



Noticias sobre ciberataques

Jose Almirón Lopez
21/10/2023

Indice

Ciberataque a Phone House.....	1
Ciberataque a Sony.....	2
Ciberataque al Sistema de salud de la India.....	3

Ciberataque a Phone House

En abril de 2021, la compañía telefónica Phone House sufrió un grave incidente de ciberseguridad al ser víctima de un ataque de ransomware llevado a cabo por el grupo Babuk. Este ataque resultó en un acceso parcial no autorizado a la base de datos de Phone House, poniendo en riesgo la información confidencial de sus clientes.

Los atacantes llevaron a cabo el ataque cifrando los datos y exigieron un rescate a cambio de la clave de descifrado. Además, amenazaron con publicar los datos comprometidos en la Dark Web si no se cumplía su demanda. Este incidente tuvo un impacto significativo y afectó a más de 13 millones de usuarios de Phone House.

The logo for the Babuk ransomware group, featuring the word "BABUK" in white capital letters on a red rectangular background.

Phone House España 13 millions customers data has been stolen, including passports and other privacy information

PHONEHOUSE.ES - MORE THEN 100GB OF SENSITIVE DATA



We have downloaded full dump of your 10 Oracle databases which contains GDPR information/full name, date of birth, email, phone, address, nationality, imei, etc of more than 3 MILLION clients and employees.
If you do not pay - all this information will be published on our public blog, darknet forums, send to all your partners and competitors.

DB names:
INFOVENTAS
PHONE
POS
PP
SEGUROSPH
SMARTHOUSE
TARVAR
VENTASONLINE
VISIOFRANK

Ciberataque a Sony

El 26 de septiembre de 2023, un nuevo grupo de hackers llamado Ransomed.vc se atribuyó el ataque a los sistemas de Sony. Este grupo logró acceder a capturas de pantalla de las páginas de inicio de sesión internas de Sony, presentaciones de PowerPoint con información técnica, archivos Java y más de 6.000 documentos internos de la empresa. Ransomed.vc afirmó haber comprometido completamente los sistemas de Sony y anunció su intención de vender los datos en lugar de solicitar un rescate, debido a la negativa de Sony a pagar. El grupo planea filtrar esta información el 28 de septiembre.

Ransomed.vc parece ser un grupo especializado en ataques de ransomware que operan desde Rusia o Ucrania. No es la primera vez que Sony es víctima de un ataque de este tipo, en 2011, sufrieron uno de los mayores ataques en sus sistemas Playstation Network, que comprometió más de 77 millones de cuentas personales.

The screenshot displays the RansomedVC website with a dark background and red accents. At the top, navigation links include "/ FAQ / NEWS / FAQ / Contact Us". Below this, two Tor proxy addresses are listed: "f6amq3lzzsgtna4vw24rpyhy3ofwazlgex2zqdsszavervkkmtudxjad.onion - Tor Proxy" and "f6amq3lzzsgtna4vw24rpyhy3ofwazlgex2zqdsszavervkkmtudxjad.onion.ly - clearnet proxy". The main heading "RANSOMEDVC" is centered. A paragraph states: "We offer a secure solution for addressing data security vulnerabilities within companies. As penetration testers, we seek compensation for our professional services. Our operations are conducted in strict compliance with GDPR and Data Privacy Laws. In cases where payment is not received, we are obligated to report a Data Privacy Law violation to the GDPR agency!". Below this, a "News" section mentions "SONY.com data and access for sale". A "NOTICE" states: "Downtime has been resolved, very sorry! PS: We need affiliates :))". A red button labeled "Join Our Affiliate Program" is present. The "SONY.COM / Post Date: 28.9.2023" section reports a "Revenue: \$88,000,000,000 (\$88b)". A bullet point identifies Sony Group Corporation. The text continues: "We have successfully compromised all of sony systems. We wont ransom them! we will sell the data. due to sony not wanting to pay. DATA IS FOR SALE". It provides links for "R File tree" and "Sample Of Data". The phrase "WE ARE SELLING IT" is followed by a long alphanumeric string: "192D52C7C18F3D2693ED2453E64C53EC0CCF0255AB2291F019B65BA84442B313C410DE132E59". A red button labeled "Buy" is at the bottom.

Ciberataque al Sistema de salud de la India

Un grupo de hacktivistas rusos llamado Phoenix afirma haber infiltrado el sistema de gestión de la salud de la India, que almacena información de millones de ciudadanos. La firma CloudSek descubrió el ataque el 15 de marzo de 2023. Phoenix alega que este ataque es una respuesta a las sanciones de la India contra Rusia, relacionadas con temas como el precio del petróleo y las sanciones del G20 debido a la invasión de Ucrania. El grupo amenaza con paralizar el sistema de salud de la India, ya que afirma tener acceso a hospitales y personal médico.

Los ciberataques respaldados por el gobierno ruso aumentaron en el periodo previo a la invasión de Ucrania en 2021. Como medida preventiva, CloudSek aconseja a las agencias gubernamentales monitorear las cuentas de usuario en busca de anomalías, utilizar protección DDoS y bloquear direcciones IP innecesarias.

