Un nuevo grupo de hackers con motivaciones políticas llamado *«Bastón de Moisés»*, se ha relacionado con una ola de ataques dirigidos contra organizaciones israelíes desde septiembre de 2021, con el objetivo de saquear y filtrar información confidencial antes de cifrar sus redes, sin opción de recuperar el acceso o negociar un rescate.

> *«El grupo declara abiertamente que su motivación para atacar a las empresas israelíes es a causa de daños por fugas de los datos sensibles robados y el cifrado de redes de la víctima, sin petición de rescate. En el lenguaje de los atacantes, su propósito es luchar contra la resistencia y exponer los crímenes de los sionistas en los territorios ocupados»,* dijo Check Point.

Se han filtrado datos de al menos 16 víctimas hasta ahora, según las estadísticas publicadas por el colectivo.

Se cree que el actor de amenazas aprovecha las vulnerabilidades conocidas públicamente como un medio para violar los servidores de la compañía y obtener acceso inicial, siguiendo con la implementación de un shell web personalizado que se utiliza para eliminar malware adicional. Una vez dentro, los intrusos aprovechan las técnicas de vivir fuera de la tierra (LotL) para moverse lateralmente a través de la red e implementar malware para bloquear las máquinas detrás de barreras de cifrado por medio de un malware PyDcrypt especialmente diseñado.

Los ataques se basan de forma específica en la biblioteca de código abierto DiskCryptor, para realizar el cifrado de volumen, además de infectar los sistemas con un cargador de arranque que evita que se inicien sin la clave de cifrado correcta. El objetivo, dijeron los investigadores, es interrumpir las operaciones e infligir *«daños irreversibles»* a las víctimas.

De este modo, los archivos cifrados se pueden recuperar en ciertos escenarios, ya que el grupo utiliza un mecanismo de clave simétrica para generar las claves de cifrado. Check Point no atribuyó al adversario a ningún país específico, y citó la falta de evidencia definitiva, pero dijo que algunos artefactos del conjunto de herramientas del grupo se habían enviado a

VirusTotal desde Palestina meses antes del primer ataque.

Moses Staff también opera en Twitter y Telegram para publicitar sus ataques, con actividad maliciosa reportada apenas el 14 de noviembre. El propio sitio web del grupo asegura que ha atacado a más de 257 sitios web, así como datos y documentos robados con un peso de 34 terabytes.

> *«El personal de Moses todavía sigue activo, impulsando mensajes y videos provocativos en sus cuentas de redes sociales. Las vulnerabilidades explotadas en los ataques del grupo no son días cero, y por lo tanto, todas las víctimas potenciales pueden protegerse mediante el parcheo inmediato de todos los sistemas públicos»*, dijeron los investigadores.