Universidad de Buenos Aires
Facultad de Ciencias Económicas

Virus y Malware

AR Tema extractado del libro "**Análisis Funcional de Sistemas y Tecnologías de la Información**" de Aníbal M. Mazza Fraquelli - ISBN 978-987-26981-3-3

Presentación del Tema

Los **virus, troyanos, gusanos, spyware y otras formas de malware** constituyen categorías de software malicioso diseñadas para infiltrarse, dañar, alterar o explotar sistemas de información sin el consentimiento del usuario. En el contexto de las Tecnologías de la Información (TI), el malware representa una de las principales amenazas para la continuidad operativa, la integridad de los datos y la seguridad organizacional.

El término **malware (Malicious Software / Software Malicioso)** engloba cualquier programa o código desarrollado con fines perjudiciales. Estas amenazas pueden afectar hardware, software, redes, bases de datos y dispositivos móviles, impactando directamente la infraestructura tecnológica que sostiene los procesos organizacionales.

Para estudiantes de licenciatura en administración, comprender la naturaleza, funcionamiento e impacto del malware implica reconocer que los riesgos digitales no son exclusivamente técnicos, sino estratégicos. Una infección masiva puede paralizar operaciones, comprometer datos sensibles, generar sanciones regulatorias y afectar la reputación corporativa.

Desarrollo

1. Concepto General de Malware

El malware es cualquier software diseñado para:

- Interrumpir operaciones.
- Obtener acceso no autorizado.
- Robar información.
- Espiar actividades.
- Extorsionar a la organización.

Su evolución ha sido constante, acompañando el crecimiento de Internet, la movilidad y la computación en la nube.

El análisis del malware debe realizarse bajo el modelo CIA (Confidentiality, Integrity, Availability / Confidencialidad, Integridad y Disponibilidad), ya que estas amenazas suelen atacar uno o más de estos pilares.

---

2. Virus Informáticos

Un **virus informático** es un programa que se inserta en archivos o aplicaciones legítimas y se activa cuando estos se ejecutan. Requiere intervención humana para propagarse.

Características principales:

- Se adjunta a archivos ejecutables.
- Se replica al ejecutarse.
- Puede alterar o destruir datos.

Ejemplo organizacional:

Un empleado descarga un archivo infectado que altera hojas de cálculo financieras.

Impacto:

- Pérdida de integridad de datos.
- Interrupción operativa.
- Costos de recuperación.

---

3. Gusanos (Worms)

Un **gusano (Worm)** es un tipo de malware que se replica automáticamente y se propaga a través de redes sin necesidad de interacción humana.

Características:

- Autopropagación.
- Alta velocidad de expansión.
- Saturación de redes.

Ejemplo:

Un gusano que explota una vulnerabilidad en un servidor sin parches puede propagarse en minutos a toda la red corporativa.

Impacto:

- Caída de sistemas.
- Consumo excesivo de recursos.
- Paralización de servicios.

---

4. Troyanos (Trojans)

Un **troyano (Trojan Horse / Caballo de Troya)** es un programa que aparenta ser legítimo pero contiene código malicioso oculto.

A diferencia del virus, el troyano no se replica por sí mismo.

Objetivos comunes:

- Crear puertas traseras (Backdoors).
- Robar credenciales.
- Permitir acceso remoto no autorizado.

Ejemplo:

Un software aparentemente gratuito que, al instalarse, permite al atacante controlar remotamente el sistema.

Desde la administración, la instalación de software no autorizado constituye una vulnerabilidad crítica.

---

5. Spyware

El **spyware** es un tipo de malware diseñado para recopilar información sin el conocimiento del usuario.

Puede capturar:

- Credenciales.
- Historial de navegación.
- Información financiera.
- Actividad de teclado (Keylogging).

Impacto organizacional:

- Robo de datos estratégicos.
- Pérdida de confidencialidad.
- Violaciones regulatorias.

---

6. Ransomware

El **ransomware** cifra datos y exige un rescate para su liberación.

Es una de las amenazas más significativas para organizaciones.

Características:

- Cifrado masivo de archivos.
- Bloqueo de sistemas.
- Extorsión económica.

Ejemplo:

Una empresa que pierde acceso a su sistema ERP durante varios días por ataque de ransomware.

La existencia de backups adecuados puede mitigar el impacto.

---

7. Malware Avanzado y Persistente

Las amenazas avanzadas incluyen:

- APT (Advanced Persistent Threat / Amenaza Persistente Avanzada).

- Rootkits.
- Botnets.

Estas amenazas buscan permanecer ocultas durante largos períodos.

Desde la perspectiva estratégica, requieren monitoreo continuo y arquitectura Zero Trust.

---

8. Vectores de Infección

El malware puede ingresar mediante:

- Correos electrónicos (phishing).
- Descargas no seguras.
- Dispositivos USB.
- Vulnerabilidades sin parchear.
- Redes Wi-Fi inseguras.

La combinación de debilidades técnicas y humanas facilita la infección.

---

9. Impacto Organizacional

El malware puede generar:

- Pérdidas financieras directas.
- Multas regulatorias.
- Interrupción de servicios.
- Daño reputacional.
- Pérdida de confianza del mercado.

Desde la administración, el malware constituye un riesgo estratégico.

---

10. Prevención y Controles

La mitigación requiere combinación de:

- Antivirus y antimalware.
- Actualización de parches.

- Segmentación de red.
- MFA (Multi-Factor Authentication / Autenticación Multifactor).
- Capacitación en seguridad.
- Políticas de uso aceptable.

El enfoque Zero Trust refuerza la prevención.

---

11. Relación con Gestión de Riesgos

El riesgo asociado al malware puede analizarse mediante:

Riesgo = Amenaza × Vulnerabilidad × Impacto.

Reducir vulnerabilidades (actualizaciones, controles de acceso) disminuye exposición.

---

12. Ejemplo Integrado

Empresa sin actualización de parches:

Amenaza: gusano.

Vulnerabilidad: software desactualizado.

Impacto: caída total de red.

Con actualizaciones periódicas y monitoreo, el impacto puede evitarse.

---

13. Dimensión Estratégica para la Administración

Para los administradores, la gestión del malware implica:

- Evaluar inversión en seguridad.
- Diseñar políticas preventivas.
- Integrar seguridad en planificación estratégica.
- Supervisar cumplimiento.

El costo de prevención suele ser inferior al costo de recuperación.

Conclusión

Los virus, gusanos, troyanos, spyware y otras formas de malware representan amenazas críticas para los sistemas de información organizacionales. Su impacto trasciende el plano técnico, afectando dimensiones financieras, operativas y reputacionales.

La comprensión de sus características, vectores de ataque y mecanismos de mitigación es esencial para la gestión estratégica de TI. Desde la perspectiva administrativa, la prevención del malware requiere integración de controles técnicos, administrativos y culturales, fortaleciendo la resiliencia organizacional frente a amenazas digitales crecientes.

En un entorno digital altamente interconectado, la gestión proactiva del malware constituye una condición indispensable para la sostenibilidad del negocio.

Preguntas de autoevaluación

1. ¿Cuál es la diferencia principal entre virus, gusano y troyano?
2. ¿Por qué el ransomware representa una amenaza estratégica para las organizaciones?
3. ¿Qué rol cumple la capacitación en la prevención de malware?
4. ¿Cómo se aplica la ecuación del riesgo al análisis de amenazas de malware?
5. ¿Por qué la gestión del malware debe integrarse en la estrategia corporativa?

Material de Clases

Compilado por **Aníbal M. Mazza Fraquelli** Doctor de la Universidad de Buenos Aires para el uso de sus clases en la Facultad de Ciencias Económicas de la Universidad de Buenos Aires.

Contenidos de esta página

Los contenidos **aquí incluidos integran desarrollos y escritos propios del autor, así como materiales de terceros (documentos, textos, fragmentos, conceptos, imágenes, esquemas, definiciones u otros recursos),** los cuales son utilizados a título ilustrativo, explicativo o formativo, respetando la normativa vigente en materia de derechos de autor y citando las fuentes cuando corresponde.
La selección, organización, adaptación pedagógica y contextualización de los contenidos constituye un trabajo original del autor, orientado a facilitar los procesos de enseñanza y aprendizaje.
Este material no persigue fines comerciales y su reproducción, total o parcial, queda limitada al ámbito educativo, debiendo preservarse siempre la mención de la autoría y las fuentes originales.

Autorización de uso

Se permite la reproducción, comunicación pública, distribución y utilización total o parcial de los contenidos de su material, en formato físico o digital, con fines exclusivamente educativos, académicos o de divulgación, siempre que se respete la integridad del contenido y se incluya la correspondiente referencia a la fuente y a la autoría.
Las ideas, opiniones e interpretaciones contenidas en este material corresponden exclusivamente al autor.
Queda expresamente excluido cualquier uso con fines comerciales.