Noticias sobre ciberataques

Jose Almirón Lopez
21/10/2023

Indice

Ciberataque a Phone House

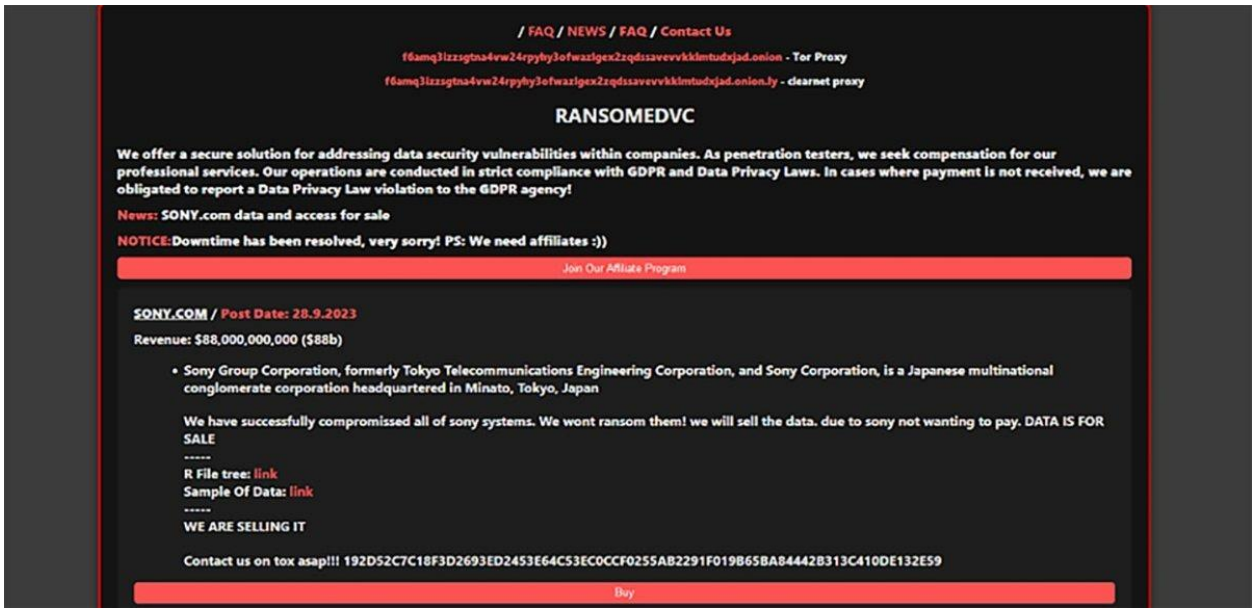
En abril de 2021, la compañía telefónica Phone House sufrió un grave incidente de ciberseguridad al ser víctima de un ataque de ransomware llevado a cabo por el grupo Babuk. Este ataque resultó en un acceso parcial no autorizado a la base de datos de Phone House, poniendo en riesgo la información confidencial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

Ciberataque a Sony

El 26 de septiembre de 2023, un nuevo grupo de hackers llamado Ransomed.vc se atributo el ataque a los sistemas de Sony. Este grupo logro acceder a capturas de pantalla de las paginas de inicio de sesion internas de Sony, presentaciones de PowerPoint con infromacion tecnica, archivos Java y mas de 6.000 documentos internos de la empresa. Ransomed.vc afirmo haber comprometido completamente los sistemas de Sony y anuncio su intencion de vender los datos en lugar de solicitar un rescate, debido a la negativa de Sony a pagar. El grupo planeo filtrar esta informacion el 28 de septiembre.

Ransomed.vc parece ser un grupo especializados en ataques de ransomware que operadesde Rusia o Ucrania. No es la primera vez que Sony es victima de un ataque de este tipo, en 2011, sufrieron uno de los mayores ataques en sus sistemas Playstation Network, que comprometio mas de 77 millones de cuentas personales.



Ciberataque al Sistema de salud de la India

Un grupo de hacktivistas rusos llamado Phoenix afirma haber infiltrado el sistema de gestion de la salud de la India, que almacena informacion de millones de ciudadanos. La firma CludSek descubrio 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 petroleo y las sanciones del G20 debido a la invasion de Ucrania. El grupo amenaza con paralizar el sistema de salud de la India, ya que afrima tener acceso a hospitales y personal medico.

Los ciberataques respaldados por el gobierno ruso aumentaron en el periodo previo a la invasion de Ucrani en 2021. Como medida preventiva, CloudSek aconseja a las agencias gubernamentales monitorear las cuentas de usuario en busca de anomalias, utilizar proteccion DDoS y bloquear direcciones IP inecesarias.