10 DE ABRIL DE 2024

PRÁCTICA 4.4 MITRE ATT&CK

INCIDENTES DE CIBERSEGURIDAD

ERIC SERRANO MARÍN
I.E.S MARTINEZ MONTAÑES
CETI

Contenido

ENUNCIADO

Estudia la amenaza asignada a través de la matriz MITRE ATT&CK proponiendo un entorno (características de los sistemas, software utilizado...) para presentar, las tácticas y técnicas que podrían afectar a los sistemas, así como las acciones de detección y mitigación que podrían llevarse a cabo. Adapta tu entorno a la amenaza, por ejemplo: El sistema amenazado por este malware tiene un SO Windows y usa Office 365.

En mi caso me ha tocado JPIN.

Entrega un informe con tu estudio orientado a tu propuesta de entorno, eligiendo una táctica que le pudiera afectar, explicando cómo le afecta y presentando las posibilidades de mitigación y detección que propone MITRE para esa táctica.

MITIGACIÓN Y DETECCIÓN DE UNA TÁCTICA.

Pequeño resumen de BITS Jobs.

Los atacantes pueden usar trabajos BITS para ejecutar código de manera persistente. BITS es un servicio de Windows para transferir archivos en segundo plano, comúnmente utilizado por actualizadores y aplicaciones que prefieren operar sin interrumpir otras aplicaciones en red. Las tareas de transferencia de archivos se organizan en trabajos BITS.

¿Cómo puede afectar al entorno esta táctica?

El abuso de BITS como táctica por parte de una amenaza puede tener impactos significativos en la seguridad y la integridad del entorno, incluida la ejecución de código malicioso persistente, la transferencia de archivos maliciosos y la ex filtración de datos sensibles.

Mitigación.

1. **Filtrar tráfico de Red** y modificar las reglas del firewall de red y host, así como otros controles de red, para permitir únicamente el tráfico BITS legítimo.
2. **Configuración del Sistema Operativo** habría que considerar reducir el tiempo de vida predeterminado de los trabajos BITS en la Política de Grupo o editando los valores del Registro obInactivityTimeout y MaxDownloadTime en HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\BITS.
3. **Gestión de Cuentas de Usuario** limitar el acceso a la interfaz BITS a usuarios o grupos específicos.

Detección

1. **Ejecución de comandos:** Monitorizar los comandos ejecutados y los argumentos desde la herramienta BITSAdmin (especialmente las opciones de comando 'Transfer', 'Create', 'AddFile', 'SetNotifyFlags', 'SetNotifyCmdLine', 'SetMinRetryDelay', 'SetCustomHeaders' y 'Resume'). Revisar los registros de administrador, los registros de PowerShell y el registro de eventos de Windows para la actividad de BITS. También hay que considerar investigar información más detallada sobre los trabajos analizando la base de datos de trabajos BITS.
2. **Creación de Conexiones de Red:** Monitorizar la actividad de red recién creada generada por BITS. Los trabajos BITS utilizan HTTP(S) y SMB para conexiones remotas y están vinculados al usuario que los crea, funcionando solo cuando ese usuario está conectado (esta regla se aplica incluso si un usuario adjunta el trabajo a una cuenta de servicio).
3. **Proceso de Creación:** Para monitorear la creación de procesos asociados con tareas BITS recién construidas se sugiere utilizar la herramienta BITSAdmin con el comando bitsadmin/list/allusers/verbose para enumerar estas tareas. Hay dos tipos de análisis.
    - **Persistencia de Trabajos BITS:** Se enfoca en buscar la creación de procesos de bitsadmin.exe que programan un trabajo BITS para

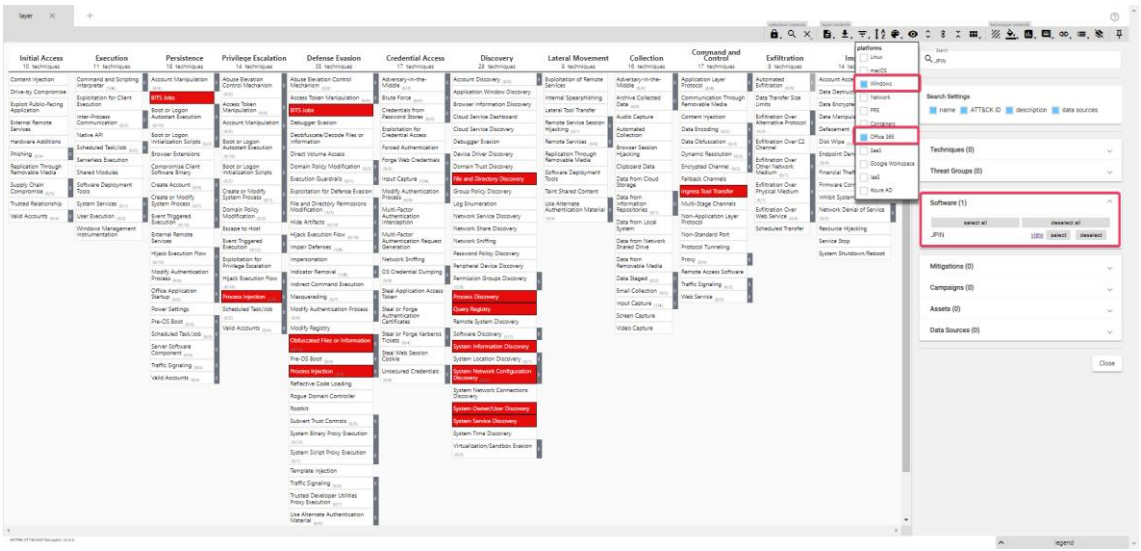
persistir en un punto final. Se identifican los parámetros de línea de comandos utilizados para crear, reanudar o agregar un archivo a un trabajo BITS.

- **Descarga de Archivos con BITSAdmin:** Se centra en identificar el uso del parámetro de transferencia de bitsadmin.exe para descargar un objeto remoto. Se recomienda buscar también descargas o subidas en la línea de comandos. Es importante revisar los procesos paralelos y secundarios para capturar cualquier comportamiento y artefacto relacionado con BITS. Se menciona que en algunos casos sospechosos y maliciosos, se crearán trabajos BITS.

4. **Metadato del Servicio:** BITS se ejecuta como un servicio y su estado puede ser verificado con la unidad Sc query (sc query bits).

https://attack.mitre.org/techniques/T1197/

Como podemos observar en la siguiente imagen en filtros hemos puesto Windows y Office 365. En software hemos buscado JPIN y lo hemos seleccionado.



Aquí usando export de la herramienta mitre-attack, aunque hay que ampliarlo mucho para poder leerlo.