Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

Ministerio de Relaciones Exteriores de Guatemala bajo ataque cibernético.

03/Octubre/2022

Contenido

Introducción

Desde el 19 de septiembre pasado el Ministerio de Relaciones Exteriores (Minex) está bajo un ataque cibernético, y desde ese entonces, empezó a reportar fallas en su sitio web.

Sin embargo, fue el 27 de septiembre del presente año, que la entidad se encuentra dentro de la lista de sitios que fueron vulnerados, entre ellos, varios subdominios y el dominio principal del Minex, aproximadamente son 49 los sitios web que fueron afectados.

Ministerio de Relaciones Exteriores bajo Ataque

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

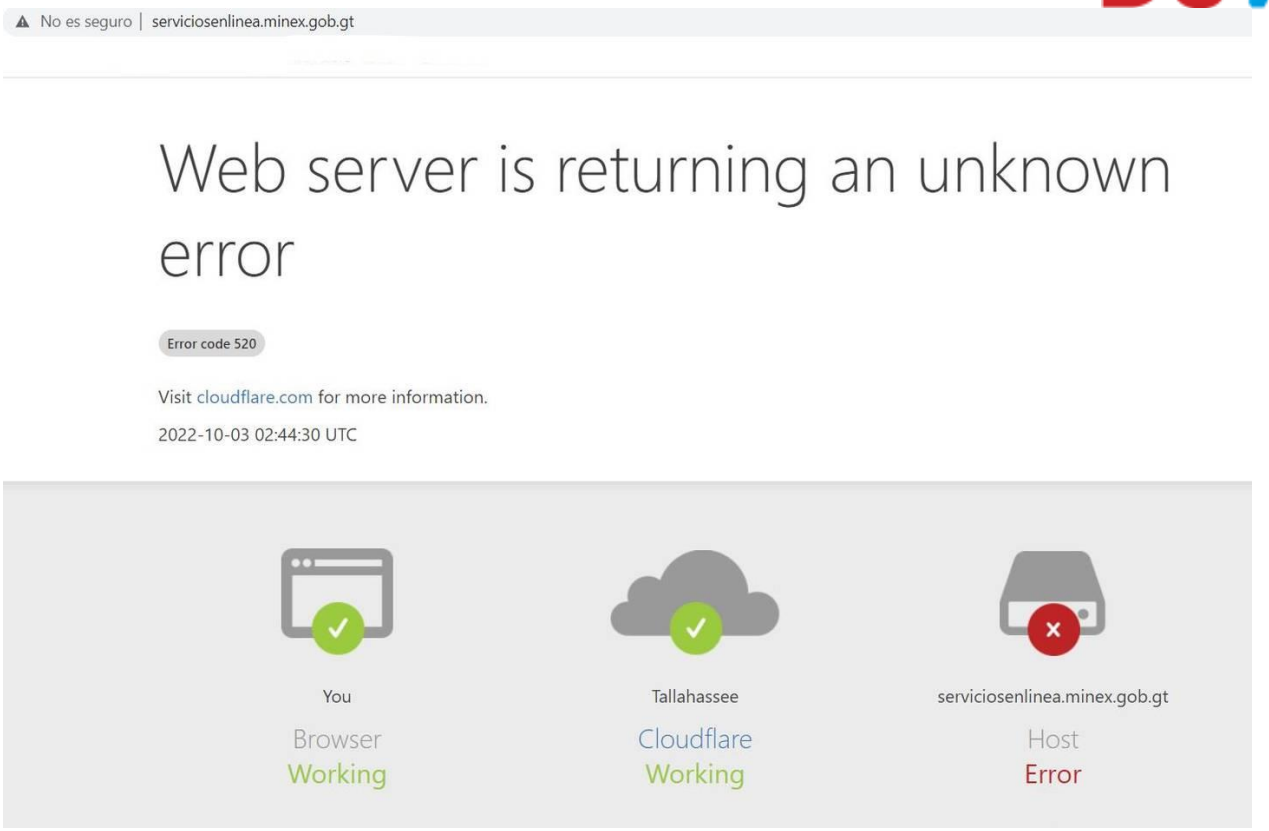
ID de alerta:	DSOC-CERT_2022_10_03_01
Clasificación de alerta:	Noticia
Tipo de Impacto:	Medio
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	03/10/2022
Es día cero (0 day):	No

Resumen

También se incluyen sitios que forman parte de los servicios que el Minex presta de forma digital, los cuales están temporalmente suspendidos debido a dicho ataque. Por ejemplo, la página serviciosenlinea.minex.gob.gt, que actualmente no está disponible para los usuarios.

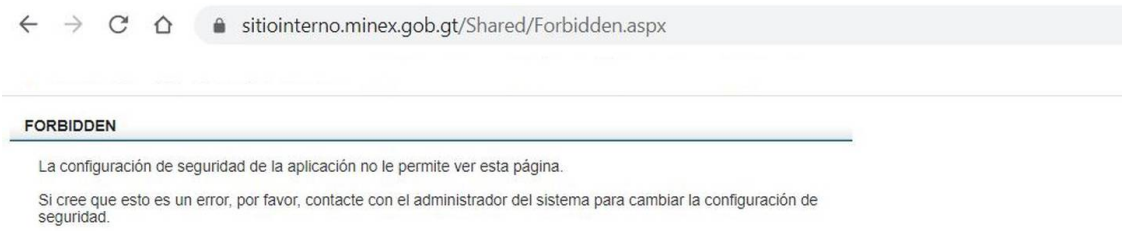
De acuerdo con la información obtenida, la entidad Cloudflare es la red encargada de la seguridad de los sitios web del Minex, ya que al momento de que un visitante se dirige a uno de sus sitios, Cloudflare analiza y autoriza o deniega la solicitud para ingresar al mismo.

Como se observa a continuación, todo parece indicar que el problema se encuentra en los servidores que hospedan los sitios y/o subdominios del Minex.



El servicio principal que ofrece Cloudflare es la protección contra ataques DDoS, que protege a un servidor que almacena una página web de solicitudes falsas que no provenga de visitantes reales, sin embargo, no es el único servicio que la empresa ofrece y no se tienen identificados los servicios que el Minex contrató con ellos.

Por otro lado, el Minex cuenta con un sitio interno que actualmente no se muestra disponible para los visitantes en la web, pero se desconoce si este sitio no está disponible porque únicamente se puede visitar a través de un acceso VPN o bien también ha sido víctima del ataque cibernético.



Ransomware Onix

El ransomware que creó la brecha de seguridad en el Minex es el llamado Onix, y es uno de los grupos más recientes que ha surgido en la escena de los ciberataques, el grupo ha generado una gran cantidad de problemas para sus víctimas, en su sitio web ya tiene seis empresas que figuran como víctimas, detalló la página Digital Recovery.

El malware del grupo no sólo ha cifrado los archivos, sino que también los ha corrompido; y está diseñado para cifrar archivos de al menos de 2 Megabytes, los archivos más grandes son destruidos e incluso después de pagar el rescate y recibir la clave de descifrado, estos archivos no se pueden recuperar.

Esta es una de las tácticas más dañinas de los últimos años, y al grupo no parece importarle su imagen ni la posibilidad de que las víctimas no paguen el rescate, el grupo es altamente destructivo.

El día 27 de septiembre pasado se confirmó que los sitios del Ministerio de Relaciones Exteriores fueron atacados por el ransomware Onix, hasta el momento, la entidad gubernamental no ha dado declaraciones respecto al impacto, exigencias y/o pagos para recuperar la información o los sitios que aún se encuentran fuera de línea.

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.

– Realizar capacitaciones de forma continua a su personal sobre detección y reporte de Phishing.

Noticia Completa

https://devel.group/blog/ministerio-de-relaciones-exteriores-sufre-ataque-de-ransomware/

Indicadores de Compromiso

https://github.com/develgroup/SOC_IOCs/tree/main/20221003_01_Onyx
https://github.com/develgroup/SOC_IOCs/tree/main/20220524_01_ChaosRansomware

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