Malware: una amenaza latente para las PyMES

Hugo Gonzalez

Universidad Politécnica de San Luis Potosí

Noviembre 6 de 2019, Congreso Anual de Ciberseguridad

Contenido

- Sobre el expositor
- Definiciones
- PyMES y seguridad
- Malware: Ataques
- Malware y PyMES
- Recomendaciones

Sobre el expositor

- Hugo Gonzalez, PhD
- Profesor Investigador en la UPSLP
- Su línea de trabajo incluye:
  - Seguridad en redes y servidores,
  - Análisis de malware,
  - Malware para Android,
  - Aprendizaje Máquina y
  - explotación de vulnerabilidades.

Definiciones

Empresa micro, pequeña o mediana en cuanto a volumen de ingresos, valor del patrimonio y numero de trabajadores. Las MiPyMEs generan el **72%** del empleo y el **52%** del PIB de Mexico.[a]

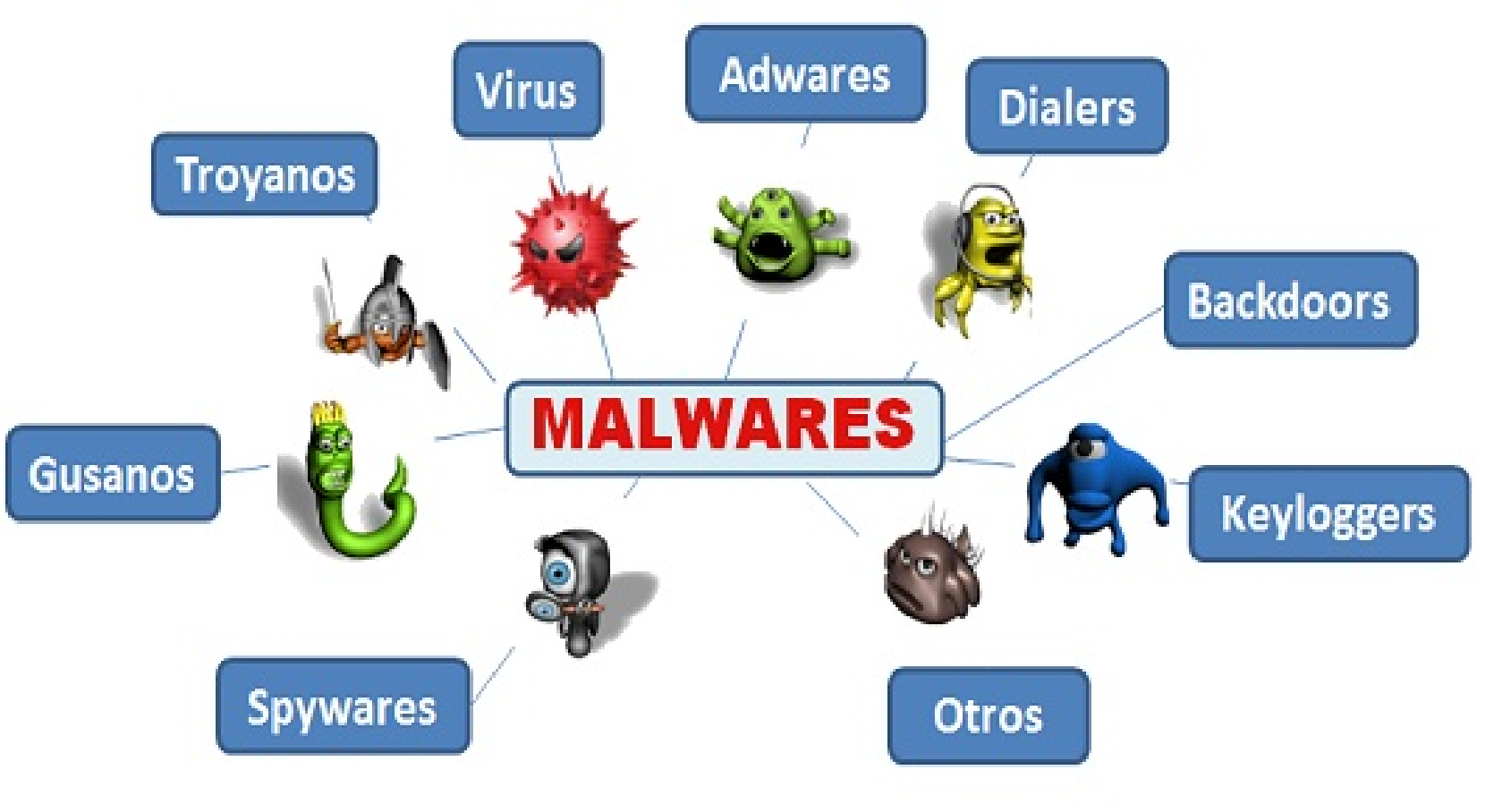
[a] https://www.condusef.gob.mx/Revista/index.php/u
inteligente/educacion-financiera/492-pymes

Definiciones

Del Inglés, malware significa **Software Malicioso**. Este software esta diseñado para dañar los datos y los sistemas o para obtener acceso no autorizado a los equipos y redes corporativos y residenciales.[a]

[a] https://www.forcepoint.com/cyber-edu/malware

Tipos de malware



Objetivos

- Daños
- Secuestro de información o del equipo
- Robo de información
- Robo de dinero
- Acceso ilícito a recursos

Creadores

Actualmente el malware es diseñado y creado por *profesionales*, que buscan beneficios económicos o políticos.

México esta entre los tres paises de latinoamérica de mayour desarrollo de malware (especialmente malware financiero). Brasil y Perú son los otros dos países. [a]

[a] https://expansion.mx/tecnologia/2017/09/16/mexicanos-creadores-de-malware-financiero

PyMES y seguridad

- Falta personal capacitado
- Mi información no le interesa a nadie
- Falta de recursos
- No se considera el riesgo
- Cero planes de respaldo o de respuesta
- Uso de soluciones para hogar
- No mantenimiento a la ciberseguridad
- No firmar acuerdos de confidencialidad

- Empleados descontentos
- Empleados descuidados
- BYOD
- Software Obsoleto [a]

[a] https://cepymenews.es/amenazas-ciberseguridad-pueden-afectar-a-las-pymes-en-2019

Malware: Ataques

- Correo electrónico
- Documentos Office
- Medios removibles (USB, cables USB)
- Dispositivos personales infectados
- Páginas web infectadas
- Botnets
- Software vulnerable (ataques dia cero) expuesto en Internet
  - RDP
  - Nginx

Malware y PyMES

- En 2017 53% de las PyMes consultadas por CISCO reportaron brechas de seguridad.
- PWC también detectó que hasta un 44% de las empresas mexicanas no cuentan con soluciones de ciberseguridad.
- Solo 8% tiene infraestructura de protección

Recomendaciones

Recomendaciones

Desarrollar una estrategia de ciber seguridad

1. Capacitación del personal
2. Servicios de seguridad TI
3. Análisis de riesgos y amenazas
4. Respaldos
5. Plan de continuidad del negocio

1. Contar con especialistas
2. Implementar un Sistema de Gestión de la Seguridad Informática

UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

Hugo F. González Robledo

Académia de Tecnologías de la Información y Telemática

Investigación y asesoría en Seguridad Informática

bitly.com/hugoglez

@hugo_glez

(444) 8126367 ext 223

github.com/hugo-glez/

linkedin.com/in/hugoxglez

hugo.gonzalez@upslp.edu.mx