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.

Link de VT (por si lo quieren seguir viendo): https://www.youtube.com/watch?v=whq3zTsbWrc&ab_channel=tmtcomunica

Muy recomendable su Libro "Hackearán tu mente", explica también como fue el "I Love You".

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?

  Rtta: Son dos amenazas, backdoor y un troyano de acceso remoto (RAT) que nombramos, respectivamente, BalkanDoor y BalkanRAT

- ¿Cómo comienza y cómo se propaga esta amenaza?

  Rtta: Utiliza correos electrónicos maliciosos como mecanismo de distribución, termina teniendo ambas herramientas implementadas en su computadora, cada una de ellas capaz de controlar totalmente la máquina afectada.

  BalkanDoor se ejecuta como un servicio de Windows, lo que le permite desbloquear la pantalla de inicio de sesión de Windows de forma remota y sin la contraseña o iniciar un proceso con los privilegios más altos posibles. En el caso de BalkanRAT utiliza indebidamente un software de escritorio remoto (RDS) legítimo y utiliza herramientas adicionales y scripts para ocultar a la víctima su presencia, como ocultar la ventana, el icono de la barra de tareas, el proceso, etc.

- ¿Hay más de una amenaza aplicada?

  Si, las amenazas que encontramos son:

- ❖ BalkanRAT permite al atacante controlar remotamente la computadora comprometida a través de una interfaz gráfica, es decir, manualmente;
- ❖ BalkanDoor permite controlar de forma remota la computadora comprometida a través de una línea de comando.

- ¿Qué solución o medida recomendarían?

  Para mantenerse a salvo, los usuarios que se desempeñen en áreas de negocios, así como sus superiores, deben seguir las reglas básicas de ciberseguridad: tener cuidado con los correos electrónicos y examinar tanto los archivos adjuntos como los enlaces que puedan venir en ellos; mantener actualizado sus equipos y utilizar una solución de seguridad confiable.

  Capacitación al personal sobre aspectos de ingeniería social, ya que esta usa métodos psicológicos para ingresar el virus.

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/