UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS
Acreditación Institucional de Alta Calidad

BOLETÍN INFORMATIVO

Gestión de los Sistemas de Información y las Telecomunicaciones

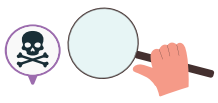
Volumen 2, número 12, marzo de 2024

CADENA DE INTRUSIÓN CIBERNÉTICA *(KILL CHAIN)*

Es el procedimiento que siguen los ciberdelincuentes para completar un ataque cibernético con éxito.

Los siete pasos de la cadena de intrusión cibernética:

01 Reconocimiento



El atacante realiza la recopilación de información de sistemas, motores de búsqueda, puertas de acceso a aplicaciones, credenciales y todos los datos para preparar un ataque contra usted o su entidad.

02 Preparación

El ciberdelincuente decide qué vector de ataque emplear según la información que ha recolectado.

Entre los vectores de ataque más comunes están *phishing*, ingeniería social, virus troyanos, ataques de denegación de servicios, entre muchos más.

03 Distribución

Cuando el ciberdelincuente logra ingresar a su sistema o al de su entidad, tiene la posibilidad de distribuir los diferentes programas para, a futuro, accionar el ataque.

El ataque puede ser un *malware, ransomware, spyware*, etc.

04 Explotación

El ciberdelincuente podrá empezar con la explotación del sistema, programando el ataque y ocultándolo para que no sea detectado.

05 Instalación

El atacante procede a instalar una puerta trasera y los programas necesarios para efectuar el ataque, así monitorea la actividad constante del usuario sin temor de ser detectado.

06 Comando y control

Una vez los programas y puertas traseras están instalados, el ciberdelincuente tomará el control de los sistemas y ejecutará los ataques que ha venido planeando contra usted o su entidad.

07 Empezar el ataque

El atacante logra emprender acciones sobre su objetivo, cifrando sus datos o extorsionándolo para pedir un rescate o algún tipo de beneficio.

Si el ataque es hacia una entidad puede hacer que todos los sistemas posibles salgan de funcionamiento.

Se debe tener en cuenta que si el ciberdelincuente logra entrar, realizará tareas de espionaje para obtener cada vez más información.

- Consulte el documento *¿Qué es Cyber Security Kill Chain?*, de la empresa Netskope®.
- Para mayor información sobre términos de seguridad informática, consulte el *Glosario de términos de ciberseguridad*, del Incide y el *Glosario del Portal de Colombia TIC.*

No se pierda nuestros próximos boletines informativos, se publicarán en la página web.

VIGILADO MINEDUCACIÓN - DISEÑO: RED DE DATOS UDNET - CORRECCIÓN DE ESTILO: UNIDAD DE PUBLICACIONES