Trojans

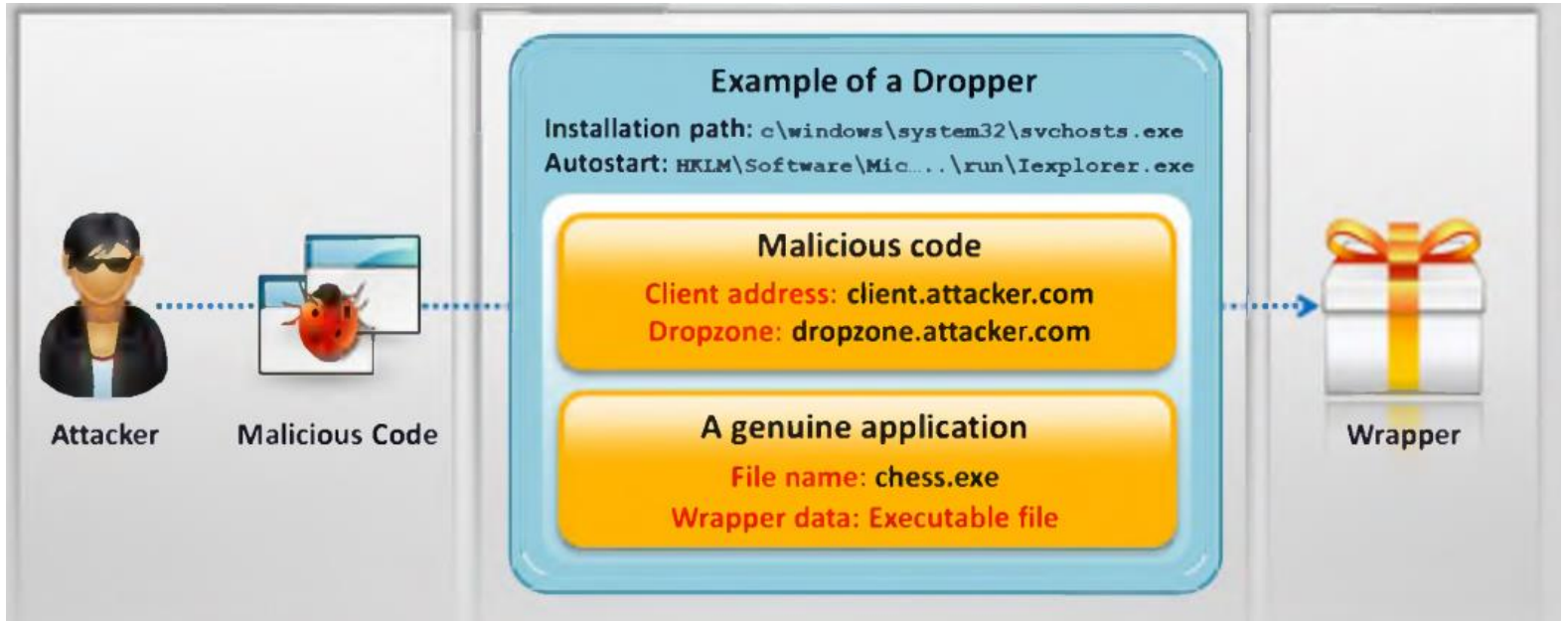
Mayo 2014

Trojan Horses (Caballos de Troya)

- Programas maliciosos que afectan sistemas computacionales sin conocimiento de la victima.
- El propósito del troyano es:
  - Eliminar o reemplazar archivos críticos del sistema
  - Generar tráfico falso para crear ataques DOS
  - Descargar spyware, adware, y archivos maliciosos
  - Grabar pantallas, audio y video
  - Robar información como passwords, códigos de seguridad, tarjetas de crédito
  - Desactivar firewalls y antivirus
  - Crear puertas traseras para obtener acceso remoto
  - Infectar una Pc como un servidor proxy para retransmitir ataques
  - Usar Pc de la victima para efectuar ataques DDoS

Infección

- Empaquetar una aplicación o un paquete troyano (trojan horse construcción kit)
- Ocultar el código del troyano en una aplicación genuina



Proceso de infección

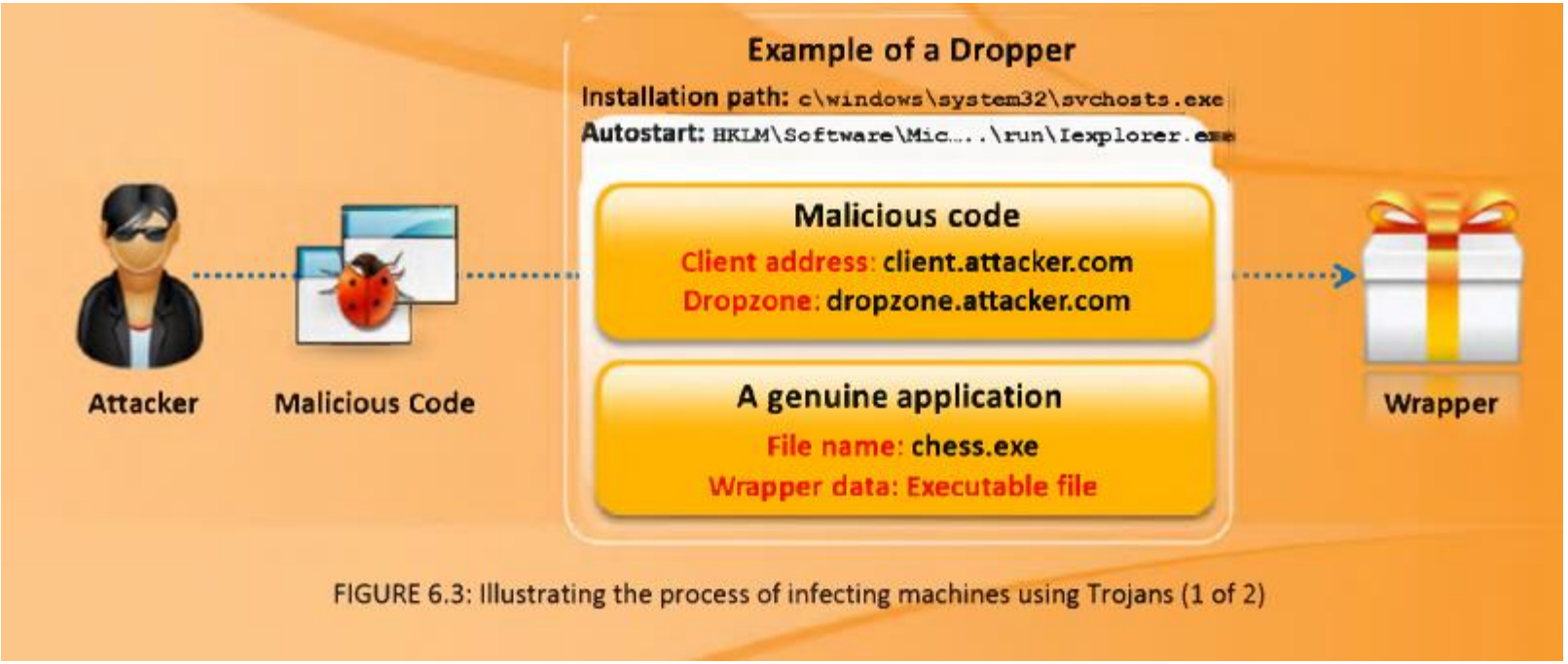
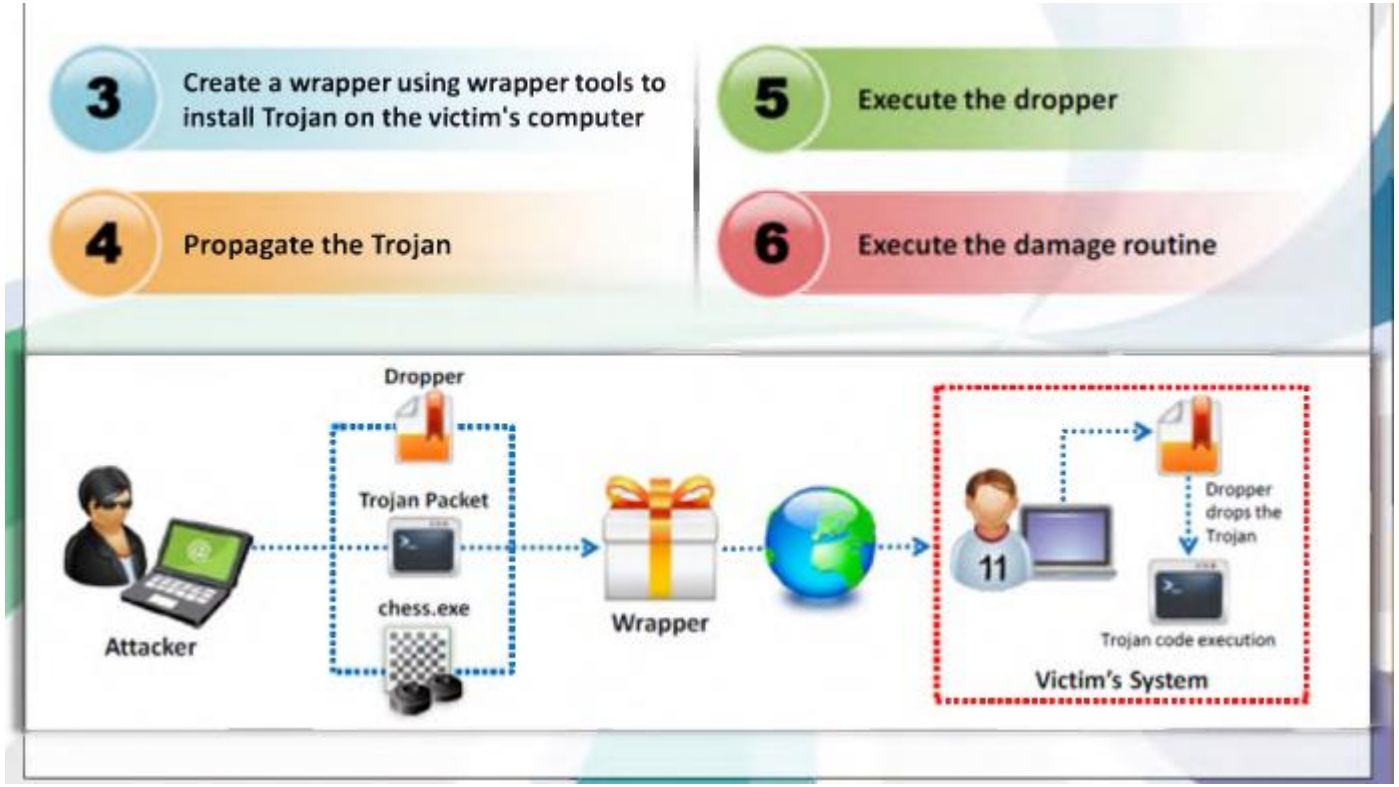


FIGURE 6.3: Illustrating the process of infecting machines using Trojans (1 of 2)

¿Cómo infectar un sistema?



Wrappers

- Son utilizados para incrustrar el troyano ejecutable en una aplicación genuina.
  - Por ejemplo:
    - Juegos, videojuegos, antivirus,
    - editores de texto, etc.

FIGURE 6.5: Wrappers

Wrappers

- Kriptomatik
- Advanced File Joiner
- SCB LAB’s Professional Malware Tool

Formas de introducir un troyano

- Aplicaciones de mensajes instantáneos
- IRC
- Acceso físico
- Navegadores y bugs en clientes de correo
- Programas falsos
- Sitios de dudosa procedencia
- NetBIOS
- Descarga de archivos

Tipos de Troyano