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:

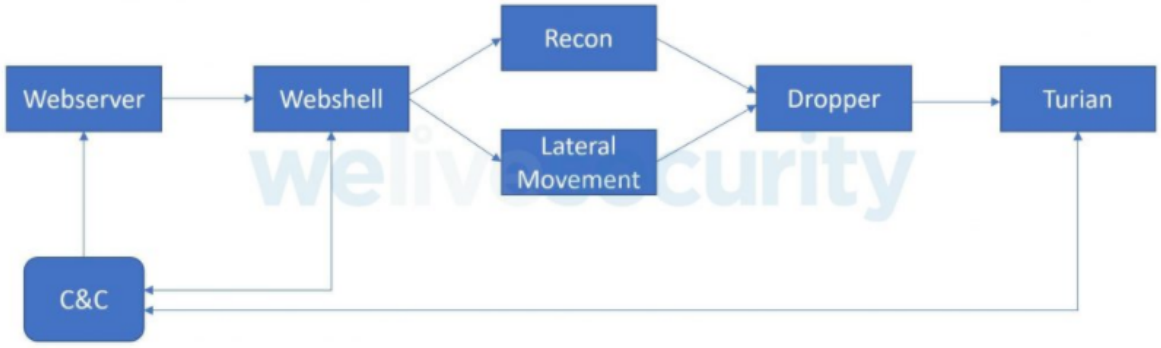
- ¿Qué tipo de amenaza es? Amenaza backdoor:

BackdoorDiplomacy es un grupo que apunta principalmente a organizaciones diplomáticas en Oriente Medio y África y, con menor frecuencia, a empresas de telecomunicaciones. Su metodología de ataque inicial consiste en explotar aplicaciones vulnerables expuestas a Internet en servidores web, con el fin de droppear y ejecutar un webshell. Después del compromiso, a través del webshell, BackdoorDiplomacy utiliza software de código abierto para el reconocimiento y la recopilación de información, y hace uso de la técnica DLL

search order hijacking para instalar su backdoor: Turian. Finalmente, BackdoorDiplomacy emplea de manera separada un ejecutable para detectar medios extraíbles, probablemente unidades flash USB, y copiar su contenido en la papelera de reciclaje de la unidad principal.

- ¿Cómo comienza y cómo se propaga esta amenaza?

El acceso interactivo se logra de dos maneras: (1) a través de un backdoor personalizado que llamamos Turian que deriva del backdoor Quarian; y (2) en menos casos, cuando se requiere un acceso más directo e interactivo, se implementan ciertas herramientas de acceso remoto de código abierto.



Esta cadena explica la forma en la que ataca la amenaza.

Otras formas de ataque:

Un subconjunto de víctimas fue atacado con ejecutables de recopilación de datos que fueron diseñados para buscar medios extraíbles (probablemente

unidades flash USB). El implante busca de forma rutinaria dichos medios extraíbles (el valor de retorno de GetDriveType es 2).

- ¿Hay más de una amenaza aplicada?

BackdoorDiplomacy comparte tácticas, técnicas y procedimientos con otros actores de amenazas asiáticos. **Turian** probablemente representa una próxima etapa de evolución de **Quarian**

- ¿Qué solución o medida recomendarían?

Recomendamos manejar la información valiosa en servidores aislados del internet, y acceder a ellos mediante una intranet.

Lo mejor para protegernos de un backdoor es contar con un buen antivirus que ofrezca protección en tiempo real, que además se mantenga actualizado con regularidad para poder detectar nuevas amenazas y, por supuesto, tener activada la protección de manera permanente.

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. Este proceso viene explicado paso a paso por el propio antivirus que estemos usando, por lo que generalmente es sencillo de hacer. También podemos recurrir a otros programas de limpieza, como CCleaner o Malwarebytes Anty-malware, para usarlos tras realizar el análisis con el antivirus.

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/