XXXI SEMANA NACIONAL DE INVESTIGACIÓN Y DOCENCIA EN MATEMÁTICAS

Ciberseguridad: “Troyanos”

Hugo Alberto Eguino Arámbula, Vesna Camile Pivac Alcaraz,
Jose Alberto Leyva Contreras, Jesus Ernesto Pesqueira Vásquez,
Maestra Asesora: María Guadalupe Cota Ortiz.

¿Qué es Ciberseguridad?

La ciberseguridad es el conjunto de procedimientos y herramientas que se implementan para proteger la información que se genera y procesa a través de computadoras, servidores, dispositivos móviles, redes y sistemas electrónicos.

Infección de troyanos

Estos son algunos de los tipos de troyanos son:

- Puertas traseras: Hacen cambios en el sistema de seguridad, lo que permite que otros Malware o Hackers puedan acceder al equipo.
- Spyware: Observar tu comportamiento, tiene acceso a tus cuentas online y facilita detalles de tus tarjetas bancarias.
- Troyanos zombis: Cuando los hackers no están interesados en tus datos, usan tu equipos como un esclavo en una red bajo su control.
- Enviar mensajes SMS: Este es en el caso se los SmartPhones, y la forma en los que lo hacen es enviando costosos mensajes a números con recargos desde tu equipo.

Historia y Origen

Término en honor a la historia del caballo de madera usado para engañar a los defensores de Troya y poder introducir soldados a hurtadillas en la ciudad.

Desde sus orígenes ha sido utilizados como armas de sabotaje por servicios de inteligencia, como la CIA.

El Sabotaje del Gasoducto Siberiano de 1982 fue de los casos más sonados

Actualmente representan más del 80% de los malwares detectados

¿Qué es un Troyano?

Un tipo de malware que a menudo se disfraza de software legítimo. Generalmente se hacen pasar por programas aparentemente inofensivos. Entre los efectos de un virus troyano está:

- Eliminar datos
- Bloquear datos
- Modificar datos
- Copiar datos
- Interrumpir el funcionamiento de computadoras

A diferencia de virus y gusanos, los troyanos no son capaces de autorreplicarse.

Protección y Seguridad

Los troyanos se llaman asi porque necesitan tu permiso para poder ejecutarse en el ordenador, con esto en mente la mejor defensa contra estos es:

- No abrir archivos adjuntos enviados a través de correo electrónico, solo de usuarios confiables.
- No visitar páginas web que sean desconocidas o de dudosa procedencia.
- Realizar las actualizaciones del sistema operativo y del antivirus.
- Usar Firewall para evitar transmisiones maliciosas de una red a otra.
- Instalar un software antitroyano o antivirus.

Conclusiones

Conocer sobre los virus y la forma en la que se comportan es ideal para poder atacarlos y defender nuestro sistema. Tener un buen antivirus como protector es indispensable en estos días, donde la Internet y sitios maliciosos van a la alza.

Referencias

1. Charles J. Brooks, Christopher Grow, Philip Craig, Donald Short. (2018). Cybersecurity Essentials. Indianapolis, Indiana, USA: John Wiley & Sons, Inc.
2, Regan, J., 2019. ¿Qué es un caballo de Troya? ¿Es un malware o un virus?. [online] AVG. Available at: <https://www.avg.com/es/signal/what-is-a-trojan>
3. Norton MX. (2014). ¿Qué es un troyano? Norton https://mx.norton.-com/internetsecurity-malware-what-is-a-trojan.html