La Agencia de Seguridad Cibernética e Infraestructura (CISA) del Departamento de Seguridad Nacional de Estados Unidos, advirtió hoy a todas las industrias que operan infraestructuras críticas, sobre una nueva amenaza de ransomware que de no ser abordada, podría generar graves consecuencias.

El aviso se produjo a raíz de un ataque cibernético dirigido a una instalación de compresión de gas natural sin nombre que empleó phishing para entregar ransomware a la red interna de la compañía, encriptando datos críticos y dejando fuera de servicio a los servidores por casi dos días.

> *«Un actor de amenaza cibernética utilizó un enlace de spear phishing para obtener acceso inicial a la red de tecnología de la información de la organización antes de pasar a su red de tecnología operativa. Luego, el actor de amenaza implementó ransomware de productos básicos para cifrar datos para impactar en ambas redes»,* dijo CISA.

A medida que los ataques de ransomware siguen aumentando en frecuencia y escala, el nuevo desarrollo es otra indicación de que los ataques de phishing siguen siendo un medio efectivo para superar las barreras de seguridad y que los hackers no siempre necesitan explotar las vulnerabilidades de seguridad para afectar a las organizaciones.

CISA agregó que el ataque no afectó a ningún controlador lógico programable (PLC), y que la víctima no perdió el control de sus operaciones. Pero después del incidente, se informó que la compañía inició un cierre operacional deliberado, lo que resultó en pérdida de productividad e ingresos.

La organización mencionó que la compañía pudo recuperarse del ataque cibernético al utilizar un equipo de reemplazo y cargar las últimas configuraciones buenas conocidas.

Aunque la notificación se apoya en los detalles específicos del ataque, esta no es la primera vez que se utilizan enlaces de phishing para entregar ransomware. La red de TI de Lake City

quedó paralizada en junio pasado luego de que un empleado abriera accidentalmente un correo electrónico sospechoso que descargó el troyano Emotet, que a su vez descargó el troyano TrickBot y el ransomware Ryuk.

Con este panorama de amenazas cibernéticas en evolución, las empresas deben considerar el alcance total de las amenazas planteadas a sus operaciones, incluyendo el mantenimiento de copias de seguridad periódicas de los datos y el diseño de mecanismos de conmutación por error en caso de cierre.

Además de asegurar el canal de correo electrónico e identificar y proteger a las personas más atacadas, esto también señala la necesidad de adoptar medidas anti-phishing adecuadas para evitar que los intentos de ingeniería social lleguen a las bandejas de entrada de sus objetivos y capacitar a las personas para detectar los correos que pasan.

También es importante que las organizaciones vulnerables salvaguarden la cadena de suministro digital segmentando la infraestructura crítica de la red usando firewalls y realizando auditorías de seguridad periódicas para identificar vulnerabilidades.