USM

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

Seguridad de Sistemas

Clase 9: Malware

Contenidos

USM

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

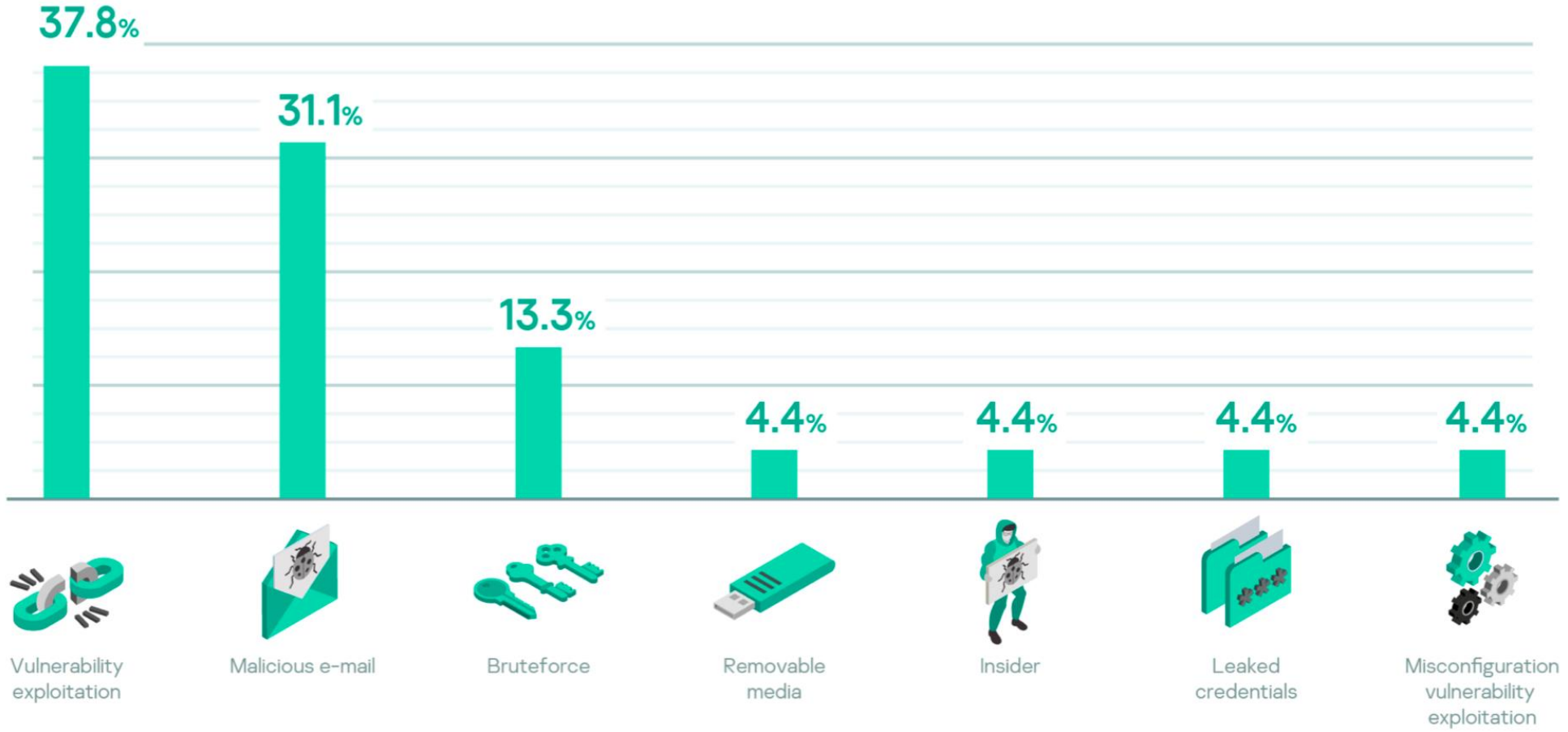
- Conocer los principales tipos de amenazas existentes en Ciberseguridad
- Conocer los diferentes tipos de malware
- Conocer las técnicas de infección y análisis de malware

Introducción

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

- **<u>Definición:</u>**
- Circunstancia desfavorable que puede ocurrir y que cuando sucede tiene consecuencias negativas sobre los activos provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor.
- Una amenaza puede tener causas naturales, ser accidental o intencionada.
- Si esta circunstancia desfavorable acontece a la vez que existe una vulnerabilidad o debilidad de los sistemas o aprovechando su existencia, puede derivar en un incidente de seguridad.

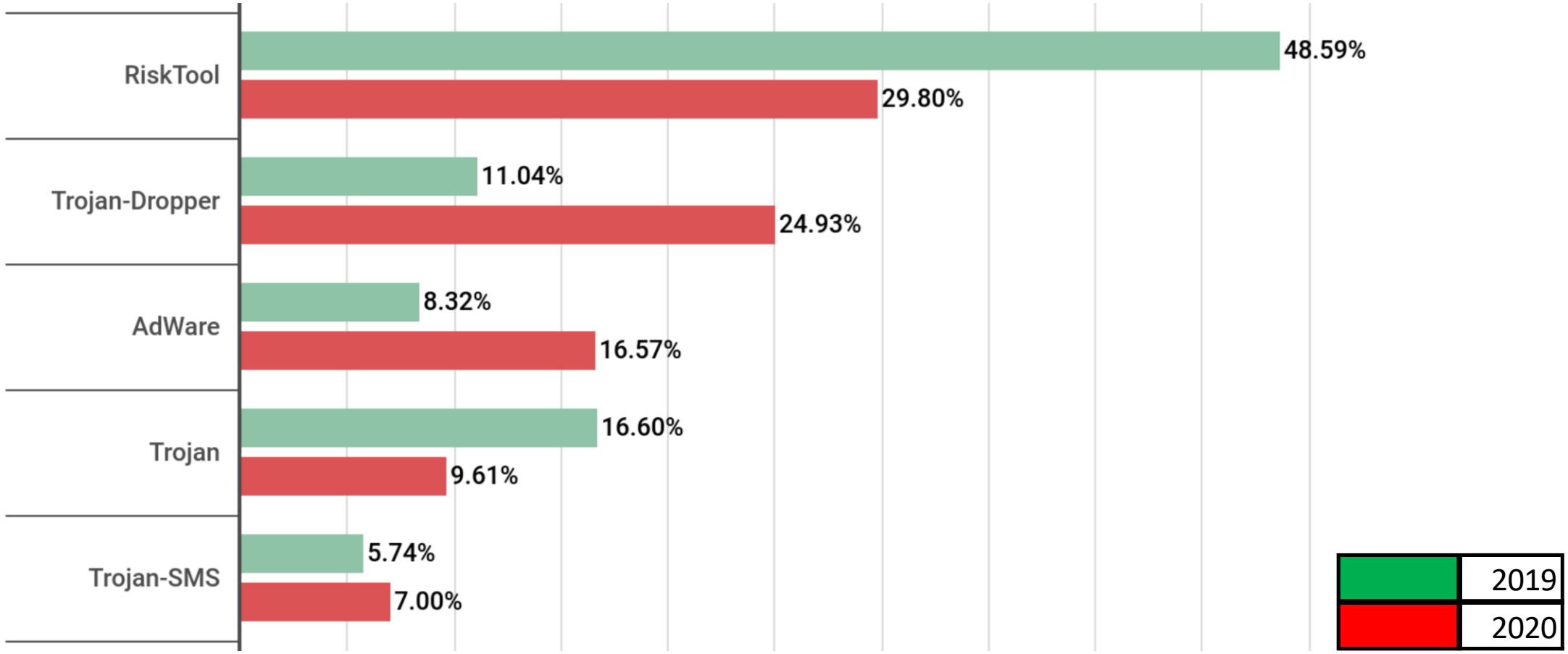
Introducción



Principales vectores de ataques: Kaspersky Q1 2021

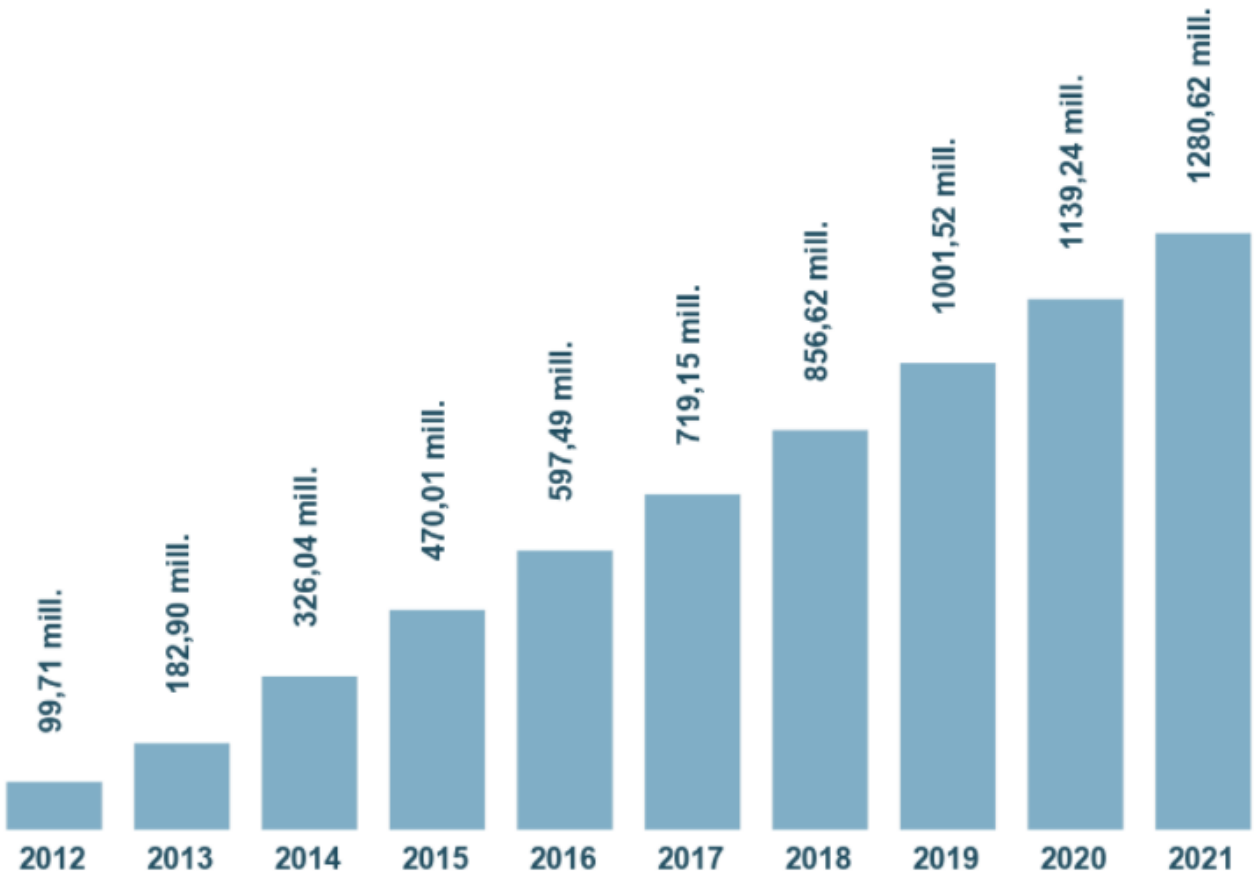
UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

Introducción



Principales amenazas informáticas: Kaspersky Lab

Introducción



Cantidad malware por año
Fuente: Av-Test

Tipos de malware

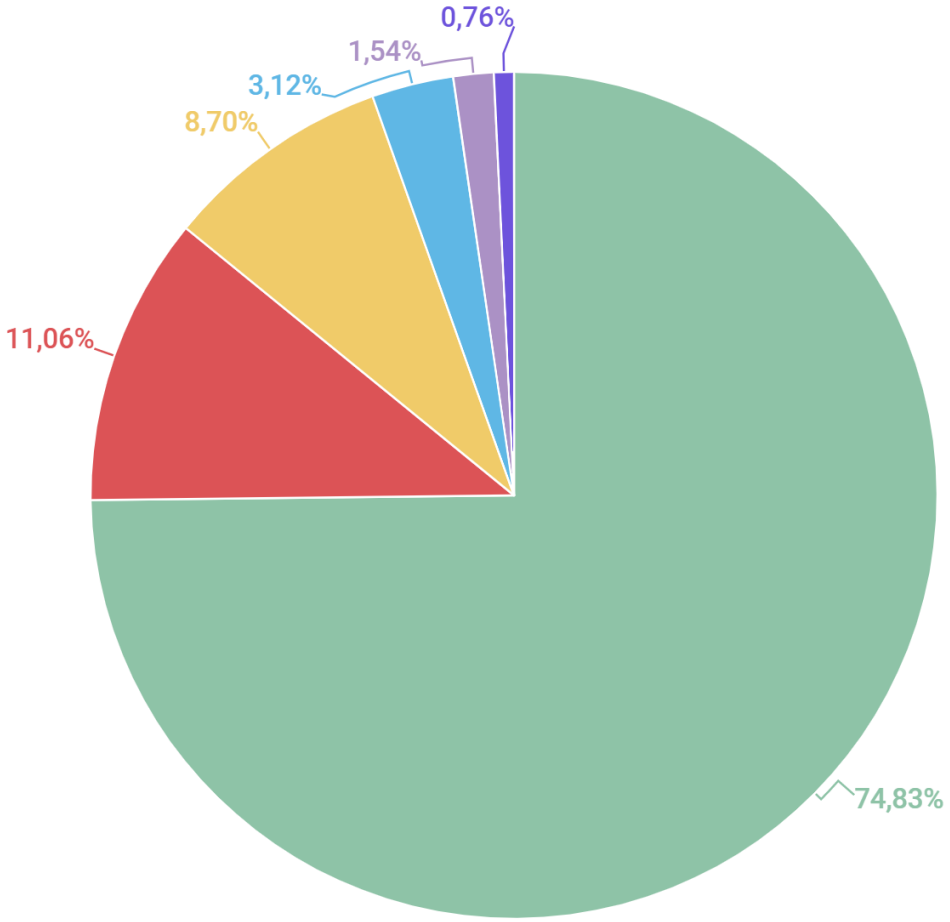
UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

Tipos de malware	
Troyano	Virus
Backdoor	Gusano
Rootkit	Spyware
Ransomware	Botnet
Adware	Crypter

Técnicas de Infección

- Ingeniería Social (click-jacking)
- Spear Phishing
- Malversiting: infección a través de sitios de publicidad
- Malware en sitios web
- Drive-by downloads
- Correo electrónico
- Dispositivos removibles (pen-drive)
- Red

App. más atacadas por malware

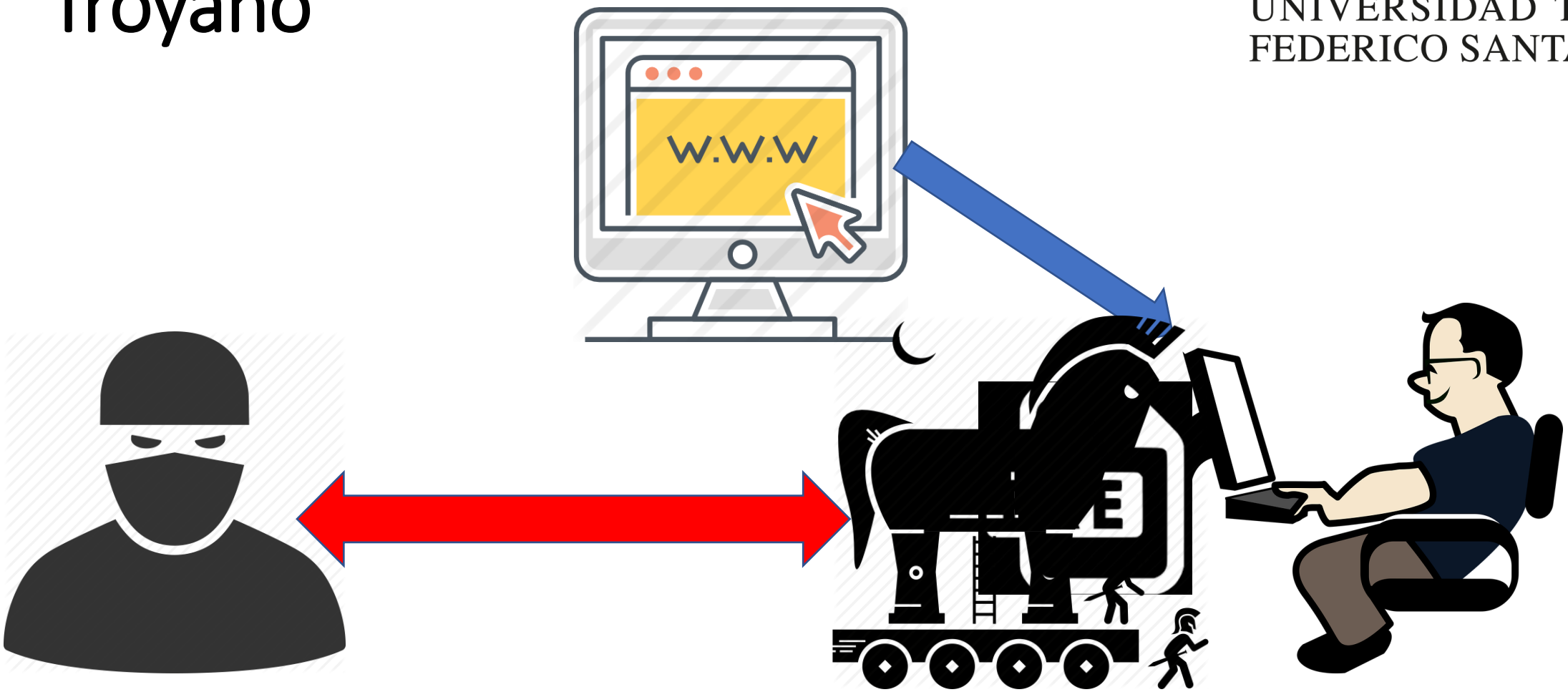


Fuente: Kaspersky Labs, Q1 2021

Troyano

- Se trata de un tipo de malware o software malicioso que se caracteriza por **carecer de capacidad de autorreplicación**. Generalmente, este tipo de malware requiere del uso de la ingeniería social para su propagación.
- Una de las características de los troyanos es que al ejecutarse no se evidencian señales de un mal funcionamiento; sin embargo, mientras el usuario realiza tareas habituales en su ordenador, el programa **puede abrir diversos canales** de comunicación con un equipo malicioso remoto que permitirán al atacante controlar nuestro sistema de una forma absoluta.

Troyano



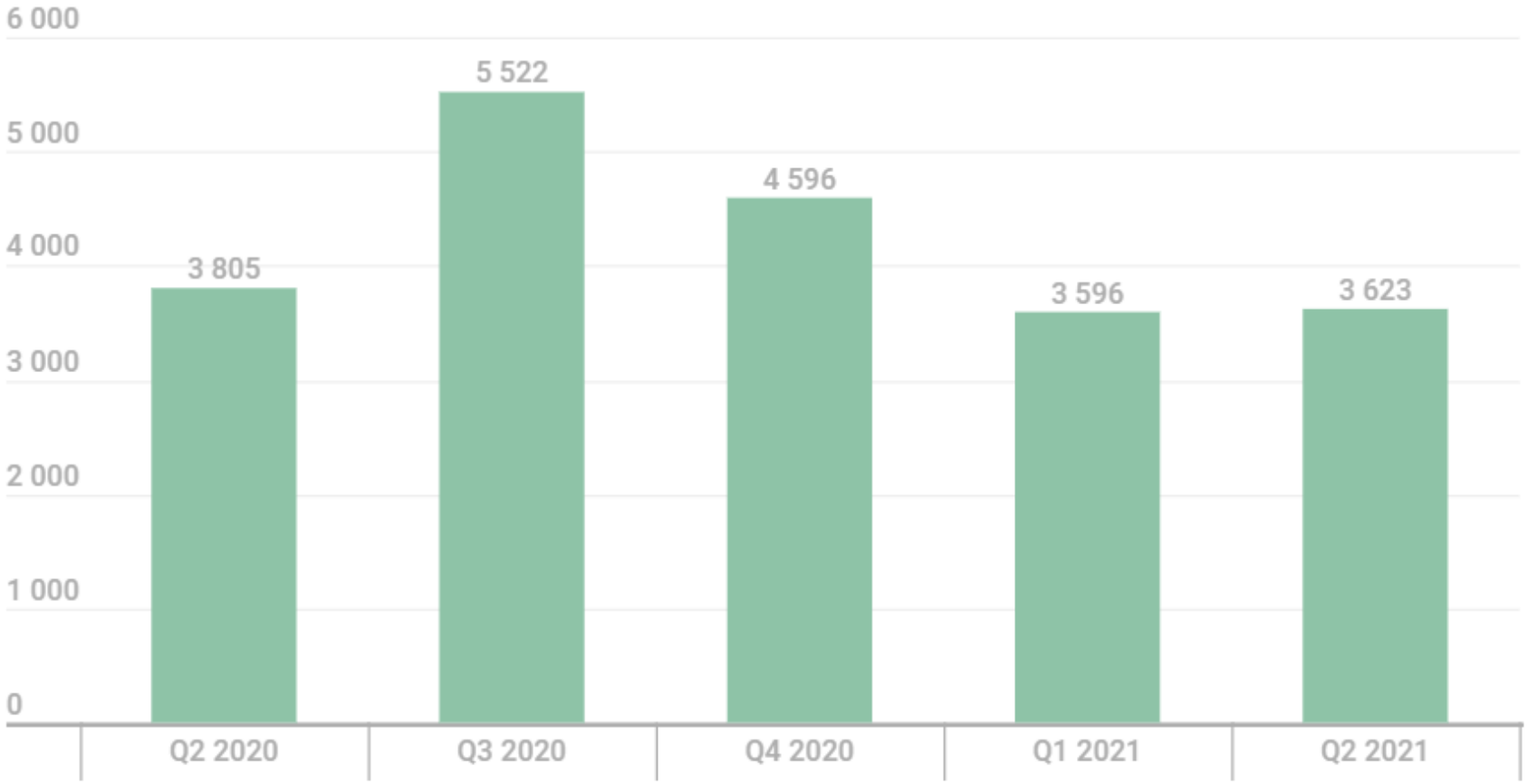
Método de infección de un troyano

Troyano

- **Acciones típicas de un troyano una vez que infecta a un usuario**
- Borrado de archivos
- Robo de datos
- Deshabilitar controles de seguridad (FW, AV)
- Bajar otros malware
- Generar Backdoors
- Botnet
- Secuestro de capacidades de HW (GPU)

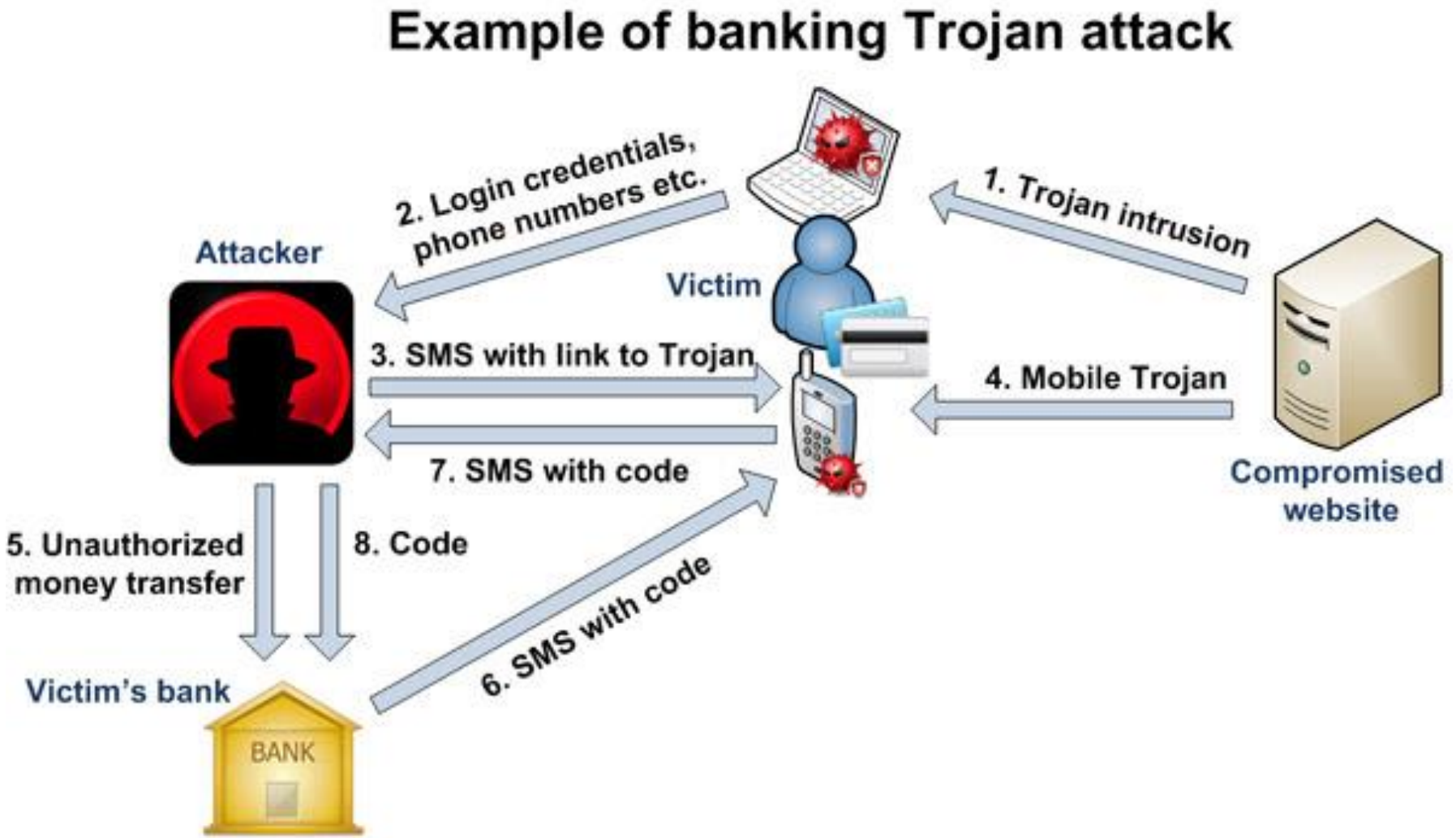
Troyano

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA



Troyano Mobile: Kaspersky Labs

Troyano


Example of banking Trojan attack
Attacker
Victim
Compromised website
Victim's bank
BANK
1. Trojan intrusion
2. Login credentials, phone numbers etc.
3. SMS with link to Trojan
4. Mobile Trojan
5. Unauthorized money transfer
6. SMS with code
7. SMS with code
8. Code

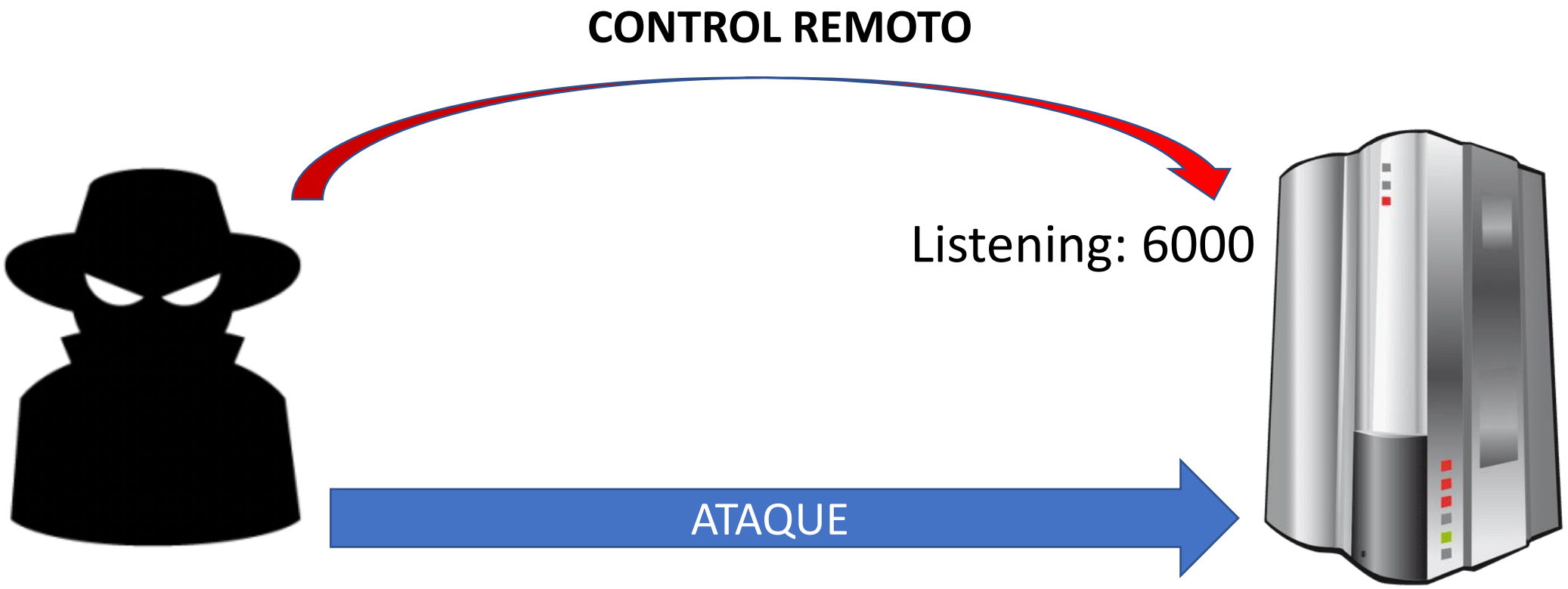
Backdoor

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

- Se denomina backdoor o puerta trasera a cualquier punto débil de un programa o sistema mediante el cual una **persona no autorizada** puede acceder a un sistema.
- Las puertas traseras pueden ser errores o fallos, o pueden haber sido creadas a propósito, por los propios autores pero al ser descubiertas por terceros, pueden ser utilizadas con **fines ilícitos**.
- Por otro lado, también se consideran puertas traseras a los programas que, una vez instalados en el ordenador de la víctima, dan **el control de éste de forma remota** al ordenador del atacante.

Backdoor

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA



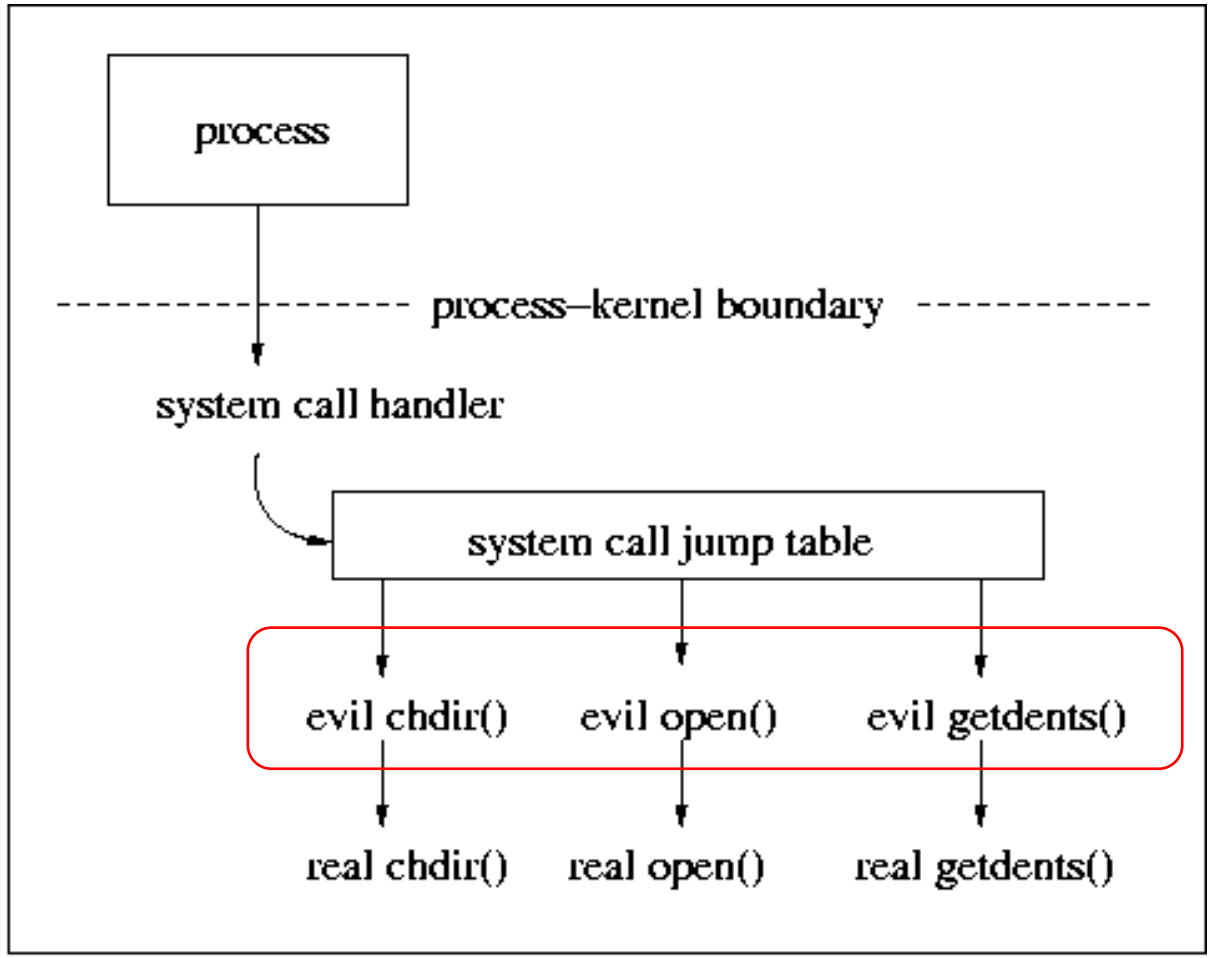
Rootkit

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

- **Definición:**
- Es un conjunto de herramientas usadas frecuentemente por los intrusos informáticos o crackers que consiguen acceder ilícitamente a un sistema informático. Estas herramientas sirven para **esconder los procesos y archivos** que permiten al intruso mantener el acceso al sistema, a menudo con fines maliciosos.
- Puede esconder una aplicación que lance una consola cada vez que el atacante se conecte al sistema a través de un determinado puerto. Los rootkits del kernel o núcleo pueden contener funcionalidades similares.

Rootkit

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA



Operación de un RootKit

Ransomware

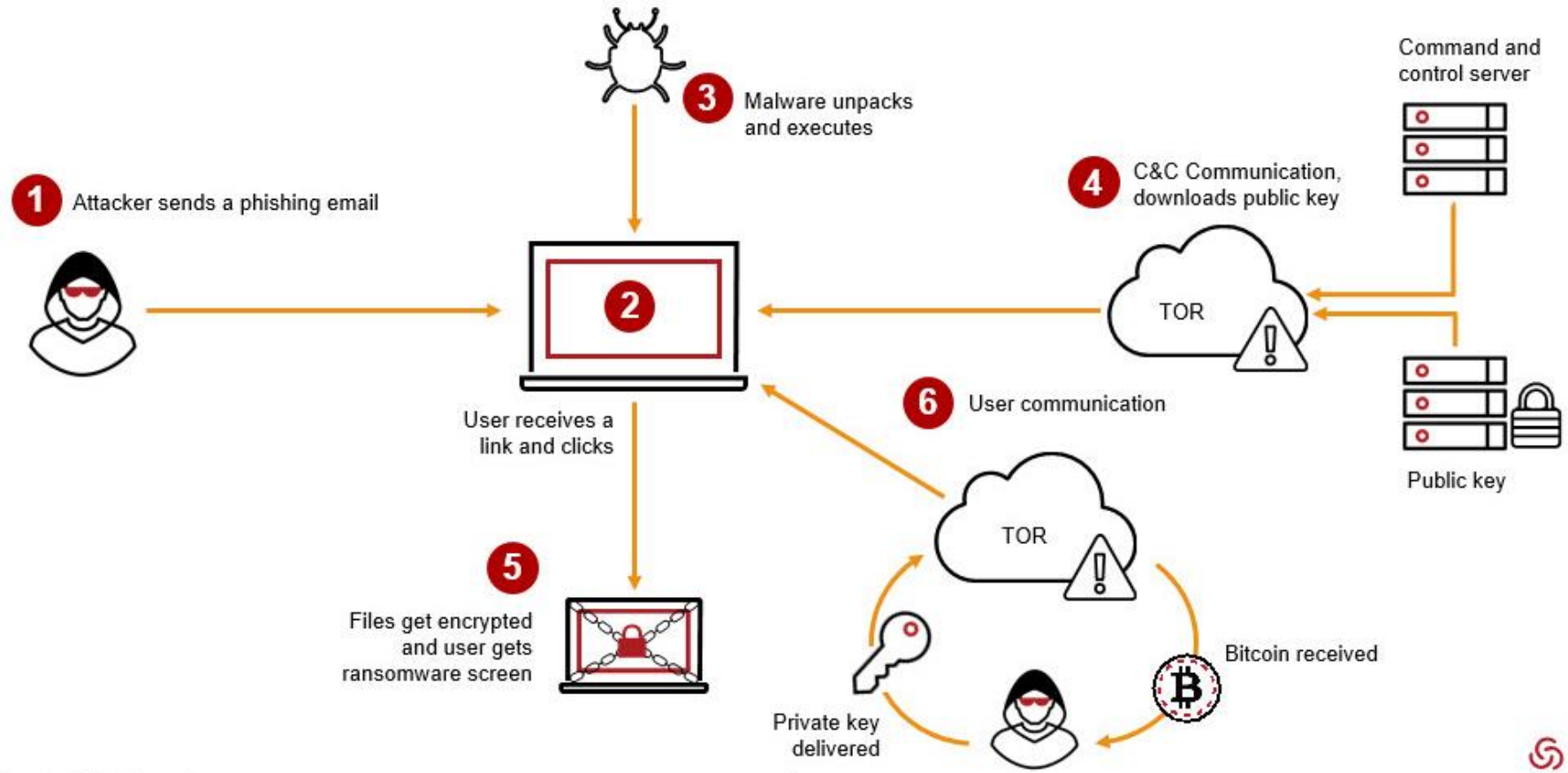
UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

- **<u>Definición:</u>**
- El ciberdelincuente, toma control del equipo infectado y «secuestra» la información del usuario **cifrándola**, de tal forma que permanece ilegible si no se cuenta con la contraseña de descifrado. De esta manera extorsiona al usuario pidiendo un rescate económico a cambio de esta contraseña para que, supuestamente, pueda recuperar sus datos.
- La seguridad del sistema está basada en la **dificultad de factorización** de grandes números. Su funcionamiento se basa en el envío de un mensaje cifrado mediante la clave pública del destinatario, y una vez que el mensaje cifrado llega, éste se encarga de descifrarlo con su clave privada.

Ransomware

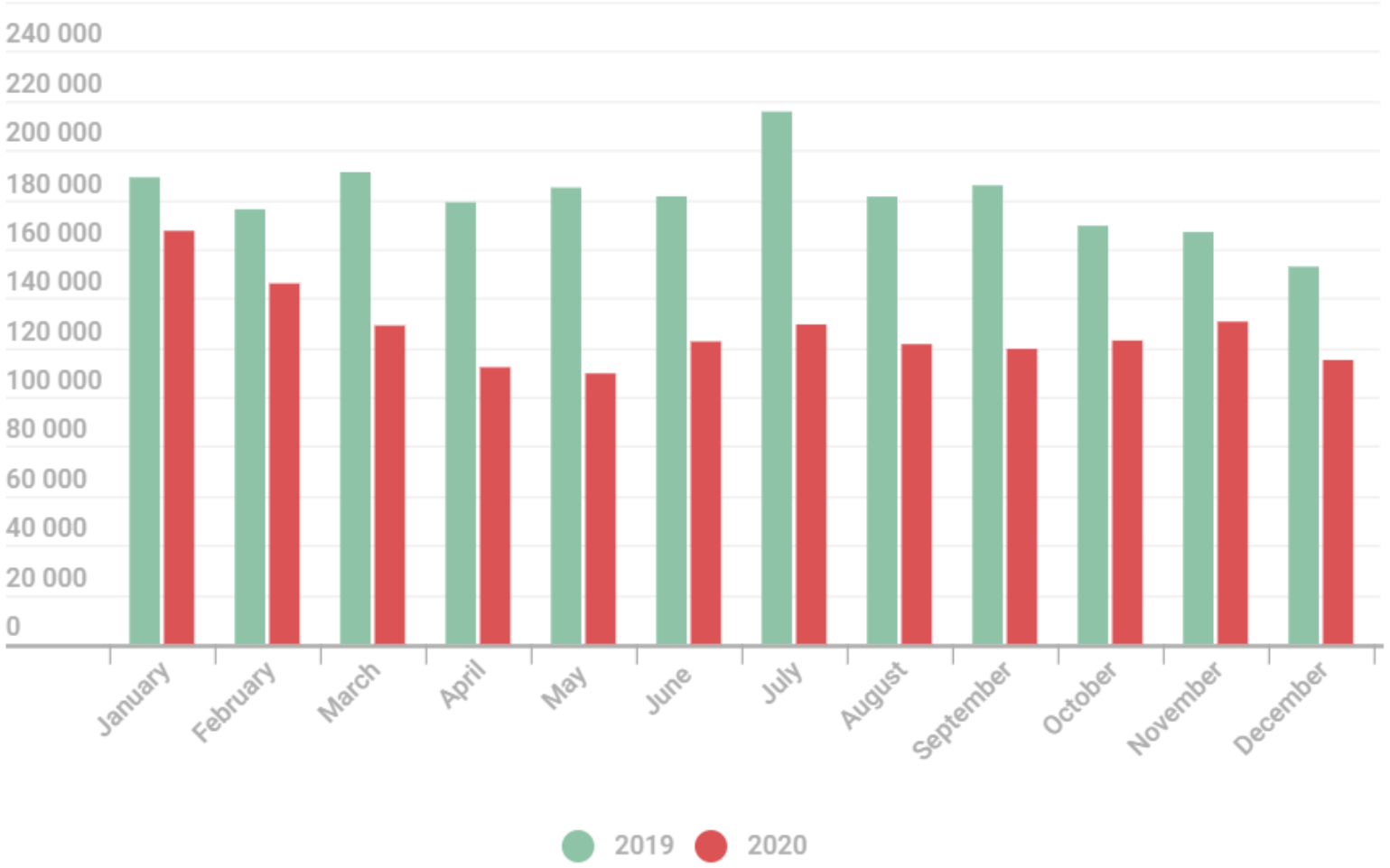
UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

The Anatomy of a Ransomware Attack



Centrify
ZERO TRUST PRIVILEGE

Ransomware



Estadística Ransomware: Kaspersky Labs

Adware

- Es cualquier programa que automáticamente va mostrando **publicidad** al usuario durante su instalación o durante su uso y con ello genera beneficios a sus creadores.
- Aunque se asocia al malware, no tiene que serlo forzosamente, ya que puede ser un medio legítimo usado por desarrolladores de software que lo implementan en sus programas, generalmente en las versiones shareware, haciéndolo desaparecer en el momento en que adquirimos la versión completa del programa. Se convierte en **malware** en el momento en que empieza a recopilar información sobre el ordenador donde se encuentra instalado.

Adware

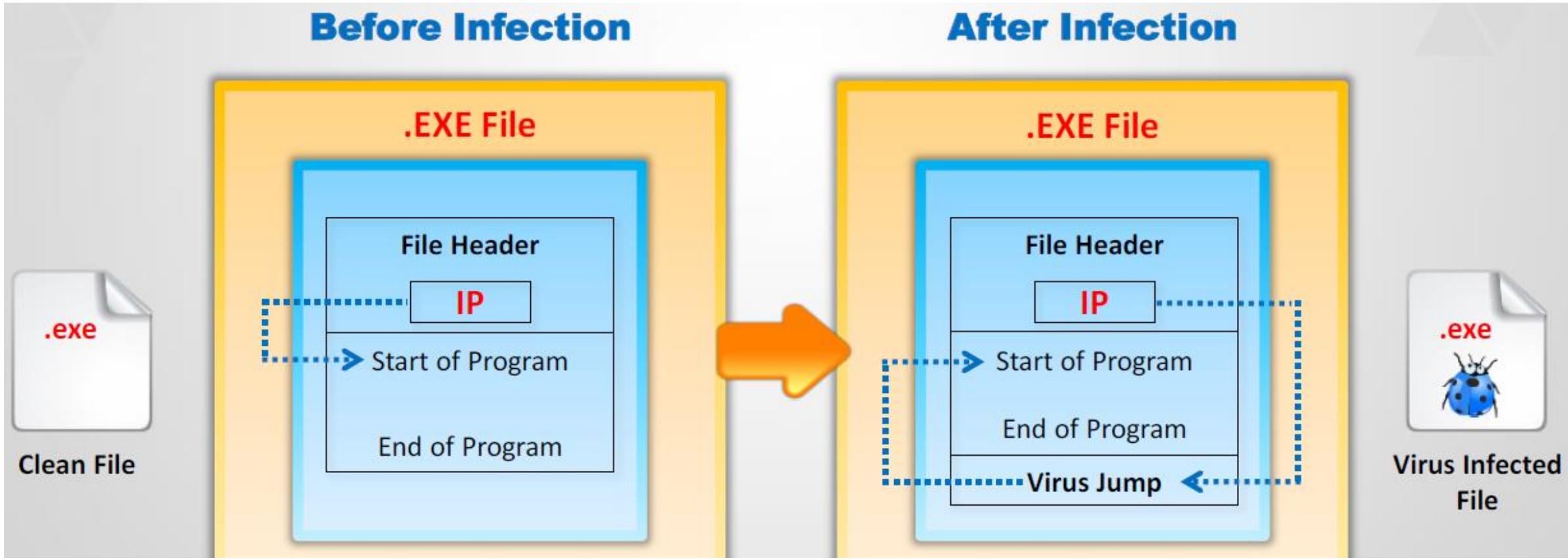
Operación de un Adware

Virus

UNIVERSIDAD TECNICA FEDERICO SANTA MARIA

- **<u>Definición:</u>**
- Programa diseñado para que al ejecutarse, **se copie a sí mismo** adjuntándose en aplicaciones existentes en el equipo. De esta manera, cuando se ejecuta una aplicación infectada, puede infectar otros archivos.
- A diferencia de otro tipo de malware, como los gusanos, no se necesita acción humana para que un virus se propague entre máquinas y sistemas.
- Los más comunes son los que infectan a **ficheros ejecutables**.

Virus



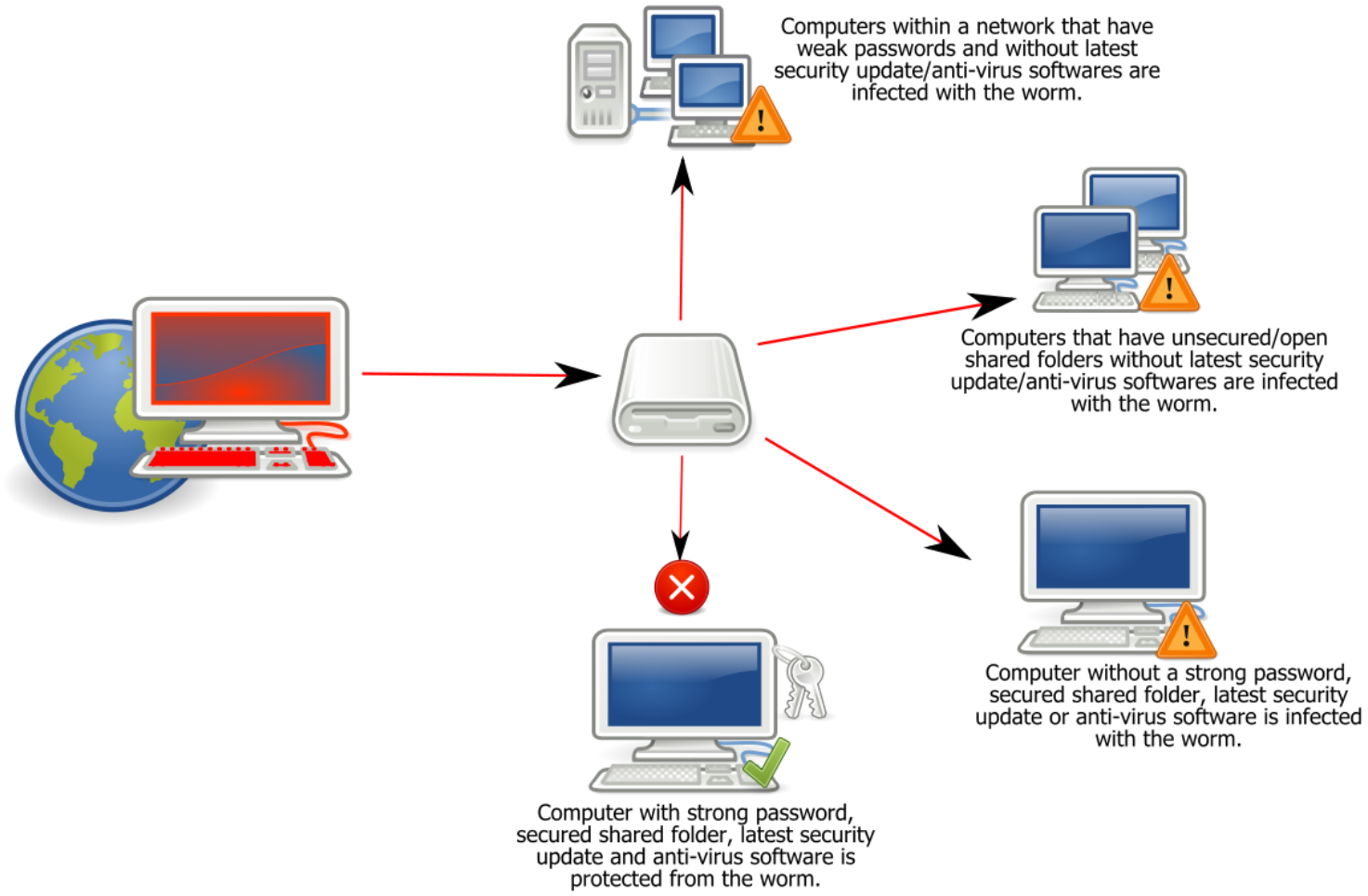
Mecanismo de operación de un virus informático

Gusano

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

- Es un programa malicioso que tiene como característica principal su alto grado de **dispersabilidad**, es decir, lo rápidamente que se propaga.
- Mientras que los troyanos dependen de que un usuario acceda a una web maliciosa o ejecute un fichero infectado, los gusanos realizan **copias de sí mismos**, infectan a otros ordenadores y se propagan automáticamente en una red independientemente de la acción humana.
- Su fin es **replicarse a nuevos sistemas** para infectarlos y seguir replicándose a otros equipos informáticos, aprovechándose de todo tipo de medios como el correo electrónico, IRC, FTP, correo electrónico, P2P y otros protocolos específicos o ampliamente utilizados.

Gusano



Mecanismo de propagación de un gusano

Spyware

UNIVERSIDAD TECNICA FEDERICO SANTA MARIA

- Es un malware que recopila información de un ordenador y después la **envía a una entidad remota** sin el conocimiento o el consentimiento del propietario del ordenador.
- El término spyware también se utiliza más ampliamente para referirse a otros productos como adware, falsos antivirus o troyanos.
- Sus principales acciones son:
  - Captura de pantalla
  - Secuestro de micrófono
  - Secuestro de cámara de video
  - Robo de datos

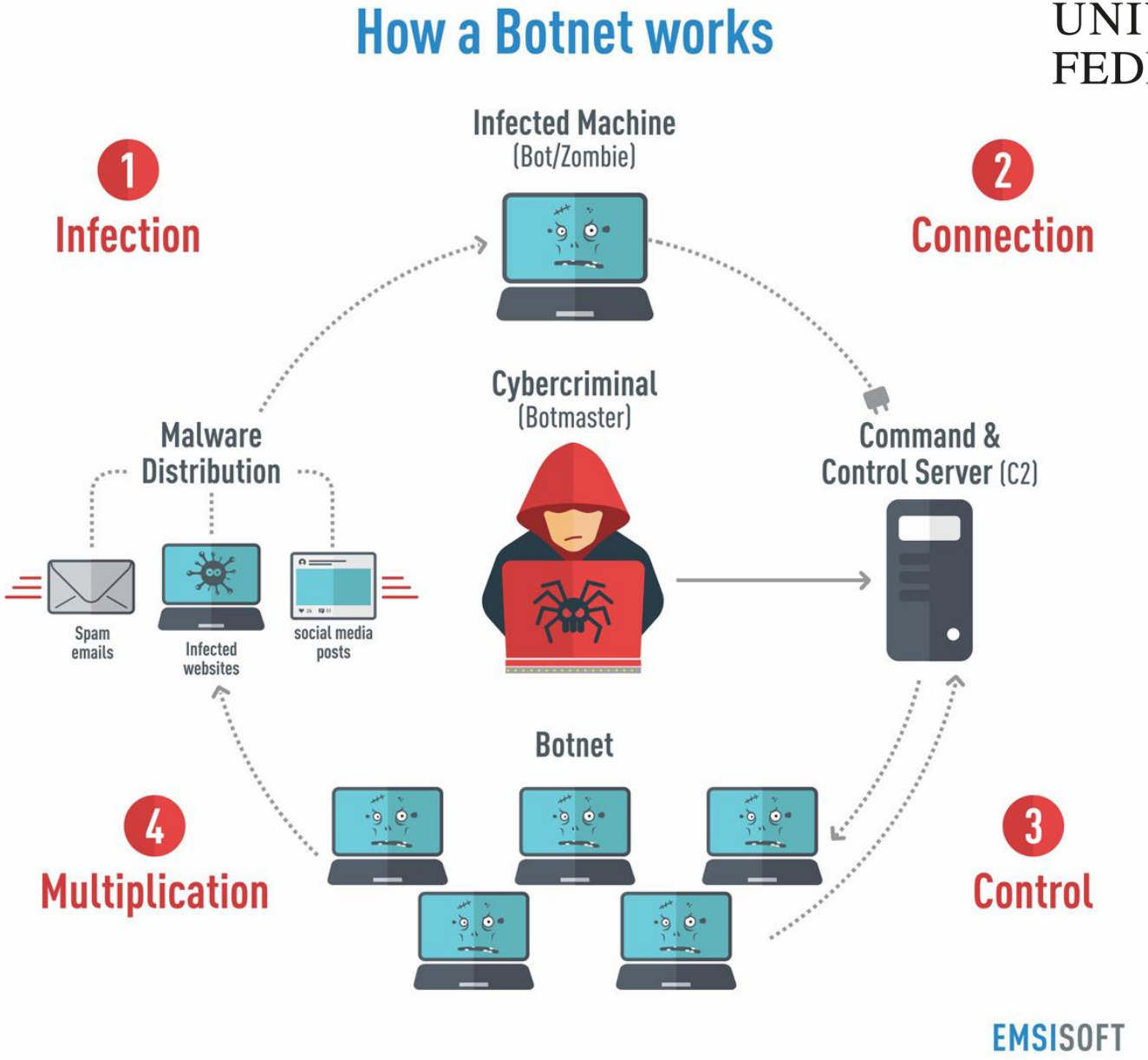
Botnet

UNIVERSIDAD TECNICA FEDERICO SANTA MARIA

- **<u>Definición:</u>**
- Una botnet es un conjunto de ordenadores (denominados bots) **controlados remotamente** por un atacante que pueden ser utilizados en conjunto para realizar actividades maliciosas como envío de spam, ataques de DDoS, etc.
- Las botnets se caracterizan por tener un **servidor central** (C&C, de sus siglas en inglés Command & Control) al que se conectan los bots para enviar información y recibir comandos.
- Existen también las llamadas botnets P2P que se caracterizan por carecer de un servidor C&C único.

Botnet

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA



Botnet

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

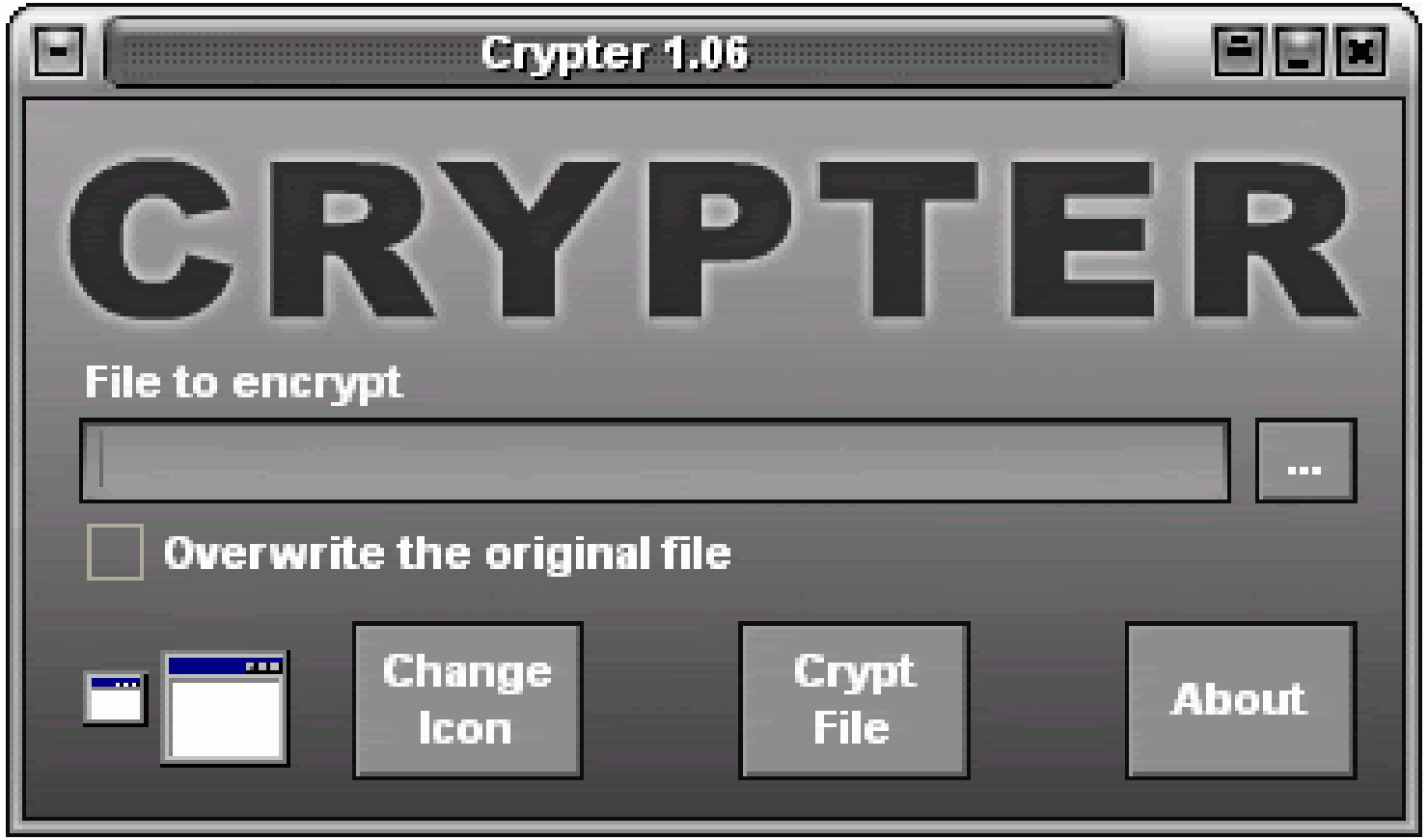
Cantidad de Botnets detectadas por SpamHaus este 2021

Crypter

- Un cifrador es un tipo de software que puede **cifrar, ofuscar y manipular** el malware para que sea más difícil de detectar por los programas de seguridad. Los ciberdelincuentes lo utilizan para crear malware que puede eludir los programas de seguridad presentándose como un programa inofensivo hasta que se instala.
- Los cifradores estáticos utilizan diferentes códigos auxiliares para hacer que cada archivo cifrado sea único.
- Los cifradores polimórficos se consideran más avanzadas. Utilizan **algoritmos de última generación** que utilizan variables aleatorias, datos, claves, decodificadores, etc.

Crypter

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

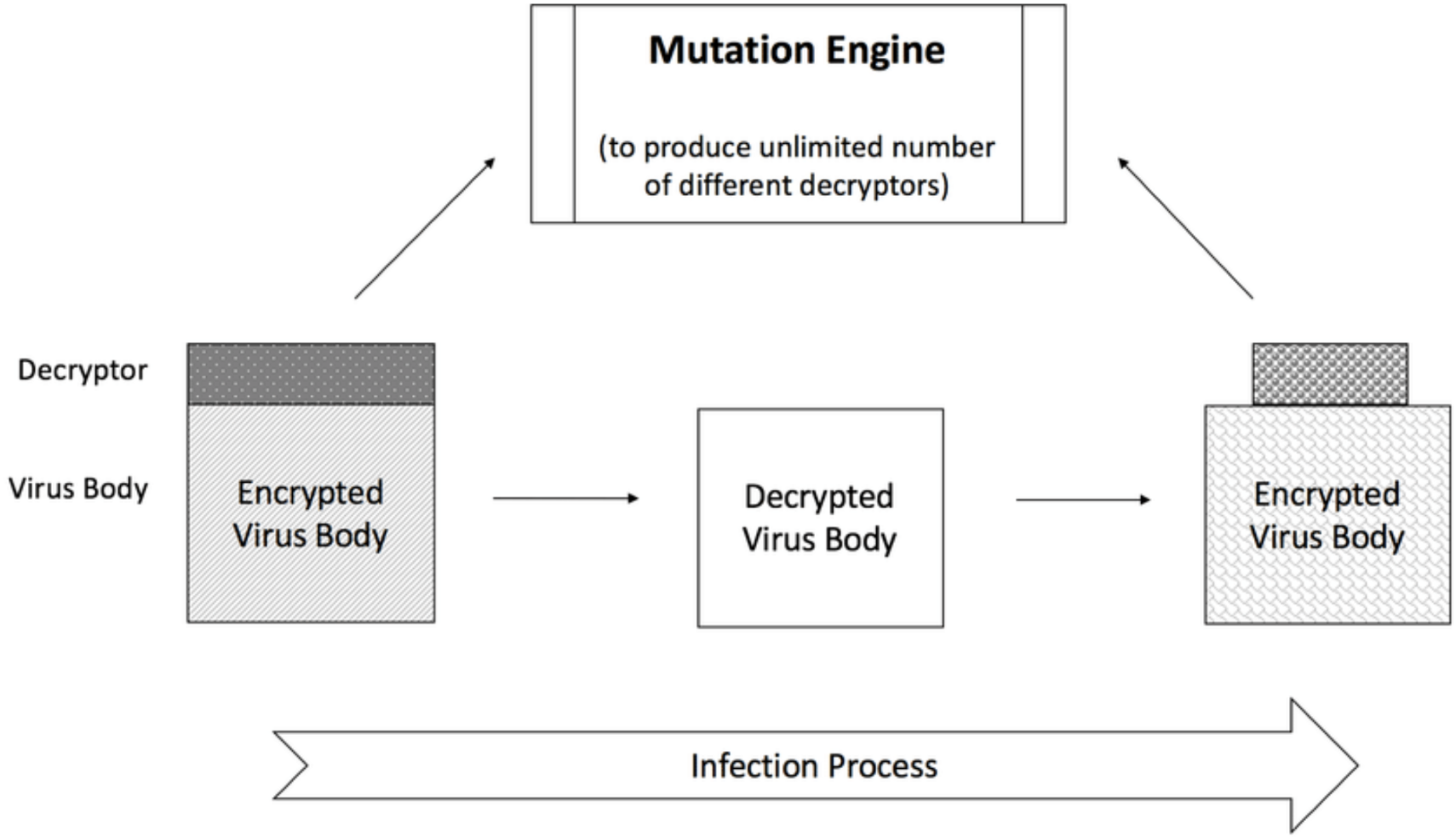


Operación de un malware Crypter

Malware Polimórfico

- Se refiere a aquel tipo de malware que tiene un núcleo que siempre actúa de la **misma manera**. No importa cuántas veces cambie. Siempre realiza las mismas acciones y siempre ataca de la misma manera. Eso sí, sigue modificando el resto de su código para evadir a los antimalware basados en firma.
- El polimorfismo se utiliza para **evadir la detección** de coincidencia de patrones en la que se basan las soluciones de seguridad como el software antivirus.

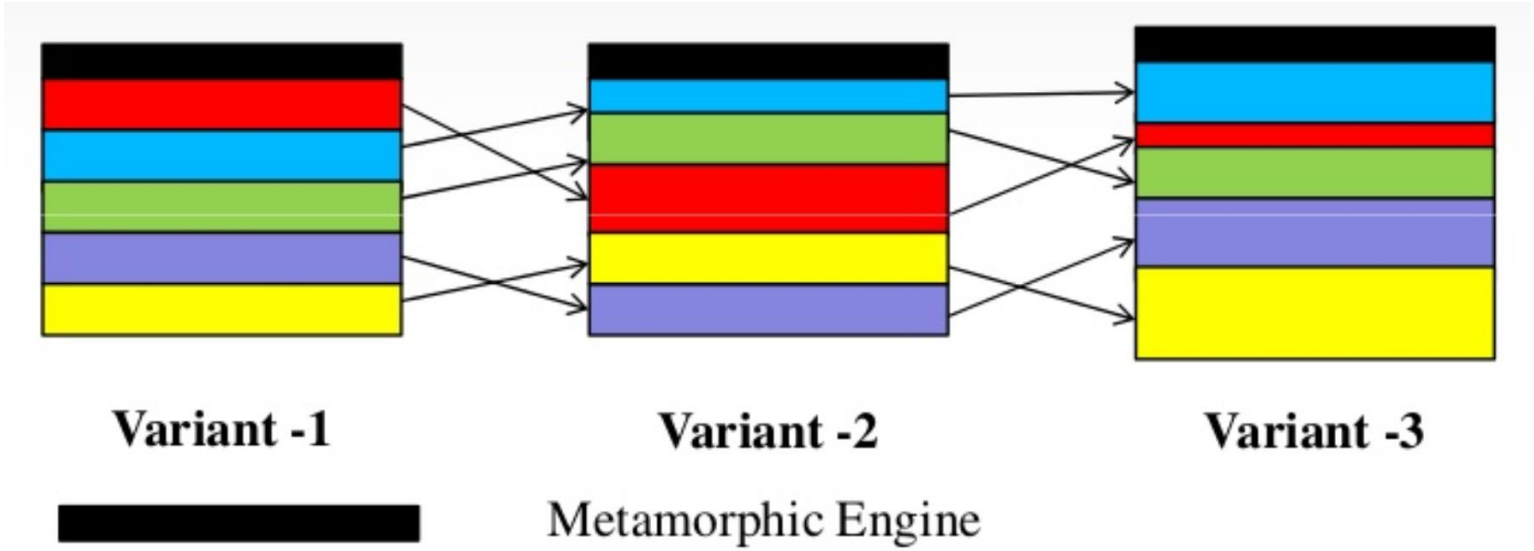
Malware Polimórfico



Malware Metamórfico

UNIVERSIDAD TECNICA FEDERICO SANTA MARIA

- Por su parte, el malware metamórfico intenta **reorganizar todo su código** con cada iteración. Esto significa que funciona de manera similar, pero en cada acto agrega elementos al código distintos. También diferentes funciones reorganizadas para que se vea distinto y sea mucho más difícil detectarlo.



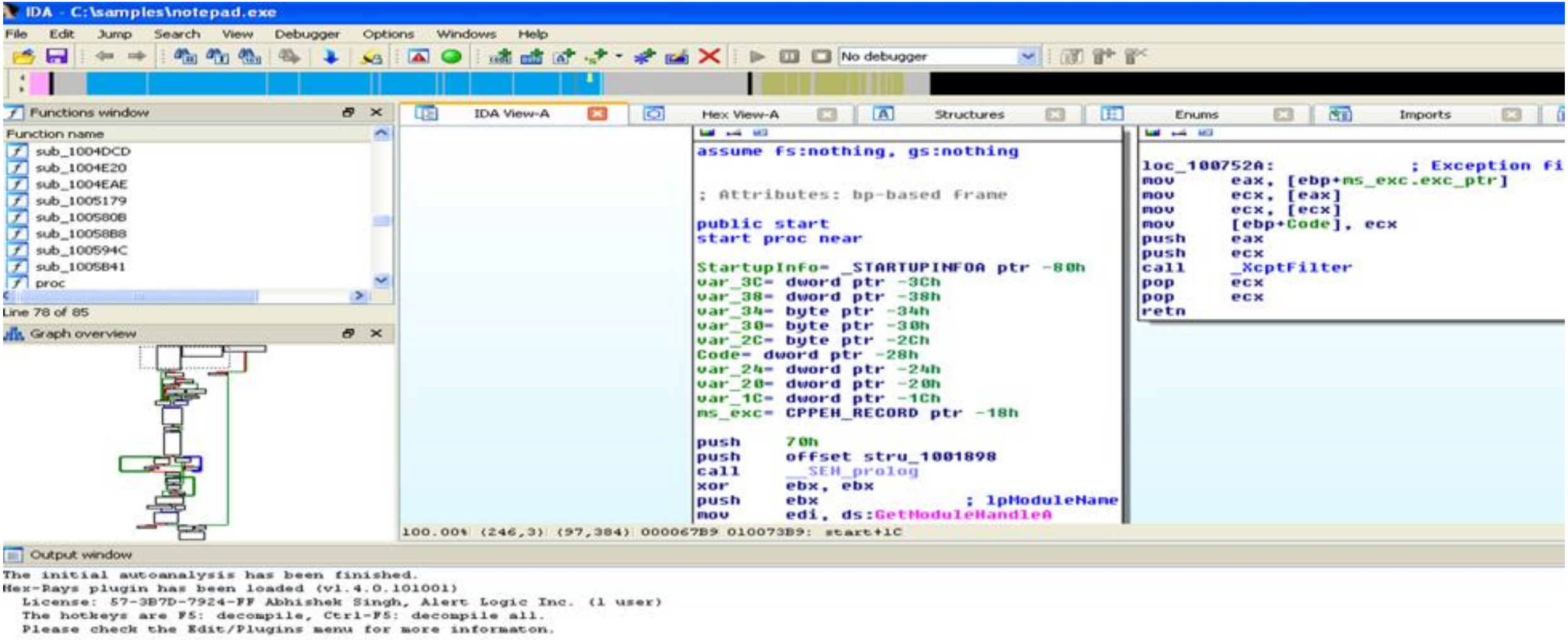
Análisis de Malware

USM
UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

- Es el estudio o proceso para determinar la funcionalidad, el origen y el impacto potencial de una muestra determinada de malware.
- **Análisis estático:** Se realiza normalmente diseccionando los diferentes recursos del archivo binario sin ejecutarlo y estudiando cada componente.
- **Análisis dinámico:** se realiza observando el comportamiento del malware mientras se está ejecutando en un sistema host. Esta forma de análisis se realiza a menudo en una “sandbox” para evitar que el malware infecte realmente a los sistemas de producción.

Análisis estático de malware

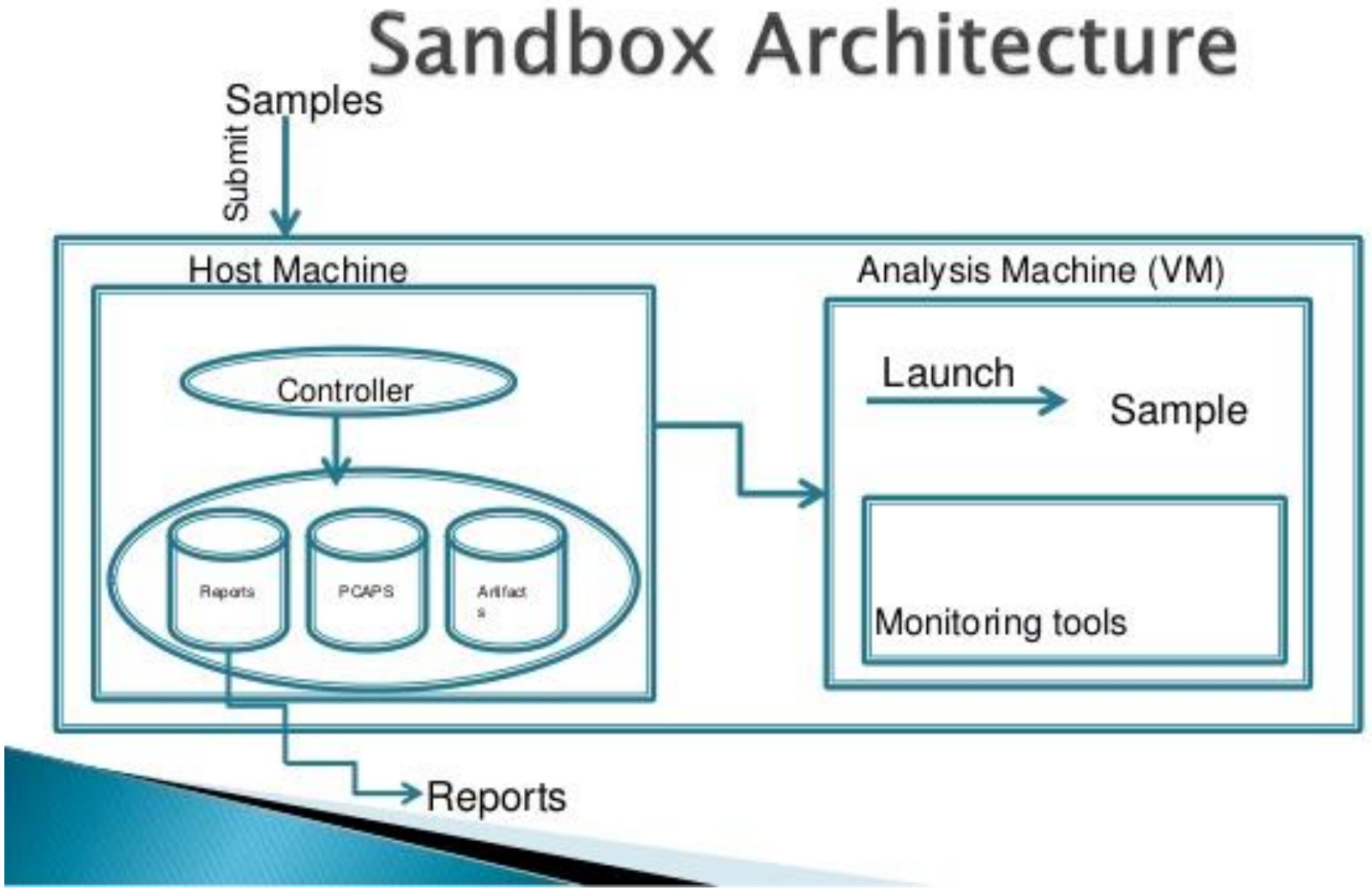
UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA



Análisis estático online

Análisis dinámico de malware

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA



Análisis dinámico de malware

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

- Monitoreo de procesos
- Cambios durante la instalación
- Cambios en la registrería
- Cambios en archivos y directorios
- Log de eventos
- Consultas DNS
- Tráfico hacia redes externas
- Cambio en drivers de dispositivos

Resumen

- Amenazas en Ciberseguridad
- Tipos de malware
  - Técnicas de infección
  - Clasificación
- Evasión de anti-malware
- Análisis de malware
  - Estático
  - Dinámico