Universidad de Buenos Aires
Facultad de Ciencias Económicas

Las Acciones de los Virus

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 **ataques y acciones maliciosas ejecutadas por virus y otros tipos de malware (Malicious Software / Software Malicioso)** constituyen una de las amenazas más persistentes y disruptivas en el ámbito de los Sistemas de Información (SI – *Information Systems*). Estas acciones no se limitan a la mera infección técnica de dispositivos, sino que pueden comprometer procesos críticos, alterar información estratégica, interrumpir operaciones y generar pérdidas económicas significativas.

En términos de seguridad informática, las acciones maliciosas suelen analizarse en función de su impacto sobre los tres pilares del modelo **CIA (Confidentiality, Integrity, Availability / Confidencialidad, Integridad y Disponibilidad)**. Los virus y programas maliciosos pueden producir:

- **Interrupción (Interruption)** de servicios.
- **Intercepción (Interception)** de información.
- **Espionaje (Espionage)** digital.
- **Modificación (Modification)** de datos.
- **Destrucción (Destruction)** de información.
- Ataques a la integridad de los datos.

Desde la perspectiva administrativa y de gestión de TI, comprender estas acciones no es solo un ejercicio técnico, sino un requisito estratégico para diseñar políticas de prevención, evaluar riesgos y proteger la continuidad del negocio.

Desarrollo

1. Interrupción (Interruption)

La interrupción consiste en la imposibilidad temporal o permanente de acceder a sistemas, datos o servicios.

1.1 Naturaleza del Ataque

Puede producirse mediante:

- Ransomware.
- Gusanos que saturan la red.
- Virus que bloquean sistemas operativos.
- Ataques de denegación de servicio (DoS – *Denial of Service* / Denegación de Servicio).

1.2 Impacto Organizacional

La interrupción afecta directamente la **disponibilidad (Availability)**.

Ejemplo:

Una empresa de comercio electrónico que sufre un ataque ransomware durante una campaña de ventas experimenta pérdidas financieras inmediatas y deterioro reputacional.

Desde la administración, la interrupción implica:

- Costos operativos.
- Pérdida de ingresos.
- Incumplimiento contractual.

La existencia de un DRP (Disaster Recovery Plan / Plan de Recuperación ante Desastres) reduce el impacto.

2. Intercepción (Interception)

La intercepción implica acceso no autorizado a información en tránsito o almacenada.

2.1 Modalidades

- Keyloggers (registro de pulsaciones).
- Malware de sniffing de red.
- Troyanos con puertas traseras (Backdoors).

2.2 Impacto

Afecta la **confidencialidad (Confidentiality)**.

Ejemplo:

Un spyware que captura credenciales financieras y permite transferencias fraudulentas.

La intercepción suele pasar desapercibida, lo que aumenta su peligrosidad.

---

3. Espionaje Digital

El espionaje digital es una forma sofisticada de intercepción orientada a obtener información estratégica.

3.1 Amenazas Persistentes

APT (Advanced Persistent Threat / Amenaza Persistente Avanzada) son ataques prolongados diseñados para extraer información sensible.

3.2 Impacto Estratégico

Puede comprometer:

- Secretos comerciales.
- Planes estratégicos.
- Información de investigación y desarrollo.

Desde la perspectiva organizacional, el espionaje afecta la ventaja competitiva.

---

4. Modificación de Datos (Modification)

La modificación implica alterar información sin autorización.

4.1 Formas Comunes

- Cambios en registros contables.
- Manipulación de bases de datos.
- Alteración de configuraciones críticas.

4.2 Impacto

Afecta la **integridad (Integrity)**.

Ejemplo:

Un virus que modifica valores financieros en un ERP, generando reportes incorrectos.

La toma de decisiones basada en datos alterados puede provocar errores estratégicos graves.

---

5. Destrucción de Datos (Destruction)

La destrucción implica eliminación permanente o irreversible de información.

5.1 Modalidades

- Virus destructivos.
- Borrado masivo de archivos.
- Sobrescritura de datos.

5.2 Consecuencias

- Pérdida de historial financiero.
- Incumplimiento regulatorio.
- Daño reputacional.

La estrategia de backup 3-2-1 es fundamental para mitigar este riesgo.

---

6. Ataques a la Integridad de los Datos

Más allá de la modificación visible, existen ataques sutiles que afectan integridad:

- Alteraciones mínimas que pasan inadvertidas.
- Inserción de registros falsos.
- Manipulación gradual de información.

Estos ataques pueden ser más dañinos que la destrucción inmediata, porque generan decisiones basadas en datos incorrectos.

---

7. Ataques Combinados

En la práctica, las acciones maliciosas suelen combinar múltiples efectos.

Ejemplo:

Un ransomware puede:

- Interrumpir servicios.
- Interceptar información.
- Amenazar con publicar datos.
- Destruir archivos si no se paga rescate.

El impacto se multiplica.

---

8. Propagación Interna

Una vez dentro del sistema, el malware puede desplazarse lateralmente.

La ausencia de segmentación de red amplifica el daño.

El modelo Zero Trust (Confianza Cero) limita la propagación.

---

9. Dimensión Humana

Muchos ataques comienzan mediante:

- Phishing.
- Ingeniería social.

- Descarga de archivos no verificados.

La capacitación reduce vulnerabilidades humanas.

---

10. Evaluación del Riesgo

Las acciones maliciosas deben analizarse bajo la ecuación:

Riesgo = Amenaza × Vulnerabilidad × Impacto.

Reducir vulnerabilidades (actualización de parches, MFA, segmentación) disminuye probabilidad de éxito.

---

11. Ejemplo Integrado

Empresa sin segmentación ni backups adecuados.

Amenaza: virus destructivo.

Vulnerabilidad: falta de actualización.

Impacto: pérdida total de datos financieros.

Con:

- Backup externo.
- Segmentación de red.
- Monitoreo SIEM (Security Information and Event Management / Gestión de Eventos de Seguridad).

El impacto se reduce significativamente.

---

12. Dimensión Estratégica para la Administración

Las acciones maliciosas afectan:

- Continuidad operativa.
- Confianza de clientes.
- Valor de marca.
- Cumplimiento normativo.
- Estabilidad financiera.

La prevención requiere inversión estratégica en seguridad.

Conclusión

Las acciones maliciosas ejecutadas por virus y otros tipos de malware pueden producir interrupción, intercepción, espionaje, modificación y destrucción de datos, comprometiendo los pilares fundamentales de la seguridad de la información. Estas amenazas no solo afectan la infraestructura tecnológica, sino que impactan directamente en la estabilidad y sostenibilidad organizacional.

Desde la perspectiva administrativa, la comprensión de estas acciones permite diseñar estrategias de prevención y mitigación alineadas con la gestión de riesgos. La combinación de controles técnicos, administrativos y culturales constituye la base de una arquitectura resiliente frente a amenazas digitales cada vez más sofisticadas.

En un entorno digital interconectado, proteger la integridad y disponibilidad de los datos es una responsabilidad estratégica que trasciende el ámbito puramente técnico.

Preguntas de autoevaluación

1. ¿Cómo se relacionan las acciones maliciosas con el modelo CIA?
2. ¿Cuál es la diferencia entre intercepción y espionaje digital?
3. ¿Por qué la modificación de datos puede ser más peligrosa que su destrucción inmediata?
4. ¿Cómo contribuye la segmentación de red a limitar la propagación de malware?
5. ¿Por qué la gestión de riesgos es esencial frente a ataques maliciosos?

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.