DragonJAR®

SEGURIDAD INFORMÁTICA

Top 10 Técnicas de Bypass de EDR Usadas por Bandas de Ransomware

www.dragonjar.org

1 Deshabilitar EDR o Antivirus

Deshabilitar EDR y antivirus (T1562) es usado por delincuentes para evadir la detección y mantener acceso en un sistema, usando herramientas o scripts.

Usado por los siguientes grupos:

- *LockBit 3.0*
- *Black Basta*
- *Play, Akira*
- *AvosLocker*
- *Snatch*
- *BianLian*
- *RansomHub*
- *Rhysida*
- *Phobos*

Top 10 Técnicas de Bypass de EDR Usadas por Bandas de Ransomware

2

Uso de PowerShell Living off the Land

Living off the Land (LotL) con PowerShell (T1059.001) permite usar herramientas del sistema para ejecutar comandos maliciosos sin levantar sospechas.

Usado por los siguientes grupos:

- *Black Basta*
- *BianLian*
- *Akira*
- *Phobos*
- *LockBit 3.0*

Top 10 Técnicas de Bypass de EDR Usadas por Bandas de Ransomware

3

Eliminación de indicadores

Eliminar los indicadores de compromiso y los archivos de registro (T1070) es una táctica utilizada para borrar evidencias de actividad maliciosa, complicando la detección y el análisis posterior al ataque.

Usado por los siguientes grupos:

- *RansomHub*
- *Play*
- *Snatch*

4 Uso de Controladores Vulnerables (BYOVD)

Bring Your Own Vulnerable Driver (BYOVD) (T1068) explota controladores legítimos pero vulnerables, permitiendo pasar desapercibido en las defensas.

Usado por los siguientes grupos:

- *RansomHub*
- *AvosLocker*
- *ALPHV Black*

Top 10 Técnicas de Bypass de EDR Usadas por Bandas de Ransomware

5

Modificación de Políticas de Grupo

Modificar políticas de grupo (T1484.001) permite desactivar antivirus y otras defensas en un entorno de dominio, facilitando el acceso sin alertas.

Usado por los siguientes grupos:

- *Blacksuit (Royal)*
- *LockBit 3.0*

Top 10 Técnicas de Bypass de EDR Usadas por Bandas de Ransomware

6 Acceso Remoto con Credenciales Robadas

Usar credenciales válidas robadas (T1078) para SSH, RDP o VPN permite el movimiento lateral sin activar las defensas, dificultando la detección.

Usado por los siguientes grupos:

- *Rhysida*
- *Blacksuit (Royal)*

Top 10 Técnicas de Bypass de EDR Usadas por Bandas de Ransomware

7

Modificación del Registro de Windows

Modificar el registro de Windows (T1112) permite desactivar funciones críticas de antivirus y protección de manipulación, manteniendo la persistencia en el sistema.

Usado por los siguientes grupos:

- *BianLian*
- *Snatch*

Top 10 Técnicas de Bypass de EDR Usadas por Bandas de Ransomware

8

Modificación de Firewall

Modificar configuraciones de firewall (T1562.004) mediante comandos permite eludir restricciones de red y expandir el acceso.

Usado por los siguientes grupos:

- *Phobos*

9

Reinicio en Modo Seguro

Reiniciar el sistema en Modo Seguro (Safe Mode) (T1562.009) permite a los atacantes desactivar muchas herramientas de seguridad que no operan en este entorno.

Usado por los siguientes grupos:

- *Snatch*

Top 10 Técnicas de Bypass de EDR Usadas por Bandas de Ransomware

10 Escaneo y Detección de Software de Seguridad

Escanear la red y detectar soluciones de seguridad (T1016 y T1518.001) permite a los atacantes identificar software de seguridad activo y desactivarlo de forma efectiva.

Usado por los siguientes grupos:

- *Play*

Top 10 Técnicas de Bypass de EDR Usadas por Bandas de Ransomware

DragonJAR®

SEGURIDAD INFORMÁTICA

¿Quieres que expertos evalúen la seguridad de tus soluciones de seguridad?

Hablemos...

Valentina Nieto F.

Directora Comercial

comercial@dragonjar.org

(+57) 304 384 9657