Los investigadores de seguridad han proporcionado más detalles sobre la operación de minería de criptomonedas realizada por la banda 8220, aprovechando vulnerabilidades conocidas en el servidor Oracle WebLogic.

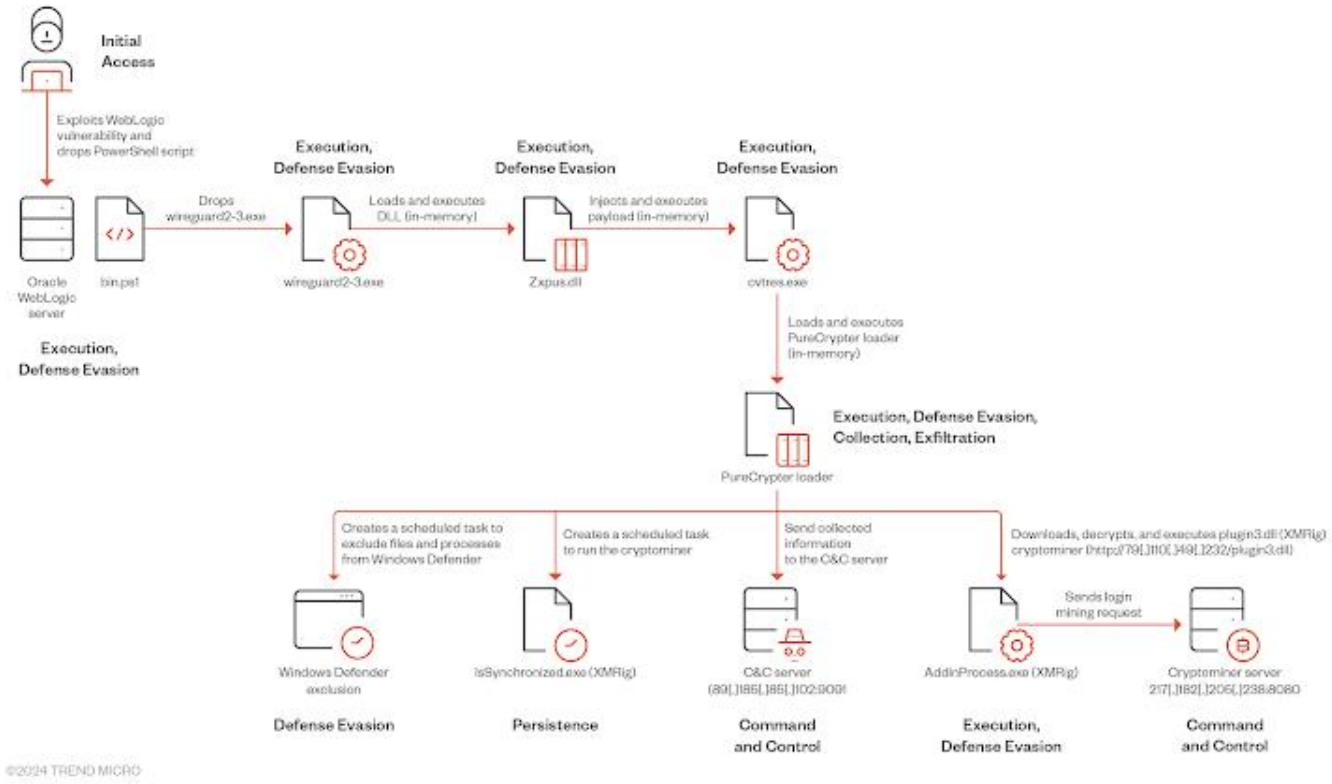
> *«El actor de amenaza utiliza técnicas de ejecución sin archivos, empleando inyección de procesos y DLL reflectiva, lo que permite que el código malicioso se ejecute exclusivamente en la memoria y evite los mecanismos de detección basados en el disco»,* explicaron los investigadores de Trend Micro, Ahmed Mohamed Ibrahim, Shubham Singh y Sunil Bharti en un nuevo análisis publicado hoy.

La firma de ciberseguridad está siguiendo a este actor motivado por ganancias financieras bajo el nombre Water Sigbin, conocido por explotar vulnerabilidades en Oracle WebLogic Server como CVE-2017-3506, CVE-2017-10271 y CVE-2023-21839 para obtener acceso inicial y desplegar la carga del minero mediante una técnica de carga en varias etapas.

Después de establecer un punto de apoyo exitoso, se despliega un script de PowerShell encargado de soltar un cargador de primera etapa («wireguard2-3.exe») que imita la aplicación legítima de VPN WireGuard, pero que en realidad lanza otro binario («cvtres.exe») en la memoria mediante una DLL («Zxpus.dll»).

El ejecutable inyectado actúa como un conducto para cargar el cargador PureCrypter («Tixrgtluffu.dll»), que, a su vez, exfiltra información de hardware a un servidor remoto y crea tareas programadas para ejecutar el minero, además de excluir los archivos maliciosos del antivirus Microsoft Defender.

En respuesta, el servidor de comando y control (C2) envía un mensaje encriptado que contiene los detalles de configuración de XMRig, después de lo cual el cargador recupera y ejecuta el minero desde un dominio controlado por el atacante, disfrazándolo como «AddinProcess.exe«, un binario legítimo de Microsoft.



El avance se produce mientras el equipo de QiAnXin XLab ha detallado una nueva herramienta de instalación utilizada por la banda 8220, conocida como k4spreader, desde al menos febrero de 2024, para distribuir el botnet Tsunami DDoS y el programa de minería PwnRig.

El malware, que está en desarrollo y tiene una versión de shell, ha estado explotando vulnerabilidades de seguridad en Apache Hadoop YARN, JBoss y Oracle WebLogic Server para infiltrarse en objetivos vulnerables.

> *«k4spreader está escrito en cgo, incluye persistencia del sistema, descarga y actualización automática, y la liberación de otro malware para su ejecución»,* indicó la compañía, añadiendo que también está diseñado para desactivar el firewall, eliminar botnets rivales (por ejemplo, kinsing) e informar sobre su estado operativo.