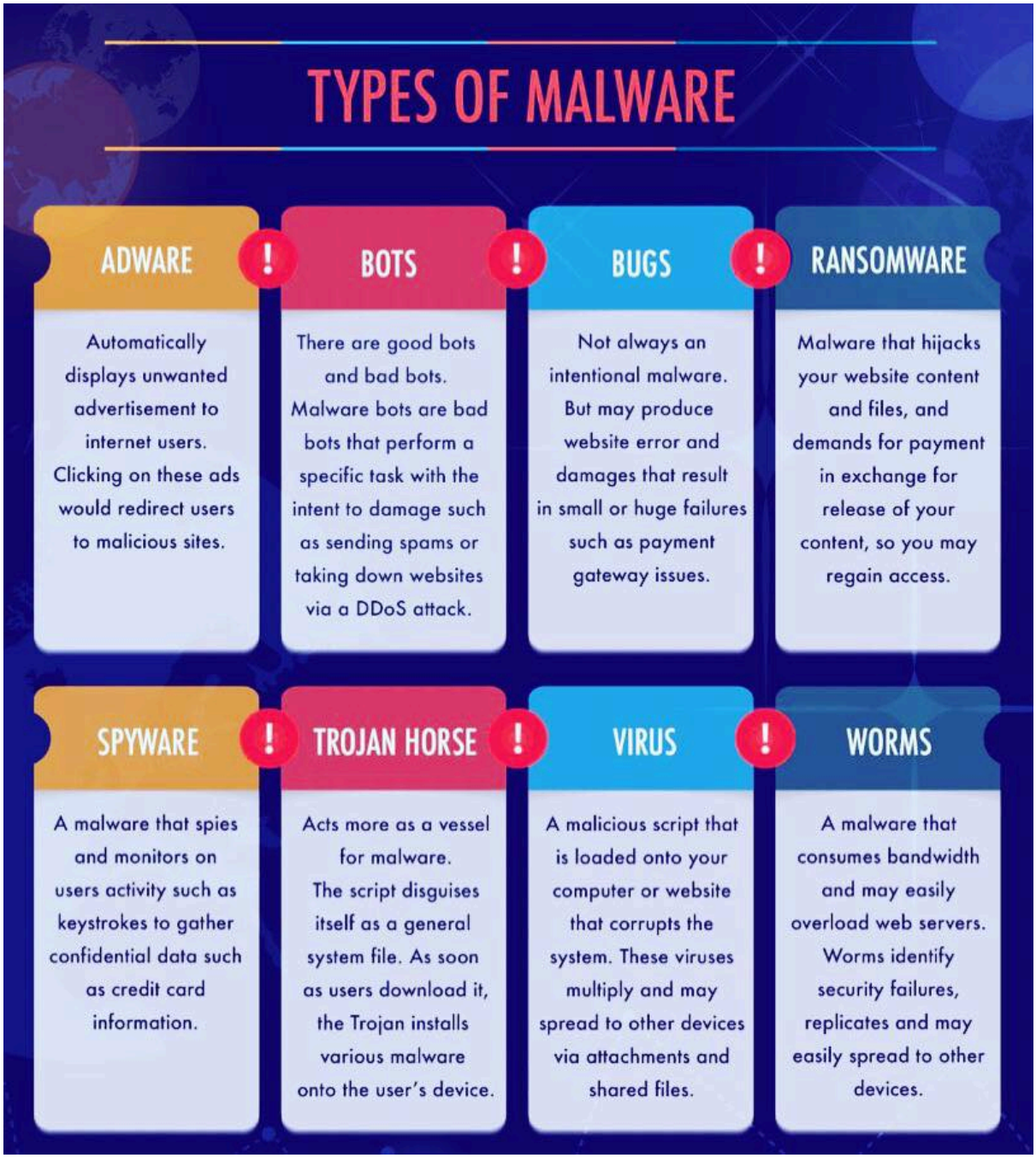
Universidad de Buenos Aires
Facultad de Ciencias Económicas

Tipos de Malware

Material de Estudio



Traducción y Comentarios

1. Adware

Traducción y explicación:

Software que **muestra automáticamente publicidad no deseada** a los usuarios de Internet. Al hacer clic en estos anuncios, el usuario puede ser **redirigido a sitios maliciosos**.

Qué debe considerar la administración:

- Impacta en la **experiencia del usuario** y la productividad.
- Puede ser una **puerta de entrada a otros tipos de malware**.
- Suele aparecer por instalaciones de software sin control o licencias poco claras.

---

2. Bots

Traducción y explicación:

Existen **bots buenos y bots malos**.

Los **bots maliciosos** son programas automatizados que realizan tareas dañinas, como **enviar spam** o **derribar sitios web mediante ataques DDoS**.

Siglas:

- **DDoS – Distributed Denial of Service / Denegación de Servicio Distribuida**

Qué debe considerar la administración:

- Riesgo para la **disponibilidad de sistemas y servicios online**.
- Puede afectar portales web, plataformas de e-commerce o servicios al cliente.
- Requiere monitoreo y medidas de seguridad en infraestructura.

---

3. Bugs

Traducción y explicación:

No siempre son malware intencional. Son **errores de software** que pueden provocar fallos en sitios web o sistemas, desde problemas menores hasta **fallas críticas**, como errores en **pasarelas de pago**.

Qué debe considerar la administración:

- Afectan la **calidad del sistema de información**.
- Pueden generar pérdidas económicas indirectas.
- Relevan la importancia de pruebas, control de cambios y mantenimiento.

---

4. Ransomware

Traducción y explicación:

Malware que **secuestra archivos o sistemas**, bloqueando el acceso y **exigiendo un pago** a cambio de liberarlos.

Qué debe considerar la administración:

- Riesgo crítico para la **continuidad del negocio**.
- Puede paralizar operaciones administrativas, contables o logísticas.
- Hace indispensable contar con **copias de seguridad (backups)** y planes de contingencia.

---

5. Spyware

Traducción y explicación:

Malware que **espía y monitorea la actividad del usuario**, como pulsaciones del teclado, para obtener información confidencial (por ejemplo, **datos de tarjetas de crédito**).

Qué debe considerar la administración:

- Compromete la **confidencialidad de la información**.
- Riesgo legal y reputacional para la empresa.
- Relacionado con la protección de datos personales y financieros.

---

6. Trojan Horse (Caballo de Troya)

Traducción y explicación:

Actúa como un **contenedor de malware**. Se disfraza de archivo o programa legítimo y, al ser descargado, **instala otros tipos de malware** en el dispositivo del usuario.

Qué debe considerar la administración:

- Aprovecha el **error humano** y la falta de capacitación.
- Refuerza la necesidad de políticas de descarga y concientización.
- No se replica solo, depende de la acción del usuario.

---

7. Virus

Traducción y explicación:

Script o programa malicioso que **infecta computadoras o sitios web**, corrompe el sistema, se **multiplica** y se propaga mediante **archivos compartidos o adjuntos**.

Qué debe considerar la administración:

- Afecta la **integridad de los sistemas de información**.
- Puede propagarse rápidamente dentro de una organización.
- Requiere controles antivirus y actualizaciones constantes.

---

8. Worms (Gusanos)

Traducción y explicación:

Malware que **consume ancho de banda**, sobrecarga servidores y se **propaga de forma autónoma** explotando fallas de seguridad.

Qué debe considerar la administración:

- Impacta en el **rendimiento de redes y sistemas**.
- No necesita intervención del usuario para replicarse.
- Destaca la importancia de la gestión de parches y actualizaciones.

Síntesis desde la mirada administrativa

- El malware no es solo un problema técnico, sino un **riesgo organizacional**.
- Afecta costos, continuidad operativa, reputación y cumplimiento normativo.
- La administración debe integrar la **seguridad de la información** como parte de la gestión estratégica de los sistemas de información.

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.