Un grupo de Amenaza Persistente Avanzada (APT), se ha relacionado con ataques cibernéticos a dos compañías de biofabricación que ocurrieron este año con la ayuda de un cargador de malware personalizado llamado Tardigrade.

Según un aviso publicado por el Centro de Análisis e Intercambio de Información de Bioeconomía (BIO-ISAC) esta semana, el malware se está propagando activamente por todo el sector con el objetivo probable de perpetrar el robo de propiedad intelectual, manteniendo la persistencia durante períodos prolongados de tiempo e infectar los sistemas con ransomware.

BIO-ISAC, que inició una investigación luego de un ataque de ransomware dirigido a una instalación de biofabricación sin nombre a inicios de la primavera, caracterizó a Tardigrade como una pieza sofisticada de malware con *«un alto grado de autonomía y capacidades metamórficas».* Después, el mismo malware se utilizó para atacar a una segunda entidad en octubre de 2021.

Las intrusiones de *«propagación activa»* no se han atribuido a un actor de amenaza específico o una nación, pero la agencia dijo a The Hill que los esfuerzos reflejaban ataques anteriores de un grupo de piratería vinculado a Rusia.

Propagado a través de correos electrónicos de phishing o unidades USB infectadas, Tardigrade es una rama avanzada de SmokeLoader, una backdoor basada en Windows operada por un grupo conocido como Smoky Spider, y disponible para la venta en mercados clandestinos que se remonta a 2011, además es el primero que contó con capacidades para capturar pulsaciones de teclas, moverse lateralmente a través de la red comprometida y escalar privilegios.

Además, el malware actúa como un punto de entrada para cargas útiles de malware adicionales y está diseñado para funcionar de forma autónoma incluso cuando está desconectado de su servidor de comando y control para llevar a cabo sus actividades maliciosas. Se recomienda a las organizaciones de la industria de la biofabricación que apliquen actualizaciones de software, hagan cumplir la segmentación de la red y prueben las

copias de seguridad fuera de línea de la infraestructura biológica crítica para mitigar las amenazas.

> *«Este malware es extremadamente difícil de detectar debido al comportamiento metamórfico. La vigilancia de las computadoras corporativas del personal clave es importante. Muchas máquinas en el sector usan sistemas operativos obsoletos. Segmentarlos de forma agresiva y acelerar los plazos de actualización es importante»,* dijeron los investigadores.