Certified Tech Developer
The Ultimate Degree

Práctica integradora - Equipo 1

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?**

  un malware, en esencia un ransomware, pero éste es especial ya que está compuesto por tres tipos que trabajan mancomunadamente para ocultarse, robar la información y finalmente encriptarla de manera que no tengan más acceso a ésta y así tienen que pagar para recuperarlos.

- **¿Cómo comienza y cómo se propaga esta amenaza?**

Todo inicia a través de un ataque de phishing basado en Emotec, un troyano que cambia su código cada poco tiempo a fin de no ser detectado por las

soluciones de seguridad y que tiene la capacidad de interceptar, registrar, y guardar todo el tráfico de red. Después un botnet llamado Trickbot roba las credenciales de inicio de sesión. Y finalmente el ransomware Ryuk encripta la información y deja sin acceso al usuario.

- ¿Hay más de una amenaza aplicada?

  Si, hay un **troyano**, **botnet** y **ransomware**.

- **¿Qué solución o medida recomendarían?**

  - Se debería aumentar el **presupuesto en ciberseguridad** (no es un problema de voluntad de los CISOs sino de presupuesto y del **tiempo de reacción contra las amenazas**).
  - **Hay que adaptarse a un entorno cada vez más cambiante** y que tiene nuevas técnicas de ataque cada menos tiempo". Ya que las defensas estáticas no son suficientes.
  - Implementación de **herramientas más avanzadas**.

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/