

Incidente de ciberseguridad

Fecha: 16/04/2024

Problemática: Ciberataque a proveedor de servicios de mensajería en Charleston, Estados Unidos

Correlativo: AC-0016

Institución / Sector: Público y Privado

SITUACIÓN

La empresa The Post and Courier de la ciudad de Charleston, Estados Unidos fue afectada por un ciberataque que interrumpió la disponibilidad de sus sistemas. El actor de amenazas «BlackSuit_ransomware» se atribuyó ataque a través de sus canales donde divulgaron la información extraída.

RIESGOS

- Cifrado de Información
- Daños críticos a la infraestructura tecnológica
- Suplantación de identidad
- Campañas de censura y desprestigio

RECOMENDACIONES

- Implementar y/o reforzar la seguridad perimetral
- Emplear contraseñas seguras
- Cambiar contraseñas periódicamente
- Utilizar la autenticación de dos factores
- Nunca haga clic en enlaces o descargue archivos adjuntos de fuentes desconocidas.

Nivel de priorización

Prioridad	Actualización
Urgente / No Urgente	Seguimiento/Preventiva/Resiliente
No Urgente	Preventiva

Matriz de evaluación

Riesgo	Nivel de Afectación		
	Integridad	Disponibilidad	Confidencialidad
Alto/Medio/Bajo			
Alto	Alto	Alto	Alto

ANEXO

BLACK SUIT

Search query Search

The Post and Courier
Website

The Post and Courier is the main daily newspaper in Charleston, South Carolina. It traces its ancestry to three newspapers, the Charleston Courier, founded in 1803, the Charleston Daily News, founded 1865, and The Evening Post, founded 1894. Through the Courier, it brands itself as the oldest daily newspaper in the South and one of the oldest continuously operating newspapers in the United States. It is the flagship newspaper of Evening Post Industries, which in turn is owned by the Manigault family of Charleston, descendants of Peter Manigault and Mr. Pierre Manigault himself as a president for a group of companies.

Our team breached The Post and Courier's network and stayed there for over 2 weeks. As a result 500GB of data leaked from Evening Post's network.

Leaked data belongs to following companies:

- Alken SC News
- Post And Courier
- Evening Post Industries
- Evening Post Publishing
- Evening Post Books
- Courier Square LLC.
- Post and Courier Advertising

What kind of data leaked from the network:

Contracts

Documents

Ads layout data (layouts data)

Brainworks data (publisher soft data)

Personal data (address, emails, phone)

Customers data (contacts, emails, payments, etc)

Subscribers data (card payment info, home address, emails, contacts)

Financial data (bank balances, wire transfers, payments, taxes, etc)

Credit Cards data (owner names, valid thru, card holders address, payments, etc)

Employees data (ssn, home address, passports, DL, family data, contracts, emails, payments, etc)

Files being stored within Personal Computers and NAS shares

We have contacted The Post and Courier management with an offer to protect leaked data for a fee. Mr.Manigault refused to pay for data protection, that is why you're reading this message. All the data leaked from The Post and Couriers' network was released to the public as a result of Mr.Manigault decisions.

Feel free to use the data as you wish, because there is no reason to care about Mr.Manigault business and his customers if Mr.Manigault doesn't care about such things at all.

It is strongly not recommended to deal with the Evening Post Industries in terms of security and data protection. The Manigault family is interested only in money, no one would care about your data or privacy there. Take care!

All data will be released in 72 hours.

REFERENCIAS

Fuente: <https://www.ransomlook.io/screenshots/black%20suit/The%20Post%20and%20Courier.png>