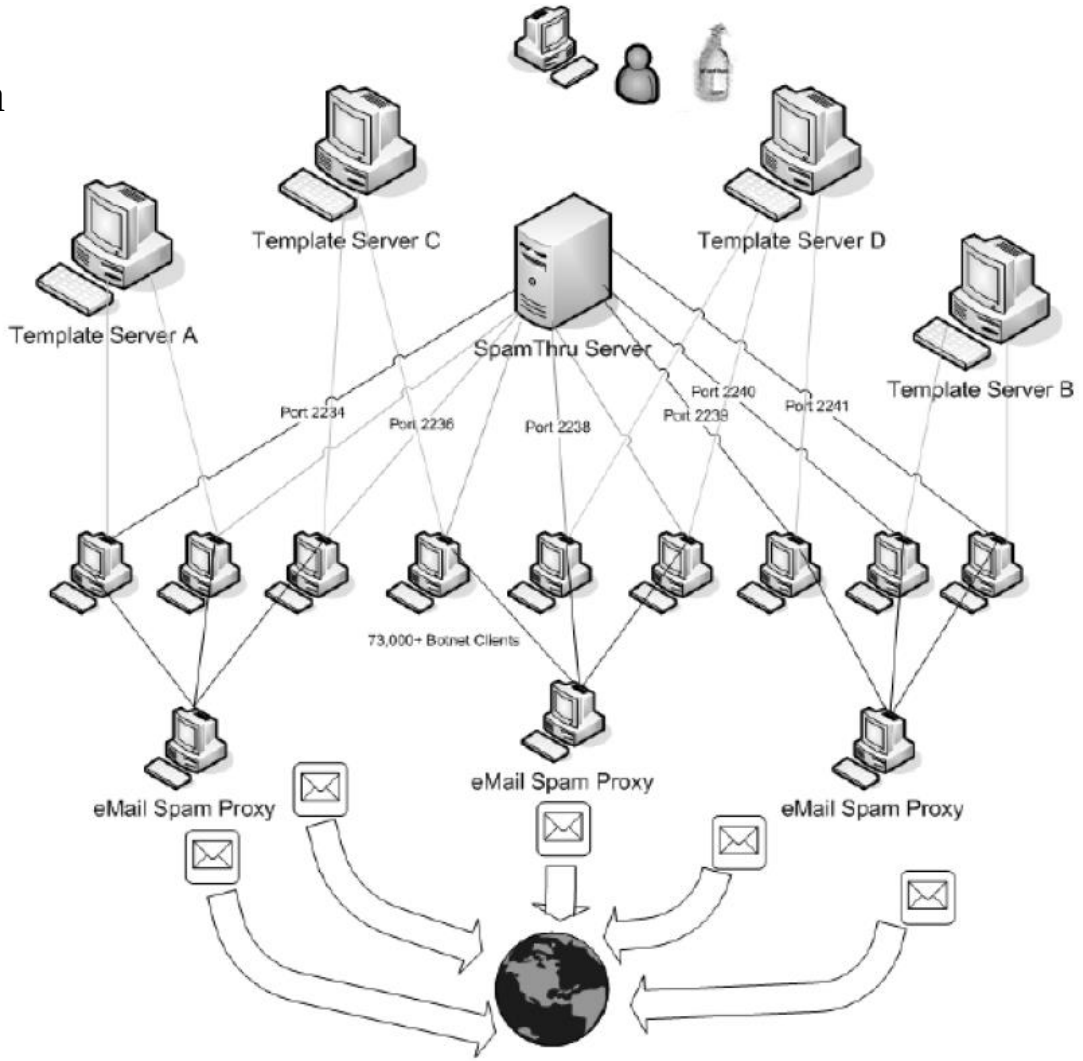
Botnets

Una **botnet** es un conjunto de computadoras comprometidas, cada una conocida como 'bot', conectadas a Internet. El "botmaster" controla esas computadoras mediante protocolos standard como IRC y HTTP



Botnets

Otro ejemplo de utilización de una botnet: Envío de SPAM



Tipos de detección malware

Basada en firmas

- Se basa en buscar dentro de los archivos analizados secuencias de bytes que coincidan con estas firmas conocidas.

Heurística

- Se analiza el software que se ejecuta en el equipo en busca de patrones anómalos o peligrosos de comportamiento que puedan dañar el sistema.