

CYBER **SECURITY** **NEWS**

SECURITY OPERATIONS CENTER

**SCHNEIDER ELECTRIC GOLPEADA POR RANSOMWARE
CACTUS EN SU DIVISIÓN DE SOSTENIBILIDAD**

31 / 01 / 2024

CONTENIDO

INTRODUCCIÓN	3
RESUMEN	5
INDICADORES DE COMPROMISO	6
NOTICIA COMPLETA	6
CONTACTOS DE SOPORTE	7

INTRODUCCIÓN

Schneider Electric, líder en el sector energético, enfrenta un desafío digital al ser víctima de un ataque de ransomware llamado 'Cactus' en su división de sostenibilidad. Este incidente resalta la vulnerabilidad de incluso las empresas más grandes frente a las amenazas cibernéticas. La resiliencia de Schneider Electric se pone a prueba mientras busca recuperarse y fortalecer sus medidas de seguridad para salvaguardar la integridad de sus operaciones sostenibles.

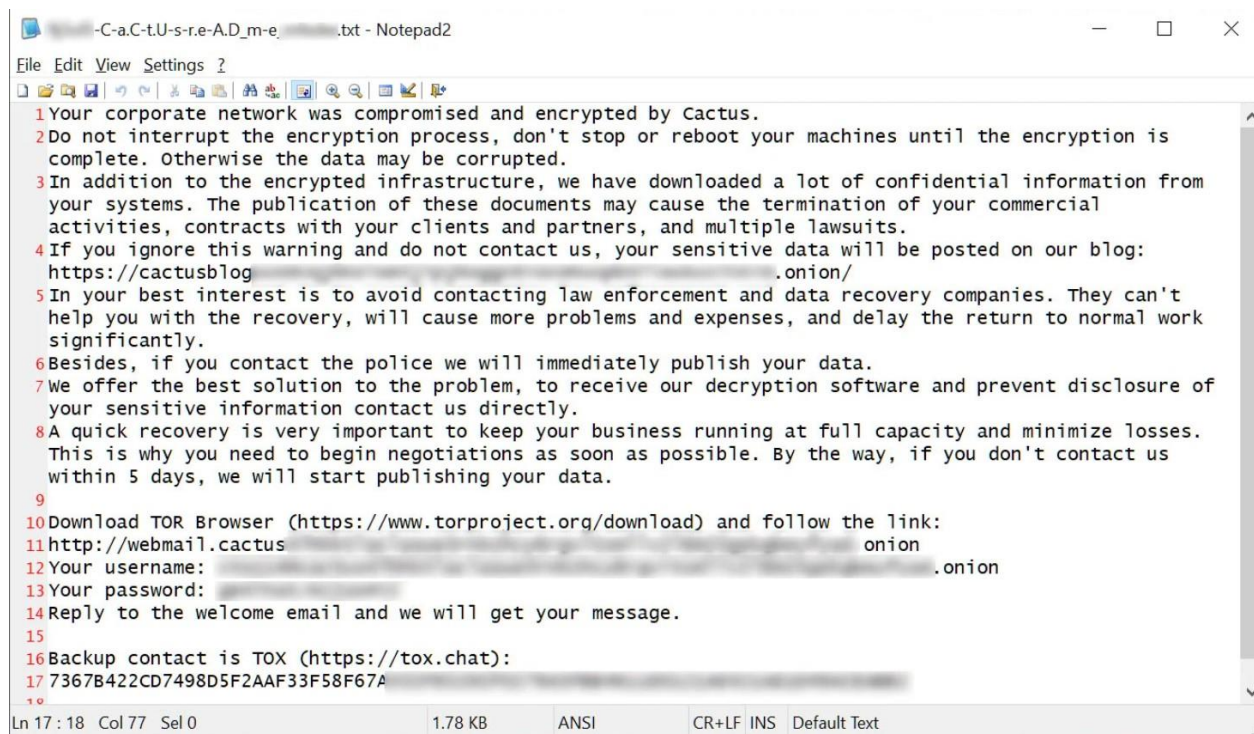
SCHNEIDER ELECTRIC GOLPEADA POR RANSOMWARE CACTUS EN SU DIVISIÓN DE SOSTENIBILIDAD

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

ID de alerta:	DSOC-CERT_2024_01_31_2
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	CLEAR
Fecha de publicación:	31/01/2024
Es día cero (0 day):	No

RESUMEN

El pasado 17 de enero del 2024, el temido ransomware CACTUS hizo su entrada triunfal, apuntando directamente a las entrañas de Scheider Electric. ¿El blanco? Nada más y nada menos que la plataforma de EcoStruxure Resource Advisor, utilizada por más de 2,000 empresas en todo el mundo para monitorear datos energéticos y de recursos.

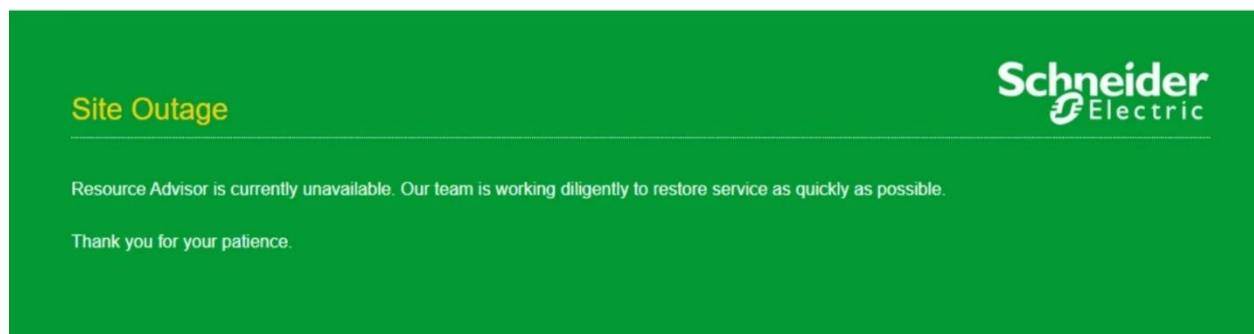


```

-C-a.C-t.U-s-r.e-A.D_m-e_...txt - Notepad2
File Edit View Settings ?
1 Your corporate network was compromised and encrypted by Cactus.
2 Do not interrupt the encryption process, don't stop or reboot your machines until the encryption is
  complete. Otherwise the data may be corrupted.
3 In addition to the encrypted infrastructure, we have downloaded a lot of confidential information from
  your systems. The publication of these documents may cause the termination of your commercial
  activities, contracts with your clients and partners, and multiple lawsuits.
4 If you ignore this warning and do not contact us, your sensitive data will be posted on our blog:
  https://cactusblog...onion/
5 In your best interest is to avoid contacting law enforcement and data recovery companies. They can't
  help you with the recovery, will cause more problems and expenses, and delay the return to normal work
  significantly.
6 Besides, if you contact the police we will immediately publish your data.
7 We offer the best solution to the problem, to receive our decryption software and prevent disclosure of
  your sensitive information contact us directly.
8 A quick recovery is very important to keep your business running at full capacity and minimize losses.
  This is why you need to begin negotiations as soon as possible. By the way, if you don't contact us
  within 5 days, we will start publishing your data.
9
10 Download TOR Browser (https://www.torproject.org/download) and follow the link:
11 http://webmail.cactus...onion
12 Your username: ...onion
13 Your password: ...onion
14 Reply to the welcome email and we will get your message.
15
16 Backup contact is TOX (https://tox.chat):
17 7367B422CD7498D5F2AAF33F58F67A
Ln 17 : 18 Col 77 Sel 0 1.78 KB ANSI CR+LF INS Default Text
  
```

El impacto se ha sentido. Aunque aún estamos desentrañando la magnitud del ataque, se ha confirmado que los intrusos manipularon algunos datos. Pero el resto de las divisiones y unidades de negocios de Schneider Electric están a salvo.

¿Cómo ha respondido Schneider? ¡Con todo! En un comunicado de prensa, la compañía anunció que desplegó un equipo global de respuesta de incidentes, tanto interno como con expertos externos en ciberseguridad, para contener la situación y restaurar los sistemas afectados. Además, están notificando a los clientes que podrían haber sido impactados.



Site Outage

Resource Advisor is currently unavailable. Our team is working diligently to restore service as quickly as possible.

Thank you for your patience.

Y hablando de impacto, hoy, 31 de enero del 2024, Schneider Electric sigue trabajando arduamente para devolver la funcionalidad completa a sus sistemas. La mayoría de ellos se espera que vuelvan a estar en línea en los próximos días.

Este ataque podría causar algunos dolores de cabeza a los clientes de Schneider Electric y existe el riesgo de que datos importantes hayan caído en malas manos.

Los expertos en ciberseguridad ya están dando sus opiniones. Alertan sobre la creciente tendencia de ataques de ransomware contra organizaciones industriales. John Gallagher, vicepresidente de Viakoo Labs, nos aconseja sobre la importancia de redes aisladas y del uso efectivo de los principios de confianza cero para evitar movimientos laterales.

En resumen, la ciberseguridad es más crucial que nunca. ¡Mantengan sus sistemas seguros y sus redes aisladas! Este episodio nos recuerda que, en el mundo digital, ¡Nunca se sabe cuándo puede llegar la tormenta!

INDICADORES DE COMPROMISO

https://github.com/develgroup/SOC_IOCs/tree/main/20240131_2_CactusRansomware

NOTICIA COMPLETA

<https://devel.group/blog/scheider-electric-golpeada-por-ransomware-cactus-en-su-division-de-sostenibilidad/>

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>