China utiliza un ciberataque de doble método contra las organizaciones checas

China está robando datos de objetivos de alto valor a través de una campaña de spear-phishing furtivo de doble capa que incluye el malware Azureveil.

Foto de Alexander Culafi

Alexander Culafi,Escritor Senior De Noticias,Lectura oscura

2 de junio de 2026

Puente de Carlos en Praga.

Fuente: GarySandyWales vía Getty Images

Los actores de amenazas del Estado-nación están apuntando a organizaciones específicas en la República Checa y Taiwán para la exfiltración de datos, con un enfoque en verticales bien definidos: el gobierno y el sector público; investigación y academia; tecnología y software; y servicios financieros.

Eso es según el proveedor de seguridad Seqrite, que publicó una investigación la semana pasada sobre la "Operación Dragon Weave", una campaña de spear-phishing que comienza con el envío de correo electrónico a un objetivo con un archivo zip adjunto e instrucciones para abrirlo, bajo el disfraz de algo así como una próxima reunión de negocios o, en el caso de una instancia temática de la República Checa, una cita con la Administración de Seguridad Social Checa (CSSZ).

La conexión checa: en la mira de ciberataque de China

Seqrite atribuyó la campaña a China con una confianza moderada, aunque el proveedor no llegó a conectarla con un grupo específico de amenazas persistentes avanzadas (APT).

Relacionado: Los sindicatos cibercriminales asiáticos de SE se convierten en una potencia global

La polémica conexión entre China y Taiwán está bien establecida, por lo que una campaña como esta no sería una sorpresa. Menos conocida es la compleja relación de China con la República Checa. Si bien son socios comerciales importantes, el gobierno checo y China se han enfrentado a la alianza de la primera a Taiwán y el apoyo de este último a Rusia en la invasión de Ucrania. Esto tal vez explicaría el interés de China en la República Checa como un posible objetivo cibernético, según Alexis Rapin, analista de amenazas cibernéticas de ESET.

"La República Checa (CZ) es probablemente el país europeo con los lazos más estrechos con Taiwán actualmente, lo que lo convierte en un objetivo 'natural' para los actores de amenazas alineados con China", explica. "Basándonos en nuestra telemetría, parece que el interés de los APT chinos se alinea aproximadamente con esta línea de tiempo amplia: los vimos comenzar a apuntar a CZ con bastante frecuencia en 2023, con las organizaciones gubernamentales como el objetivo más común. La academia y el sector sin ánimo de lucro ocupan el segundo lugar".

Y añade: "Por su aspecto, y teniendo en cuenta el contexto más amplio, parece probable que la República Checa se encuentre entre las prioridades recurrentes de recopilación de inteligencia de los APT alineados con China en Europa".

Cómo funciona el ataque de 2 frentes de China

El archivo zip adjunto al correo electrónico de spear-phishing contiene múltiples archivos, incluido un ejecutable que abre un PDF señuelo que contiene información plausible, como instrucciones sobre qué hacer durante el día de la supuesta cita CSSZ. La forma principal en que se inicia la infección es haciendo clic en un archivo de acceso directo LNK adjunto, que ejecuta un script PowerShell para descifrar todos los componentes necesarios; luego los ejecuta a través de un archivo llamado RuntimeBroker_update.exe.

Relacionado: La policía interrumpe un anillo de fraude cibernético de 140M € en España

Sin embargo, si la víctima abre ese ejecutable inicial mencionado anteriormente, el archivo también "actúa como un cuentagotas autónomo basado en Rust que extrae todos los componentes requeridos por sí mismo y luego lanza el mismo RuntimeBroker_update.exe", según la publicación del blog Seqrite. Esto le da al malware dos medios diferentes de implementación.

RuntimeBroker_update.exe carga una DLL maliciosa que ejecuta un cargador basado en Rust rastreado como "Rustcloak". El cargador descifra y ejecuta la carga útil definitiva, rastreada como "Azureveil", que es un agente de comando y control (C2) de Adaptix.

Double Whammy: Rustcloak y Azureveil Malware

Además de continuar la cadena de infección, Rustcloak es notable porque incluye la funcionalidad anti-detección y anti-análisis. La función recupera el nombre del equipo y lo compara con una lista de

más de 100 nombres conocidos de sandbox y máquina de analista; si hay una coincidencia, el cargador sale del proceso y no se activa ninguna carga útil.

Azureveil, por su parte, destaca por su componente C2, que depende de Microsoft Azure Blob Storage.

"En lugar de usar un modelo C2 tradicional basado en tirones, Azureveil sigue un enfoque de caída muerta", según la investigación. "El atacante y el sistema infectado nunca se comunican directamente. En cambio, ambas partes utilizan el mismo contenedor de almacenamiento de Azure para intercambiar datos".

Relacionado: ¡Guten Tag, Bonjour, Hola a nuestros ciberdefensores europeos!

Añadió: "El agente carga periódicamente una pequeña baliza cifrada (alrededor de 124 bytes) para indicar que está activa. El atacante coloca comandos en el mismo contenedor. Azureveil recupera estos comandos, los descifra, los ejecuta y carga los resultados de vuelta como burbujas cifradas.

Una vez que el atacante está en este punto, puede ejecutar comandos y filtrar archivos desde el sistema de destino al contenido de su corazón.

¿Qué deben hacer las organizaciones? El equipo de investigación de Seqrite le dice a Dark Reading que debido a que la Operación Dragon Weave comienza con el spear-phishing y conduce a malware convencional, las organizaciones que quieren protegerse contra estas amenazas tienen algunas opciones tecnológicas más allá de la capacitación de conciencia del usuario anti-phishing. Deben realizar evaluaciones periódicas de conciencia de seguridad sobre amenazas, vulnerabilidades, riesgos e impacto relevantes; monitorear y centralizar los registros utilizando una solución de gestión de incidentes y eventos de seguridad (SIEM); implementar EDR, XDR y defensas de monitor de integridad de archivos (FIM); monitorear la ejecución del proceso para detectar anomalías; y emplear el filtrado de correo electrónico para proteger contra mensajes maliciosos como los descritos aquí.