La empresa rumana de ciberseguridad Bitdefender ha lanzado un descifrador gratuito para ayudar a las víctimas a recuperar sus datos encriptados por el ransomware ShrinkLocker.

Este descifrador es el resultado de un análisis detallado de los mecanismos internos de ShrinkLocker, lo cual permitió a los investigadores encontrar una *«ventana específica de oportunidad para recuperar datos inmediatamente después de eliminar los protectores en discos encriptados con BitLocker».*

ShrinkLocker fue documentado por primera vez en mayo de 2024 por Kaspersky, quien detectó el uso de la herramienta nativa BitLocker de Microsoft en este malware para encriptar archivos, como parte de ataques de extorsión dirigidos a México, Indonesia y Jordania.

Bitdefender, que investigó un caso de ShrinkLocker contra una empresa de salud en el Medio Oriente (no identificada), afirmó que el ataque probablemente comenzó desde un dispositivo de un contratista. Esto subraya cómo los actores de amenazas explotan cada vez más las relaciones de confianza para infiltrarse en la cadena de suministro.

En la siguiente fase, el atacante se movió lateralmente a un controlador de dominio de Active Directory usando credenciales legítimas de una cuenta comprometida y creó dos tareas programadas para iniciar el proceso de ransomware.

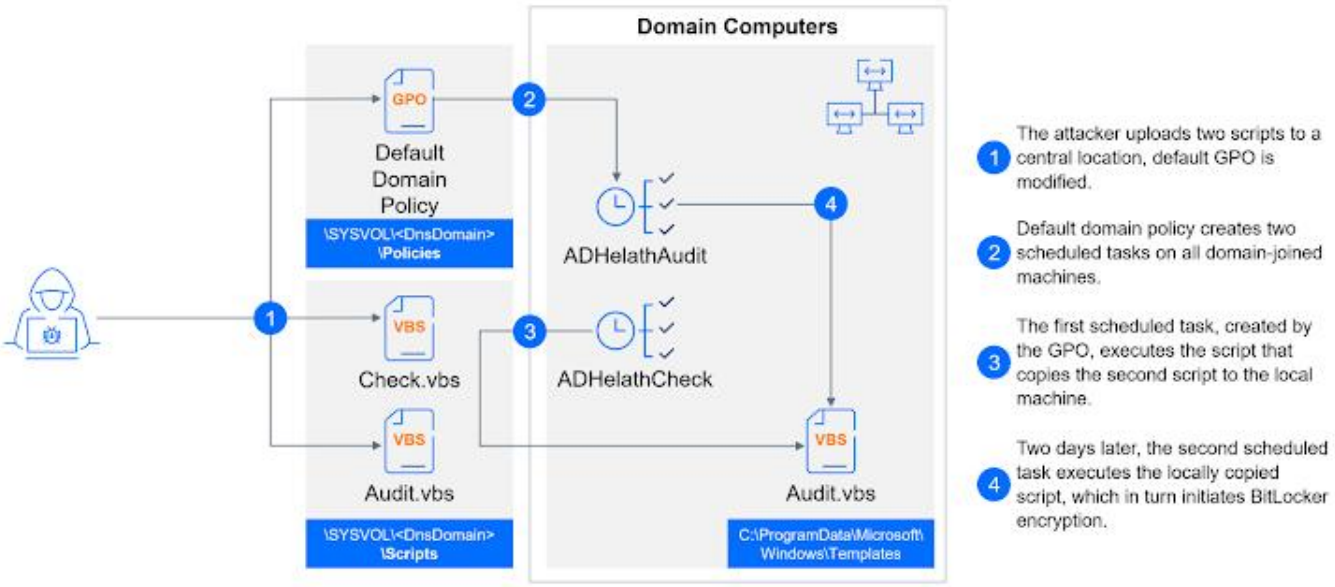
La primera tarea ejecutaba un script en Visual Basic («Check.vbs») que copiaba el programa de ransomware a todas las máquinas conectadas al dominio, mientras que la segunda tarea, programada para dos días después, ejecutaba el ransomware localmente desplegado («Audit.vbs»).

Bitdefender explicó que el ataque logró encriptar sistemas que usaban Windows 10, Windows 11, Windows Server 2016 y Windows Server 2019. Además, se cree que la versión de ShrinkLocker utilizada fue una modificación de la versión original.

Descripto como sencillo pero eficaz, el ransomware llama la atención por estar escrito en

VBScript, un lenguaje de scripting que Microsoft ha anunciado que comenzará a eliminar a partir de la segunda mitad de 2024. En lugar de implementar su propio algoritmo de cifrado, el malware utiliza BitLocker para alcanzar sus objetivos.

El script está diseñado para recopilar información sobre la configuración del sistema y el sistema operativo, verificar si BitLocker ya está instalado en una máquina con Windows Server, y, si no lo está, instalarlo mediante un comando de PowerShell y realizar un *«reinicio forzado»* usando Win32Shutdown.



Sin embargo, Bitdefender identificó un error que provoca que esta solicitud falle con un mensaje de *«Privilegio No Concedido»,* lo que hace que el VBScript quede atrapado en un bucle infinito debido a un reinicio fallido.

> *«Incluso si el servidor se reinicia manualmente (por ejemplo, por un administrador sin sospechas), el script no tiene un mecanismo para continuar su ejecución después del reinicio, lo que significa que el ataque podría ser interrumpido o prevenido»*, explicó Martin Zugec, director de soluciones técnicas en Bitdefender.

El ransomware genera una contraseña aleatoria derivada de información específica del sistema, como el tráfico de red, la memoria y el uso del disco, y la utiliza para cifrar las unidades del sistema.

Esa contraseña única luego se carga en un servidor controlado por el atacante. Tras el reinicio, el usuario debe ingresar la contraseña para desbloquear la unidad encriptada. La pantalla de BitLocker también se configura para mostrar la dirección de correo electrónico del atacante para iniciar el pago a cambio de la contraseña.

Además, el script realiza varias modificaciones en el Registro para restringir el acceso al sistema, desactivando las conexiones remotas RDP y bloqueando los inicios de sesión locales basados en contraseñas. Como parte de su «limpieza», también desactiva las reglas del Firewall de Windows y borra los archivos de auditoría.

Bitdefender también señaló que el nombre ShrinkLocker es algo confuso, ya que la funcionalidad de reducción de particiones se limita solo a sistemas Windows antiguos y no está disponible en los sistemas operativos actuales.

> *«Utilizando una combinación de Objetos de Directiva de Grupo (GPO) y tareas programadas, puede cifrar varios sistemas dentro de una red en solo 10 minutos por dispositivo. Como resultado, es posible comprometer un dominio completo con un esfuerzo mínimo»,* comentó Zugec.
>
> *«La monitorización proactiva de ciertos registros de eventos de Windows puede ayudar a las organizaciones a detectar y reaccionar ante posibles ataques de BitLocker desde sus etapas iniciales, por ejemplo, cuando los atacantes están probando sus capacidades de cifrado.»*
>
> *«Al configurar BitLocker para que almacene la información de recuperación en los Servicios de dominio de Active Directory (AD DS) y aplicar la política de 'No habilitar*

> *BitLocker hasta que la información de recuperación esté almacenada en AD DS para unidades del sistema operativo,' las organizaciones pueden reducir considerablemente el riesgo de ataques basados en BitLocker.»*