Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

EMPRESAS GUATEMALTECAS ENFRENTAN UNA OLEADA DE ATAQUES CIBERNÉTICOS: RANSOMWARE MEDUSA EN AUMENTO

19 / 02 / 2024

CONTENIDO

INTRODUCCIÓN

En Guatemala, 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.

EMPRESAS GUATEMALTECAS ENFRENTAN UNA OLEADA DE ATAQUES CIBERNÉTICOS: RANSOMWARE MEDUSA EN AUMENTO

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

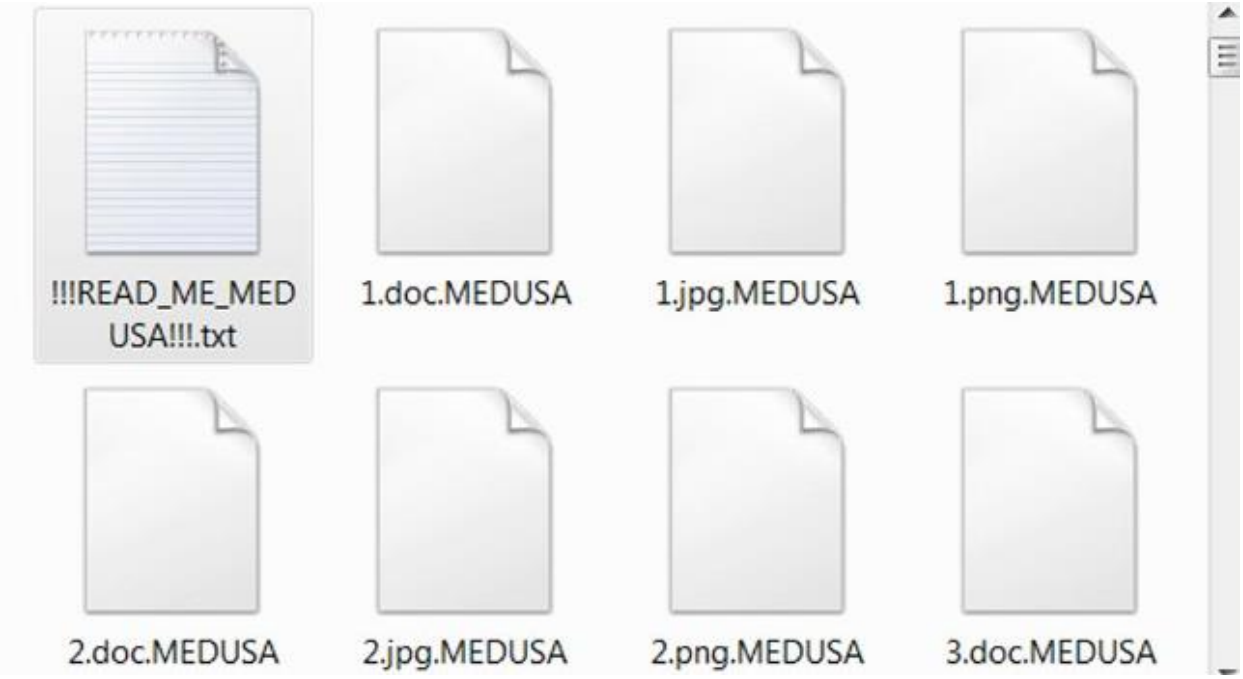
En un informe reciente, Palo Alto Networks reveló que las empresas en Guatemala están enfrentando un promedio de mil ataques a la semana, con el sector financiero siendo el principal blanco de estas acciones. Esta situación refleja el creciente desafío que enfrentan tanto las organizaciones privadas como gubernamentales para protegerse contra amenazas de seguridad en línea, incluido el ransomware.

Durante el último semestre del 2023, se registraron un total de 6,316 ataques en Guatemala, de los cuales 2,635 estuvieron dirigidos a empresas y 3,681 afectaron al sector gubernamental, según los datos recopilados por Palo Alto Networks. Este alarmante número de incidentes resalta la importancia de tomar medidas proactivas para proteger los sistemas y datos sensibles contra posibles amenazas cibernéticas.

Expertos en seguridad informática señalan que el 92% de los incidentes de seguridad tienen su origen en correo electrónicos, lo que subraya la necesidad de que las organizaciones refuercen sus medidas de seguridad en la gestión de correos electrónicos y concienticen a sus empleados sobre las mejores prácticas de ciberseguridad.

El Ransomware MEDUSA: Una Amenaza en aumento.

Además de los ataques siberneticos en general, las empresas y usuarios en Guatemala también enfrentan la amenaza del ransomware MEDUSA. Este malware cifra os datos de los usuarios y añade la extensión ." MEDUSA" a los nombres de archivo, dejando una nota de rescate que exige un pago por la herramienta de descifrado.



La nota de rescate de MEDUSA advierte que los datos han sido copiados y almacenados en una nube privada, y amenaza con hacer públicos los datos si no se paga el rescate en tres días. Este tipo de

ransomware representa una amenaza grave para la seguridad de los datos y la privacidad de los usuarios en Guatemala y todo el mundo.

> $$\ $$\ $$$$$$$$\ $$$$$$$\ $$\ $$\ $$$$$$\ $$$$$$\
> $$$\ $$$ |$$ _____|$$ __$$\ $$ | $$ |$$ __$$\ $$ __$$\
> $$$$\ $$$$ |$$ | $$ | $$ |$$ | $$ |$$ / \__|$$ / $$ |
> $$\$$\$$ $$ |$$$$$\ $$ | $$ |$$ | $$ |\$$$$$$\ $$$$$$$$ |
> $$ \$$$ $$ |$$ __| $$ | $$ |$$ | $$ | ____$$\ $$ __$$ |
> $$ |\$ /$$ |$$ | $$ | $$ |$$ | $$ |$$\ $$ |$$ | $$ |
> $$ | \_/ $$ |$$$$$$$$\ $$$$$$$ |\$$$$$$ |\$$$$$ |$$ | $$ |
> __| __|________|_______/ _____/ _____/ __| __|
> ----------[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.

INDICADORES DE COMPROMISO

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

NOTICIA COMPLETA

https://devel.group/blog/empresas-guatemaltecas-enfrentan-una-oleada-de-ataques-ciberneticos-ransomware-medusa-en-aumento/

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