Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

CIBERATAQUE DE RANSOMWARE AL MINISTERIO DE DESARROLLO LOCAL DE EL SALVADOR

31 / 01 / 2024

CONTENIDO

INTRODUCCIÓN....3
RESUMEN....5
INDICADORES DE COMPROMISO....7
NOTICIA COMPLETA....7
CONTACTOS DE SOPORTE....8

INTRODUCCIÓN

El Ministerio de Desarrollo Local de El Salvador ha sido blanco de un ciberataque por parte de Rhysida, un tipo de ransomware asociado con el grupo Vice Society. El ataque, que fue anunciado en el blog de Rhysida el 23 de abril de 2024, pone de manifiesto la creciente amenaza de la ciberdelincuencia en organismos gubernamentales. Los atacantes demandan 8 BTC (Bitcoin) a cambio de información comprometida, aunque no se ha confirmado si los sistemas afectados quedaron completamente inoperativos. Este incidente subraya la necesidad de que las organizaciones mantengan fuertes medidas de seguridad y protocolos de respuesta para minimizar el impacto de estos ataques.

CIBERATAQUE DE RANSOMWARE AL MINISTERIO DE DESARROLLO LOCAL DE EL SALVADOR

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

ID de alerta:	DSOC-CERT_2024_04_23_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	23/04/2024
Es día cero (0 day):	No

RESUMEN

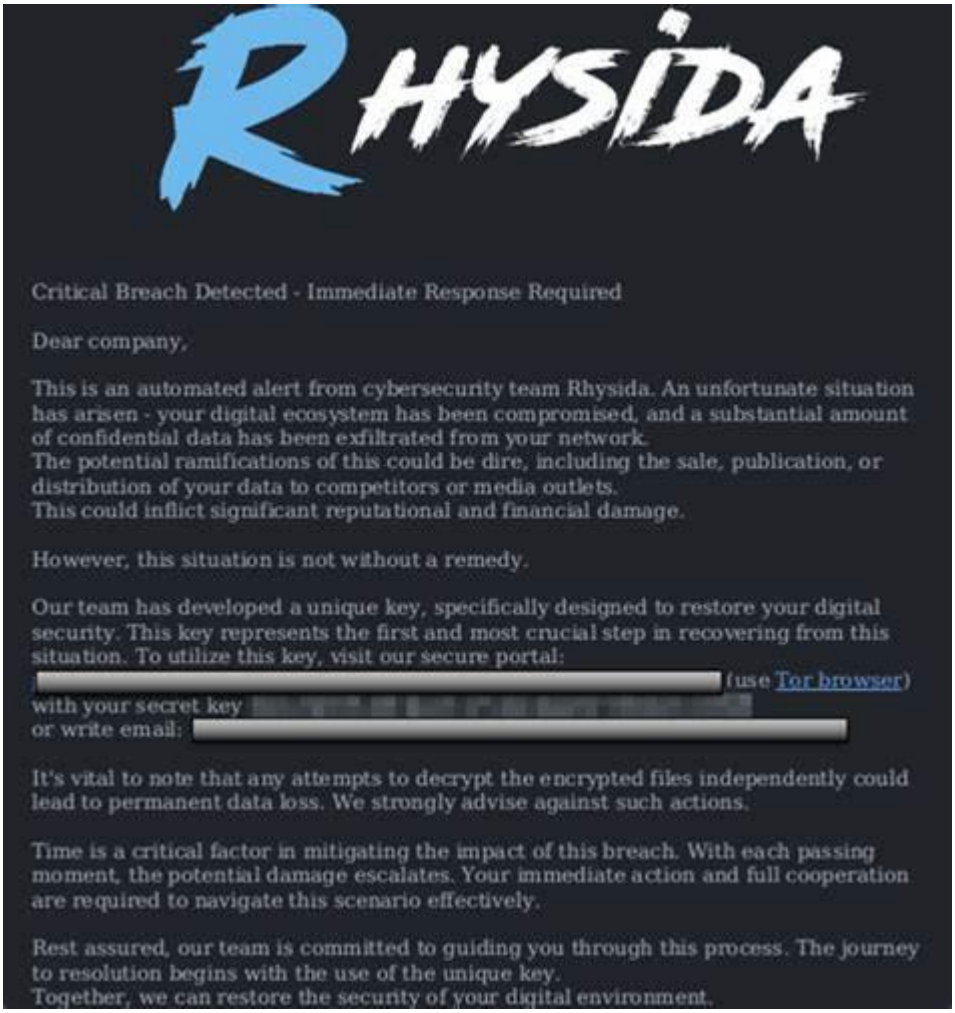
El Ministerio de Desarrollo Local de El Salvador ha sido objeto de un ciberataque de ransomware conocido como Rhysida. Este ataque fue confirmado el 23 de abril de 2024, cuando la banda de ransomware publicó sobre el altercado en su blog.

Sobre Rhysida y Su Operación

Rhysida es un ransomware asociado con el grupo conocido como Vice Society, que ha estado activo en el ámbito del cibercrimen. Este tipo de ransomware cifra datos y archivos importantes de la organización, solicitando un rescate a cambio de la clave para descifrarlos. En este caso, Rhysida está exigiendo 8 BTC (Bitcoin) por la compra de información, que es una suma considerable.

La Nota de Rescate y Sus Implicaciones

La nota de rescate de Rhysida no solo exige el pago de 8 BTC, sino que también implica posibles consecuencias si la organización atacada no cumple con el pago. Aunque no se ha confirmado una pérdida significativa de sistemas inoperativos, la amenaza de no pagar puede llevar a la divulgación pública de datos confidenciales o al daño permanente de los sistemas afectados.



Medidas de Seguridad y Prevención

Aunque el alcance completo del ataque aún no se ha confirmado, este incidente resalta la importancia de contar con medidas de seguridad cibernética robustas y de realizar copias de seguridad regulares. Las organizaciones gubernamentales y empresariales deben estar preparadas para estos tipos de ataques y tener un plan de respuesta a incidentes bien definido.

Conclusión

El ciberataque de ransomware al Ministerio de Desarrollo Local de El Salvador es un recordatorio de los riesgos cibernéticos que enfrentan las organizaciones hoy en día. Las consecuencias de no tomar medidas preventivas pueden ser costosas y dañinas para la reputación de las instituciones afectadas. Se espera que las autoridades y expertos en ciberseguridad trabajen para mitigar el impacto del ataque y evitar futuros incidentes similares.

INDICADORES DE COMPROMISO

https://github.com/develgroup/SOC_IOCs/tree/main/20240423_1_RhysidaRansomware

NOTICIA COMPLETA

https://devel.group/blog/ciberataque-de-ransomware-al-ministerio-de-desarrollo-local-de-el-salvador/

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