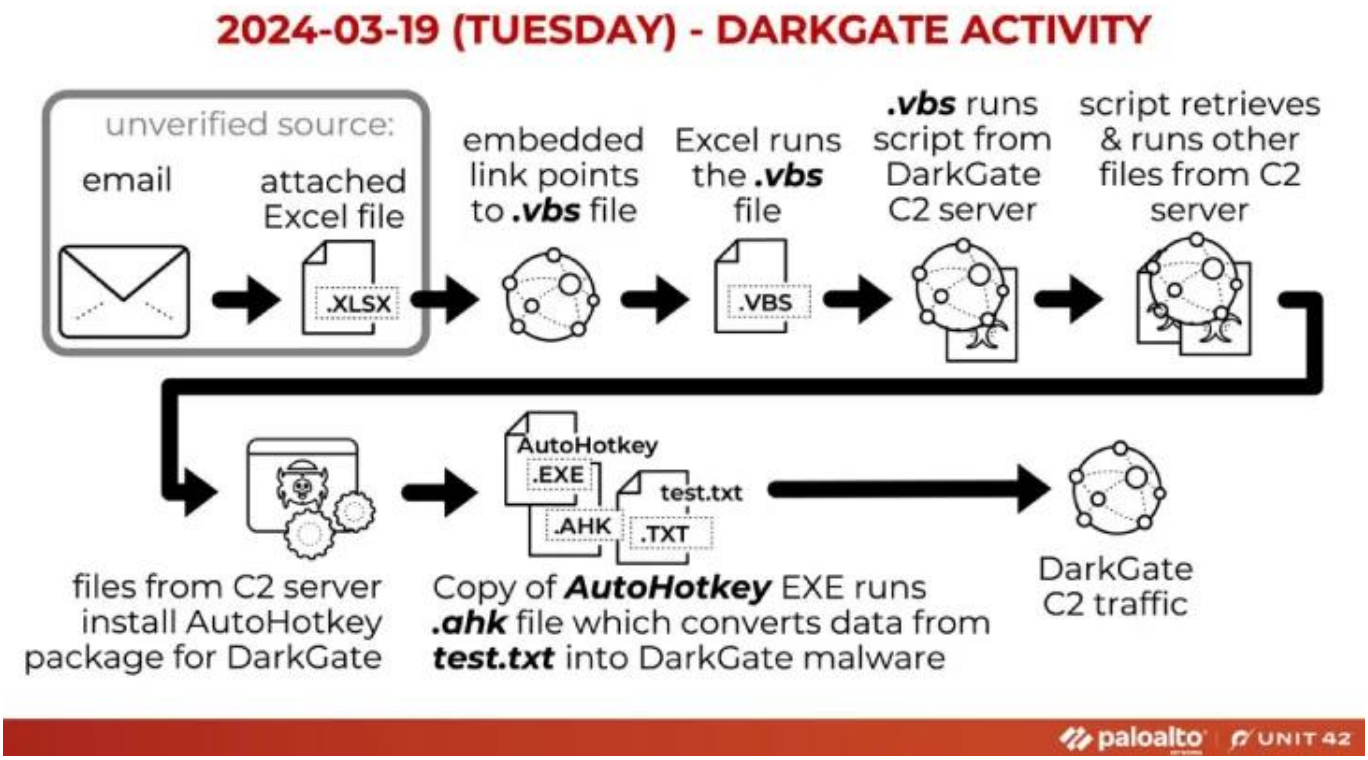
Los investigadores en ciberseguridad han revelado detalles sobre una campaña de malware de corta duración llamada DarkGate, que explotó los recursos compartidos de archivos Samba para iniciar infecciones.

Unit 42 de Palo Alto Networks indicó que la actividad se desarrolló durante los meses de marzo y abril de 2024, utilizando servidores con recursos compartidos de archivos Samba de acceso público que alojaban archivos de Visual Basic Script (VBS) y JavaScript. Los objetivos incluían América del Norte, Europa y algunas regiones de Asia.

> *«Esta fue una campaña relativamente breve que demuestra cómo los actores maliciosos pueden abusar creativamente de herramientas y servicios legítimos para distribuir su malware»,* señalaron los investigadores de seguridad Vishwa Thothathri, Yijie Sui, Anmol Maurya, Uday Pratap Singh y Brad Duncan.

DarkGate, que apareció por primera vez en 2018, ha evolucionado hacia una oferta de malware como servicio (MaaS) utilizada por un número limitado de clientes. Tiene capacidades para controlar remotamente los sistemas comprometidos, ejecutar código, minar criptomonedas, lanzar shells inversas y desplegar cargas útiles adicionales.

Los ataques que involucran este malware han aumentado notablemente en los últimos meses, tras la operación multinacional de desmantelamiento de la infraestructura de QakBot en agosto de 2023.




La campaña documentada por Unit 42 comienza con archivos de Microsoft Excel (.xlsx) que, al ser abiertos, instan a los usuarios a hacer clic en un botón de «Abrir» incrustado, lo que a su vez descarga y ejecuta código VBS alojado en un recurso compartido de archivos Samba.

El script de PowerShell está configurado para recuperar y ejecutar otro script de PowerShell, que luego se utiliza para descargar un paquete de DarkGate basado en AutoHotKey.

Las secuencias alternas que utilizan archivos JavaScript en lugar de VBS son similares en que también están diseñadas para descargar y ejecutar el script de PowerShell siguiente.

DarkGate funciona escaneando varios programas antimalware y verificando la información de la CPU para determinar si se está ejecutando en un sistema físico o en un entorno virtual, permitiendo así dificultar el análisis. También examina los procesos en ejecución del sistema para detectar la presencia de herramientas de ingeniería inversa, depuradores o software de

virtualización.

> *«El tráfico C2 de DarkGate utiliza solicitudes HTTP no cifradas, pero los datos están ofuscados y aparecen como texto codificado en Base64»,* dijeron los investigadores.
>
> *«A medida que DarkGate continúa evolucionando y refinando sus métodos de infiltración y resistencia al análisis, sigue siendo un recordatorio contundente de la necesidad de defensas de ciberseguridad robustas y proactivas.»*