Certified Tech Developer

The Ultimate Degree

Práctica Integradora

Objetivo

Vamos a poner en práctica los conocimientos que hemos adquirido hasta el momento. Se crearán 10 grupos, divididos en sus respectivas salas y realizarán la siguiente ejercitación.

Micro desafíos

Deberán leer cada una de las noticias asignadas y responder en un documento (ustedes deben abrirlo) las siguientes consignas:

- ¿Qué tipo de amenaza es?
- ¿Cómo comienza y cómo se propaga esta amenaza?
- ¿Hay más de una amenaza aplicada ?

Una vez resueltas volveremos a la sala principal en la cual el grupo debe compartir sus respuestas a los demás compañeros.

1	https://thehackernews.com/2021/05/new-stealthy-rootkit-infiltrated.html
2	https://thehackernews.com/2021/04/experts-uncover-new-banking-trojan.html
3	https://thehackernews.com/2021/04/alert-theres-new-malware-out-there.html
4	https://thehackernews.com/2019/10/42-adware-apps-with-8-million-downloads.html
5	https://thehackernews.com/2020/03/android-apps-ad-fraud.html
6	https://thehackernews.com/2021/02/first-malware-designed-for-apple-m1.html
7	https://thehackernews.com/2021/04/passwordstate-warns-of-ongoing-phishing.html
8	https://thehackernews.com/2021/04/hackers-threaten-to-leak-stolen-apple.html
9	https://thehackernews.com/2021/04/facebook-busts-palestinian-hackers.html
10	https://thehackernews.com/2021/02/chinese-hackers-using-firefox-extension.html
11	https://thehackernews.com/2021/04/cybercriminals-using-telegram-messenger.html
12	https://thehackernews.com/2021/05/researchers-uncover-iranian-state.html

SEGURIDAD INFORMÁTICA

La seguridad informática, o ciberseguridad, es una disciplina que se encarga de proteger la integridad y la privacidad de los datos y toda la información que se encuentre alojada en un sistema informático. La idea principal es que se pueda evaluar la seguridad de los sistemas de cómputo y redes para, posteriormente, protegerlos de los ataque informáticos que se pueden llevar a cabo a los sistemas.

La seguridad informática va a identificar, eliminar vulnerabilidades y proteger de ataques maliciosos a los equipos de cómputo, servidores, redes informáticas y todo aquel medio informático por el cual se transmita información.

El atacante utiliza un tipo de software maligno denominado malware para que realice todo el proceso de pirateria. Es un término que se utiliza para describir a todos los software maliciosos que tienen como objetivo infiltrarse o dañar un sistema de información sin el consentimiento del usuario. Para que este software malicioso pueda completar sus objetivos es primordial que esté oculto al usuario ya que esto

le permite seguir actuando. Cuando el usuario nota que hay algún tipo de malware, hará lo necesario para eliminarlo. Dentro de este concepto se engloban los virus, los troyanos, etc.

- Virus: componente de software cuyo objetivo es permanecer en un sistema copiandose a sí mismo en varios lugares desde el momento en que se ejecuta en el sistema. Así, cuando intentamos eliminar un archivo o programa infectado, el virus seguirá en la memoria ya que se infectaron otras partes del sistema. El objetivo de estos virus es destruir o inhabilitar archivos o programas que tengamos en los dispositivos, además de afectar el funcionamiento del mismo. La mayoría se adhiere en archivos ejecutables o también en el registro maestro de arranque. No tienen la capacidad por sí mismos de infectar a otros dispositivos, a menos que los pasemos por medio de un hardware como un usb. Por esto último, decimos que son de poca infección, porque se replican a sí mismos sólo dentro del mismo dispositivo.
- Gusano: aparece cuando las computadoras se empiezan a conectar a la red. Este malware, no solo se copia a sí mismo en el sistema sino que ademas, utiliza la red para copiarse a otras máquinas, a través de las vulnerabilidades de la red o agujeros de seguridad. Por ello tiene una mayor capacidad de infección. Esto se debe a la evolución de la tecnología. El objetivo de este, es replicarse a sí mismos, hasta saturar el funcionamiento del sistema.
- Troyanos: no causan daños en sí mismos sino que están basados en el caballo de troya. O sea, una estructura utilizada para cargar cosas ocultas, en este caso virus, gusanos o demás malwares. Generalmente, son esos programas sin licencia que instalamos pensando que no hacen ningún daño porque no somos conscientes de que pueden ser un troyano. Requieren de la ejecución del usuario ya que no pueden replicarse a sí mismos. También puede crear backdoors, que es una puerta trasera para que un dispositivos pueda ser controlado de forma remota por alguien más. Se puede usar como un servidor proxy para ocultar ataques o para introducir spam a nuestro equipo. Estos últimos, son muy parecidos a los adwares, cuyo objetivo es bombardear nuestro dispositivo con publicidad. Estos últimos no son dañinos y por lo general vienen dentro de troyanos.

Existen otros malwares más peligrosos ya que cuentan con un modo de ataque más sutil para robar que los diferencia de los virus, gusanos y adwares.

- Spywares o software espía: este malware no daña los dispositivos pero roba toda la información del sistema. Su objetivo es permanecer oculto para robar todo tipo de datos desde contraseñas, información bancaria, redes sociales, entre otros. También puede acceder por la cámara o micrófono del dispositivo sin que el usuario lo note. Suelen ingresar en troyanos o también pueden ser

instalados como es el caso de keylogger (spyware que registra las pulsaciones del teclado para detectar qué es lo que el usuario escribe).

- Rootkits: conjunto de software. Se diferencian en que los demás malwares atacan el sistema operativo por lo que reinstalando el sistema, el malware desaparece. En cambio, los rootkits van dirigidos al firmware del sistema o los programas de usuario y tienen acceso al dispositivo en modo sistema o kernel. Este acceso le permite a los rootkits realizar modificaciones a los procesos internos del SO, a los archivos del sistema como los registros e incluso a las cuentas de usuario. Además, los rootkits, logran esconderse de los softwares antimalwares o antivirus.
- Botnets: mezcla entre bot y net. Es una red de robots que es puesto por un atacante en una red de computadoras para ser controladas todas al mismo tiempo. Principalmente se usa con el objetivo de cometer crímenes digitales o crimeware, como robo de identidad o de información bancaria, chantaje, entre otros. Los troyanos suelen ser los principales causantes de la propagación de estos.
- Ransomware: Todos los anteriores se mantienen ocultos al usuario, a diferencia de este. Son software de secuestro que suelen ser utilizados contra empresas para secuestrar la información de sus servicios y productos y luego pedir dinero a cambio del rescate. El ciberatacante hace visible el secuestro a través de la solicitud de una contraseña para acceder al sistema. Se pueden encontrar en archivos adjuntos de correos electrónicos no deseados, o al hacer click en vínculos que aseguran venir de bancos o instituciones legales. También se encuentran en redes para compartir archivos como las P2P.

Es importante tener cuidado con las descargas que realizamos, el uso de aplicaciones no autorizadas, evitar las páginas peligrosas y usar un software antimalware.