Los perpetradores vinculados al ransomware Medusa han intensificado sus operaciones tras el lanzamiento de un sitio exclusivo en la dark web en febrero de 2023 para divulgar datos sensibles de víctimas que se niegan a cumplir con sus exigencias.

> *«Como parte de su estrategia de multiextorsión, este grupo ofrece a las víctimas diversas opciones cuando sus datos aparecen en su sitio de filtración, como una prórroga de tiempo, eliminación de datos o descarga de toda la información»,* informaron los investigadores Anthony Galiette y Doel Santos de Palo Alto Networks Unit 42 en un informe compartido con The Hacker News.
>
> *«Todas estas opciones tienen un costo, dependiendo de la organización afectada por este grupo».*

Medusa (no debe confundirse con Medusa Locker) se refiere a una familia de ransomware que surgió a finales de 2022 antes de destacar en 2023. Se caracteriza por dirigirse de manera oportunista a diversas industrias como alta tecnología, educación, manufactura, salud y comercio minorista.

Se estima que hasta 74 organizaciones, principalmente en Estados Unidos, Reino Unido, Francia, Italia, España e India, fueron impactadas por el ransomware en 2023.

Los ataques de ransomware ejecutados por este grupo comienzan con la explotación de activos o aplicaciones expuestas en internet con vulnerabilidades conocidas y sin parches, además del secuestro de cuentas legítimas, a menudo con intermediarios de acceso inicial para establecer un punto de apoyo en las redes objetivo.

En una instancia observada por la firma de ciberseguridad, se explotó un servidor Microsoft Exchange para cargar una shell web, que luego se utilizó como conducto para instalar y ejecutar el software de monitoreo y gestión remota de ConnectWise.

Un aspecto destacado de estas infecciones es la dependencia de técnicas de *«living-off-the-land»* (LotL) para mezclarse con actividades legítimas y evadir la detección. También se observa el uso de un par de controladores de kernel para desactivar una lista predefinida de productos de seguridad.

La fase inicial de acceso es seguida por el descubrimiento y reconocimiento de la red comprometida, con los perpetradores finalmente lanzando el ransomware para enumerar y cifrar todos los archivos, a excepción de aquellos con extensiones como .dll, .exe, .lnk y .medusa (la extensión asignada a los archivos cifrados).

En el sitio de filtración de Medusa, se muestra información sobre las organizaciones afectadas, el rescate exigido, el tiempo restante antes de que los datos robados se publiquen públicamente y el número de visualizaciones, con la intención de ejercer presión sobre la empresa.

Los perpetradores también ofrecen diversas opciones a la víctima, todas las cuales implican algún tipo de extorsión para eliminar o descargar los datos robados y buscar una prórroga de tiempo para evitar la publicación de los datos.

A medida que el ransomware sigue siendo una amenaza desenfrenada, dirigida a empresas tecnológicas, atención médica, infraestructura crítica y más, los actores detrás de estas acciones están adoptando tácticas más audaces, yendo más allá de la mera exposición pública de organizaciones al recurrir a amenazas de violencia física e incluso estableciendo canales de relaciones públicas dedicados.

«El ransomware ha cambiado muchos aspectos del panorama de amenazas, pero un desarrollo clave reciente es su creciente comercialización y profesionalización», afirmaron los investigadores de Sophos el mes pasado, calificando a las bandas de ransomware de *«cada vez más hábiles en los medios».*

Según la Unit 42, Medusa no solo cuenta probablemente con un equipo de relaciones públicas para manejar sus esfuerzos de marca, sino que también aprovecha un canal público

de Telegram llamado *«información de soporte»,* donde se comparten archivos de organizaciones afectadas y se puede acceder a través de la clearnet. El canal fue establecido en julio de 2021.

> *«La aparición del ransomware Medusa a finales de 2022 y su notoriedad en 2023 marca un desarrollo significativo en el panorama del ransomware. Esta operación demuestra métodos complejos de propagación, aprovechando tanto las vulnerabilidades del sistema como los intermediarios de acceso inicial, y eludiendo hábilmente la detección mediante técnicas 'living-off-the-land»*, dijeron los investigadores.

Este desarrollo surge cuando Arctic Wolf Labs hizo públicos dos casos en los que las víctimas de las bandas de ransomware Akira y Royal fueron blanco de terceros maliciosos que se hacían pasar por investigadores de seguridad para intentos secundarios de extorsión.

> *«Los actores de amenazas crearon una narrativa de tratar de ayudar a las organizaciones víctimas, ofreciéndose a hackear la infraestructura del servidor de los grupos de ransomware originales involucrados para eliminar los datos sustraídos»*, dijeron los investigadores de seguridad Stefan Hostetler y Steven Campbell, señalando que el actor de amenazas solicitaba aproximadamente 5 bitcoins a cambio del servicio.

También sigue a un nuevo aviso del Centro Nacional de Ciberseguridad de Finlandia (NCSC-FI) sobre un aumento en los incidentes de ransomware Akira en el país hacia finales de 2023, explotando una falla de seguridad en los dispositivos VPN de Cisco (CVE-2023-20269, puntuación CVSS: 5.0) para violar entidades domésticas.