Certified Tech Developer
The Ultimate Degree

Práctica integradora

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 Presentations para todas las mesas, las siguientes consignas:

- ¿Qué tipo de amenaza es?

  Es un troyano de puerta trasera (tipo backdoor), permite tener un control total del equipo de forma remota.

- ¿Cómo comienza y cómo se propaga esta amenaza?

  Comienza con la instalación del dropper, Vyveva usa la biblioteca Tor, que se basa en el código fuente oficial de Tor, para comunicarse con un servidor de C&C seleccionado al azar de la configuración. Se pone en contacto con el C&C en intervalos de tres minutos, enviando

información sobre la computadora de la víctima y sus unidades antes de recibir comandos, incluso si el

- ¿Hay más de una amenaza aplicada?

  Se lograron encontrar tres de los múltiples componentes que componen Vyveva: su instalador, loader y backdoor

- ¿Qué solución o medida recomendarían?

La eliminación manual de un backdoor no es fácil y, de hecho, lo mejor es recurrir a una herramienta para su eliminación automática; los antivirus cuentan con esta opción, de manera que cuando encuentran un virus lo marcan para su posterior eliminación.

Como medidas se deberían tener los equipos y antivirus actualizados, revisar el sistema periódicamente y tener activada la protección de forma permanente.

Una vez resueltas, volveremos a la sala principal en la cual el grupo debe compartir sus respuestas a los demás compañeros y compañeras, exponiendo la problemática y el análisis que realizaron.

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