Píldora Informativa

GPIT

RansomHouse
Casa de Rescate

No. 006

UNAD
GRUPO FUNCIONAL DE SEGURIDAD
IFORMATICA - GFSI
26/12/2022

¿Quiénes son?

Son un grupo de ciberdelincuentes que secuestran datos y los hacen públicos. Existen desde diciembre de 2021 aproximadamente. No son un grupo reconocido, pero si trabajan como apoyo a otras organizaciones dedicadas a la ciberdelincuencia, y su negocio se basa en la negociación para la liberación de la información robada.

Les gusta actuar como protectores de los clientes de empresas en general, demostrando que estas empresas no protegen adecuadamente los datos. Realizan un ataque informático y luego extorsionan a la empresa para que pague y no publicar la información.

Empresas atacadas anteriormente

- AMD
- Ataques a municipalidades en Italia
- ADATA (no está confirmado)
- Grupo Keralty - Sanitas

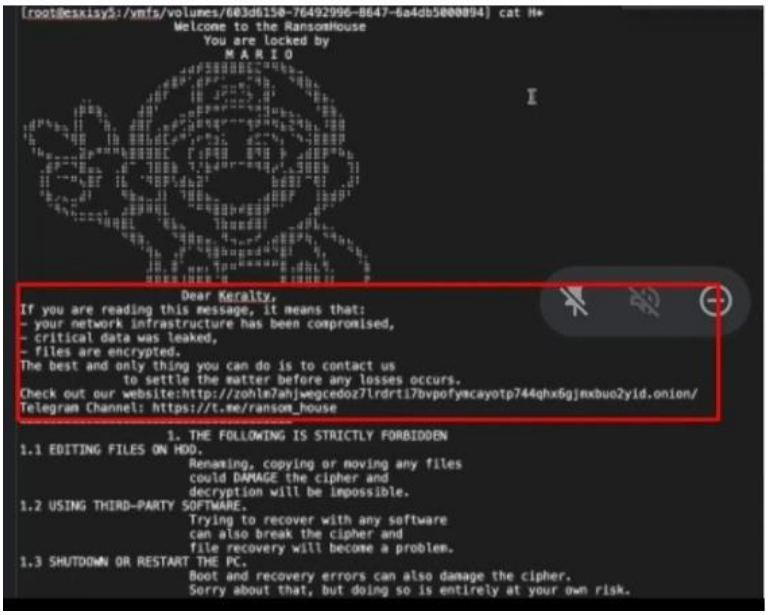
Ataque al Grupo Keralty

El 29 de noviembre de 2022, el Grupo Keralty, emitió una comunicación donde confirmó que tenían una interrupción en sus sistemas, debido a un ciberataque que provocó fallas técnicas en sus sistemas de TI.

Tomado de https://digitalcorp.cl/ciberseguridad/2022/12.Diciembre/01.12/ComunicadoKeralty.png

Ejecución del ataque al Grupo Keralty

Los ciberdelincuentes cambiaron el nombre del cifrador del Ransomware con la extensión [.]mario, dándole una funcionalidad multiplataforma para cifrar dispositivos Windows y Linux.



Tomado de https://digitalcorp.cl/ciberseguridad/2022/12.Diciembre/01.12/NotadeRescate.png

Algunas formas de prevenir estos ataques

- La detección de amenazas debe tener sus firmas actualizadas.
- Se debe realizar un Backup continuo de todos los sistemas de la empresa.
- Comprobar que los Backup funcionan.
- Garantizar que el equipo de TI tiene deshabilitado todos los puertos y protocolos que no sean necesarios para la operación.
- Proteger el protocolo RDP (Remote Desktop Protocol – Protocolo de Escritorio Remoto).
- Implementar el MFA (Multi Factor de Autenticación).
- Restringir que los usuarios reenvíen correos electrónicos a cuentas fuera de su dominio.
- Otros.

BIBLIOGRAFÍA

¿Quiénes son los responsables del hackeo a EPS Sanitas? Ya son populares por hackeo a otras empresas. Tomado de: https://www.publimetro.co/tecnologia/2022/12/21/quienes-son-los-responsables-del-hackeo-a-eps-sanitas-ya-son-populares-por-hackeo-a-otras-empresas/

Ataque cibernético a Sanitas: la SuperSalud se pronunció al respecto. Esto fue lo que dijo. Tomado de: https://www.semana.com/salud/articulo/ataque-cibernetico-a-sanitas-la-supersalud-se-pronuncio-al-respecto-esto-fue-lo-que-dijo/202249/

Entrevista con RansomHouse, el grupo que habría atacado al Grupo Keralty. Tomado de: https://muchohacker.lol/2022/12/entrevista-con-ransomhouse-el-grupo-que-habria-atacado-al-grupo-keralty/

Si usted está afiliado a Sanitas y Colsanitas preocúpese: sigue el secuestro de los hackers, que estarían publicando información de pacientes para presionar pago. Tomado de: https://www.semana.com/salud/articulo/se-agrava-situacion-de-sanitas-hackers-que-hicieron-ciberataque-estarian-publicando-datos-de-los-pacientes/202226/

La precaria ciberseguridad de Colombia. Tomado de: https://elpais.com/america-colombia/2022-12-24/la-precaria-ciberseguridad-de-colombia.html

El Ransomware RansomHouse compromete el sistema de Salud Keralty de Colombia. Tomado de: https://portal.cci-entel.cl/Threat_Intelligence/Boletines/1436/