Grupo Guacamaya hackeó la Agencia Nacional de Hidrocarburos y empresas del sector petrolero

La Agencia Nacional de Hidrocarburos y la New Granada Energy Corporation fueron hackeados por el grupo Guacamaya, el mismo que espió a la Fiscalía General de la Nación. EPM fue hackeado por otros ciberdelincuentes.

GUARDAR COMPARTIR

EL GRUPO GUACAMAYA JUSTIFICA HACKEAR LAS PETROLERAS POR LA IRRESPONSABILIDAD DE LOS DERRAMES CAUSADOS Y LOS DAÑOS AMBIENTALES. FOTO EL COLOMBIANO

NÉSTOR ESPINOSA ROBLEDO | PUBLICADO HACE 7 HORAS

Los tentáculos del grupo Guacamaya, conocido por hackear más de 5 terabytes (TB) de correos de la Fiscalía General de la Nación (FGN) y otras agencias de seguridad nacional de Latinoamérica, se extendieron tanto que lograron espiar a empresas e instituciones cuyo quehacer se relaciona con la explotación de hidrocarburos.

En las fauces de los hackers cayeron la Agencia Nacional de Hidrocarburos (ANH) y la multinacional New Granada Energy Corporation, empresas a las que los hábiles espías ilegales les extrajeron 2TB de información compuesta por correos electrónicos de empresas mineras y petroleras de países como Brasil, Colombia, Ecuador, Guatemala y Venezuela, como conoció EL COLOMBIANO.

En las entrañas de la información recopilada por Guacamaya, se registran los mensajes sobre el estado de la exploración de los pozos y los contratistas. Lo curioso es que, mientras a la Fiscalía le revisaban hasta los tuétanos de su información, a la Agencia de Hidrocaruburos le sucedía lo mismo y no se daban por enterados.

La información obtenida por los hackers fue clasificada en 91 gigabytes (GB) de mensajería de funcionarios y 50 GB de los contratistas directos. La

MÁS RECIENTES LO MÁS LEÍDO

1 Así fue el alcance que tuvo la injerencia rusa en Twitter a favor de Petro

2 Grupo Guacamaya hackeó la Agencia Nacional de Hidrocarburos y empresas del sector petrolero

3 Las voces del pasado que habitan las máquinas de La Remington

4 Benedicto XVI: el Papa que marcó a la Iglesia moderna

5 Hochi

NOTAS DE LA SECCIÓN

Así fue el alcance que tuvo la injerencia rusa en Twitter a favor de Petro

Grupo Guacamaya hackeó la Agencia Nacional de Hidrocarburos y empresas del sector petrolero

Venezuela respaldó a Gobierno Petro en objetivo de mantener cese bilateral y paz total

Finalizó la reunión entre Petro y Maduro; se abrirán cuatro consulados más en Venezuela

Denuncian que científicos estarían maltratando a monos ardilla en un proyecto que es financiado por el Estado

mensajería de funcionarios y 50 GB de los contratistas directos. La correspondencia está desde 2016 hasta junio de este año y se menciona el estado de los pozos de Arauca y Magdalena Medio, cruciales para la operación de hidrocarburos en el país. Pero una de las informaciones más delicadas extraídas por los "exploradores ilegales", se relaciona con las empresas que sostienen contratos con la distribución de los recursos provenientes de las regalías.

Según los correos, Arauca comparte con Venezuela uno de los yacimientos más grandes del país, aunque es una de las regiones más azotadas por la presencia de grupos al margen de la ley. Tiene el pozo que hizo que el país se convirtiera en exportador desde la década de 1980.

ANTIOQUIA

Hackers piden plata a EPM para devolverle información robada

En Arauca hay 111 pozos productores de los cuáles 42 están inactivos, 69 suspendidos y solo seis están en evaluación para ser un yacimiento. Estos datos fueron pedidos para la circular 5 de 2019 de ANH y se mantenían en reserva porque además de ser información confidencial, deja entrever como la dependencia del petróleo va en declive.

Para defenderse, la Agencia Nacional de Hidrocarburos, que se encuentra en cambio de planta laboral, implementó un "parche" en los servidores donde estaba ocurriendo la filtración, tarea que fue encomendada a su equipo de seguridad informática.

Así se roban la información

Durante 2022 los sectores de seguridad, minería y salud se vieron afectados por el secuestro de su información de parte de hacktivistas y ciberdelincuentes. Varias instituciones y empresas grandes del país estuvieron en la lupa de estos espías y algunos de estos ataques terminaron en la publicación de su información confidencial, afectando a usuarios para el acceso a la salud y otros servicios básicos.

Fueron dos los escenarios donde principalmente el fin de la irrupción a los servidores fue por motivos políticos o monetarios, liderados por diferentes grupos y asociaciones clandestinas que buscan negociar su liberación.

Los ataques proceden de diferentes grupos, el más reciente fue de BlackCat a EPM, un grupo de ciberdelincuentes que encriptan una gran parte de datos sensibles de las empresas para luego exigir el pago del rescate, preferiblemente en criptomonedas.

Según reportes de Microsoft, BlackCat es sucesor de los grupos Darkside y BlackMatter, quienes realizaban extorsión por datos robados, los mismos que encriptan y filtran si no se paga un rescate.

Estos comunican por medio de grupos de Telegram y blogs de la DeepWeb, donde suben pequeñas muestras.

Darkside fue el grupo responsable del ataque a la empresa Colonial Pipeline, que tuvo como consecuencia la suspensión de las operaciones y cierre del sistema de oleoductos más grande de EE. UU. el año antepasado.

Otros ataques

El grupo delincuencial también realizó ataques a la empresa TI NJVC, que funciona como proveedor de servicios para agencias gubernamentales y el Departamento de Defensa de EE. UU., utilizando el virus ExMatter, el cual parece ser el mismo con el que infectaron a EPM.

El Instituto de Vigilancia de Medicamentos y Alimentos (Invima) también fue víctima de dos ataques públicos en 2022. El primero fue en febrero e hizo que el restablecimiento de sus operaciones se demorará más de 30 días. Aunque no hubo fuga de información, si hubo intento de extorsión a funcionarios.

El segundo ataque fue en octubre, esta vez por medio de una amenaza directa al exdirector Francisco Rossi, en el que debía pagar más de cinco millones de dólares en criptomonedas o serian filtrados más de 700 GB de datos confidenciales.

El Invima emitió un comunicado donde confirman que hubo infiltración, pero cuentan con copias de seguridad (backups) de toda la información digital, además, de que la información esta encriptada y reposa en sus servidores

COLOMBIA

Hackers no paran ni en Navidad: millonario robo a cuenta de la Gobernación de Putumayo

Mientras tanto, la Fiscalía sigue sin poder superar y cerrar lo que ha sido considerado como el robo informático del siglo en Colombia. Varios medios nacionales, incluido este diario, han publicado diferentes hallazgos relacionados con el escándalo de corrupción de Odebrecht, redes de extorsión, interceptaciones ilegales desde el búnker e irregularidades relacionadas con capturas, todo esto encontrado en los correos.

Lo más reciente es que la Fiscalía denunció a Telefónica por falsedad de documento privado en medio de la adjudicación de un contrato de $179 mil millones de pesos, que tiene como fin prestar el servicio de seguridad informática los próximos 4 años. Todo indica que la documentación presentada contiene alteraciones en la certificación y garantía de equipos.

Hace unos días, la Fiscalía eligió a la Unión Temporal Fiscalía Seguridad Integral y Yak Til SAS como los encargados de la seguridad informática del ente investigador. La unión temporal ganadora está compuesta por Comcel (Claro), Sonda de Colombia y Teseract.

Principalmente, intercede porque las entidades y empresas realicen constantemente actualizaciones, copias de seguridad y un plan de recuperación compuesto de contraseñas robustas, largas y complejas, en las que se tenga que realizar su cambio periódicamente.

2TB De correos de empresas e instituciones latinas de petróleo fueron filtrados en internet.

CONTEXTO DE LA NOTICIA

PARA SABER MÁS

RECOMENDACIONES DEL COLCERT

Desde el equipo de respuestas a emergencias informáticas (ColCert) que es del Ministerio TIC, emitieron recomendaciones de seguridad para saber que hacer antes, durante y después de algún ciberataque proveniente de algún software malicioso (ransomware). Principalmente recomienda que las entidades y empresas realicen constantemente actualizaciones, copias de seguridad y un plan de recuperación compuesto de contraseñas robustas, largas y complejas, en las que se tenga que realizar su cambio periódicamente.

SI QUIERE MÁS INFORMACIÓN:

MEDIO AMBIENTE | PETRÓLEO | HACKER | BOGOTÁ

Correo electrónico

Confirmar Correo electrónico

ACEPTO TERMINOS Y CONDICIONES PRODUCTOS Y SERVICIOS GRUPO EL COLOMBIANO

VER TERMINOS Y CONDICIONES

ENVIAR

CONTINÚA LEYENDO