Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

MEDUSA RANSOMWARE SE ATRIBUYE ATAQUE A MULTINACIONAL BIMBO

19 / 02 / 2024

CONTENIDO

INTRODUCCIÓN

Las empresas se enfrentan a un creciente desafío: una oleada de ataques cibernéticos que amenazan su seguridad y estabilidad. En medio de esta situación, el ransomware MEDUSA ha surgido como una preocupación adicional, cifrando datos y exigiendo pagos para su liberación. Este escenario subraya la urgente necesidad de fortalecer las defensas cibernéticas y tomar medidas proactivas para proteger la información sensible contra estas amenazas digitales.

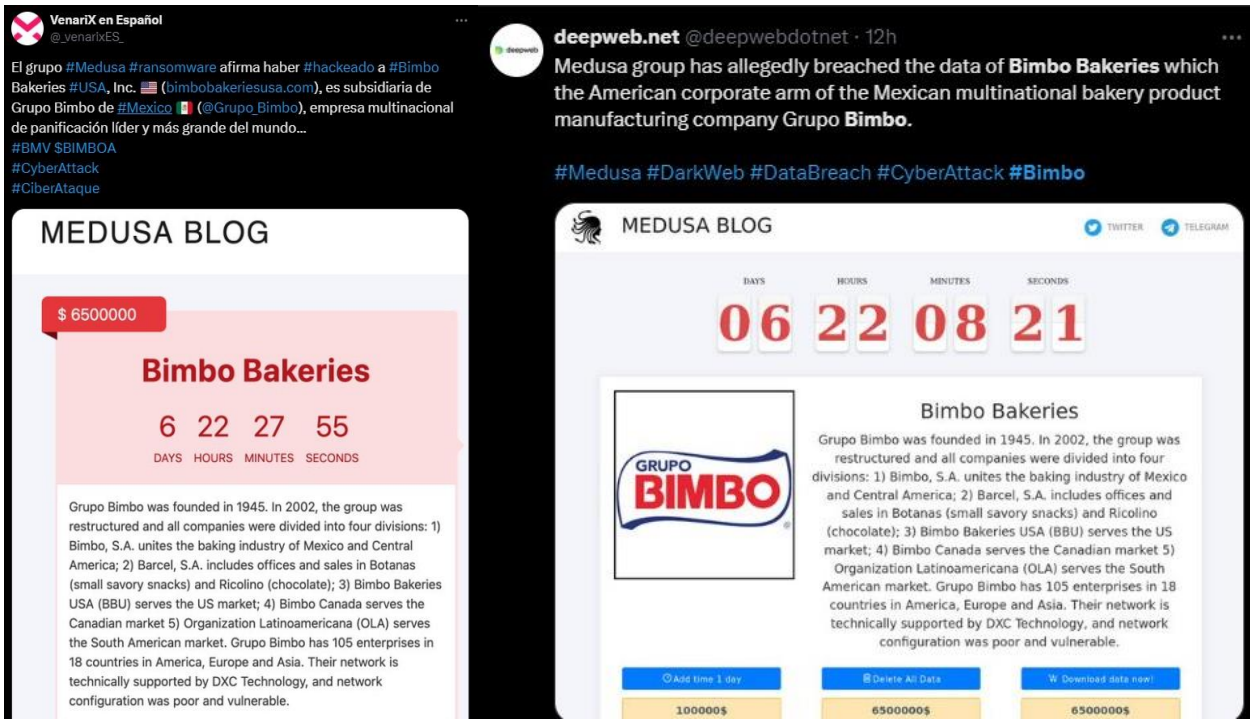
MEDUSA RANSOMWARE SE ATRIBUYE ATAQUE A MULTINACIONAL BIMBO

A continuación, se encuentra en cuadro de identificación de la amenaza.

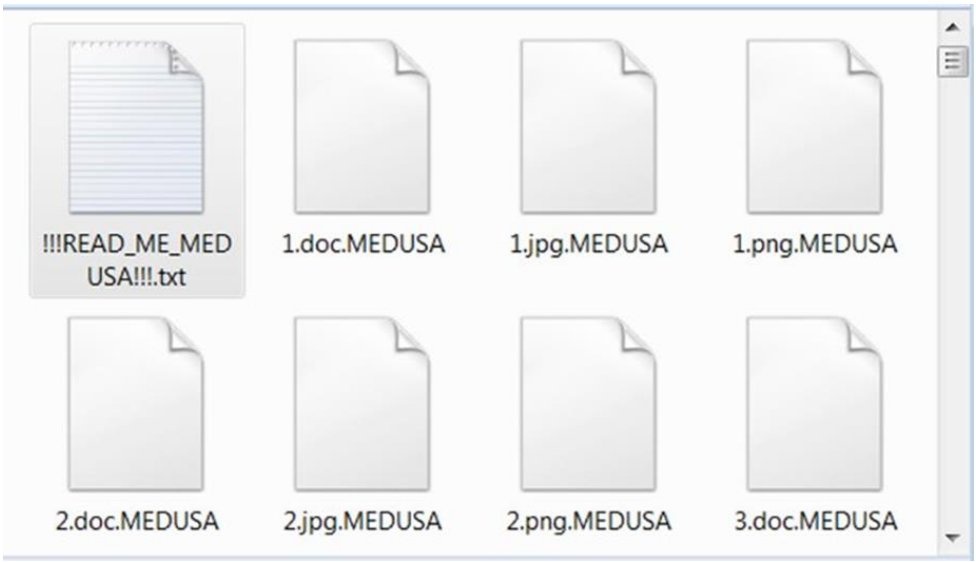
ID de alerta:	DSOC-CERT_2024_02_19_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	19/02/2024
Es día cero (0 day):	No

RESUMEN

En un reciente informe de seguridad informática, se ha confirmado que el ransomware MEDUSA es el culpable detrás del ataque dirigido a la multinacional Bimbo.



Este tipo de malware es conocido por su capacidad para cifrar los datos de los usuarios y añadir la extensión “. MEDUSA" a los nombres de archivo comprometidos



.

Una vez que los archivos han sido cifrados, MEDUSA deja una nota de rescate en la que exige un pago por una herramienta de descifrado.

> $$\ $$\ $$$$$$$$\ $$$$$$$\ $$\ $$\ $$$$$$\ $$$$$$\
> $$$\ $$$ |$$ _____|$$ __$$\ $$ | $$ |$$ __$$\ $$ __$$\
> $$$$\ $$$$ |$$ | $$ | $$ |$$ | $$ |$$ / \__|$$ / $$ |
> $$\$$\$$ $$ |$$$$$\ $$ | $$ |$$ | $$ |\$$$$$$\ $$$$$$$$ |
> $$ \$$$ $$ |$$ __| $$ | $$ |$$ | $$ | ____$$\ $$ __$$ |
> $$ |\$ /$$ |$$ | $$ | $$ |$$ |$$\ $$ |$$ | $$ |
> $$ | _/ $$ |$$$$$$$$\ $$$$$$$ |\$$$$$$ |\$$$$$$ |$$ | $$ |
> __| __|________|_______/ ______/ ______/ __| __|
> ----------[Hello, ******** !!!]----------
> WHAT HAPPEND?
> ---
> 1. We have PENETRATE your network and COPIED data.
> * We have penetrated entire network including backup system and researched all about your data.
> * And we have extracted all of your important and valuable data and copied them to private cloud storage.
> 2. We have ENCRYPTED your files.
> While you are reading this message, it means all of your files and data has been ENCRYPTED by world's strongest ransomware.
> All files have encrypted with new military-grade encryption algorithm and you can not decrypt your files.
> But don't worry, we can decrypt your files.
> There is only one possible way to get back your computers and servers - CONTACT us via LIVE CHAT and pay for the special
> MEDUSA DECRYPTOR and DECRYPTION KEYs.
> This MEDUSA DECRYPTOR will restore your entire network, This will take less than 1 business day.
>
> WHAT GUARANTEES?
> ---
> We can post your data to the public and send emails to your customers.
> We have professional OSINTs and media team for leak data to telegram, facebook, twitter channels and top news websites.
> You can suffer significant problems due disastrous consequences, leading to loss of valuable intellectual property and other sensitive information,
> costly incident response efforts, information misuse/abuse, loss of customer trust, brand and reputational damage, legal and regulatory issues.

Lo que diferencia a MEDUSA de otros ransomware es su enfoque altamente sofisticado y destructivo. Utiliza técnicas avanzadas de encriptación para bloquear el acceso a los datos de manera efectiva, lo que dificulta enormemente su recuperación sin la clave de descifrado correspondiente. Además, el ransomware MEDUSA ha sido diseñado para borrar copias de seguridad y someter a los usuarios a una presión adicional al amenazar con la divulgación de datos si no se realiza el pago del rescate dentro de un período de tiempo específico.

Una característica preocupante de MEDUSA es su capacidad para infiltrarse en los sistemas de manera sigilosa, aprovechando vulnerabilidades en el software o utilizando técnicas de ingeniería social para engañar a los usuarios y obtener acceso no autorizado. Una vez dentro del sistema, el ransomware se

propaga rápidamente a través de la red, cifrando archivos en múltiples dispositivos y dejando a la organización afectada en un estado de parálisis.

La nota de rescate dejada por MEDUSA suele contener instrucciones detalladas sobre cómo realizar el pago del rescate, junto con advertencias sobre las consecuencias de no cumplir con las demandas del atacante. Además, se han reportado casos en los que los atacantes han utilizado tácticas de intimidación, amenazando con publicar los datos robados si no se realiza el pago del rescate.

Ante la creciente amenaza de ransomware como MEDUSA, es fundamental que las organizaciones refuercen sus medidas de seguridad cibernética. Esto incluye la implementación de soluciones de seguridad avanzadas, la capacitación de los empleados en ciberseguridad y la creación de protocolos de respuesta ante incidentes para mitigar el impacto en caso de un ataque. La colaboración con expertos en seguridad informática y el intercambio de información sobre amenazas también son clave para mantenerse un paso adelante de los ciberdelincuentes y proteger los activos digitales de la empresa.

INDICADORES DE COMPROMISO

https://github.com/develgroup/SOC_IOCs/tree/main/20220630_01_MedusaLocker-Ransomware

NOTICIA COMPLETA

https://devel.group/blog/medusa-ransomware-se-atribuye-ataque-a-multinacional-bimbo/

CONTACTOS DE SOPORTE

Correo electrónico: cert@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://www.devel.group/reporta-un-incidente