Por Jordan Nathaniel Fenster
CT INSIDER

El FBI emite una advertencia a los usuarios de Gmail y Outlook

Así es como se detecta el ransomware Medusa

Un grupo desconocido ha estado utilizando un ciberataque llamado "Medusa" para robar información y luego extorsionar a las víctimas, advierten funcionarios federales.

Se trata de un ataque de ransomware llamado Medusa y ha afectado a más de 300 víctimas en una amplia variedad de sectores, como la medicina, la educación, el derecho, los seguros, la tecnología y la manufactura.

Los ataques han estado ocurriendo desde 2021, según una alerta emitida la semana pasada por el Buró Federal de Investigaciones (FBI), la Agencia de Seguridad de Infraestructura y Ciberseguridad (CIA) y el Centro Multiestatal de Intercambio y Análisis de Información.

Pero parecen estar extendiéndose. Si bien anteriormente los ciberataques se atribuían a un solo grupo de "actores de amenazas" que desarrollaron el software, ahora se han expandido utilizando un "modelo de afiliación", aunque "operaciones importantes como la negociación de rescates aún están controladas centralmente por los desarrolladores", según el aviso.

Aquí tiene todo lo que necesita saber sobre el ataque de ransomware Medusa:

¿Cómo funciona Medusa?

Quizás comience con un correo electrónico o un mensaje de texto. Parece legítimo, pero en realidad se trata de una estafa llamada "phishing", en la que los estafadores roban la información del usuario, a menudo contraseñas y nombres de usuario, además de otros datos.

Según investigadores federales, quienes están detrás de los ataques de ransomware Medusa compran esas credenciales en la dark web, "en foros y mercados de cibercriminales".

Luego, ejecutan un ataque de dos pasos. Primero, cifran un sistema y comparten públicamente una muestra de la información robada. Después, envían una nota de rescate electrónicamente a través de un sitio web imposible de rastrear.

"La nota de rescate exige que las víctimas se pongan en contacto en un plazo de 48 horas", decía la alerta de CISA. "A menudo, si la víctima no responde a la nota de rescate, los actores de Medusa se ponen en contacto con ella directamente por teléfono o correo electrónico".

Las exigencias de rescate se publican en un sitio web, con enlaces directos a monederos de criptomonedas. Simultáneamente, la información se pone a la venta. "Las víctimas pueden pagar adicionalmente $10,000 en criptomonedas para añadir un día a la cuenta regresiva", decía la alerta, aunque a menudo la cosa no termina ahí. "Las investigaciones del FBI identificaron que, tras pagar el rescate, una víctima fue contactada por otro agente de Medusa, quien alegó que el negociador había robado el monto del rescate ya pagado y solicitó que se reembolsara la mitad del pago para proporcionar el 'descifrador real', lo que podría indicar un triple esquema de extorsión".

¿Ha ocurrido esto en Connecticut?

La ley estatal de Connecticut exige que cualquier empresa que recopile información personal de sus clientes informe sobre ciberataques, y los datos muestran numerosos casos de ataques de ransomware similares que involucran a organizaciones en Connecticut.

En total, se han reportado 2,278 ataques de ransomware a la Fiscalía General del estado desde agosto de 2021, 151 desde principios de año.

El número de ataques de ransomware reportados en Connecticut parece estar aumentando. Se reportaron 861 en 2024, en comparación con los 644 de 2023 y los 562 de 2022. Entre agosto de 2021, cuando el estado comenzó a recopilar datos, y finales de ese año, se reportaron relativamente pocos ataques de ransomware: 60.

En 2022, los sitios web de 5000 escuelas públicas dejaron de funcionar cuando FinalSite, con sede en Glastonbury y proveedor de servicios web para escuelas, fue víctima de un ataque de ransomware.

Los servicios ambulatorios de dos hospitales de Connecticut, propiedad de Prospect Medical Holdings, fueron cerrados tras un ataque de ransomware en 2023.

Xerox, con sede en Norwalk, sufrió un ataque de ransomware en diciembre de 2023, y Subway, con sede en Connecticut, sufrió un ataque similar un mes después.

¿Quién está detrás de estos ataques?

Las autoridades federales no identificaron a ninguna persona o grupo investigado por los ataques de ransomware Medusa.

Sin embargo, Symantec, desarrollador de ciberseguridad, afirmó que un grupo llamado Spearwing está detrás de los ataques y que hasta el momento ha habido más de 400 víctimas. Spearwing ha exigido rescates de entre 100.000 y 15 millones de dólares.

Quienquiera que esté detrás de la variante del ransomware Medusa, no es el único. Se dice que un grupo llamado LockBit estuvo detrás del ataque de ransomware Subway, y un grupo llamado Inc Ransom se atribuyó el ataque a Xerox.

¿Cómo puede protegerse?

Cualquier persona es vulnerable a un ciberataque, pero las grandes organizaciones, desde municipios hasta cadenas de sándwiches, parecen ser los objetivos más comunes de los ataques de ransomware. Si usted o su organización han sido víctimas de un ciberataque de cualquier tipo, denúncielo a la Fiscalía General del estado.

El FBI y la CISA mantienen una guía sobre cómo detener el ransomware, desarrollada por el Grupo de Trabajo Conjunto contra el Ransomware.

La guía sugiere que las personas u organizaciones preparen un plan para esta eventualidad y conserven múltiples copias de datos y servidores confidenciales o de propiedad exclusiva en una ubicación físicamente separada, segmentada y segura, como un disco duro independiente.

Todos los empleados deben usar contraseñas largas y usar autenticación multifactor, especialmente para correo web, redes privadas virtuales y cualquier cuenta y sistema crítico.

Todos los sistemas operativos, software y software de seguridad deben mantenerse actualizados, y las organizaciones deben considerar realizar copias de seguridad de los datos sin conexión con copias de seguridad programadas regularmente.