FASES DE UN ATAQUE INFORMÁTICO

La clave para detectar, detener, interrumpir y recuperarse ante un ciberataque radica en comprender cuál es su ciclo de vida y así desarrollar e implementar todas las operaciones necesarias que garanticen el mayor grado de seguridad y protección. A este ciclo de vida se le conoce como **Cyber Kill Chain**.

Reconocimiento

Se trata de la fase en la que el ciberdelincuente recopila información sobre su objetivo.

Preparación

Se prepara el ataque de forma específica sobre un objetivo. Por ejemplo, un atacante podría crear un documento PDF o de Microsoft Office e incluirlo en un correo electrónico.

Distribución

En esta etapa se produce la transmisión del ataque, por ejemplo, mediante la apertura del documento infectado que había sido enviado por correo electrónico

Explotación

Esta fase implica la ***detonación*** del ataque, comprometiendo al equipo y a la red que pertenezca. Esto se suele producir explotando una vulnerabilidad ya conocida.

Instalación

Fase en la que el atacante instala el malware en la víctima. También puede darse la circunstancia de que no se requiera instalación, como en el robo de credenciales

Comando y control

Atacante cuenta con el control del sistema de la víctima, en el que podrá realizar o desde el que lanzar sus acciones maliciosas dirigidas desde un servidor central conocido como C&C (Command and Control), pudiendo sustraer credenciales, tomar capturas de pantalla, llevarse documentación confidencial, instalar otros programas, conocer cómo es la red del usuario, etc.

Acciones sobre los objetivos

Esta es la fase final en la que el atacante se hace con los datos e intenta expandir su acción maliciosa hacia más objetivos. Esto explica por qué la kill chain no es lineal sino cíclica, ya que se volverían a ejecutar todas y cada una de sus fases de cara a infectar a más víctimas.

CSIRT AIG
CSIRT
EQUIPO DE RESPUESTA A INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

E-Mail: info@cert.pa
Phone: +507 520-2378
Web: https://cert.pa
Twitter: @CSIRTPanama