Informe de ETEK sobre ciberamenazas

Colombia

www.etek.com - www.cyble.com

CYBLE ETEK

www.cyble.com www.etek.com

Tabla de contenido

Introducción

Colombia desempeña un papel fundamental en el continente americano debido a su paisaje geográfico rico en minerales y recursos naturales. La producción de estos recursos constituye una parte importante en la conformación de Colombia como una de las mayores economías de América Latina.

Al igual que otros países latinoamericanos, Colombia también cuenta con una infraestructura de TI y modelos de digitalización en desarrollo para dar cabida al constante crecimiento de la nación en TI, telecomunicaciones, banca, salud y comercio internacional.

Sin embargo, la preocupación de Colombia por la ciberseguridad ha crecido en los últimos años y parece haber sido descuidada por muchas empresas, lo que la hace susceptible a los ciberataques y un blanco fácil para los ciberdelincuentes. En 2022 se observó un gran número de ciberataques, incluidos ataques de ransomware, que afectaron a operaciones industriales y gubernamentales y expusieron graves vulnerabilidades en las empresas

Durante el 2021-2022, Colombia también se enfrentó a un aumento masivo de ciberataques y filtraciones de datos causados por actores con motivaciones políticas para protestar contra el gobierno o las empresas, con el fin de disuadir los procesos democráticos, incluidos los intentos de alterar la opinión pública.

Los cibercriminales continúan ampliando su perímetro de ataque en Colombia en el transcurso de 2023. Cyble Research and Intelligence Labs (CRIL) en este informe de actividad de amenazas, describe el panorama de las ciberamenazas que afectan a las empresas y al gobierno colombiano.

Ataques de Ransomware

Durante el último año, varias empresas en Colombia experimentaron múltiples ciberataques, afectando sus operaciones a nivel global. Según las estadísticas, a finales de diciembre de 2022, Colombia reportó un aumento del 133% en el número de organizaciones impactadas por ataques de ransomware en comparación con el mismo periodo de 2021.

Entre enero de 2022 y marzo de 2023, CRIL ha observado ataques de ransomware dirigidos a 21 organizaciones, incluidas infraestructuras críticas en esta región.
En noviembre de 2022, un proveedor colombiano de servicios sanitarios sufrió un ataque de ransomware que interrumpió las operaciones de la empresa, así como de dos de sus filiales.
Al mes siguiente, el mayor proveedor público de energía, agua y gas de Colombia, fue víctima de un grupo de ransomware Alphav que causó interrupciones operativas en Telecomunicaciones, aplicaciones móviles e intranet.
Las entidades públicas también fueron víctimas de ataques de ransomware en marzo de 2022.

A continuación se resumen los principales ataques de ransomware durante este periodo:

Date	Ransomware Group	Impacted Organization
23 Mar, 2023	CL0P	
23 Mar, 2023	CL0P	
11 Mar, 2023	LOCKBIT	
6 Feb, 2023	LOCKBIT	
6 Ene, 2023	Vice Society	
5 Ene, 2023	CL0P	
30 Dic, 2022	HiveLeaks	
27 Dic, 2022	Alphavm	
30 Nov, 2022	RansomHouse	
30 Oct, 2022	LOCKBIT	
28 Oct, 2022	Alphavm	
7 Oct, 2022	Qilin	
15 Sep, 2022	LOCKBIT	
14 Sep, 2022	LOCKBIT	
5 Seo, 2022	LOCKBIT	
29 Ago, 2022	LOCKBIT	
31 May, 2022	HiveLeaks	
28 Abr, 2022	Vice Society	
30 Mar, 2022	BlackByte Auction	
26 Mar, 2022	LOCKBIT	
16 Mar, 2022	RansomEXX	
12 Mar, 2022	LOCKBIT	
21 Ene, 2022	HiveLeaks	

Actividades de amenaza en foros clandestinos

Los actores de amenazas ("threat actor", "TA") aprovechan el anonimato de los foros clandestinos para comprar y vender accesos y datos no autorizados, que luego se utilizan como vectores iniciales de ciberataques a gran escala. El CRIL observó las siguientes actividades destacables en foros clandestinos:

- El TA Mary vendió dos accesos de correo electrónico de cuentas de las Fuerzas Armadas colombianas por 10 USD cada uno, de forma privada. Es probable que las credenciales de las cuentas comprometidas procedieran de los registros del ladrón de información.
- El TA GhostSec, en su canal de Telegram, ofreció a la venta la base de datos supuestamente perteneciente al Ministerio de Minas y Energía de Colombia. La base de datos comprometida de 1GB de tamaño (comprimida), incluía información del ministerio, datos de las redes sociales e información de varios tablones de datos.

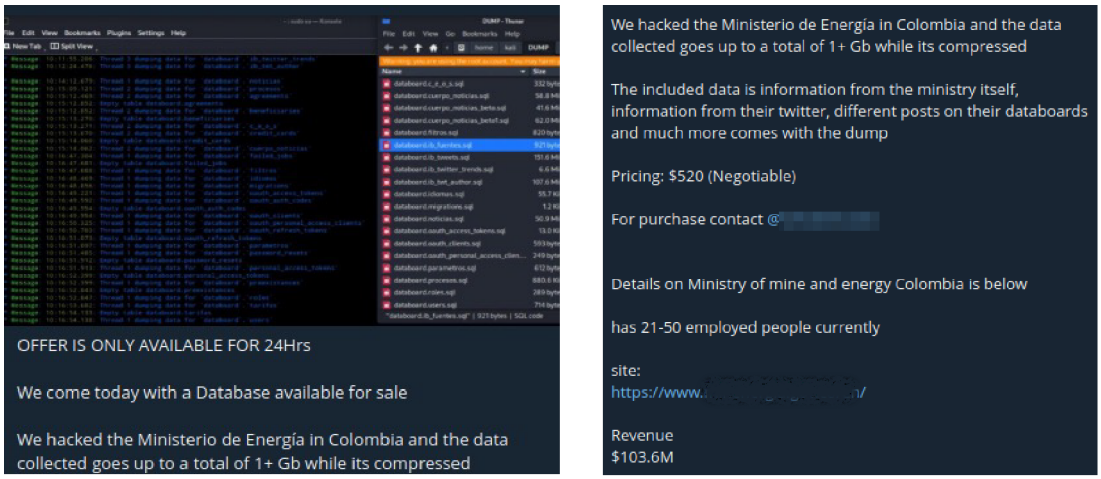


Imagen 1: Base de datos del Ministerio de Minas y Energía de Colombia en venta

- El canal de Telegram del TA Spectre, llamado Spectre's Intel Repository filtró una base de datos supuestamente perteneciente al gobierno colombiano.

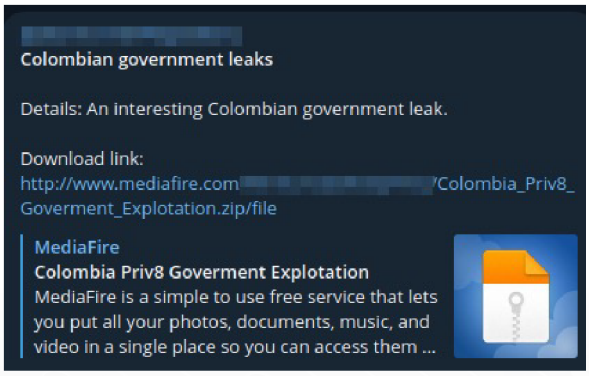


Imagen 2: Base de datos supuestamente perteneciente al gobierno colombiano

- El acceso de administrador a un portal web de una Alcaldía, Colombia, se vendió en el canal de Telegram de TA KelvinSecurity.

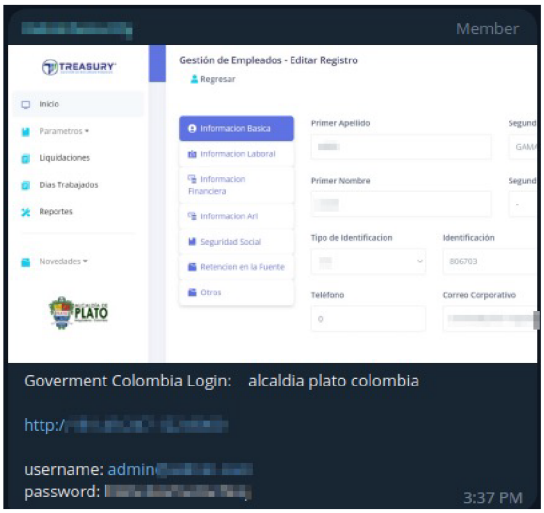
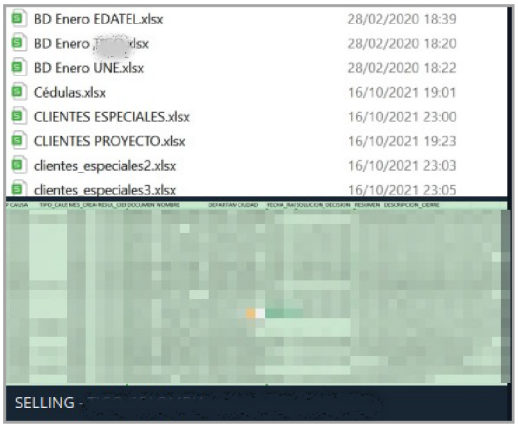


Imagen 3: filtración del acceso de administración del portal del Ayuntamiento de Platón

- La base de datos de la empresa de telecomunicaciones con sede en Colombia, fue filtrada por un actor de amenazas KelvinSecurity en su canal de Telegram.



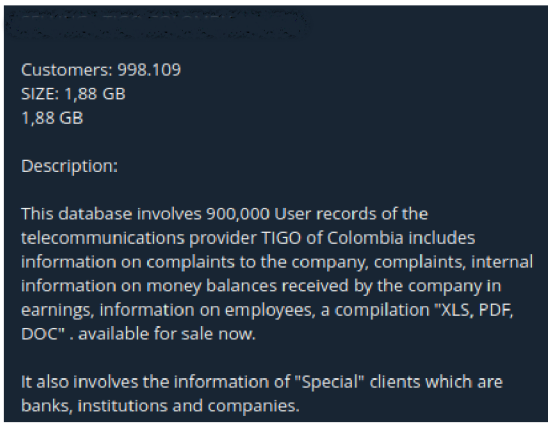


Imagen 4: Base de datos de [redacted] en venta

- Intercambios confidenciales de correos electrónicos de una Corporación para el Desarrollo Sostenible fueron filtrados por el TA amn3s1a.

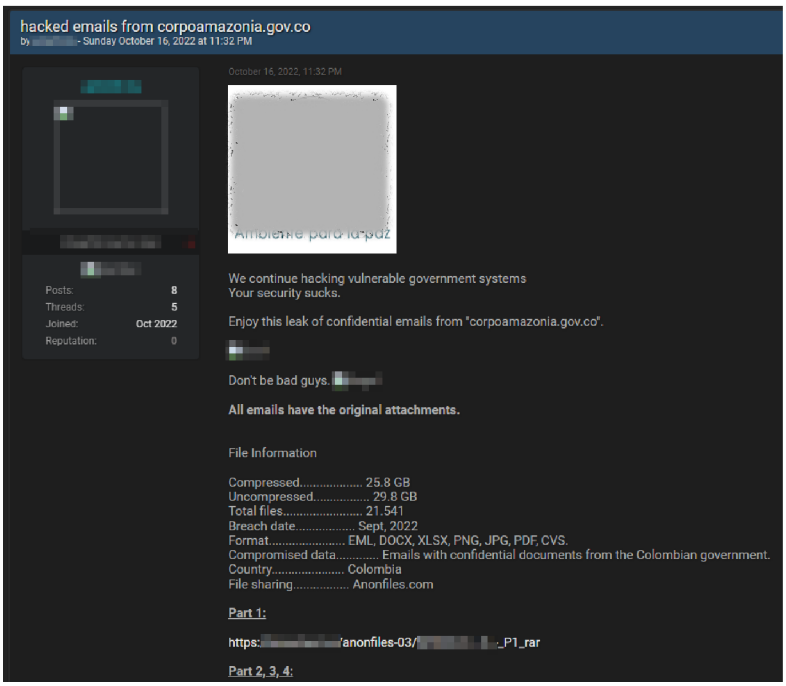


Imagen 5: Correos electrónicos de la Corporación para el D... Sur filtrados

- El TA amn3s1a reivindicó el pirateo de los servidores de correo electrónico a una empresa de soluciones de software con sede en Colombia. El incidente filtró más de 13 GB de intercambios de correos electrónicos confidenciales con los clientes.

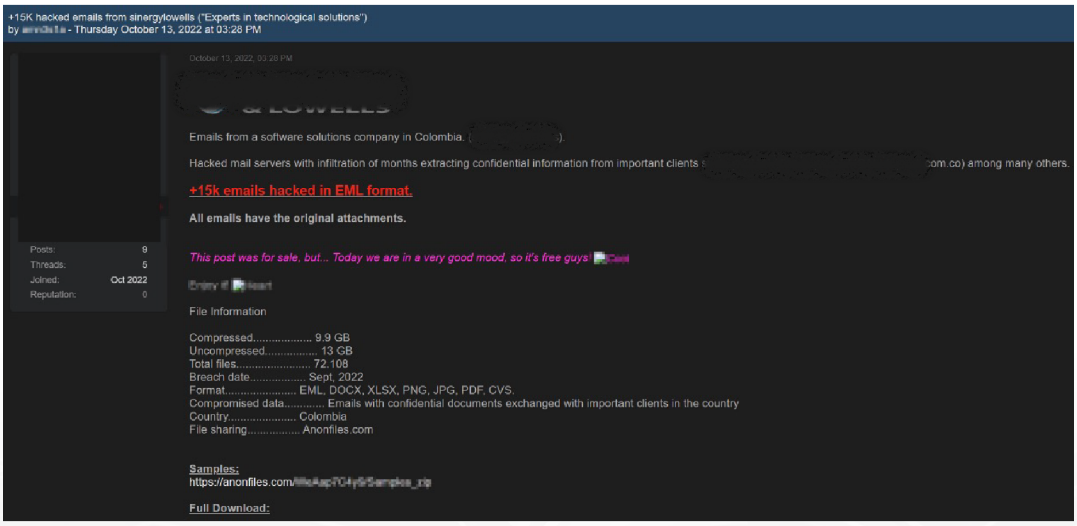


Imagen 6: Filtración de correos electrónicos presuntamente robados a Sinergy...

- El TA intelbroker fue identificado vendiendo el código fuente comprometido del Sistema de Votación Colombiano, que incluía código en Java, C#, HTML y Kotlin

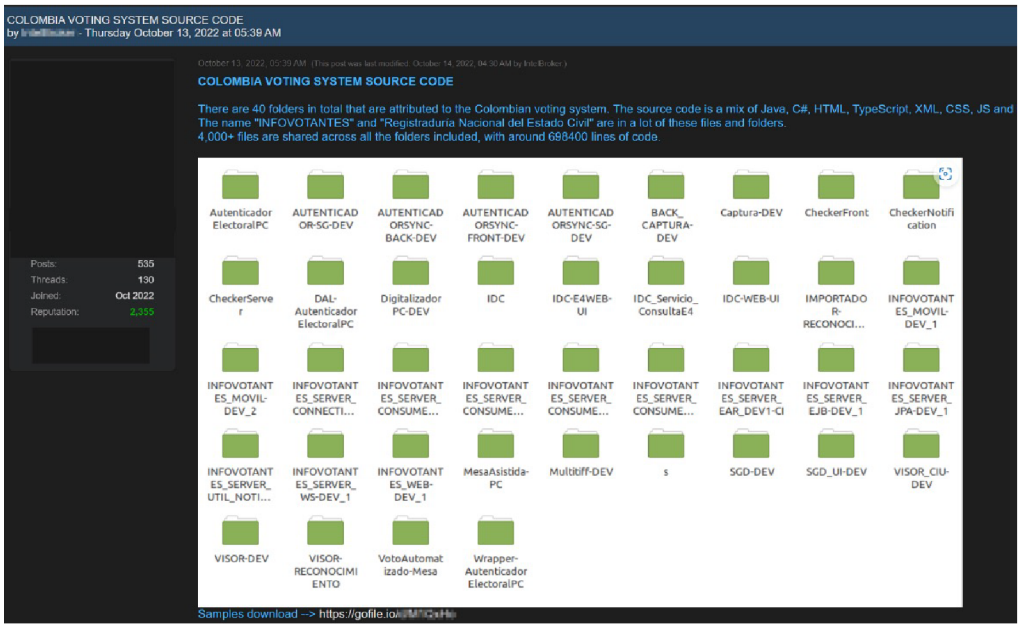


Imagen 7: Venta del código fuente del sistema de votación de Colombia

- El TA LeakBase filtró la base de datos de una empresa de transporte y logística con sede en Colombia. La base de datos comprometida incluía registros de más de 408k usuarios, junto con datos personales e información de pago.

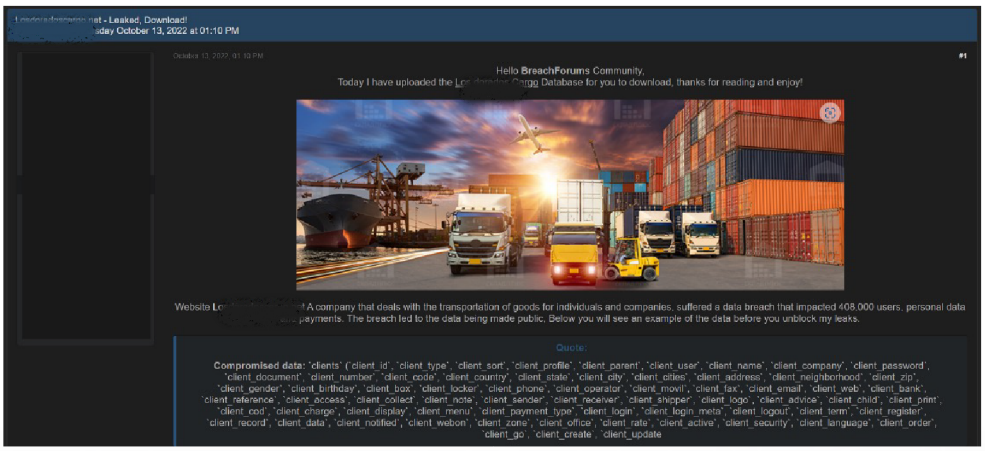


Imagen 8: Base de datos de Los Andes Cargo filtrada

- Se observó a varios actores de amenazas distribuyendo conjuntos de datos masivos que contenían información sobre números de WhatsApp activos y datos de titulares de tarjetas de consumidores en Colombia.

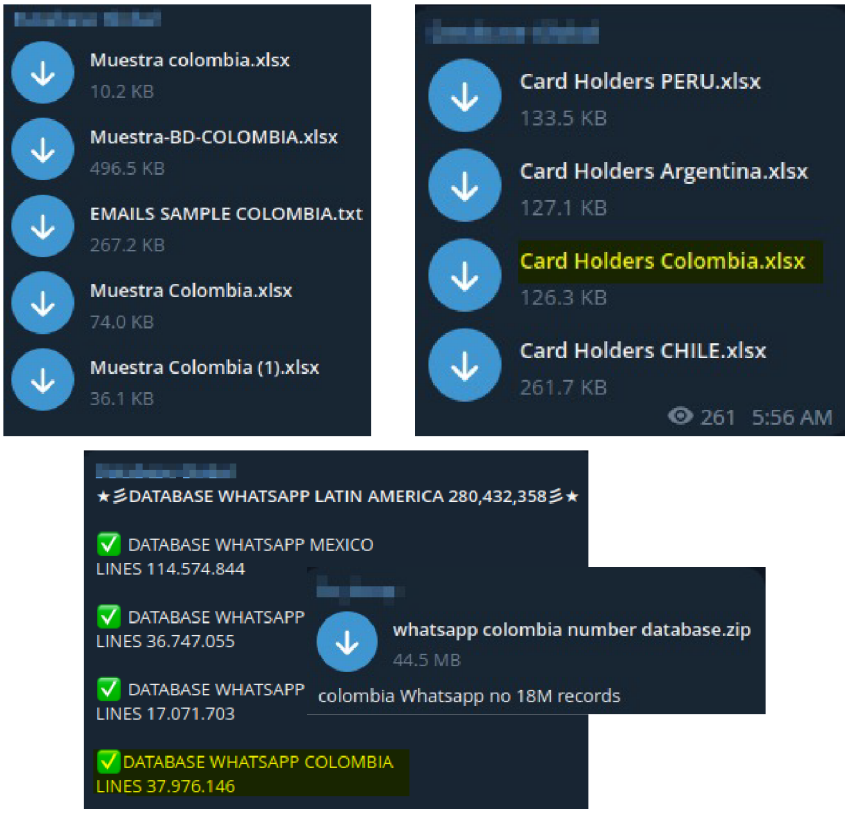


Imagen 9: Distribución de conjuntos de datos a granel en el canal de Telegram

- Aparte de esto, también observamos mensajes en los que los TA compartían registros de robos relacionados con usuarios de la región de Colombia.

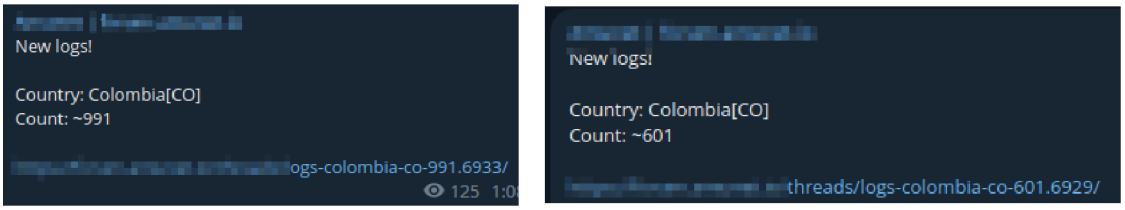


Imagen 10: Registros de robos relacionados con la región de Colombia

A continuación se resumen otras amenazas de impacto relativamente menor:

Fecha de Actividad	Actor de amenaza	Descripción de Actividad
1 Mar, 2023	sombraman1919	Se filtran 48.913 registros robados de la web de anuncios, c
27 Feb, 2023	Lanted	Se ofrece acceso no autorizado a una empresa colombiana de energía y servicios públicos con un ingreso aproximados de 50 millones de USD.
14 Feb, 2023	Tailmon	Se ofrece una base de datos con los datos de pago de los clientes registrados en varios hoteles hispanos.
1 Feb, 2023	Markitto35	Se ofrece base de datos de una plataforma de ventas basada en IA, Ke
17 Feb, 2023	Alan Wake	Se ofrece acceso no autorizado a una empresa colombiana de energía ecológica con unos ingresos 48 millones de dólares.
17 Ene, 2023	Crazyoldfart	Se ofrecen 12.5K registros PHI pertenecientes a residentes colombianos.
3 Ene, 2023	Romero666	Se ofrece acceso al panel administrativo de la empresa de telecomunicaciones Lo
21 Dic, 2022	Arynz_Clem	Se filtran de datos SQL robados de H
16 Dic, 2022	The Archivists Domain	Se filtran credenciales de administrador web de Si un distribuidor autorizado de
9 Dic, 2022	Nazil Blackhat (aka Baran)	Se ofrece acceso al panel WordPress de un dominio web en la infraestructura del gobierno colombiano.
2 Nov, 2022	KelvinSecurity	Se ofrece acceso a a.
27 Oct, 2022	chakalaka	Se ofrece acceso a una empresa de transportes con sede en Colombia.
15 Oct, 2022	KelvinSecurity	Se filtra la base de datos del P por el Pueblo.
10 Oct, 2022	amn3s1a	Se filtra base de datos del Hospital L Colombia.
10 Oct, 2022	amn3s1a	Se filtra base de datos del Hospital S mbia.
13 Sep, 2022	19cm	Se ofrece acceso a una empresa de recursos con sede en Colombia.
15 Jul, 2022	KelvinSecurity	Se ofrece base de datos de Colombia.
27 Jun, 2022	orangecake	Se pone a la venta el acceso de una empresa agrícola con sede en Colombia.
24 Jun, 2022	KelvinSecurity	Se filtra la base de datos de la Universi
24 Jun, 2022	KelvinSecurity	Se filtra la base de datos de la Farmacia
11 Jun, 2022	KelvinSecurity	Acceso al panel de administración de P
15 May, 2022	KelvinSecurity	Se filtra la base de datos de la U a.
12 May, 2022	KelvinSecurity	Acceso al portal de administración de l
31 Mar, 2022	KelvinSecurity	Acceso al portal de la clininca de La a.
23 Mar, 2022	KelvinSecurity	Acceso al portal de .
9 Mar, 2022	KelvinSecurity	Vulnerabilidad de inyección SQL compartida para acceder a uno de los portales de Colombia Más TV.
9 Mar, 2022	KelvinSecurity	Se ofrece la base de datos del centro sanitario colombian
22 Feb, 2022	kristina	Se ofrecen registros de los candidatos a las elecciones de Colombia de 2022.
14 Feb, 2022	KelvinSecurity	Acceso al portal de administración del A
28 Ene, 2022	KelvinSecurity	Se filtran los registros de usuarios de AMAZONAS ERP, una empresa de soluciones de software con sede en Colombia

Campañas hacktivistas contra Colombia

A continuación figuran las campañas hacktivistas más destacadas de 2022-23 identificadas durante nuestra investigación:

Operación "Fuerzas Represivas" contra las fuerzas armadas colombianas

Durante 2022, la organización hacktivista 'Guacamaya' llevó a cabo una serie de ciberataques conocidos como Operación "Fuerzas Represivas", cuyo objetivo eran entidades gubernamentales de América Latina.

Entre las actividades más destacadas cabe mencionar las siguientes:

- Una serie de ataques dirigidos a las fuerzas armadas de la región latinoamericana fueron reivindicados durante el mes de septiembre de 2022. La operación hacktivista supuestamente comprometió 10 TB de datos de las fuerzas armadas de Colombia, Chile, México, Perú y El Salvador.

- El 19 de septiembre de 2022, el grupo publicó un comunicado en su página wiki anónima EnlaceHacktivista, afirmando haber comprometido 275 GB de datos del Comando General de las Fuerzas Militares de Colombia. Los datos sólo estaban disponibles previa solicitud para limitar su distribución.

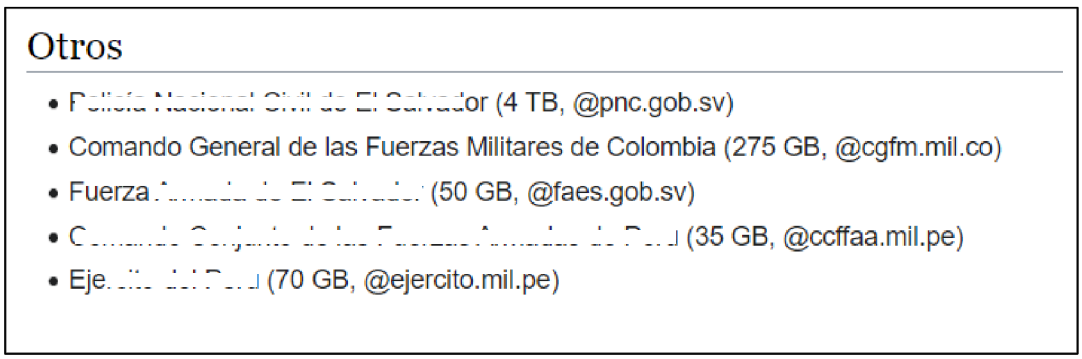
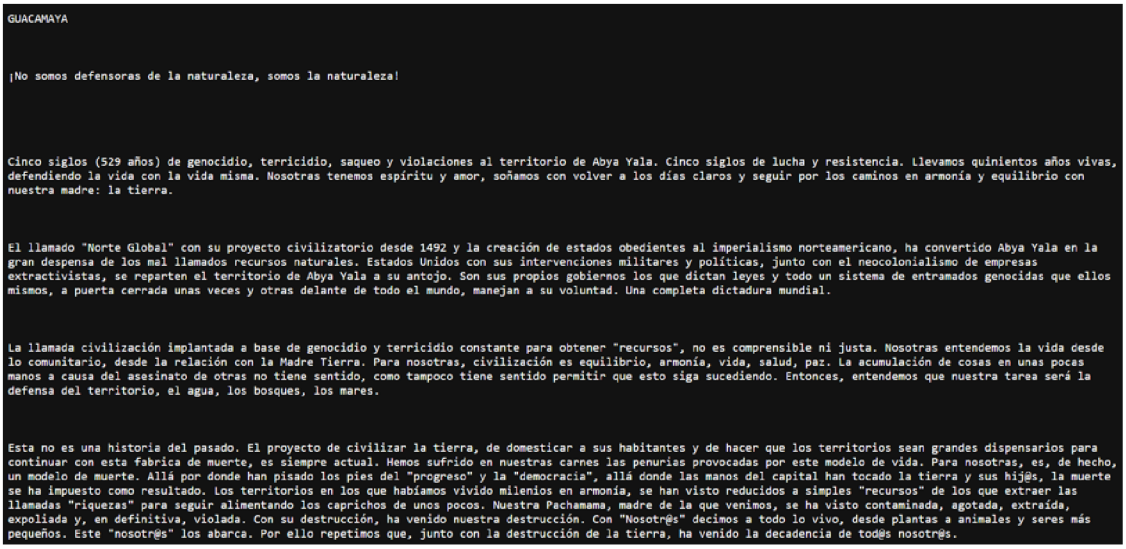


Imagen 11: Resumen de los datos comprometidos en su página wiki

- El 7 de agosto de 2022, el grupo afirmó haber comprometido 5 TB de datos de una istitución colombiana y que estaban disponibles para su descarga previa solicitud.

"Guacamaya" tiene como objetivo las industrias energéticas y las fuerzas armadas de América Latina

Durante agosto de 2022, 'Guacamaya' en su página wiki anónima Enlace Hacktivista, publicó 2 Terabytes (TB) de datos presuntamente robados de cuentas de correo electrónico comprometidas de varios productores de petróleo y empresas mineras en Colombia, Ecuador, Brasil, Chile, Venezuela y Guatemala.



GUACAMAYA

¡No somos defensoras de la naturaleza, somos la naturaleza!

Cinco siglos (529 años) de genocidio, terricidio, saqueo y violaciones al territorio de Abya Yala. Cinco siglos de lucha y resistencia. Llevamos quinientos años vivas, defendiendo la vida con la vida misma. Nosotras tenemos espíritu y amor, soñamos con volver a los días claros y seguir por los caminos en armonía y equilibrio con nuestra madre: la tierra.

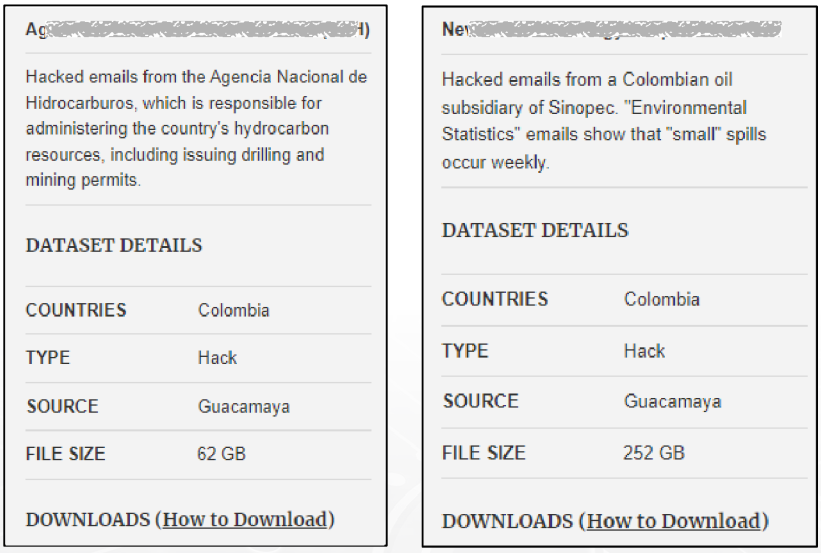
El llamado "Norte Global" con su proyecto civilizatorio desde 1492 y la creación de estados obedientes al imperialismo norteamericano, ha convertido Abya Yala en la gran despensa de los mal llamados recursos naturales. Estados Unidos con sus intervenciones militares y políticas, junto con el neocolonialismo de empresas extractivistas, se reparten el territorio de Abya Yala a su antojo. Son sus propios gobiernos los que dictan leyes y todo un sistema de entramados genocidas que ellos mismos, a puerta cerrada unas veces y otras delante de todo el mundo, manejan a su voluntad. Una completa dictadura mundial.

La llamada civilización implantada a base de genocidio y terricidio constante para obtener "recursos", no es comprensible ni justa. Nosotras entendemos la vida desde lo comunitario, desde la relación con la Madre Tierra. Para nosotras, civilización es equilibrio, armonía, vida, salud, paz. La acumulación de cosas en unas pocas manos a causa del asesinato de otras no tiene sentido, como tampoco tiene sentido permitir que esto siga sucediendo. Entonces, entendemos que nuestra tarea será la defensa del territorio, el agua, los bosques, los mares.

Esta no es una historia del pasado. El proyecto de civilizar la tierra, de domesticar a sus habitantes y de hacer que los territorios sean grandes dispensarios para continuar con esta fabrica de muerte, es siempre actual. Hemos sufrido en nuestras carnes las penurias provocadas por este modelo de vida. Para nosotras, es, de hecho, un modelo de muerte. Allá por donde han pisado los pies del "progreso" y la "democracia", allá donde las manos del capital han tocado la tierra y sus hij@s, la muerte se ha impuesto como resultado. Los territorios en los que habíamos vivido milenios en armonía, se han visto reducidos a simples "recursos" de los que extraer las llamadas "riquezas" para seguir alimentando los caprichos de unos pocos. Nuestra Pachamama, madre de la que venimos, se ha visto contaminada, agotada, extraída, expoliada y, en definitiva, violada. Con su destrucción, ha venido nuestra destrucción. Con "Nosotr@s" decimos a todo lo vivo, desde plantas a animales y seres más pequeños. Este "nosotr@s" los abarca. Por ello repetimos que, junto con la destrucción de la tierra, ha venido la decadencia de tod@s nosotr@s.

Imagen 12: : Un manifiesto publicado por Guacamaya

Los 62 Gigabytes (GB) de datos pertenecientes a la Agencia [redacted] y los 252 GB de datos de [redacted] oration Sucursal Colombiana se publicaron para su descarga en el sitio de filtraciones DDoSecrets bajo el título "ExtractivistLeaks". El grupo Guacamaya afirmaba en su manifiesto que los ciberataques que siguieron a las filtraciones de datos se llevaron a cabo en relación con la degradación del medio ambiente y los problemas causados por las operaciones de minería y refinado de petróleo de las organizaciones atacadas.



Ag[redacted])

Hacked emails from the Agencia Nacional de Hidrocarburos, which is responsible for administering the country's hydrocarbon resources, including issuing drilling and mining permits.

DATASET DETAILS

COUNTRIES	Colombia
TYPE	Hack
SOURCE	Guacamaya
FILE SIZE	62 GB

DOWNLOADS (How to Download)

Ne[redacted]

Hacked emails from a Colombian oil subsidiary of Sinopec. "Environmental Statistics" emails show that "small" spills occur weekly.

DATASET DETAILS

COUNTRIES	Colombia
TYPE	Hack
SOURCE	Guacamaya
FILE SIZE	252 GB

DOWNLOADS (How to Download)

Imagen 13 : Página de descarga del sitio de filtraciones DDoSecrets

Campañas de motivación política durante las elecciones presidenciales de 2022

En junio de 2022, los intentos de grupos radicales de perturbar las elecciones presidenciales fueron seguidos, al parecer, por protestas en todo el país en apoyo del candidato presidencial de izquierda (en aquel entonces), Gustavo Petro, que prometía grandes reformas económicas y sociales. A las protestas sobre el terreno se unieron múltiples grupos de hacktivistas que provocaron ciberataques contra la infraestructura gubernamental.

Los siguientes grupos fueron encontrados asociados a los ataques hacktivistas en Colombia:

- El actor de amenazas NEFERİAN, administrador de la organización hacktivista DDoSEmpire, lanzó ataques distribuidos de denegación de servicio (DDoS) el 19 de junio de 2022 contra varios sitios web del gobierno colombiano, como la Policía Nacional de Colombia, la Registraduría Nacional del Estado Civil, el Ministerio de Relaciones Exteriores de Colombia y la Embajada de Estados Unidos en Colombia.

La información sobre los atentados también fue promovida por el "Atlas Intelligence Group" en su canal de Telegram.

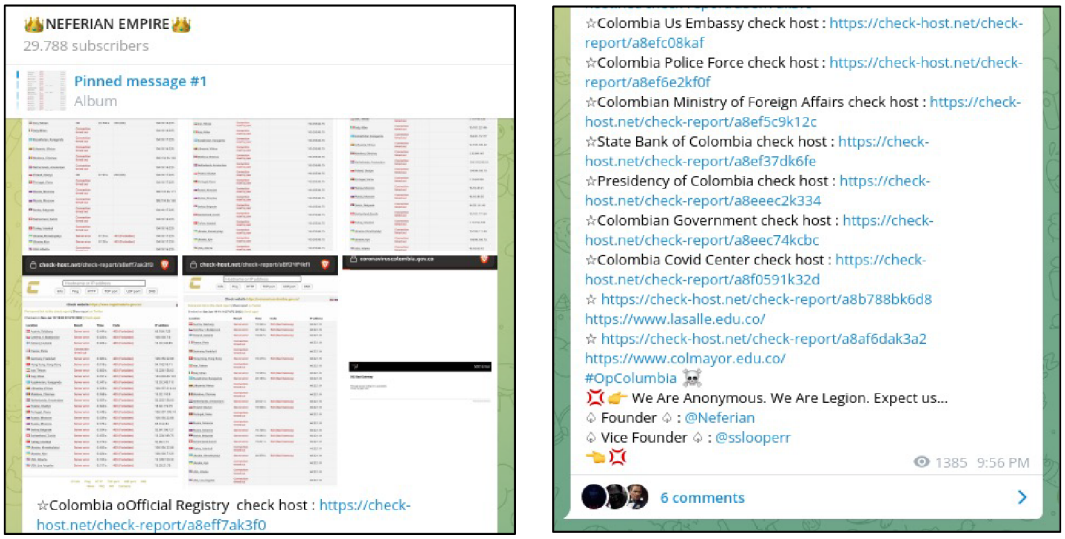


Imagen 14: Extractos del canal de Telegram

- El 15 de abril de 2022, el famoso grupo de hacktivistas GhostSec tuiteó un comunicado en el que afirmaba que la infraestructura del municipio de Villeta, en Colombia, había sido comprometida por el hacktivista YourAnonJack (Anonymous), miembro de GhostSquadHackers y YourAnonS0ul.

Cabe mencionar que GhostSec también estuvo involucrado en ataques dirigidos a Colombia durante 2021 y continuó su apoyo a otros grupos hacktivistas con ideología común.

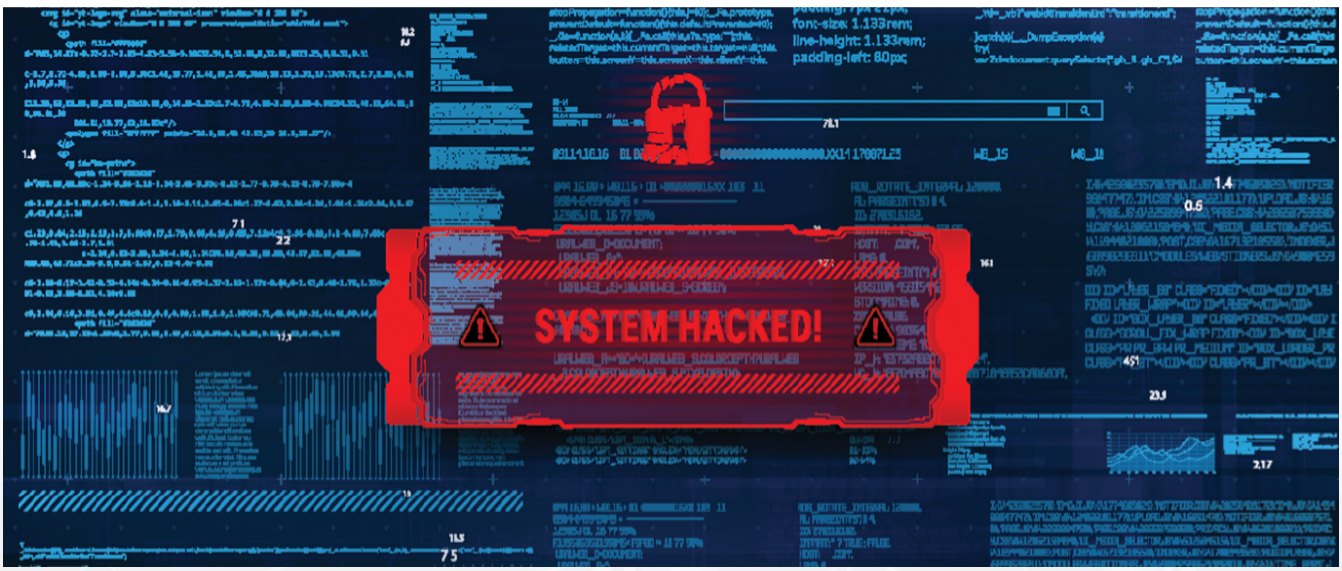
Otros ataques de hacktivistas contra entidades colombianas

El archivo de difamación en línea sugirió que alrededor de 75 ataques de difamación contra entidades gubernamentales colombianas fueron llevados a cabo por varios grupos de facciones hacktivistas desde enero de 2022.

El hacktivista conocido por el alias "0x1998" reivindicó la difamación de 26 sitios web gubernamentales desde enero de 2022, incluido el mayor número de ataques realizados con éxito en noviembre de 2022.

Date	Notifier	H	M	R	L	Domain	OS	View
2022/11/01	0x1998		M			pruebas.ticdosquebradas.gov.co...	Linux	mirror
2022/11/01	0x1998		M			pruebaseducacion.dosquebradas....	Linux	mirror
2022/11/01	0x1998		M			turismo.dosquebradas.gov.co/ku...	Linux	mirror
2022/11/01	0x1998		M			diger.dosquebradas.gov.co/kurd...	Linux	mirror
2022/11/01	0x1998		M			mesadeayuda.ticdosquebradas.go...	Linux	mirror
2022/11/01	0x1998		M			observatoriosocial.dosquebrada...	Linux	mirror
2022/11/01	0x1998		M			plandesarrollo.dosquebradas.go...	Linux	mirror
2022/11/01	0x1998		M			planeacion.dosquebradas.gov.co...	Linux	mirror
2022/11/01	0x1998		M			politicaspublicas.dosquebradas...	Linux	mirror
2022/11/01	0x1998		M			pot.dosquebradas.gov.co/fuckin...	Linux	mirror
2022/11/01	0x1998		M			presupuestoparticipativo.dosqu...	Linux	mirror
2022/11/01	0x1998		M			proteccionalconsumidor.dosqueb...	Linux	mirror
2022/11/01	0x1998					consultavacuna.palmira.gov.co/...	Linux	mirror
2022/11/01	0x1998		M			mesadeayuda.palmira.gov.co/kur...	Linux	mirror
2022/11/01	0x1998		M			emprendimiento.palmira.gov.co/...	Linux	mirror
2022/11/01	0x1998		M			galerias.palmira.gov.co/kurd.html	Linux	mirror
2022/11/01	0x1998		M			gobiernoabierto.palmira.gov.co...	Linux	mirror
2022/11/01	0x1998		M			oldpage.palmira.gov.co/kurd.html	Linux	mirror
2022/10/31	0x1998					ticdosquebradas.gov.co/kurd.html	Linux	mirror
2022/10/30	0x1998					www.municipiodeyotoco.gov.co/k...	Linux	mirror
2022/10/30	0x1998					sonsonantioquia.gov.co/kurd.html	Linux	mirror
2022/10/25	AnonCoders Kurdistan			R		www.medellindigital.gov.co/ima...	Unknown	mirror
2022/10/15	Bla3k_D3vil			R		cardique.gov.co/d.htm	Linux	mirror
2022/10/07	aDriv4			R		rionegro.gov.co/vz.txt	Linux	mirror
2022/09/21	0x1998			R		espvilleta.gov.co/kurd.htm	Linux	mirror

Imagen 15: Reclamaciones de difamación publicadas en el archivo de difamación de Zone-H



Exposición de activos de Internet que afectan a entidades colombianas

Los dispositivos expuestos a Internet, los servidores web, las aplicaciones, los protocolos, los cortafuegos, los dispositivos de supervisión de redes y los servidores de correo electrónico suponen un riesgo significativo para las infraestructuras de las organizaciones privadas y gubernamentales. Estos activos potencialmente vulnerables pueden ser aprovechados por los ciberatacantes para iniciar actividades de vigilancia no autorizadas, robar información sensible, aprovecharse de las vulnerabilidades y obtener acceso a las redes para lanzar posteriormente sofisticados programas maliciosos o ataques de ingeniería social.

Durante nuestra investigación, descubrimos que la mayor parte de la infraestructura expuesta, ubicada en Colombia, albergaba dispositivos de cámaras IP de Hikvision, dispositivos de red de ZTE, aplicaciones de Fortinet, Zimbra Collaboration Suite y SonicWall VPN. La exposición a Internet de los productos de ZTE fue la más alta, con 69.000 dispositivos de red expuestos que suponen un riesgo potencial.

La siguiente Imagen proporciona una visión general de los activos expuestos en la región de Colombia:

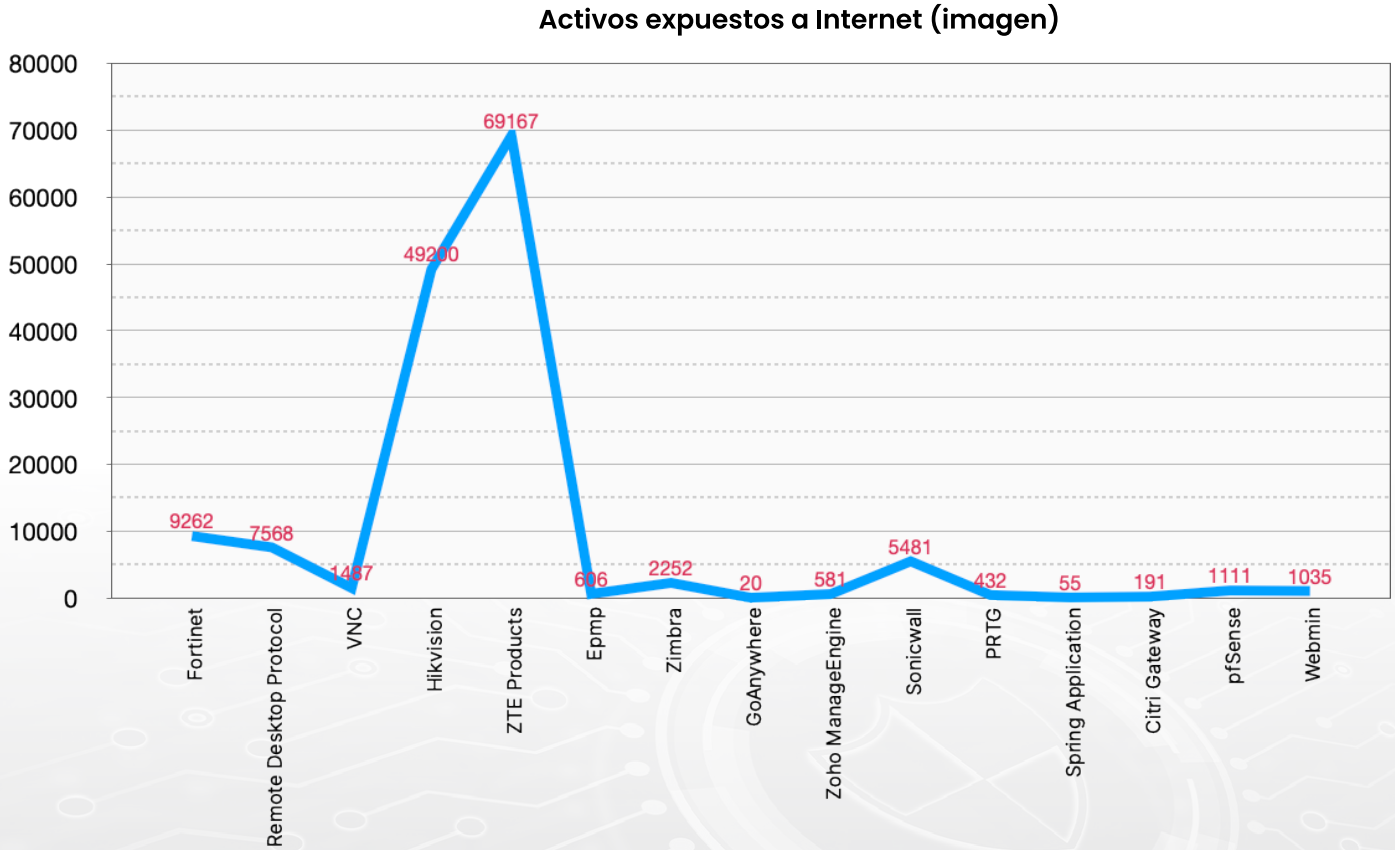


Imagen 16: Activos expuestos a Internet en Colombia

La visibilidad de los activos es imprescindible

Los siguientes casos de uso revelan el uso masivo de los dispositivos y aplicaciones mencionados durante 2022:

- **Vulnerabilidad de GoAnywhere (CVE-2023-0669):** A finales de febrero de 2023, el grupo de ransomware CL0P se aprovechó activamente de una vulnerabilidad de día cero dirigida al servicio de transferencia de archivos gestionados GoAnywhere para extorsionar a varias organizaciones de todo el mundo. El ransomware ha seguido filtrando partes de los datos comprometidos en su sitio de filtraciones.

- **Vulnerabilidad de bypass de autenticación de Fortinet (CVE-2022-40684):** Una reciente investigación de CRIL ha revelado los ataques de ransomware que aprovechan activamente los protocolos de escritorio remoto (RDP) en Internet. La investigación encontró familias del ransomware Reedemer, NYX ransomware, Vohuk, Blackhunt y Amelia ransomware detrás de esta campaña.

- **Ataques activos a Zimbra Collaborative Suite (ZCS) en 2022:** La investigación identificó un TA que vendía acceso a instancias de Fortinet a través de la uso de CVE-2022-40684. Nuestra red Cyble Global Sensor Intelligence (CGSI) también descubre varios indicadores de compromiso (IoC) que sugieren la uso activo de la vulnerabilidad crítica de Fortinet.

- **Ataques activos a Zimbra Collaborative Suite (ZCS) en 2022:** Durante agosto de 2022, los actores de amenaza sacaron provecho de instancias sin parches de Zimbra Collaborative Suite (ZCS) desplegadas en organizaciones estatales y privadas. Entre las vulnerabilidades que se aprovecharon de ZCS se encuentran las siguientes: CVE-2022-27924, CVE-2022-27925 (encadenada con CVE-2022-37042), CVE-2022-30333 y CVE-2022-24682. Se publicaron múltiples pruebas de concepto, scripts maliciosos y módulos que conducían al uso activo de las vulnerabilidades de ZCS. Los ataques también fueron aprovechados por los actores de amenazas activos en varios foros de ciberdelincuencia. En ese momento, nuestra investigación había encontrado más de 70.000 instancias expuestas.

- **Exposiciones en Internet de productos Zyxel:** Durante junio de 2022, varios medios de comunicación informaron de amenazas que explotaban la vulnerabilidad crítica de ejecución remota de código (RCE) (CVE-2022-30525) que afectaba a los dispositivos VPN de Zyxel. En ese momento, encontramos 21.583 dispositivos WLAN expuestos ubicados globalmente, incluidos 37 ubicados en Colombia, que eran potencialmente vulnerables a CVE-2022-30525. El siguiente gráfico indica la tasa de aumento de la exposición de los dispositivos Zyxel desde 2018.

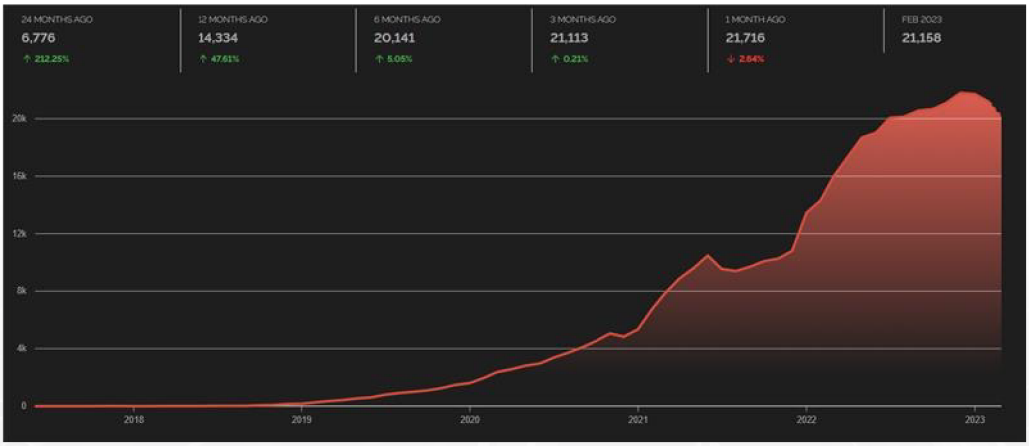
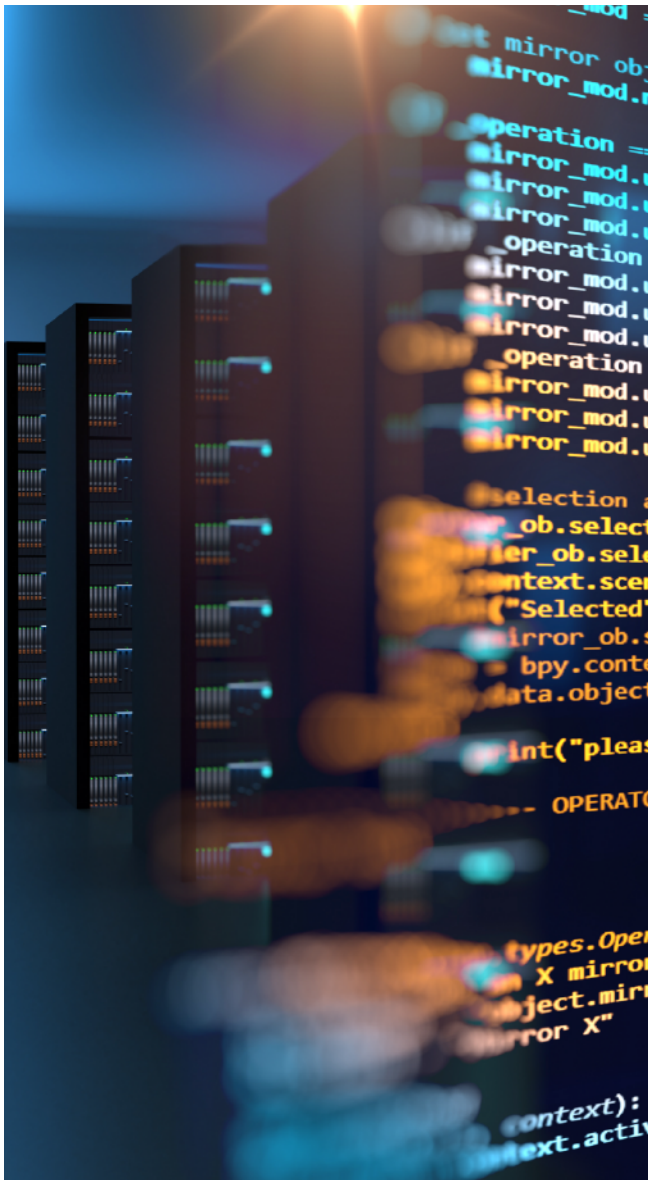


Imagen 17 : Gráfico que indica la tasa de aumento de la exposición de los dispositivos Zyxel

En un caso similar de marzo de 2023, observamos a un actor de amenazas en un foro clandestino de habla rusa que ofrecía una vulnerabilidad RCE preautenticada dirigida a las versiones 5.10 a 5.35 de los dispositivos de las series VPN50, VPN100, VPN300 y VPN1000. El actor de la amenaza también compartió una consulta de Shodan que revelaba más de 3.000 dispositivos expuestos potencialmente susceptibles al ataque en todo el mundo. Tres de los dispositivos expuestos se encontraban en Colombia.

Almacenamiento en la nube mal configurado que provoca la exposición de datos

Los directorios abiertos expuestos a Internet son motivo de gran preocupación en las industrias, ya que plantean el riesgo de exponer potencialmente información sensible o confidencial a partes no autorizadas. Los directorios abiertos son carpetas de cualquier servidor web que no están protegidas por contraseña y pueden identificarse mediante herramientas de escaneado de puertos en línea.
Los actores de amenazas que busquen instancias expuestas debido a tales errores de configuración pueden encontrar los almacenamientos en la nube comprometidos que contienen información sensible. Esto puede conducir al robo de identidades, pérdidas financieras y daños a la reputación. Los directorios abiertos también pueden exponer vulnerabilidades en la postura de seguridad de una organización, indicando una falta de atención a la seguridad y convirtiéndolas en un objetivo más fácil para los ciberataques.



La investigación encontró más de 500 directorios expuestos pertenecientes a la infraestructura web con sede en Colombia que pueden ser utilizados por los actores de amenazas maliciosas para obtener acceso a información confidencial, datos financieros, registros médicos, registros corporativos y otros PII. Los datos filtrados se venden a menudo en foros clandestinos y son utilizados por los actores de amenazas en campañas de ingeniería social.
Nuestra investigación identificó uno de los activos de Internet de una empresa minera agrícola en Colombia que exponía directorios compuestos por documentos de identidad escaneados de los residentes.

Imagen 18: Extracto de los documentos de identidad expuestos de los residentes colombianos

Grupos APT dirigidos a la región

APT-C-36

APT-C-36 también conocido como Blind Eagle, es un grupo de espionaje que ha estado activo desde al menos 2018 y se sospecha que tiene su sede en América del Sur. El grupo ha estado involucrado en ataques dirigidos contra organizaciones en Colombia y Ecuador desde al menos 2019. El grupo emplea correos electrónicos de spear-phishing personalizados y enviados a empresas específicas para llevar a cabo sus campañas.

A principios de este año, los investigadores identificaron una nueva campaña maliciosa orquestada por APT-C-36, también conocida como Blind Eagle. Esta campaña tenía motivaciones financieras y se inició mediante ataques de spear phishing dirigidos en Ecuador, Colombia y otros países sudamericanos desde 2018. Blind Eagle ha redefinido sus capacidades y se observa que utiliza conjuntos de herramientas personalizados y prueba cadenas de infección elaboradas en los usuarios objetivo.

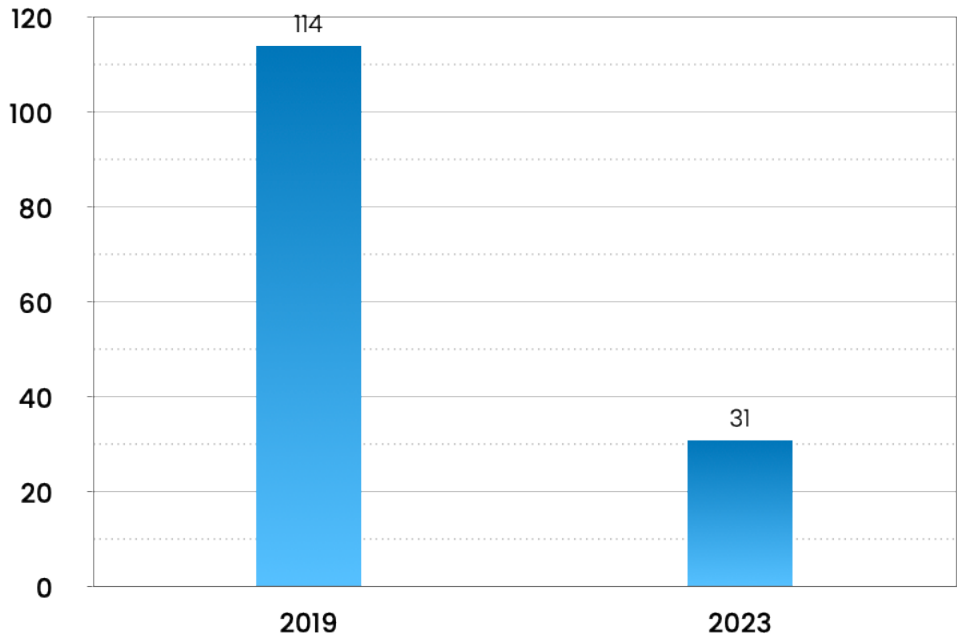


Imagen 19: Cronología de la actividad de APT-C-36

Ke3chang

El grupo Ke3chang, también conocido como APT15, es un grupo de amenazas atribuido a actores que operan desde China. Se tuvo noticia de él por primera vez en 2012, cuando utilizó un troyano de acceso remoto (RAT) Mirage para atacar objetivos de alto perfil en todo el mundo. El grupo ha atacado varios sectores, entre ellos organizaciones petroleras, gubernamentales y militares.

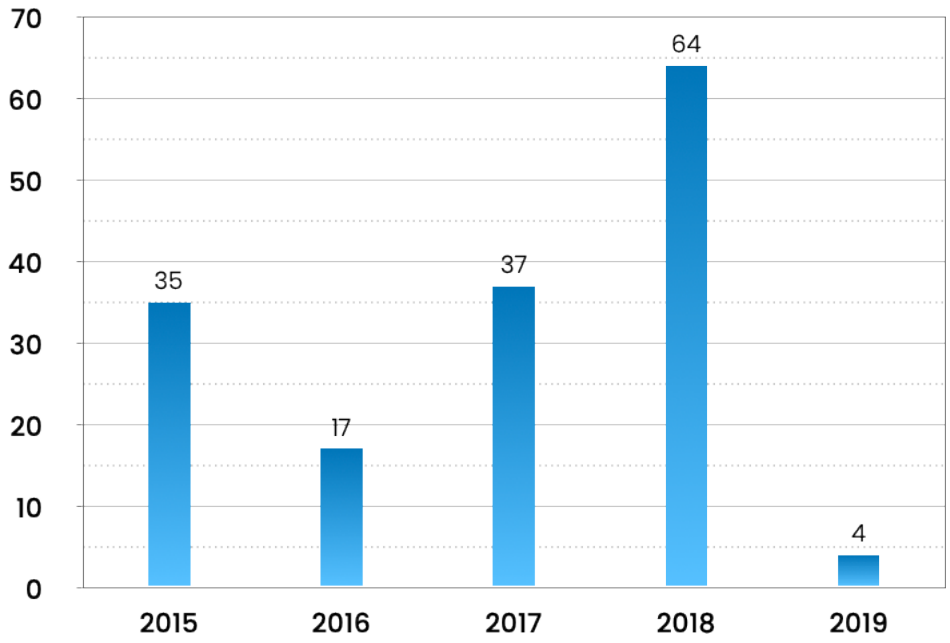


Imagen 20: Cronología de la actividad de Ke3chang alias APT15

El Machete

Los actores de amenazas de habla hispana que operan detrás del grupo se identifican como El Machete y también son conocidos por diferentes alias - APT-C-43, ATK 97, TAG-NS1. Su campaña maliciosa comenzó en 2010 y se renovó con una infraestructura mejorada en 2012. El malware se distribuía a través de correos electrónicos de spear-phishing y un blog de phishing.

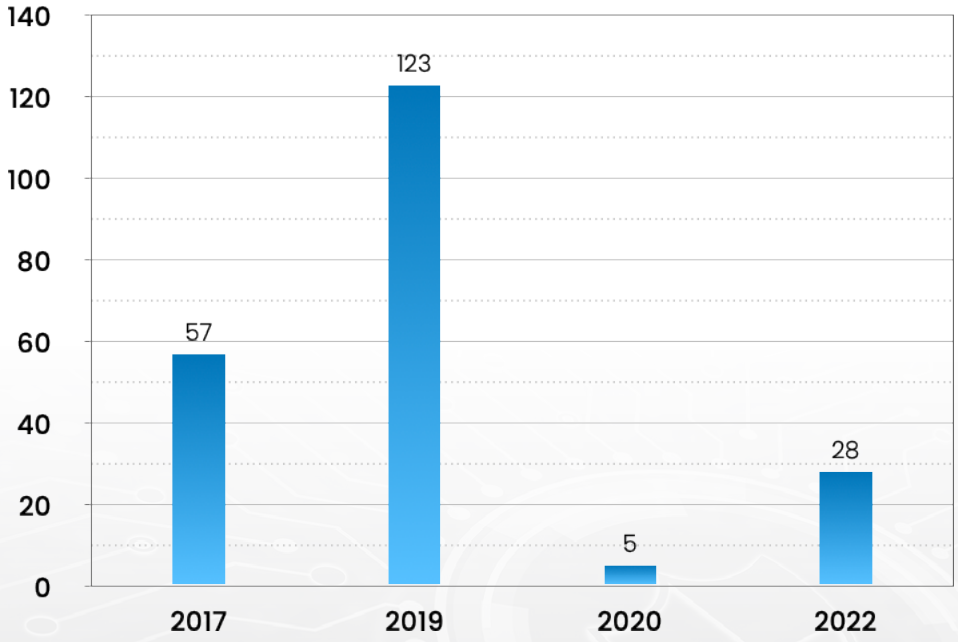


Imagen 21: Cronología de la actividad de El Machete

Recomendaciones

Las empresas pueden aplicar las siguientes medidas para contrarrestar estos ciberataques:

Las industrias de infraestructuras críticas deben desarrollar prácticas eficientes de mitigación y programas de gestión de vulnerabilidades.

Supervisar y revisar las divulgaciones de vulnerabilidades de software por parte de los proveedores y realizar evaluaciones independientes de vulnerabilidades y auditorías periódicas.

Parche oportuno para corregir los bugs reportados en los productos vulnerables.

Aplicar políticas y procedimientos adecuados de control de acceso a los sistemas de información que conservan activos de información sensibles.

Evalúe las reglas de control de acceso lógico y físico y los derechos de los usuarios y grupos para cada aplicación.

Los perfiles de acceso estándar de los usuarios (roles) deben estar claramente definidos en función de la necesidad de conocer, la necesidad de compartir, los mínimos privilegios y otros requisitos aplicables.

Impartir a los empleados la formación necesaria para identificar y notificar posibles amenazas, incluidas las internas.

Formación y sensibilización continuas de los empleados y proveedores externos para evitar las campañas de spear-phishing.

En caso de futuros ataques, adoptar medidas para llevar a cabo el plan de respuesta a tiempo.

Aplicar medidas para contrarrestar eficazmente las repercusiones de los ataques.

Referencias

https://ddosecrets.substack.com/p/extractivist-leaks-colombia-ecuador-chile-brazil

https://ti.360.net/blog/articles/apt-c-36-continuous-attacks-targeting-colombian-government-institutions-and-corporations-en/

https://research.nccgroup.com/2018/03/10/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/

https://www.welivesecurity.com/wp-content/uploads/2019/07/ESET_Okrum_and_Ketrican.pdf

https://research.nccgroup.com/2018/03/10/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/

https://www.bloomberglinea.com/english/successive-cyberattacks-in-colombia-expose-countrys-vulnerability/

https://blogs.blackberry.com/en/2017/03/el-machete-malware-attacks-cut-through-latam

https://www.welivesecurity.com/2019/08/05/sharpening-machete-cyberespionage/

https://github.com/eset/malware-ioc/tree/master/machete

https://blog.360totalsecurity.com/en/apt-c-43-steals-venezuelan-military-secrets-to-provide-intelligence-support-for-the-reactionaries-hpreact-campaign/

https://research.checkpoint.com/2022/state-sponsored-attack-groups-capitalise-on-russia-ukraine-war-for-cyber-espionage/

Los cibercriminales continúan ampliando su perímetro de ataque en Colombia en el transcurso de 2023.

www.cyble.com www.etek.com