Seguridad Informática

Tema 5

Ejercicio 2

PABLO CORNAGO GÓMEZ
11-1-2022

Ejercicio 2

Enunciado

Realiza un ejercicio de investigación sobre noticias de los últimos incidentes que se hayan producido en el mundo, relacionados con los diferentes términos que hemos visto a lo largo de este tema en cuanto a malware e ingeniería social. Procura que sea de la mayor parte de ellos.

Construye una tabla donde, por ejemplo, se detalle el incidente, dónde se originó, cuántos equipos se vieron afectados, consecuencias económicas, etc. Cuanto más completo, mejor.

Resolución

Para conocer noticias relacionadas con la ciberdelincuencia, debemos acudir a medios de comunicación específicos de informática o directamente a los medios de comunicación convencionales, ya que estos suelen disponer de un apartado destinado a este ámbito.

Ejemplos de medios de comunicación específicos son: **Xataka**, **Computer Hoy**, **El Chapuzas Informatico**, etc.

Algunos de los medios convencionales, que tengan un apartado específico a la informática son: **El País**, **ABC**, **El Español**, entre otros.

Una vez obtenidas las fuentes de información, basta con hacer el uso de la búsqueda rápida, poniendo palabras clave como: malware, estafa informática, phishing, etc. Otro método es el de mirar todas las noticias, este es más lento, pero más efectivo ya que de la otra forma te limitas a esos términos y puede que no encuentres una noticia por no caer en ese momento de ese término. A la hora de conocer el alcance y las consecuencias económicas, es bastante complicado ya que las empresas afectadas no suelen dar estos datos o los tratan de mitigar a su favor.

Dicho esto, las noticias que yo he encontrado son:

MALWARE

RedLine Stealer (30/12/2021) - Troyano (Stealer)

Como bien indica su nombre, esta infección de malware es del tipo "stealer". El objetivo de este tipo de infecciones es el de acceder y robar información privada para enviársela al atacante. En este caso, la información objetivo era la almacenada en los navegadores web de las víctimas, en concreto la relacionada con el gestor de contraseñas de los navegadores.

El malware **RedLine Stealer** se dedica a robar las credenciales (usuario o correo y contraseña) de los gestores de contraseñas de navegadores basados en Chromium (Chrome, Edge y Opera).

Ataque a la UOC (02/01/2022) - Troyano (Ransomware)

Se trata de un ataque "ransomware" a la Universitat Oberta de Cataluña. Este tipo de ataque es una infección de malware a los servidores de dicha Universidad, que tiene como objetivo bloquear y secuestrar el acceso y la información que estos tengan. El fin de esta amenaza es el de pedir un rescate a cambio de la clave de desencriptación para los archivos alojados en el equipo infectado.

En este caso, el problema no duró más de 24 horas ya que fue solventado rápidamente, salvo un 5% que aún sigue afectado en el momento de la noticia.

Varios alumnos de la Universidad se han visto afectados de forma indirecta debido a que este ataque ha llegado en un momento crítico, coincidiendo con las fechas de exámenes y entregas de trabajos.

Botnet Meris (10/09/2021) - Botnets

La botnet Meris ha conseguido el record del mayor ataque de DDoS, contando con 250.000 dispositivo y logrando un máximo de 21,8 millones de solicitudes por segundo.

Pegasus (19-07-2021) - Spyware

Este malware obtiene el control de los dispositivos móviles, es capaz de extraer los mensajes, llamadas, fotos, activar la cámara o el micrófono e incluso leer el contenido de correos o chats cifrados (Whatsapp, telegram, etc.).

Pegasus lleva activo desde 2016 y le han llegado a relacionar con acontecimientos como el asesinato de Jamal Khashoggi o el ataque a Whatsapp de 2019.

Se conoce gracias a una investigación reciente que existe un listado con más de 50.000 objetivos potenciales, entre los que figuran periodistas, políticos, activistas y políticos.

Adware en Adobe Flash Player (24-02-2021) - Adware

En diciembre de 2020, Adobe cerró Flash Player pero en China existe una versión que viene supuestamente infectada con adware. Tras la instalación, comienzan a aparecer ventanas emergentes en el navegador, mostrando anuncios.

INGENIERÍA SOCIAL

SMS de MRW (28/12/2021) - Smishing

La empresa de envíos española ha estado sufriendo una suplantación de identidad mediante SMS, donde los ciberdelincuentes incluían el nombre, apellidos y el localizador de envío reales para hacer más creíbles dichos mensajes.

Usaban una página con un diseño muy parecido o idéntico al original de MRW, pero con un dominio que no era el oficial. Con esta página fraudulenta se trataba de cobrar 0,99€ para unos supuestos gastos de envío.

Varias empresas de paquetería han sufrido ataques similares, pero este caso destaca por una previa filtración de datos con la que aprovechan para usar datos reales de clientes y envíos.

Bibliografía

MALWARE

RedLine Stealer

https://www.xataka.com/seguridad/usar-gestor-contrasenas-nuestro-navegador-parecia-excelente-idea-entonces-llego-malware-redline-stealer

Ataque a la UOC

https://elpais.com/espana/catalunya/2022-01-02/la-uoc-sufre-un-ciberataque-que-bloquea-su-campus-virtual.html

https://www.xataka.com/seguridad/uoc-sufre-ransomware-que-afecta-a-su-campus-virtual-asi-ultimo-ciberataque-que-golpea-a-universidad-espanola

Botnet Meris

https://www.xataka.com/seguridad/asi-meris-nueva-botnet-que-ha-conseguido-batir-dos-veces-record-ataque-ddos-grande-historia

Pegasus

https://www.xataka.com/seguridad/filtrada-magnitud-spyware-israeli-pegasus-miles-periodistas-opositores-espiados-gobiernos-todo-mundo-incluido-espana

https://www.elespanol.com/omicrono/software/20211123/apple-nso-creadora-pegasus-no-perjudique-usuarios/629437997_0.html

Adware Flash Player

https://www.xataka.com/seguridad/unico-adobe-flash-player-que-se-sigue-distribuyendo-esta-china-investigadores-seguridad-dicen-que-contiene-adware

INGENIERÍA SOCIAL

SMS de MRW

https://www.xataka.com/seguridad/falso-sms-mrw-que-puede-enganar-a-se-aprovechan-datos-reales-obtenidos-brecha-seguridad