Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

EMPRESA SONDA PUBLICADA EN FORO DE RANSOMWARE MEDUSA

04 /Abril /2023

CONTENIDO.

INTRODUCCIÓN.

Sonda es una empresa proveedora de servicios de tecnologías de información en Latinoamérica. Posee una base de clientes diversificada y un alto nivel de ingresos recurrentes. Sus actividades son desarrolladas a través de tres líneas de negocios: Servicios de TI (outsourcing, integración de sistemas, soporte, servicios profesionales, data center, BOP, utility), Aplicaciones (incluyendo implementación, soporte, mantenimiento, actualización y servicios asociados), y Plataformas (provisión de infraestructura computacional, estaciones de trabajo y equipos de almacenamiento, entre otros).

En el presente documenta se muestra la información relacionada con el incidente de Ransomware ocurrido en SONDA y la información relacionada con el grupo Medusa Locker Ransomware.

EMPRESA SONDA PUBLICADA EN FORO DE RANSOMWARE MEDUSA.

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

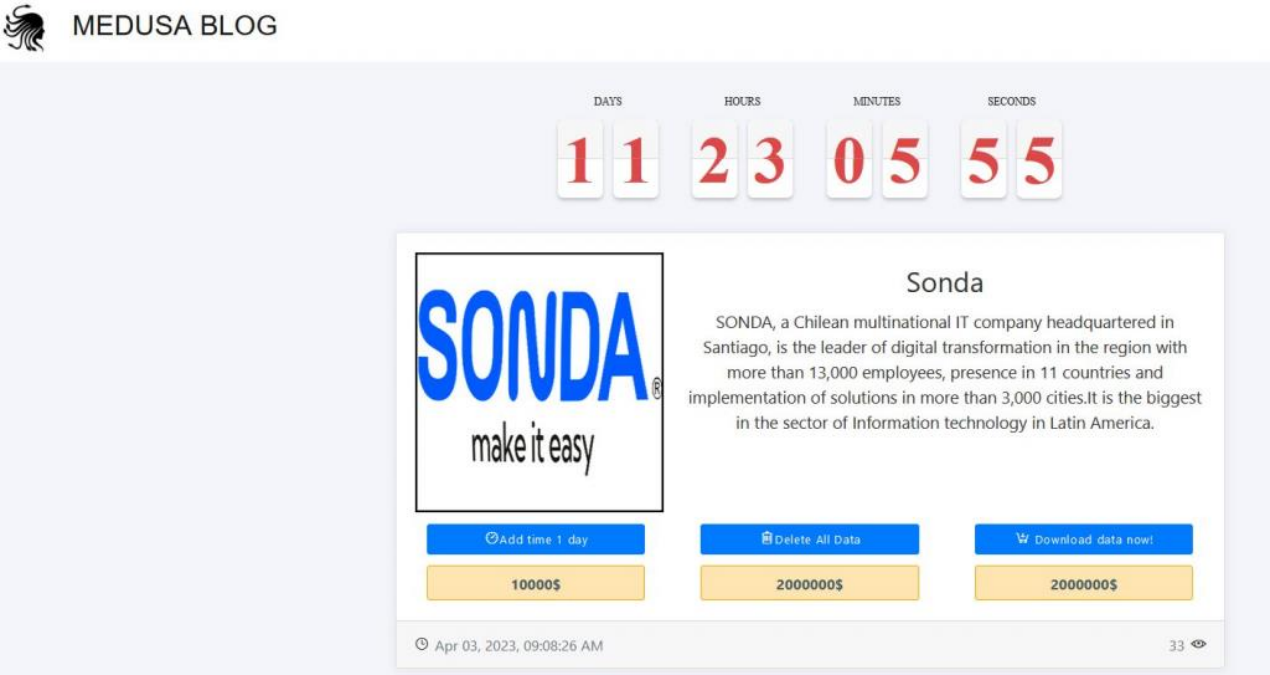
ID de alerta:	DSOC-CERT_2023_04_04_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	04/04/2023
Es día cero (0 day):	No

RESUMEN

Le empresa chilena de servicios de IT; SONDA, fue víctima de un incidente de ransomware, este hecho se lo atribuye el grupo Medusa Locker, quienes ya han lanzado un comunicado por medio de su foro.

INFORMACIÓN DEL INCIDENTE.

El lunes 03 de abril circucló en varios medios la noticia de que la empresa chilena; SONDA, había sido víctima de Ransomware, así lo confirmó el grupo de Ransomware MEDUSA LOCKER, quienes por medio de su blog anunciaron un rescate por hasta 2,000,000 USD. Dando un total de 12 días desde la fecha de publicación del anuncio para realizar el pago de la información secuestrada. Hasta el momento no hay un comunicado oficial por parte de SONDA con respecto al incidente.



RANSOMWARE MEDUSA LOCKER.

Los actores del ransomware MedusaLocker a menudo obtienen acceso a los dispositivos de las víctimas a través de configuraciones vulnerables del Protocolo de escritorio remoto (RDP) [T1133]. Los actores también utilizan con frecuencia campañas de correo electrónico no deseado y phishing por correo electrónico, adjuntando directamente el ransomware al correo electrónico, como vectores de intrusión iniciales [T1566].

El ransomware MedusaLocker utiliza un archivo por lotes para ejecutar el script de PowerShell invoke-ReflectivePEInjection[T1059.001]. Este script propaga MedusaLocker a través de la red editando el EnableLinkedConnectionsValue dentro del registro de la máquina infectada, lo que luego permite que la máquina infectada detecte hosts y redes conectados a través del Protocolo de mensajes de control de Internet (ICMP) y detecte el almacenamiento compartido a través del Protocolo de bloque de mensajes del servidor (SMB).

Procedimiento:

- Reinicia el LanmanWorkstationService, lo que permite que las ediciones del registro surtan efecto.
- Elimina los procesos de software forense, contable y de seguridad conocido.
- Reinicia la máquina en modo seguro para evitar la detección por parte del software de seguridad [T1562.009].
- Cifra los archivos de las víctimas con el algoritmo de cifrado AES-256; la clave resultante se cifra luego con una clave pública RSA-2048 [T1486].
- Se ejecuta cada 60 segundos, encriptando todos los archivos excepto aquellos críticos para la funcionalidad de la máquina de la víctima y aquellos que tienen la extensión de archivo encriptada designada.
- Establece la persistencia copiando un ejecutable (svhost.exe o svhostt.exe) en el %APPDATA%\Roaming y programando una tarea para ejecutar el ransomware cada 15 minutos.
- Intenta evitar las técnicas de recuperación estándar mediante la eliminación de copias de seguridad locales, la desactivación de las opciones de recuperación de inicio y la eliminación de instantáneas [T1490].

Los actores de MedusaLocker colocan una nota de rescate en cada carpeta que contiene un archivo con los datos cifrados de la víctima. La nota describe cómo comunicarse con los actores de MedusaLocker, por lo general proporciona a las víctimas una o más direcciones de correo electrónico en las que se puede contactar a los actores. El tamaño de las demandas de rescate de MedusaLocker parece variar según el estado financiero de la víctima según lo perciben los actores.

RECOMENDACIONES.

- Generar una regla personalizada para bloqueos de IOC's en perfiles entrantes perimetrales.
- Desconfía de los correos alarmantes. Si un mensaje le indica o incentiva a tomar decisiones apresuradas o en un tiempo limitado, probablemente se trata de phishing.
- Disponer de sistemas antispam para correos electrónicos, de esta manera se reducen las posibilidades de infección a través de campañas masivas de malspam por correo electrónico.
- Proteger el protocolo RDP:
  – Deshabilita los servicios RDP, si no es necesario.
  – La desactivación de servicios no utilizados e innecesarios ayuda a reducir su exposición a las vulnerabilidades de seguridad, y es una buena práctica de seguridad.
  – Si no es posible cerrarlos, límita las direcciones de origen que pueden acceder a los puertos.
  – Proteger el acceso a los sistemas RDP, bloqueando el sistema local en lugar del sistema remoto.
  – Incluso si el primero no tiene valor, la sesión RDP solo estará protegida limitando el acceso al sistema cliente.
  – Desconectar sesiones RDP en lugar de bloquearlas, esto invalida la sesión actual, lo que impide una reconexión automática de la sesión RDP sin credenciales.
  – Bloquear bidireccionalmente el puerto TCP 3389 utilizando un firewall o hacerlo accesible sólo a través de una VPN privada.
- Habilitar la autenticación de nivel de red (NLA).

- Tener políticas de respaldo periódico que se almacenen fuera de la red organizacional. Escanear todos los archivos adjuntos, antes de abrirlos, con un antivirus que detecte comportamientos para combatir los ransomwares.
- Mantener una buena estrategia de respaldo de información: sistemas de copias de seguridad que deben estar aisladas de la red; y políticas de seguridad. Lo anterior permitirá neutralizar el ataque, restaurar las operaciones y evitar el pago del rescate.
- Actualizar los equipos con Windows a las últimas versiones.
- Nunca seguir la instrucción de deshabilitar las funciones de seguridad, si un correo electrónico o documento lo solicita.
- Establecer políticas de seguridad en el sistema para impedir la ejecución de ficheros desde directorios comúnmente utilizados por Ransomware (App Data, Local App Data, etc.)
- Mantener listas de control de acceso para las unidades mapeadas en red restringiendo los privilegios de escritura.
  Con esto podrás identificar el impacto generado por el cifrado de archivos, entendiendo que el secuestro de información se producirá en todas las unidades de red mapeadas en el equipo víctima.
- Seguir las normativas internacionales tales como ISO 27001:2013 en su control A.7.2.2 “Concienciación con educación y capacitación en seguridad de la información” o NIST PR.AT-1: “Todos los usuarios se encuentran entrenados e informados”, a fin de tener bases para divulgar campañas educativas orientadas a nivel de usuarios respecto al correcto uso de las herramientas tecnológicas, haciendo énfasis en cómo proceder al recibir correos de orígenes desconocidos, objeto prevenir que los usuarios sean víctimas de entes maliciosos.

INDICADORES DE COMPROMISO

INDICADORES DE COMPROMISO.

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