Certified Tech Developer
The Ultimate Degree

Práctica integradora

Equipo 7: Patricia Díaz, Joselin Listur, Leonardo Franco, Leandro Escobal.

Objetivo

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

Actividad

Deberán leer cada una de las noticias asignadas y responder en un documento de Google, las siguientes consignas:

- ¿Qué tipo de amenaza es?

El tipo de amenaza es un Ransomware. El cual, es un malware que tiene como objetivo secuestrar la información y exigir el pago de un rescate a la víctima que posee el dispositivo comprometido. Es decir, es una forma de extorsión que promete a cambio recuperar los datos y evitar otros daños colaterales.

- ¿Cómo comienza y cómo se propaga esta amenaza?

Esta amenaza comienza y se propaga mediante correos de phishing con archivos adjuntos o enlaces, que intentan engañar a las personas usuarias utilizando ingeniería social. También, puede ser a través de ataques a conexiones remotas como el RDP o mediante un exploit.

- ¿Hay más de una amenaza aplicada?

Si aparte del ransomware de cifrado o criptoransomware, que utiliza la criptografía para cifrar los archivos del equipo comprometido y así impedir a la persona usuaria el acceso a ellos. También, existe el ransomware de bloqueo de pantalla o lockscreen que tiene como fin impedir la utilización y el acceso al equipo hasta que se realice el pago del rescate.

- ¿Qué solución o medida recomendarían?

Las soluciones dependen de las medidas de prevención que se hayan tenido antes del incidente de seguridad. Si en caso de verse como una persona comprometida ante esta amenaza, se debería analizar la situación y determinar por qué ocurrió dicho incidente de seguridad para evitar futuros ataques. Además, si se posee un backup actualizado de la información se puede realizar una restauración de la misma. También, se puede analizar dicho ransomware establecido en el equipo para identificar qué variante específica ha ingresado al sistema.

Por otro lado, es prácticamente irreversible la situación en caso de no poseer un backup actualizado y queda a decisión de la víctima la realización del pago como

rescate. Lo cual está desaconsejado debido a que no asegura la recuperación de la información.

Como medida de recomendación para combatir un ransomware se sugiere tener prevención ante incidentes de seguridad.

Webgrafía

5 cosas que debes saber sobre la Ingeniería Social. (2016, January 6). WeLiveSecurity. Retrieved July 8, 2022, from https://www.welivesecurity.com/la-es/2016/01/06/5-cosas-sobre-ingenieria-social/

Harán, J. M. (2021, July 5). *Ataque masivo del ransomware Revil comprometió más de 1000 compañías en mundo*. WeLiveSecurity. Retrieved July 8, 2022, from https://www.welivesecurity.com/la-es/2021/07/05/ataque-masivo-ransomware-revil-comprometio-mas-1000-companias-mundo/

Ransomware: qué es y cómo funciona. (2021, May 21). WeLiveSecurity. Retrieved July 8, 2022, from https://www.welivesecurity.com/la-es/2021/05/21/que-es-ransomware/

¿Sabes qué es un exploit y cómo funciona? (2014, October 9). WeLiveSecurity. Retrieved July 8, 2022, from

https://www.welivesecurity.com/la-es/2014/10/09/exploits-que-son-como-funcionan/

Grupo / Mesa	Link
1	https://revistabyte.es/ciberseguridad/ryuk-ministerio-de-trabajo/
2	https://www.welivesecurity.com/la-es/2021/06/10/backdoordiplomacy-actualizando-quarian-turian-backdoor-utilizado-contra-organizaciones-diplomaticas/
3	https://www.welivesecurity.com/la-es/2021/04/08/vyveva-nuevo-backdoor-grupo-apt-lazarus/
4	https://www.welivesecurity.com/la-es/2021/02/02/kobalos-amenaza-linux-afecta-infraestructuras-informaticas-alto-rendimiento/
5	https://www.welivesecurity.com/la-es/2019/10/22/navegador-tor-troyanizado-robar-bitcoins-darknet/
6	https://www.welivesecurity.com/la-es/2019/08/23/ataque-departamentos-financieros-balcanes-utiliza-backdoor-rat/
7	https://www.welivesecurity.com/la-es/2021/07/05/ataque-masivo-ransomware-revil-comprometio-mas-1000-companias-mundo/
8	https://www.welivesecurity.com/la-es/2021/05/11/ataque-ransomware-compania-oleoducto-colonia-pipeline-afecta-suministro-combustible-estados-unidos/
9	https://www.welivesecurity.com/la-es/2020/08/17/phishing-netflix-intenta-hacer-creer-cuenta-suspendida/
10	https://www.welivesecurity.com/la-es/2020/04/29/programa-quedate-casa-engano-busca-robar-informacion-usuarios/
11	https://www.welivesecurity.com/la-es/2020/07/27/club-premier-league-cerca-perder-millon-libras-estafa/
12	https://www.welivesecurity.com/la-es/2021/03/25/fraudes-traves-pa

	ypal-que-deben-saber-quienes-venden-productos/