I. DATOS GENERALES:

Clase de alerta: Malware

Tipo de incidente: Ransomware

Nivel de riesgo: Alto

II. ALERTA

En marzo de 2023, una operación de ransomware conocida como Medusa comenzó a cobrar fuerza, apuntando a víctimas corporativas en todo el mundo con demandas de rescate. La operación Medusa comenzó en junio de 2021 teniendo una actividad relativamente baja, con pocas víctimas. Sin embargo, en 2023, se aumentó su actividad y se lanzó un 'Blog de Medusa' que se utiliza para filtrar los datos de las víctimas que se niegan a pagar un rescate.

Figura No. 1.- Ilustración asociada a Medusa
Fuente: https://www.bleepingcomputer.com/

III. INTRODUCCIÓN

Medusa ganó la atención de los medios, este 2023, después de que se atribuyó la responsabilidad de un ataque en el distrito de las Escuelas Públicas de Minneapolis (MPS) y compartió un video de los datos robados.

Existen varias familias de malware que se hacen llamar Medusa, incluida una botnet basada en Mirai con capacidades de ransomware, un malware de Android Medusa y MedusaLocker; sin embargo, no son lo mismo. MedusaLocker se lanzó en 2019 como Ransomware-as-a-Service, usaba una nota de rescate comúnmente llamada How_to_back_files.html y una amplia variedad de extensiones de archivo para archivos cifrados.

La operación de ransomware Medusa se lanzó alrededor de junio de 2021 y ha estado usando una nota de rescate llamada ***!!!READ_ME_MEDUSA!!!.txt*** y una extensión de archivo cifrado ***.MEDUSA***.

IV. VECTOR DE ATAQUE:

No se indica.

V. IMPACTO:

Un ransomware que infecte una computadora personal o los equipos informáticos de una institución; compromete totalmente la integridad, confidencialidad y disponibilidad de la información; dando lugar a situaciones como:

- Información expuesta podría revelar prácticas comerciales; así mismo documentos relacionados con propiedad intelectual.
- Pérdida temporal y posiblemente permanente de datos de la empresa.
- Posible cierre de las operaciones de la empresa y la consiguiente pérdida de ingresos.
- Daño a la reputación de la empresa.
- Posibles adquisiciones de cuentas.
- Los delincuentes podrían utilizar datos personales como el nombre, la fecha de nacimiento, la dirección, etc., junto con la ingeniería social y el robo de identidad.

VI. INDICADORES DE COMPROMISO

Solo ha podido analizar el encriptador Medusa para Windows, y no se conoce si se tienen uno para Linux (Abrams, L).

El cifrador de Windows acepta opciones por línea de comandos que permiten al atacante configurar cómo se cifrarán los archivos en el dispositivo.

```
# Command Line
Option  | Description
--------------------
-V      | Get version
-d      | Do not delete self
-f      | Exclude system folder
-i      | In path
-k      | Key file path
-n      | Use network
-p      | Do not preprocess (preprocess = kill services and shadow copies)
-s      | Exclude system drive
-t      | Note file path
-v      | Show console window
-w      | Initial run powershell path (powershell -executionpolicy bypass -File %
s)
```

Figura No. 2.- Opciones de ejecución de Medusa
Fuente: https://www.bleepingcomputer.com/

Este ransomware elimina los puntos de restauración de Windows y copias de seguridad para evitar que se utilicen para recuperar los archivos. Al cifrar archivos, el ransomware agrega la extensión ***.MEDUSA*** a los nombres de archivos cifrados.

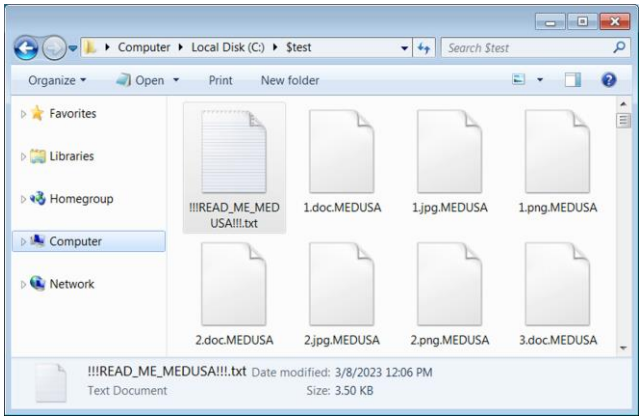

Figura No. 3.- Archivos cifrados por Medusa Ransomware
Fuente: https://www.bleepingcomputer.com/

En cada carpeta, el ransomware crea una nota de rescate denominada ***!!!READ_ME_MEDUSA!!!.txt*** que contiene información sobre lo que sucedió con los archivos de la víctima.

La nota de rescate también incluye información de contacto, un sitio de Tor donde se muestra la información robada, un sitio de negociación de Tor, un canal de Telegram, una identificación de Tox y la dirección de correo electrónico key.medusa.serviceteam@protonmail.com.

Cuando se agrega una víctima a la fuga de datos, sus datos no se publican de inmediato, el atacante les dan a las víctimas opciones de pago para extender la cuenta regresiva antes de que se publiquen los datos, eliminar los datos o descargar todos los datos. Cada una de estas opciones tiene diferentes precios, como se muestra a continuación.

Figura No. 4.- Opciones de pago Ransomware
Fuente: https://www.bleepingcomputer.com/

Hasta la fecha no se conoce alguna debilidad en el cifrado de Medusa Ransomware, para recuperar los archivos de forma gratuita, los investigadores continúan analizando el cifrador.

VII. RECOMENDACIONES:

El EcuCERT recomienda a su comunidad objetivo:

- En el caso de que la Organización/Institución se vea afectada por un ransomware, lo más importante es NO PAGAR el rescate.
- Realizar copias de respaldo de seguridad periódicas, de la información crítica para evitar la pérdida de la misma.
- No abrir, manipular, o interactuar, con correos electrónicos sospechosos que lleguen a las bandejas de correo o mensaje en redes sociales.
- Otorgar privilegios de usuario al mínimo dependiendo del tipo de labor a realizar.
- Implementar técnicas de navegación segura en toda la Institución/Organización, como por ejemplo visita únicamente de sitios con certificados SSL, y, de origen no sospechoso.
- Bloquear el acceso de usuarios, a dispositivos de almacenamiento externo, ajenos a la Institución/Organización, a través de políticas de seguridad adecuadas.
- Implementar y monitorear, plataformas de seguridad perimetral para identificar posible tráfico malicioso tanto a nivel interno como externo a la infraestructura de red de la organización/Institución
- Descargar programas, archivos y actualizaciones, solamente desde fuentes oficiales y verificadas.
- Cerrar todo tipo de conexión/protocolo de acceso remoto a infraestructuras críticas en la Organización/Institución, en el caso de requerir su implementación, realizarlo bajo estrictas normas de seguridad apalancados en plataformas de seguridad perimetral y, uso de una VPN.
- Tener actualizado y utilizar, un software anti-virus
- Mantener actualizados, y, bajo licenciamiento, (ya sea a nivel de software libre o de paga, de ser el caso), todos y cada uno de los sistemas y subsistemas de software y hardware de toda la infraestructura de IT y OT de la Institución, esto es, incluido a nivel de Firmware de todos los componentes.

- Capacitar a todos los usuarios, mediante la concientización y simulaciones para reconocer e informar sobre intentos de phishing e ingeniería social.
- Implementar un plan de respuesta a emergencias de la Organización/Institución.
- En el caso de que la Organización/Institución se vea afectada por un ransomware, visita los siguientes enlaces; a fin de establecer un panorama de la situación: https://www.nomoreransom.org/es/decryption-tools.html#LockFile (herramientas de des encriptado en el caso de existir) / https://id-ransomware.malwarehunterteam.com/ (identificación de tipo de Ransomware y herramienta de des encriptado en el caso de existir una)
- En el caso de sufrir un ataque, contacte a las Autoridades competentes en base a la Normativa Legal Vigente a nivel Nacional.

VIII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta; se proporciona con fines informativos.
- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

IX. REFERENCIAS:

Abrams, L. (2023, 11 marzo). *Medusa ransomware gang picks up steam as it targets companies worldwide*. BleepingComputer. https://www.bleepingcomputer.com/news/security/medusa-ransomware-gang-picks-up-steam-as-it-targets-companies-worldwide/

Toulas, B. (2023, 8 marzo). *Ransomware gang posts video of data stolen from Minneapolis schools*. BleepingComputer. https://www.bleepingcomputer.com/news/security/ransomware-gang-posts-video-of-data-stolen-from-minneapolis-schools/