Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

Montenegro golpeado por un ataque de ransomware, los piratas informáticos exigen $ 10 millones.

02/Septiembre/2022

Contenido

Introducción

El gobierno de Montenegro ha proporcionado más información sobre el ataque a su infraestructura crítica diciendo que el ransomware es responsable de los daños y las interrupciones.

Ransomware en Montenegro

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

ID de alerta:	DSOC-CERT_2022_09_02_01
Clasificación de alerta:	Noticia
Tipo de Impacto:	ALTO
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	09/02/2022
Es día cero (0 day):	No

Resumen

El ministro de Administraciones Públicas, Maras Dukaj, afirmó ayer en la televisión local que detrás del ataque hay un grupo organizado de ciberdelincuentes. Los efectos del incidente continúan por décimo día.

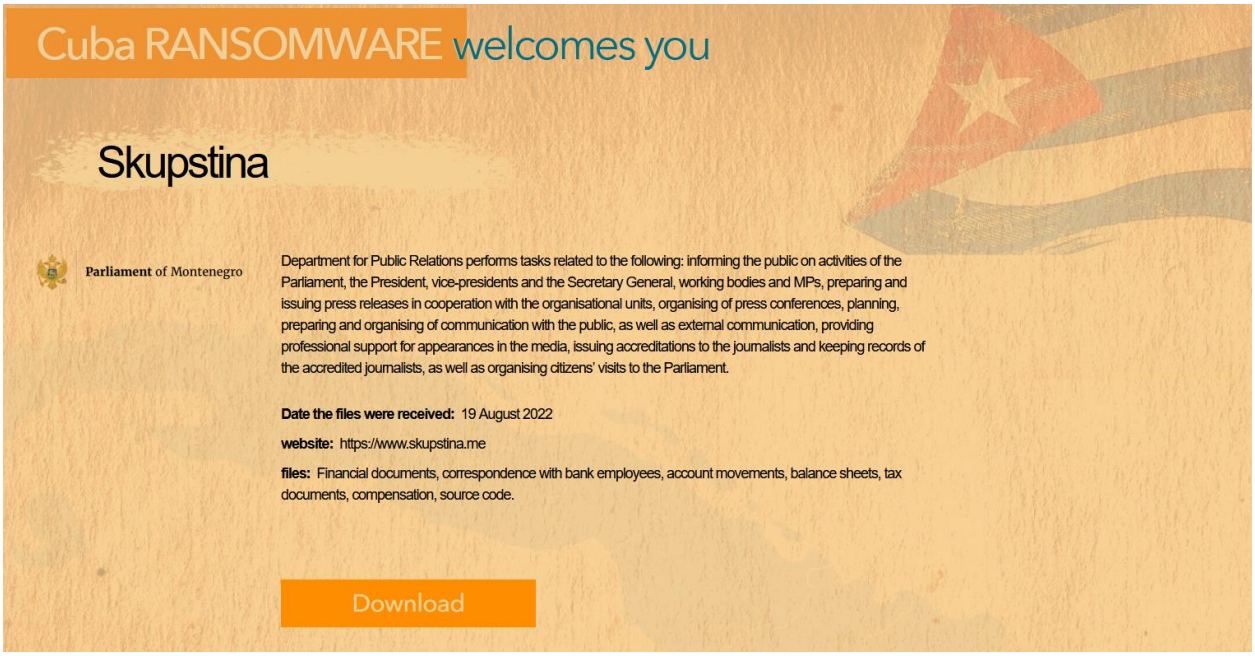
El ministro agregó que en este ataque se utiliza un "virus especial" y se pide un rescate de 10 millones de dólares. Dukaj también agregó que, en este momento, el estado no podía dar una estimación de cuándo estarán disponibles los servicios.

Falsas acusaciones y Cuba Ransomware

Previamente, el propio Dukaj, junto con el ministro de Defensa de Montenegro, dijeron a medios locales que tenían pruebas suficientes para sospechar que los ciberataques estaban dirigidos por servicios rusos .

Esto le dio al incidente un matiz geopolítico y movilizó a los aliados de la OTAN del país balcánico para ayudarlos con la respuesta al incidente, la defensa y la remediación.

Sin embargo, al día siguiente, la pandilla de ransomware Cuba incluyó al Parlamento de Montenegro (Skupstina) como su víctima y afirmó haber robado documentos financieros, correspondencia con bancos, balances, documentos fiscales, compensaciones e incluso el código fuente.



Los datos fueron publicados en la sección "gratuita" del sitio, disponible para cualquier visitante sin restricciones.

Evolución del ransomware Cuba

Cuba ransomware ha demostrado una evolución notable últimamente. Hace tres semanas, los investigadores detectaron un nuevo conjunto de herramientas utilizado por la pandilla junto con tácticas, técnicas y procedimientos nunca vistos.

En junio, el ransomware Cuba actualizó su encriptado con opciones adicionales y estableció un canal de comunicación para "apoyo a las víctimas en vivo".

Otro cambio notable se observa en el ámbito de focalización del grupo. En 2021, Cuba se centró en gran medida en las organizaciones con sede en Estados Unidos.

Se espera que el Equipo de Acción Cibernética de respuesta rápida del FBI en Montenegro ayude a lidiar con los ataques, en “otra prueba de la excelente cooperación entre los Estados Unidos de América y Montenegro”, dijo el Ministerio del Interior, Filip Adzic, en una página de Facebook , luego de reunirse con funcionarios del FBI en los Estados Unidos.

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/

Visualizar IOC

https://github.com/develgroup/SOC_IOCs/tree/main/20220816_01_CubaRansomware

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