Una campaña global de spear-phishing está dirigiéndose a organizaciones asociadas con la distribución de vacunas COVID-19 desde septiembre de 2020, según una nueva investigación.

Al atribuir la operación a un actor del estado-nación, los investigadores de IBM Security X-Force dijeron que los ataque tenían como objetivo la cadena de enfriamiento de la vacuna, empresas responsables de almacenar y entregar la vacuna a temperaturas seguras.

El desarrollo ha llevado a la Agencia de Seguridad de Infraestructura y Ciberseguridad de Estados Unidos (CISA) a emitir una alerta, instando a las organizaciones y empresas de Operation Warp Speed (OWS) involucrados en el almacenamiento y transporte de vacunas, a revisar los indicadores de compromiso (IoC) y reforzar sus defensas.

No está claro si alguno de los intentos de phishing tuvo éxito, pero la compañía dijo que ha notificado a las entidades y autoridades correspondientes sobre el ataque dirigido.

Los correos electrónicos de phishing, que datan de septiembre, estaban dirigidos a organizaciones en Italia, Alemania, Corea del Sur, República Checa, Gran Europa y Taiwán, incluida la Dirección General de Impuestos y Unión Aduanera de la Comisión Europea, fabricantes de paneles solares no identificados, un software de una empresa en Corea del Sur y una empresa alemana de desarrollo de sitios web.

IBM dijo que los ataques probablemente se dirigieron a organizaciones vinculadas a la alianza de vacunas Gavi con el objetivo de recopilar credenciales de usuario para obtener acceso no autorizado en el futuro a las redes corporativas e información confidencial relacionada con la distribución de la vacuna COVID-19.

Para que los correos electrónicos resultaran más creíbles, los operadores detrás de la campaña crearon señuelos que se hicieron pasar por solicitudes de cotizaciones para participar en un programa de vacunas. Los atacantes también se hicieron pasar por un ejecutivo comercial de Haier Biomedical, un proveedor legítimo de cadena de enfriamiento con sede en China, en un intento por convencer a los destinatarios de que abran los correos

electrónicos entrantes sin cuestionar la autenticidad del remitente.

> *«Los correos electrónicos contienen archivos adjuntos HTML maliciosos que se abren localmente, lo que solicita a los destinatarios que ingresen sus credenciales para ver el archivo»*, dijeron Claire Zaboeva y Melissa Frydrych, investigadoras de IBM.

Aunque los investigadores no pudieron establecer las identidades de los hackers, parece que el objetivo final es recolectar los nombres de usuario y contraseñas para abusar de ellos con el fin de robar propiedad intelectual y moverse lateralmente a través de los entornos de las víctimas para las campañas de espionaje posteriores.

La investigación y desarrollo de la vacuna COVID-19 ha sido blanco de ataques cibernéticos sostenidos desde principios del año.

En junio, IBM reveló detalles de una campaña de phishing similar dirigida a una entidad alemana relacionada con la adquisición de equipos de protección personal (PPE) de cadenas de suministro y compras con sede en China.

Los ataques cibernéticos llevaron al Departamento de Justicia de Estados Unidos a cobrar a dos ciudadanos chinos por robar datos confidenciales, incluso de empresas que desarrollan vacunas COVID-19, pruebas de tecnología y tratamientos, mientras operan tanto para obtener ganancias financieras privadas como en nombre del Ministerio de Seguridad del Estado de China.

En noviembre, Microsoft informó que detectó ataques cibernéticos de tres agentes estatales en Rusia (Fancy Bear, también conocido como Strontium) y Corea del Norte (Hidden Cobra y Cerium), dirigidos contra compañías farmacéuticas ubicadas en Canadá, Francia, India, Corea del Sur y Estados Unidos.

La semana pasada, se supo que los hackers norcoreanos se habían dirigido a la farmacéutica

AstraZeneca, haciéndose pasar por reclutadores en el sitio de redes LinkedIn y WhatsApp, para acercarse a sus empleados con ofertas de trabajo falsas y engañarlos para que abrieran lo que supuestamente eran documentos de descripción del trabajo para obtener acceso a sus sistemas e instalar malware.