Un nuevo ataque de criptominería explota las vulnerabilidades ProxyShell en Microsoft Exchange. Un malware recientemente descubierto llamado ProxyShellMiner aprovecha las vulnerabilidades de Microosft Exchange ProxyShell para implementar mineros de criptomonedas dentro de un dominio de Windows, generando de esta forma ganancias para los atacantes.

El término ProxyShell se refiere a tres vulnerabilidades de Exchange que Microsoft abordó y resolvió en 2021. Las vulnerabilidades, cuando se utilizan en conjunto, permiten la ejecución remota de código sin autenticación, lo que otorga a los atacantes el control total del servidor de Exchange y les permite cambiar a otras secciones de la red de la organización.

Morphisec informa que los atacantes aprovechan las vulnerabilidades de ProxyShell denominadas CVE-2021-34473 y CVE-2021-34523 para obtener acceso inicial a la red de la organización.

Después, los atacantes proceden a depositar una carga útil de malware .NET en el directorio NETLOGON del controlador de dominio, asegurándose de que todos los dispositivos conectados ejecuten el malware, que se activa solo después de recibir un parámetro de línea de comando que sirve como contraseña para el componente minero XMRig.

Según el informe de Morphisec, el malware ProxyShellMiner emplea un diccionario integrado, un algoritmo de descifrado XOR y una clave XOR que se descarga desde un servidor remoto. Después, utiliza el compilador de C# CSC.exe con parámetros de compilación «*InMemory*» para ejecutar los siguientes módulos de código incrustado.

En la siguiente fase, el malware descarga un archivo conocido como «*DC_DLL*» y realiza una reflexión .NET para extraer argumentos para el programador de tareas, XML y la clave MXRig. El archivo DLL se usa para descifrar archivos adicionales.

Para establecer la persistencia en el sistema infectado, un segundo descargador crea una tarea programada configurada para ejecutarse cuando el usuario inicia sesión. Finalmente, el segundo cargador y otros cuatro archivos se descargan desde un recurso remoto.

ProxyShellMiner selecciona un navegador de los disponibles en el sistema comprometido para inyectar el minero en su espacio de memoria, usando un proceso llamado *«vaciado de procesos».* Después selecciona de forma aleatoria un grupo de minería de una lista codificada en el malware y comienza el proceso de minería.

La etapa final en la secuencia de ataque implica la creación de una regla de firewall que prohíba todo el tráfico saliente, que se aplica a todos los perfiles de Firewall de Windows. Esta acción tiene como objetivo disminuir la probabilidad de que los defensores detecten indicadores de infección o reciban alertas sobre un posible compromiso del sistema.

Para evitar la detección por parte de las herramientas de seguridad que rastrean el comportamiento del tiempo de ejecución del proceso, el malware espera al menos 30 segundos después de que el navegador se vacíe antes de generar la regla de firewall. Es posible que el minero siga comunicándose con su pool de minería a través de una puerta trasera no supervisada.

Morphisec ha dado la alarma de que las consecuencias del malware van más allá de las interrupciones del servicio, provocando la degradación del rendimiento y el sobrecalentamiento del hardware. Tan pronto como los hackers penetran en la red, pueden ejecutar cualquier acción, desde implementar backdoors hasta ejecutar código.

Morphisec recomienda que los administradores implementen los parches de seguridad disponibles y adopten mecanismos multifacéticos de defensa y detección de amenazas para mitigar el riesgo de infecciones de ProxyShellMiner.