Ransomware Medusa

Informe de Investigación

Un poco de historia

Medusa, un servicio de ransomware (RaaS) que surgió a finales de 2022, cobrando notoriedad en 2023 al enfocarse en entornos Windows. MedusaLocker, la variante predecesora, apareció en septiembre de 2019, ambos son tipos de ransomware que cifra los archivos de la víctima y exigen un rescate para descifrarlos.

Medusa ha afectado a más de 74 organizaciones globalmente en 2023, incluyendo empresas de alta tecnología, educación, fabricación y telecomunicaciones. Notable también en Latinoamérica, incluyendo casos relevantes como el ataque masivo en Colombia en septiembre de 2023, la Comisión Nacional de Valores de Argentina atacada en noviembre de 2023, y en Venezuela, un presunto ataque a una empresa de telecomunicaciones.

DE USO PÚBLICO

El ransomware Medusa es una amenaza reciente y más peligrosa que MedusaLocker, ya que se propaga principalmente a través de correos electrónicos maliciosos.

El Ransomware Medusa es una amenaza en constante evolución que afecta a organizaciones de todo el mundo. Esta investigación tiene como objetivo comprender sus características, impacto y estrategias de prevención.

Medusa es un software malicioso que secuestra los archivos de un usuario y exige un pago para descifrarlos. Especialmente peligroso porque utiliza un algoritmo de cifrado muy fuerte(AES-256) que hace prácticamente imposible descifrar los archivos sin la clave correcta.

Además, Medusa tiene la capacidad de infectar otros dispositivos conectados a la misma red, como discos duros externos, memorias USB o servidores. Por otro lado, Medusa no se comunica con ningún servidor externo para enviar la clave de cifrado, sino que la almacena localmente en el ordenador infectado, lo que dificulta su rastreo por parte de las autoridades.

Comportamiento del Ransomware Medusa

El ransomware Medusa se infiltra en los sistemas a través de diversos métodos, como correos electrónicos fraudulentos (phishing), correos electrónicos con archivos adjuntos maliciosos infectados o enlaces de una página web infectada. Al abrir el archivo o el enlace, el ransomware se ejecuta y comienza a cifrar los archivos del sistema, incluyendo documentos, imágenes, vídeos, entre otros.

Explotación de Vulnerabilidades: Los piratas informáticos pueden aprovechar las vulnerabilidades de software sin actualizar para obtener acceso a los sistemas y secuestrar cuentas legítimas.

Ataques de Fuerza Bruta: Se pueden usar ataques de fuerza bruta para descifrar contraseñas débiles y obtener acceso a los sistemas. Tras la infección, Medusa cifra los archivos y muestra una nota de rescate en la pantalla del usuario, esta nota exige un pago generalmente en criptomoneda, a cambio de la clave de descifrado. También incluye un temporizador que indica el tiempo límite para realizar el pago, y amenaza con borrar todos los archivos o aumentar el precio del rescate si no se cumple.

Como afecta el Ransomware Medusa

Los tipos de archivos que afecta Medusa puede encriptar una amplia gama de archivos, incluyendo:

- **Documentos:** Archivos de Word, Excel, PowerPoint, PDF.
- **Imágenes:** JPEG, PNG, GIF.
- **Vídeos:** MP4, AVI, MOV.
- **Archivos de audio:** MP3, WAV.
- **Bases de datos:** SQL,MySQL.

Dentro de esta afectación, también se incluye lo siguiente:

- **Pérdida de acceso a datos:** archivos importantes, documentos y sistemas informáticos.
- **Interrupción del negocio:** pérdida de productividad, ingresos y oportunidades.
- **Daño a la reputación:** Pérdida de confianza por parte de clientes, socios e inversores.

El ransomware también se encarga de eliminar las copias de seguridad y los puntos de restauración, para así dificultar la recuperación de los datos.

Ejecución y comportamiento del Ransomware en Windows

Una vez dentro del sistema, el ransomware se ejecuta y comienza a cifrar los archivos.

- **Booteo en modo seguro:** Medusa puede iniciar el sistema en modo seguro antes de ejecutarse para evitar la detección y eliminación por parte del software de seguridad.
- **Uso de archivos BAT y PowerShell:** se pueden utilizar archivos BAT y scripts de PowerShell para automatizar el proceso de cifrado.
- **Eliminación de instantáneas y copias de seguridad**: Medusa puede eliminar las instantáneas de volumen y las copias de seguridad del sistema para dificultar la recuperación de archivos.

Actividades de Grupo Ransomware Medusa

El blog de Medusa, creado en 2023, marca un cambio en las tácticas de extorsión del grupo. Esta plataforma es utilizada por los perpetradores para revelar datos confidenciales de las víctimas que no están dispuestas a acceder a sus demandas de rescate.

El canal de Telegram utilizado por Medusa se titula "soporte de información" y se utiliza para dar a conocer y publicar datos filtrados por el grupo.

El canal de Telegram se creó en julio de 2021 y contiene algunos contenidos anteriores a la aparición de este grupo que se basan en infracciones públicas conocidas. Inesperadamente, el canal no tiene la marca Medusa ransomware, aún así, observamos publicaciones en este canal que filtran contenido relacionado con los compromisos de Medusa e incluso afirmaciones de reunirse con representantes de este grupo de amenazas.

Por otro lado, el enlace a X simplemente lleva a una página de resultados de búsqueda de "Medusa ransomware".

Descubrimiento del Ransomware Medusa

Descubrimiento por parte de los investigadores de Unit 42 observaron que los actores del ransomware Medusa utilizaban la versión portátil de Netscan, con un giro novedoso.

Un archivo de netscan.xml asociado se combinó con un software que reforzó la funcionalidad general desde el primer momento. Esto Incluyó varios tipos de detección de servicios remotos y asignaciones preconfiguradas para acciones como PsExec, así como la implementación del binario del ransomware.

Hay muchas opciones disponibles en la configuración personalizada relacionada con lo siguiente: WMI, Registro, Servicios, Archivos, SNMP, XML, SSH, PowerShell.

Las funciones de secuencias de comandos remotas amplían las capacidades de la herramienta con VBScript y JScript. Los scripts remotos que se incluyen utilizan el alfabeto cirílico.

El ransomware utiliza el cifrado asimétrico RSA para proteger la clave AES256 utilizada para cifrar los archivos de la víctima. La clave AES256 se configura mediante una clave de 32 bytes y un vector de inicialización de 16 bytes.

Los archivos cifrados se renombran con la extensión .medusa.

Durante la enumeración y el cifrado de archivos, el ejemplo evita los archivos con las siguientes extensiones:

- .Dll
- .exe
- .lnk
- .Medusa

La lista de rutas de carpeta que se deben omitir es la siguiente:

- \Windows\
- \Windows.old\
- \PerfLogs\
- \MSOCache\
- G_skp_dir
- Archivos de programa
- Archivos de programa (x86)
- Datos del programa.
- La nota de rescate ¨read_me_medusa. Txt¨

Protegerse del Ransomware Medusa

La mejor forma de protegerse contra Medusa y otros tipos de ransomware es seguir unas buenas prácticas de seguridad informática, como lo es:

- No abrir archivos adjuntos o enlaces sospechosos que lleguen por correo electrónico o por otros medios.
- Mantener actualizado el sistema operativo y los programas instalados,especialmente los antivirus y los cortafuegos.
- Realizar copias de seguridad periódicas de los archivos importantes y guardarlas en un lugar seguro y desconectado de la red.
- No pagar el rescate si se sufre un ataque de ransomware, ya que no hay garantía de que se recupere el acceso a los archivos y se puede fomentar la actividad.

Referencias Bibliográficas

- https://unit42.paloaltonetworks.com/medusa-ransomware-escalation-new-leak-site/
- https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-181a
- https://www.techradar.com/news/the-medusa-ransomware-group-is-getting-serious

Informe de Investigación

Elaborado por:

Esp. Daniela Ruíz

Esp. Elvin Vargas

Esp. Jefferson Díaz

WWW.SUSCERTE.GOB.VE

INCIDENTES.VENCERT@SUSCERTE.GOB.VE

DE USO PÚBLICO