Dirección Cibernética Naval

MINISTERIO DE DEFENSA / ARMADA NACIONAL / JEFATURA DE INTELIGENCIA NAVAL

BOLETÍN CIBERNÉTICO No.008

Bogotá / julio 2020

ARMADA DE COLOMBIA

FASES DE UN ATAQUE CIBERNÉTICO

La comprensión de los riegos cibernéticos, las técnicas y tácticas utilizadas por los adversarios permiten detectar y responder de una forma mas adecuada a los posibles ataques o intrusiones. Además, busca facilitar el proceso de identificación y aprendizaje de cada fase del ataque, lo que le permite determinar si las medidas de protección son las adecuadas en función de la etapa del ataque.

RECONOCIMIENTO

- Identificación y selección del objetivo
- Investigación y recolección de información
- Desarrollo y adquisición de ciberarmas
- Pruebas de evasión de mecanismos de seguridad

PREPARACIÓN

- Estudio de técnicas y tácticas.
- Creación de plataformas falsas.
- Pruebas de persistencia.
- Implementación de herramientas.
- Pruebas de elementos maliciosos.

DISTRIBUCIÓN

- Ejecución del planeamiento.
- Medio de engaño (correo, pagina web, etc.).
- Transmisión del ataque cibernético.

EXPLOTACIÓN

- Comprobación de acceso.
- Acceso remoto a los sistemas
- Ejecución de malware.
- Explotación de Vulnerabilidades, mediante Exploit.

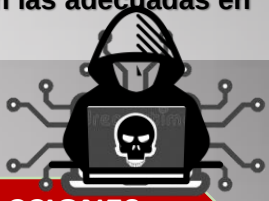
INSTALACIÓN

- Obtención de acceso a la red de la victima.
- Verificar persistencia de acceso.
- Deshabilitar reglas del Firewall.

C&C

Comando y control

- Control total del sistema de la victima
- Acciones desde un servidor central
- Robo de información, instalación de software



ACCIONES SOBRE EL OBJETIVO

- Búsqueda y filtrado de información.
- Selección y recolección de información.
- Eliminación de rastros y evidencia.

Fuente

- https://n9.cl/fasesattack
- https://n9.cl/7attackblog