

Lección 6: Malware



intypedia
INFORMATION SECURITY ENCYCLOPEDIA

Bernardo Quintero

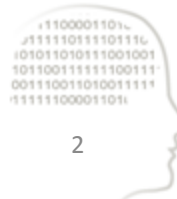
bernardo@hispasec.com

Hispacec – VirusTotal Founder

Malware: definición y tipos

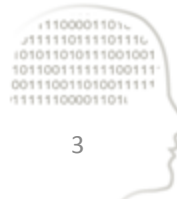
Malicious software

- Se denomina malware al software malicioso, diseñado para llevar cabo acciones no deseadas y sin el consentimiento explícito del usuario.
- Existen muchos tipos de malware, entre otros: virus, troyanos, gusanos, adware, keyloggers, dialers, rootkits, ransomware, rogueware, etc.



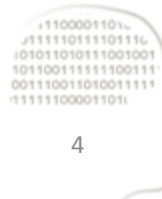
Clasificación: principales características (I)

- Virus: auto-réplica, infectan otros programas.
- Gusano: se replica mediante copias de sí mismo, pero no infecta a otros programas.
- Troyano: no se replica ni infecta a otros programas de forma automática e indiscriminada.
- Adware: presenta publicidad no deseada.
- Keylogger: captura pulsaciones en el teclado, espía lo que el usuario escribe.



Clasificación: principales características (II)

- **Rootkit**: usa técnicas para permanecer oculto en el sistema ante el usuario y las aplicaciones de seguridad.
- **Backdoor**: función de puerta trasera, permite al atacante conectarse y controlar la máquina infectada.
- **Dialer**: realiza llamadas de tarificación especial, incrementando la factura telefónica.
- **Bot**: los sistemas infectados son “zombies” que conforman una “botnet” o red de bots; esta red acepta órdenes de forma remota.



Clasificación: principales características (y III)

- **Ransomware**: cifra documentos y archivos, pide al usuario que pague un rescate si quiere la clave que permita acceder a los originales.
- **Rogueware**: falso antivirus, te hacen creer que el sistema está infectado y cobran para la supuesta desinfección.
- **Crimeware**: nueva denominación para el malware orientado al cibercrimen y fraude, con un claro interés de lucro.



Principales métodos de infección

- Descarga desde páginas webs.
- Adjuntos por email.
- Vulnerabilidades en software.
- Compartir dispositivos de almacenamiento.
- Otros protocolos y aplicaciones en Internet:
 - mensajería instantánea.
 - P2P.
 - redes sociales, etc.



Evolución del malware

- 1987-1999: virus clásicos, los creadores no tenían ánimo de lucro, motivación intelectual y protagonismo.
- 2000-2004: explosión de los gusanos en Internet, propagación por correo electrónico, aparición de las botnets.
- 2005-2009: claro ánimo de lucro, profesionalización del malware, explosión de troyanos bancarios y programas espías.
- 2010-2011: casos avanzados de ataques dirigidos, espionaje industrial y gubernamental, ataque a infraestructuras críticas, proliferación de infecciones en dispositivos móviles.



Malware y sistemas operativos

- La mayoría del malware (>99%) se diseña en la actualidad para plataformas Microsoft Windows.
- MacOS, Linux y otros sistemas operativos cuentan con especímenes de malware en menor medida.
- También existen ejemplares de malware para Android, Symbian o iOS, diseñados para infectar dispositivos y teléfonos móviles.



Efectividad de los antivirus

- Los antivirus **no** pueden proteger al 100% contra el malware, su efectividad es relativa.
- Aunque incorporan sistemas heurísticos para intentar prevenir nuevos especímenes, en la mayoría de los casos siguen teniendo una respuesta reactiva (no efectiva hasta el estudio de una primera muestra del malware).
- Pese a sus limitaciones, es recomendable su uso para tratar de minimizar las infecciones.



Medidas para prevenir infecciones

- Usar antivirus actualizado.
- Actualización del sistema operativo, navegador y resto de aplicaciones.
- Uso de usuario restringido vs administrador.
- Sentido común y uso responsable:
 - Evitar abrir correo no deseado y enlaces llamativos en las redes sociales.
 - Evitar abrir documentos e instalar software de fuentes no confiables.





intypedia

INFORMATION SECURITY ENCYCLOPEDIA