Anuncios

IBM descubre una campaña de phishing dirigida a las empresas relacionadas con la cadena de frío de la vacuna COVID-19

• Los e-mails fraudulentos buscaban recopilar credenciales, para, entre otros propósitos, acceder a información relacionada con el proceso, los métodos y los planes para distribuir la vacuna de la COVID-19

• La campaña estaba dirigida a organizaciones implicadas en el proceso de la cadena de frío como la Dirección General de Fiscalidad y Unión Aduanera de la Comisión Europea, el sector energético y el sector TI

• IBM Security X-Force insta a las empresas de la cadena de suministro de la COVID-19 a que estén atentas y permanezcan en alerta máxima durante este tiempo

Madrid, 3 de diciembre de 2020. Al inicio de la pandemia de la COVID-19, IBM Security X-Force® creó un grupo de trabajo dedicado a rastrear las amenazas en la nube del ciberespacio contra las organizaciones que mantienen en funcionamiento la cadena de suministro de las vacunas de la COVID-19. Como parte de estos esfuerzos, el equipo de expertos ha descubierto una campaña de phishing dirigida a empresas relacionadas con el proceso de la cadena de frío de las vacunas, esencial para garantizar su conservación segura en entornos de temperatura controlada durante su almacenamiento y transporte.

El análisis indica que esta operación planificada comenzó en septiembre de 2020. La campaña se extendió a seis países y se dirigió a organizaciones probablemente asociadas con el programa "Plataforma de Optimización de Equipos de Cadena de Frío" (CCEOP) de Gavi Vaccine Alliance, lanzado con el Fondo de las Naciones Unidas para la Infancia (UNICEF) y otras entidades asociadas en 2015. Su objetivo es, en última instancia, fortalecer las cadenas de suministro de las vacunas, optimizar la equidad de la inmunización y garantizar una respuesta médica ágil a los brotes de enfermedades infecciosas.

Aunque nadie se ha atribuido en firme la autoría de estos ataques, el equipo de expertos de IBM cree que podría tratarse de ataques procedentes de un Estado-Nación, debido a la precisión en la selección de los objetivos y las organizaciones mundiales clave en el proceso.

Spoofing calculado para comprometer la cadena de frío de la vacuna de la COVID-19

La campaña se llevó a cabo a través de la falsificación de correos electrónicos. Concretamente, el atacante se hizo pasar por un directivo de Haier Biomedical, una compañía china que actualmente actúa como proveedor cualificado del programa CCEOP, en coordinación con la Organización Mundial de la Salud (OMS), UNICEF y otras agencias de la ONU.

La compañía es supuestamente el único proveedor del mundo que controla la cadena de frío al completo. Haciéndose pasar por este ejecutivo, el atacante envió correos electrónicos de phishing a organizaciones proveedoras de material de transporte dentro de la cadena de frío de las vacunas de la COVID-19. IBM Security X-Force consideró que el propósito de esta campaña pudo haber sido recopilar contraseñas, posiblemente para obtener más adelante un acceso no autorizado a redes corporativas e información sensible relacionada con la distribución de la vacuna de la COVID-19.

Objetivo de alcance global

Entre los objetivos de esta campaña se incluía a la Dirección General de Impuestos y Unión Aduanera de la Comisión Europea, así como a organizaciones de los sectores de energía, fabricación, la creación de sitios web y soluciones de software y seguridad en Internet. Se trata de organizaciones mundiales con sede en Alemania, Italia, Corea del Sur, República Checa, Europa y Taiwán. Dada la especialización y la distribución mundial de las organizaciones a las que se dirigía esta campaña, es muy probable que los atacantes conocieran íntimamente los componentes críticos y a los agentes implicados en la cadena de frío de la vacuna.

Recolección de credenciales para un acceso más amplio

Los correos electrónicos de spear phishing se enviaron a varios ejecutivos de ventas, compras, tecnologías de la información y finanzas que probablemente estaban involucrados en el proceso de la cadena de frío de las vacunas. También se identificaron casos en los que la actividad se extendió a toda la organización para incluir páginas de soporte de las organizaciones objetivo.

Detectada esta campaña, IBM Security X-Force ha seguido protocolos de divulgación responsables y ha notificado a las entidades y autoridades apropiadas sobre esta operación dirigida.

Los e-mails de phishing se planteaban como solicitudes de cotizaciones (RFQ) relacionadas con el programa CCEOP. Estos e-mails contenían archivos adjuntos HTML maliciosos que se abrían localmente, lo que provocaba que los destinatarios introdujeran sus credenciales para ver el archivo. Esta técnica de phishing ayuda a los atacantes a evitar la creación de páginas web de phishing que puedan ser descubiertas y eliminadas por los equipos de investigación de seguridad y las fuerzas del orden.

El equipo de expertos de seguridad de IBM consideró que el propósito de esta campaña pudo haber sido recoger credenciales para obtener futuros accesos no autorizados. A partir de ahí, los ciberdelincuentes podrían obtener información sobre las comunicaciones internas, así como el proceso, los métodos y los planes para distribuir una vacuna de la COVID-19. Esto incluye información sobre la infraestructura que los gobiernos tienen la intención de utilizar para distribuir una vacuna a los proveedores que la suministrarán. Sin embargo, más allá de la información crítica relativa a la vacuna de la COVID-19, el acceso de los atacantes podría extenderse a los entornos de las víctimas. Moverse lateralmente a través de las redes y permanecer allí de forma sigilosa permitiéndoles realizar ciberespionaje y recopilar información confidencial adicional de los entornos de las víctimas para operaciones futuras.

¿Quién está detrás de estos ataques?

Si bien actualmente se desconoce, la precisión de los objetivos y la naturaleza de las organizaciones objetivo específicas apuntan potencialmente a la actividad de los hackers Estado-Nación. Sin el objetivo explícito de ganar dinero es poco probable que los ciberdelincuentes dediquen el tiempo y recursos necesarios para ejecutar una operación tan calculada con tantos objetivos interrelacionados y distribuidos a nivel mundial. Del mismo modo, la información sobre el transporte de una vacuna puede ser una mercancía de moda en el mercado negro, sin embargo, tener información avanzada de la compra y el movimiento de una vacuna que puede repercutir en la vida y la economía mundial es probablemente un objetivo de gran valor y de alta

prioridad para el Estado-nación.

Alerta para la cadena de suministro de COVID-19

IBM Security X-Force insta a las empresas de la cadena de suministro de la COVID-19 -desde la investigación de terapias, la prestación de servicios sanitarios hasta la distribución de una vacuna- a que estén atentas y permanezcan en alerta máxima durante este tiempo. Los gobiernos ya han advertido de que es probable que entidades extranjeras intenten realizar espionaje en la nube de Internet para robar información sobre las vacunas.

For further information: Patricia Núñez IBM Comunicación patricia.nunez@es.ibm.com Tlf.- 637 89 37 54

Additional assets available online: