Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

Empresa ubicada en Nicaragua es víctima de un ataque Ransomware.

01/Septiembre/2022

Contenido

Introducción

En las ultimas horas se ha reportado un ataque exitoso de Ransomware a una organización ubicada en Nicaragua, los atacantes han iniciado a publicar los archivos sin negociar con las víctimas, todo indica que es un ataque con justificaciones sociales.

RANSOMWARE EN NICARAGUA

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

ID de alerta:	DSOC-CERT_2022_09_01_01
Clasificación de alerta:	Noticia
Tipo de Impacto:	ALTO
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	09/01/2022
Es día cero (0 day):	No

RESUMEN

Un grupo de Hacktivistas han logrado infiltrarse en la infraestructura de una empresa nicaragüense que se dedica a venta de productos varios para el hogar, la intención de este grupo es hacer presión en lideres políticos de ese país.

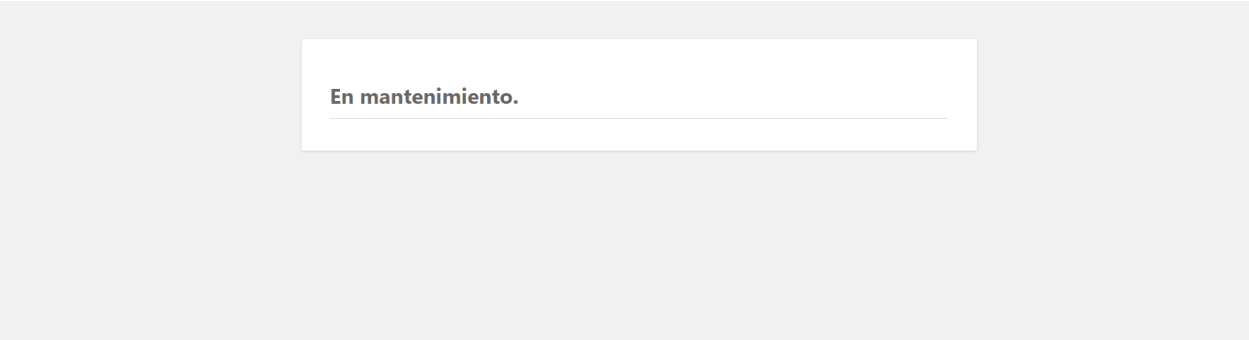
El ataque ha sucedido hoy 1 de septiembre y de forma inmediata han iniciado a publicar información obtenida de los equipos afectados mediante anonfiles y mega sin pedir rescate a los afectados.

La información filtrada incluye:

- Información personal de los empleados (foto y DNI)
- todos los recibos de transacciones (sin comprimir)
- Fotos y videos guardados en las computadoras.
- Información personal extra que los empleados manejan en esos dispositivos.

Este ataque expone de forma directa al personal y proveedores/clientes de la compañía afectada ya que por medio de la información filtrada se obtienen nombres, cuentas bancarias y demás información sensible.

El ataque ha obligado a que la compañía incluso tenga de baja su sitio web de forma temporal.



Se desconoce que método de infección fue usado, pero el grupo que ha tomado crédito de este ataque es GhostSec.

Nexos con Anonymous

GhostSec, También conocido como Ghost Security, el grupo se considera un grupo de "vigilantes" y se formó inicialmente para atacar los sitios web de ISIS que predican el extremismo islámico. Ghostsec también se conoce comúnmente como una rama de Anonymous.

RECOMENDACIONES

- Implemente un plan de recuperación que mantenga y conserve múltiples copias de datos confidenciales o de propiedad y servidores en una ubicación segura, segmentada y separada físicamente (es decir, disco duro, dispositivo de almacenamiento o la nube).

- Implemente la segmentación de la red y mantenga copias de seguridad fuera de línea de los datos para garantizar una interrupción limitada de la organización.

- Realice copias de seguridad de los datos con regularidad y proteja con contraseña las copias de seguridad almacenadas sin conexión. Asegúrese de que las copias de los datos críticos no sean accesibles para su modificación o eliminación desde el sistema donde residen los datos.

- Instale, actualice periódicamente y habilite la detección en tiempo real del software antivirus en todos los hosts.

- Instale actualizaciones para sistemas operativos, software y firmware siempre que estén disponibles y el historial de cambios no indique vulnerabilidades o bugs críticos.

- Revise los controladores de dominio, los servidores, las estaciones de trabajo y los directorios activos en busca de cuentas nuevas o no reconocidas.

- Auditar cuentas de usuario con privilegios administrativos y configurar controles de acceso según el principio de mínimo privilegio.

- Deshabilite los puertos no utilizados.

- Considere agregar un banner de correo electrónico a los correos electrónicos recibidos desde fuera de su organización.

- Hacer cumplir la autenticación multifactor (MFA).

- Considere instalar y usar una red privada virtual (VPN) para establecer conexiones remotas seguras.

- Examine el tráfico de red entrante y saliente, en busca de actividad sospechosa dentro de su red.

- Utilizar escritorio remoto solo cuando es necesario

NOTICIA COMPLETA

https://devel.group/empresa-ubicada-en-nicaragua-es-victima-de-un-ataque-ransomware/

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