Investigadores de seguridad cibernética revelaron este martes una nueva campaña de espionaje que recurre a ataques destructivos de borrado de datos dirigidos a entidades israelíes al menos desde diciembre de 2020 que camuflan la actividad maliciosa como extorsiones de ransomware.

La compañía de seguridad cibernética CentinelOne atribuyó los ataques a un actor del estado-nación afiliado a Irán al que rastrea bajo el sobrenombre de Agrius.

> *«Un análisis de lo que a primera vista parecía ser un ataque de ransomware reveló nuevas variantes de limpiaparabrisas que se desplegaron en una serie de ataques destructivos contra objetivos israelíes. Los operadores detrás de los ataques enmascararon intencionalmente su actividad como ataques de ransomware, un comportamiento poco común para los grupos motivados financieramente»*, dijeron los investigadores.

La forma en que opera el grupo implica la implementación de un malware .NET personalizado llamado Apostle que ha evolucionado para convertirse en un ransomware completamente funcional, reemplazando sus capacidades de limpiador anteriores, mientras que algunos de los ataques se han llevado a cabo utilizando un segundo limpiador llamado DEADWOOD (también conocido como Detbosit) después de una falla lógica en las primeras versiones de Apostle impidió que se borraran los datos.

Además, los actores de Agrius dejan caer un implante .NET llamado IPsec Helper que se puede utilizar para filtrar datos o implementar malware adicional. Además, las tácticas del actor de amenazas también han sido testigos de un cambio del espionaje al exigir rescates a sus víctimas para recuperar el acceso a los datos cifrados, solo para que se destruyan en un ataque de borrado.

Además de usar ProtonVPN para el anonimato, el ciclo de ataques de Agrius aprovecha las vulnerabilidades de 1 día en aplicaciones basadas en web, incluida CVE-2018-13379 para ganar un punto de apoyo inicial, y posteriormente, entregar shells web ASPXSpy para

mantener el acceso remoto a los sistemas comprometidos y ejecutar comandos arbitrarios.

En todo caso, la investigación se suma a la evidencia de que los actores patrocinados por el estado con vínculos con el gobierno iraní están considerando cada vez más las operaciones de ransomware como una técnica de subterfugio para imitar a otros grupos de ransomware ciberdelincuentes motivados financieramente.

Documentos recientemente filtrados por Lab Dookhtegan revelaron una iniciativa llamada *«Project Signal»,* que vinculaba al Cuerpo de la Guardia Revolucionaria Islámica de Irán con una operación de ransomware a través de una empresa contratante.

> *«Si bien son disruptivas y efectivas, las actividades de ransomware brindan negación, lo que permite a los estados enviar un mensaje sin responsabilizarse directamente. Otros actores patrocinados por estados nacionales han utilizado estrategias similares con efectos devastadores»,* dijeron los investigadores.