LAS 10 TÉCNICAS MÁS UTILIZADAS POR LOS CIBERCRIMINALES

BASQUE CYBERSECURITY CENTRE

... a la hora de realizar un ataque contra una empresa

01 Spear phishing adjunto

Envío de emails durante la fase inicial de un ataque con un **archivo adjunto malicioso** para obtener información confidencial o comprometer el sistema.

02 Archivos maliciosos

Busca que el usuario abra un archivo malicioso en el dispositivo objetivo, siendo las extensiones más habituales **.doc, .pdf, .xls, .rtf y .exe.**

03 Ficheros ofuscados

Busca evadir los sistemas de protección como los antivirus para cifrar los ficheros maliciosos y **que el código no sea fácilmente analizable**, sin poder determinar si es malicioso hasta que se ejecute.

04 Powershell

Incluido por defecto en el **sistema operativo Windows**, el atacante puede usarla para realizar una serie de acciones como la búsqueda de información, la ejecución de código o descargar y ejecutar archivos desde Internet en el disco y en la memoria.

05 Línea de comandos de Windows

Denominado **cmd.exe**, suele usarse por administradores de sistemas, desarrolladores o usuarios avanzados, y es también utilizada habitualmente en los ataques.

06 Transferencia de herramientas de acceso

El atacante transfiere herramientas u otros archivos a través del canal de comando y control o mediante **protocolos como FTP**.

07 Entradas de arranque del registro / Carpeta de inicio

Mantiene la persistencia en el sistema **agregando un programa a una carpeta de inicio** o haciendo referencia a éste mediante una clave de ejecución del Registro.

08 Protocolos Web

Los cibercriminales se comunican con los sistemas afectados mediante el uso de **protocolos de capa asociados al tráfico web** para evitar ser detectados o filtrados al mezclarse con el tráfico web existente.

09 Borrado de archivos

La técnica consiste en eliminar los ficheros que evidencian el ataque, **durante la misma intrusión o posteriormente**, con el objetivo de **dejar el menor rastro posible**.

10 Tareas programadas

El atacante hace uso del Programador de Tareas de Windows para colocar una **tarea con código malicioso que se ejecute al iniciarse el sistema** para mantener persistencia o que sea de tipo recurrente.

En caso de incidente de ciberseguridad...

se debe notificar inmediatamente al responsable de la organización. Puedes ponerte en contacto con nosotros llamando al 900 104 891 o enviando un email a incidencias@bcsc.eus.

GRUPO spri

EUSKO JAURLARITZA
GOBIERNO VASCO
EKONOMARIEN GARAPEN JASANGARRITASUN ETA INGURUMEN SAILA
DEPARTAMENTO DE DESARROLLO ECONÓMICO, SOSTENIBILIAD Y MEDIO AMBIENTE