Investigadores de seguridad cibernética revelaron los detalles de una campaña de malware evasiva que hace uso de certificados de firma de código válidos, con el fin de escabullirse de las defensas de seguridad y permanecer bajo el rada con el objetivo de implementar cargas útiles de Cobalt Strike y BitRAT en sistemas comprometidos.

El binario es un cargador bajo el nombre de Blister, apodado así por los investigadores de Elastic Security, y las muestras de malware tienen detecciones insignificantes o nulas en VirusTotal. Hasta este momento, se desconoce el vector de infección utilizado para organizar el ataque, así como los objetivos finales de la intrusión.

Un aspecto notable de los ataques es que aprovechan un certificado de firma de código válido emitido por Sectigo. Se ha observado que el malware está firmado con el certificado en cuestión que data del 15 de septiembre de 2021. Elastic afirmó que se comunicó con la compañía para asegurarse de que los certificados abusados sean revocados.

> *«Los ejecutables con certificados de firma de código válidos por lo general se examinan en menor grado que los ejecutables sin firmar. Su uso permite a los atacantes permanecer fuera del radar y evadir la detección durante un período de tiempo más largo»,* dijeron los investigadores Joe Desimone y Samir Bousseaden.

Blister se hace pasar por una biblioteca legítima llamada colorui.dll, y se entrega a través de un cuentagotas llamado *«dxpo8umrzrr1w6gm.exe».* Luego de la ejecución, el cargador está diseñado para dormir por 10 minutos, probablemente como un intento de evadir el análisis de sandbox, solo para seguir estableciendo persistencia y descifrando una carga útil de malware incrustado como Cobalt Strike o BitRAT.

> *«Una vez descifrada, la carga útil incorporada se carga en el proceso actual o se inyecta en un proceso WerFault.exe (Informe de Errores de Windows) recién*

> *generado»,* dijeron los investigadores.

Se puede acceder a los indicadores de compromiso (IoC) adicionales asociados con la campaña en este enlace.