Reporte ciberseguridad 2022 y tendencias 2023 en Chile y Latinoamérica

Prólogo

Hace ya algunos años definimos lo que sería nuestra visión como unidad de Ciber Inteligencia: cercanía con nuestros clientes y con el ecosistema. El objetivo que nos trazamos para cumplir con este compromiso fue desarrollar un área experta enfocada y conectada con las problemáticas de Chile y la Región, capaz de aportar conocimiento y experiencia a nuestro entorno, abordando en profundidad la realidad y desafíos específicos de nuestro país y Latinoamérica.

Nos propusimos entonces crear un Reporte de Ciberseguridad y Tendencias que nos permitiera contextualizar las principales amenazas digitales, brechas, vulnerabilidades y ciberataques en Chile y para Chile. Y lo conseguimos. Recopilamos para ello evidencias, registros de incidencias, análisis de impacto y riesgo, entre otros, con la única misión de compartirlo con ustedes: líderes de la industria, expertas y expertos del rubro o fanáticas y fanáticos de la tecnología buscando entender más sobre estos temas, siempre contingentes, de impacto y en permanente evolución.

Hoy, tras un largo camino, nos enorgullece hacer entrega de la tercera versión de nuestro informe, el que contiene un completo análisis comparativo de los escenarios global, regional y local, estadísticas actualizadas y recomendaciones en base a datos únicos de nuestro país. Un gran trabajo realizado con absoluta dedicación y profesionalismo por los equipos, líderes y expertos de Entel Ocean Cybersecurity Services, Unidad Digital de Entel Ocean a quienes quiero agradecer en forma especial por su capacidad y entrega.

Este 2022 se vio marcado por el terrible conflicto bélico que vive Europa del Este, en donde aparecen nuevos métodos de guerra desplegados en espacios digitales utilizados como "armas" para derrumbar o fragilizar a un país y a su población. Esto dejó de manifiesto que, en el ámbito TIC, la Ciberseguridad será el elemento clave para mantener operando sino resiliente a toda una Nación.

Espero que este Reporte de Ciberseguridad 2022 y Tendencias 2023 les sea útil, lo disfruten, comenten y compartan.

Cyril Delaere
Gerente de la unidad
de Ciberseguridad

ÍNDICE

ÍNDICE

ÍNDICE

Introducción

Durante el año 2022, la ciberseguridad ha enfrentado un número de amenazas cada vez mayor a nivel global y se estima que el costo de los ciberataques alcanza aproximadamente los 7.700 millones de dólares al año. Estos han puesto en tela de juicio la seguridad de múltiples organizaciones del sector público y privado, hasta lograr comprometer y exponer datos sensibles relacionados con la estabilidad nacional.

Una muestra significativa de aquello es lo ocurrido a principios de 2022 con el conflicto bélico entre Rusia y Ucrania, que ha registrado una superficie de ataques en el ciberespacio. En él se han visto involucrados diferentes ciberactores de ambos bandos, utilizando estrategias como el uso de Malware del tipo Wiper o técnicas de ingeniería social.

El costo de los ciberataques alcanza aproximadamente los 7.700 millones de dólares al año

El riesgo de estos ciberactores se conoce desde hace ya tiempo. Sin embargo, por factores como la falta de capacidades, recursos, burocracia y otros, muchas organizaciones no suelen considerarlos como una amenaza hasta que son víctima de ellos, lo que converge en un actuar reactivo que compromete la seguridad de la información e infraestructura de las empresas y la industria. Esto es especialmente grave porque, en la mayoría de los casos, los atacantes se proponen extorsiones con motivaciones financieras, cuyo impacto económico termina siendo mucho mayor al que implica tomar medidas preventivas.

Sin embargo, este contexto se ha visto fuertemente afectado por el papel que han jugado la pandemia y las cuarentenas, con sus oportunidades y desafíos. Por un lado, ha sido un impulso para grandes y valiosos avances, que empujaron a distintas industrias de todo el mundo a sumarse a la transformación digital para mantener sus operaciones activas, generando innovaciones en la forma de organizar sus proyectos.

Por otra parte, trajo nuevos conflictos, como el aumento del cibercrimen en distintas formas. Esto ha obligado a comprender la posición actual de cada organización en términos de madurez de ciberseguridad. Este entendimiento es la base para desarrollar técnicas, estrategias y operaciones preventivas que permitan cubrir adecuadamente las vulnerabilidades y ejecutar mitigaciones para solventarlas.

Con esa intención, este reporte cubre **el panorama de amenazas ocurridas en 2022 y las tendencias para 2023** a nivel global, latinoamericano y nacional. Nuestra finalidad es apoyar a que los recursos humanos y económicos de cada organización sean direccionados hacia áreas críticas, para garantizar así la homogeneidad de la red, la identificación de riesgos y el diseño de planes de trabajo que permitan resguardar la información de forma adecuada.

CAPÍTULO 1.

CIBERCRIMEN COMO SERVICIO, CÓMO Y QUIÉNES LO EJECUTAN

A lo largo de los años, los avances tecnológicos han permitido que muchas organizaciones utilicen nuevas soluciones para enfrentar sus desafíos, pero a la vez han dado espacio a nuevos riesgos y amenazas. Un ejemplo actual e interesante son los servicios basados en la nube, puesto que no sólo han beneficiado a empresas y emprendedores, sino que han servido también como guía para nuevos proyectos de ciberdelincuentes.

Algunos de estos servicios se presentan en el mercado negro como **Malware as a Service (Maas), Ransomware as a service (RaaS) y Hacking as a Service (HaaS),** para entregar a distintas personas, sin mayor sofisticación ni conocimientos, la capacidad de causar grandes daños a organizaciones para su beneficio personal.

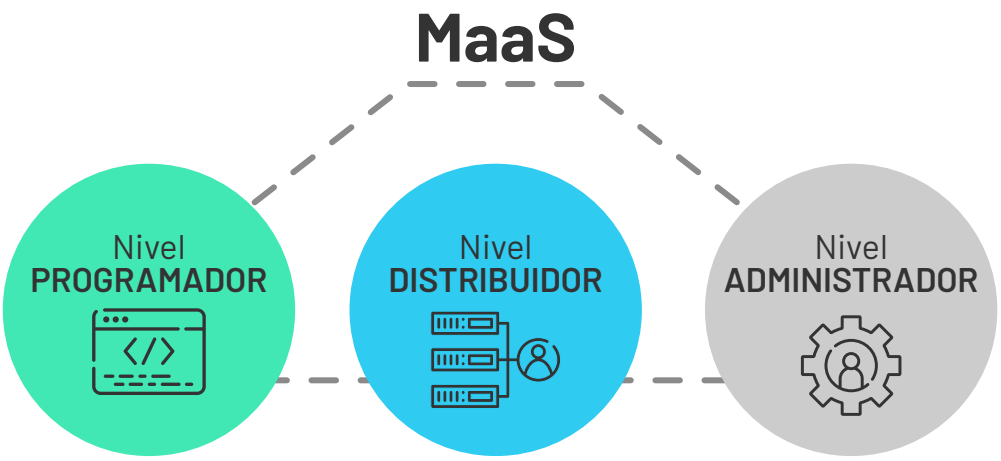
¿Cómo opera Malware-as-a-Service (MaaS)?

El MaaS se caracteriza por ofrecerse como un servicio de alquiler de software malicioso, que permite a cualquier persona con una conexión a Internet obtener acceso a soluciones personalizadas. Este servicio opera como un negocio establecido, en donde algunos proveedores ofrecen garantías de devolución de dinero, mientras que otros operan basados en comisiones vinculadas al éxito de cada campaña, que varían entre el 15% y 35%.

El malware ha pasado a generar un ambiente cibernético peligroso, donde se destacan distintos tipos a partir de características como: su capacidad disruptiva, la propagación en cortos periodos de tiempo y el daño reputacional que pueden provocar.

Las redes de MaaS operan generalmente bajo los siguientes tres niveles:

Niveles de Malware **como servicio (MaaS)**



Siendo parte del MaaS, el Ransomware como servicio es un modelo en el que los operadores permiten a terceros lanzar ataques utilizando su programa a cambio de una tarifa.

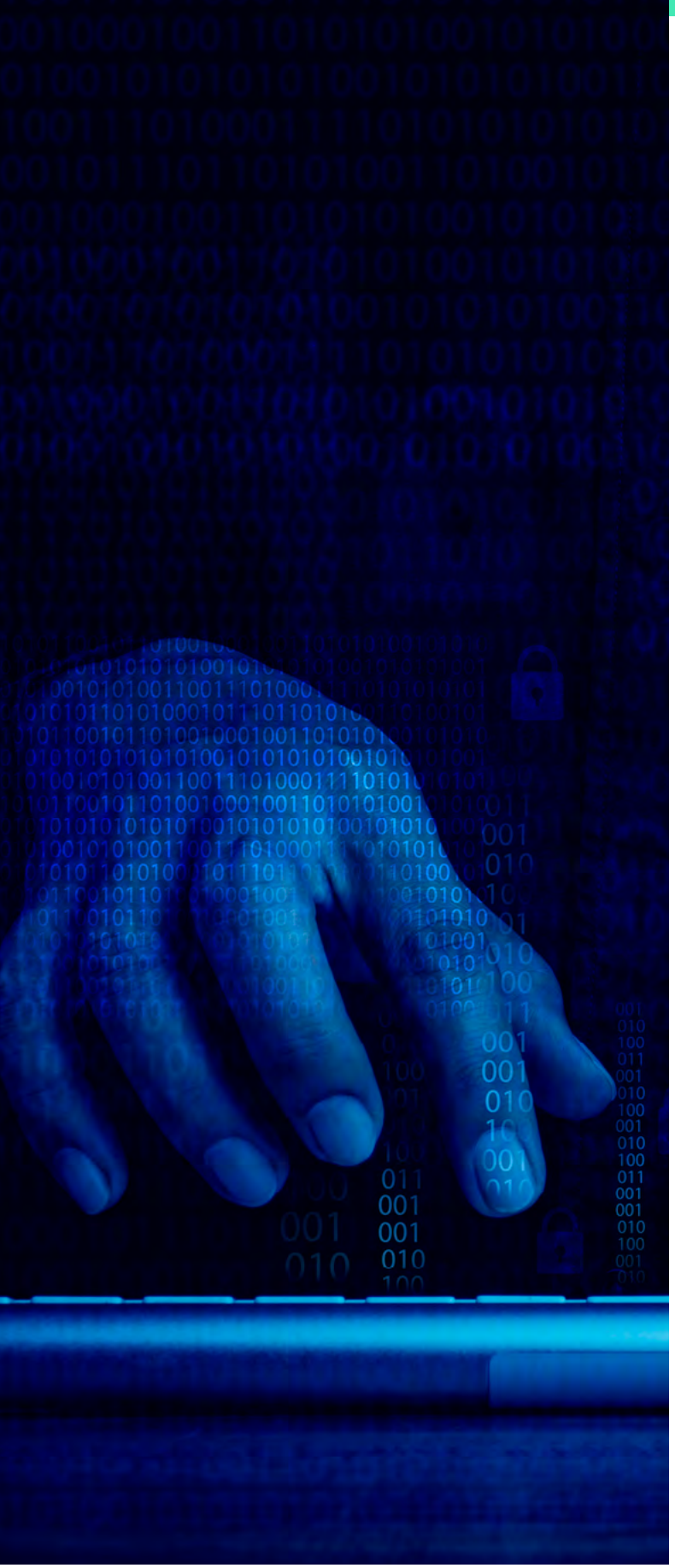
Pese a que los países comúnmente afectados por esta amenaza están en Norteamérica y Europa, Sudamérica no ha permanecido ajena a estas amenazas y proyecta nuevos riesgos para el año que viene.

Cibercrimen a través del Ransomware-as-a-Service (RaaS)

Durante lo que va del 2022, la amenaza de ransomware se mantiene en vías de crecimiento y su principal objetivo son las empresas más grandes, debido a que pueden solicitar pagos más elevados. Esto se ha visto aumentado por la aparición del RaaS, cuyo desarrollo hace proyectar que el 2023 seguirá siendo un año favorable para el cibercrimen.

Hacking as-a-Service (HaaS):

El Hacking se ofrece como servicio, para quien esté dispuesto a pagar por ello, por usuarios de la Dark o Deep web (DDW). Se asocia con actividades ilícitas y no debe confundirse con otras prácticas legales como las pruebas de penetración.



Se caracteriza por el desarrollo de herramientas privadas o de código abierto, las cuales, en su gran mayoría, son empleadas para cometer acciones ilícitas.

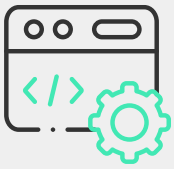
El 2022 nos ha mostrado la continuidad y crecimiento en la venta de este tipo de servicios en diferentes sitios de la DDW. Se presentan en una amplia variedad y ofrecen, en su gran mayoría, la posibilidad de conseguir datos que le generen un beneficio económico al "cliente".

Dentro de los principales motivos para elegir este tipo de soluciones se destacan: recopilar y rastrear personas, acceder a cuentas de correos electrónicos, redes sociales, teléfonos celulares, crear sitios web falsos y propagar malware.

En esta línea, algunos de los servicios más populares disponibles en los sitios de HaaS son:

- **Acceso a redes sociales, correos y teléfonos:** un usuario malintencionado puede obtener acceso no autorizado a cuentas de Facebook, Twitter, Instagram, Reddit, Gmail, Yahoo, entre otras, así como operar de forma remota el teléfono de la víctima (Spyware).

- **Vigilancia:** se usa para recopilar datos y rastrear a personas, actividad que se realiza a través de inteligencia basada en la ubicación de teléfonos y computadoras, junto con otras formas de inteligencia humana (HUMINT).



- **Manipulación del sitio:** normalmente, aquí nos encontramos con DDoS u otro tipo de sitio o servidor web que manipula desde un objetivo específico, ya sea para robo de datos o inhabilitar operaciones en la plataforma.

- **Distribución de malware:** la propagación de malware se puede utilizar en muchos otros servicios ofrecidos en el mercado HaaS, como distribución de link malicioso con estrategias de ingeniería social o Phishing, así como ataques de DDoS de botnets supervisados por spyware, entre otros.

› 1.1. Panorama de ciberactores

Este año 2022 estuvo marcado por el alza de eventos que comprometieron la seguridad de organizaciones a nivel global, con un crecimiento considerable en Latinoamérica y en Chile.

Como reacción de defensa, para erradicar la vertiginosa alza del cibercrimen, instituciones gubernamentales de las zonas afectadas continuaron realizando operaciones organizadas durante el 2022, de forma conjunta como combinada:

- **Operaciones Conjuntas**
  Son aquellas que aplican principios de planificación, organización y administración para ejecutar tareas en el campo de batalla. Se ejecutan mediante la cooperación de las distintas ramas de las Fuerzas Armadas y de organizaciones gubernamentales de carácter civil. Es decir, son operaciones entre instituciones de orden y defensa de un mismo país.

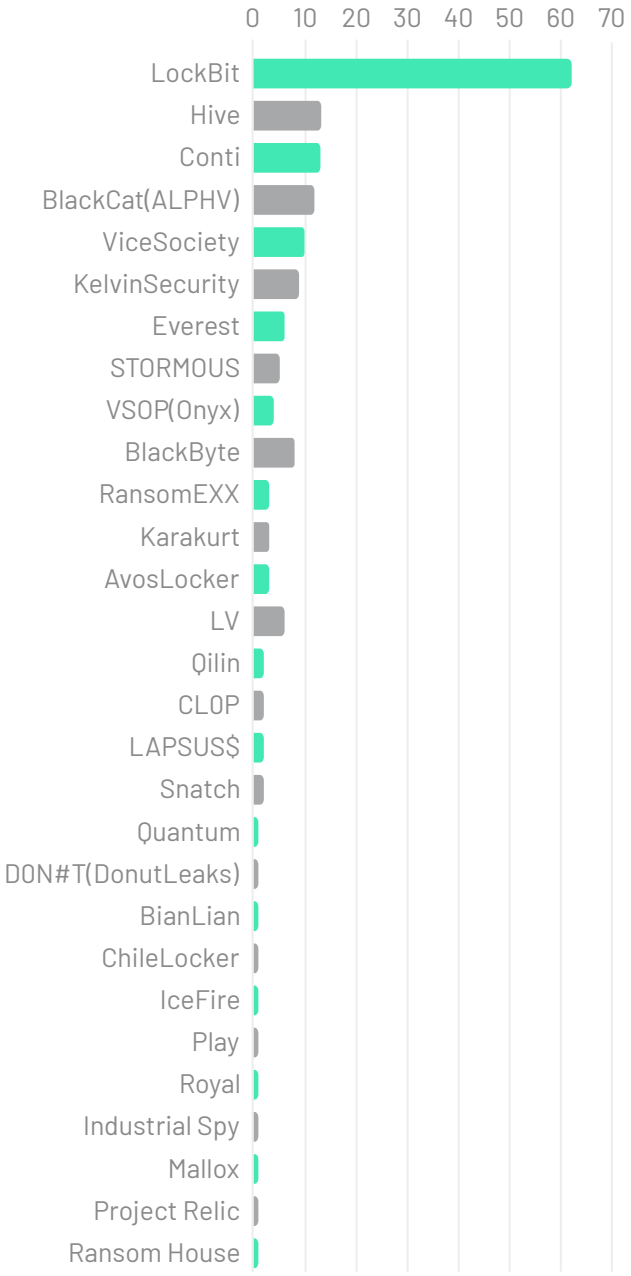
- **Operaciones Combinadas**
  Complementaria a las conjuntas, son aquellas aplicaciones de principios de planificación, organización y administración para la ejecución de tareas en las que intervienen fuerzas de varios países.

Al tanto de estas acciones, los ciberdelincuentes han tomado nuevas medidas de precaución para resguardar su identidad y evitar su exposición pública. Pese a estos esfuerzos, se ha logrado identificar una serie de organizaciones delictivas responsables de ataques de ***ransomware, data leak y phishing*** en el territorio latinoamericano, cuya procedencia es de nivel global.

Ciberactores ligados al uso de Ransomware en LATAM 2022

En este periodo se detectaron 29 ciberactores ligados al uso de ransomware presentes en la región, destacando por su impacto a Vicesociety, BlackCat(ALPHV), Conti, Hive y por último LockBit que fue la amenaza más grande, responsable de cerca del 35% de los incidentes totales.

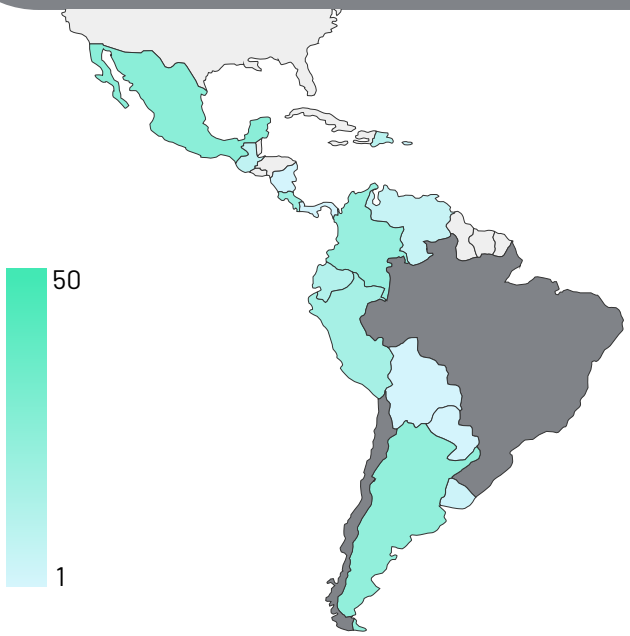
Incidencia **Ransomware LATAM**



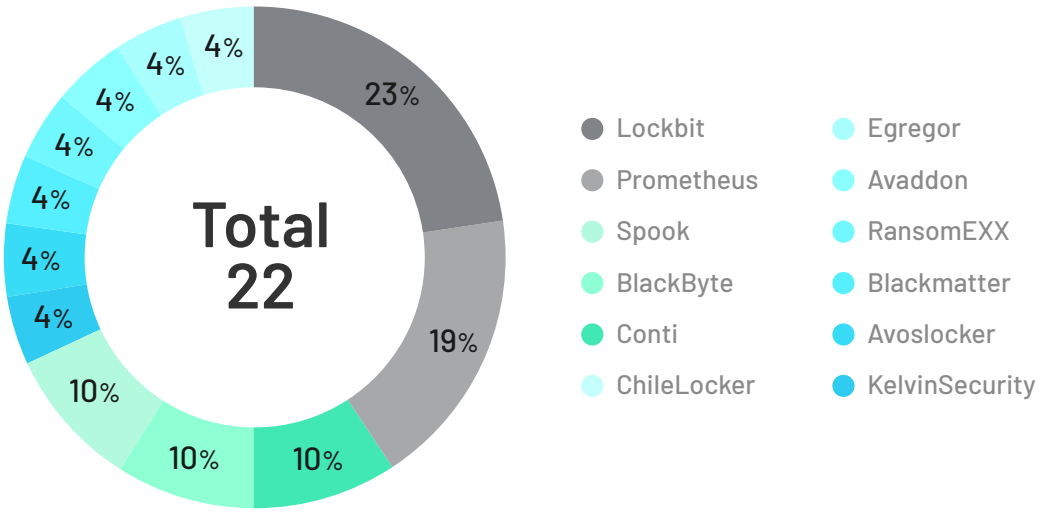
Ranking panorama latinoamericano

1° Brasil, con 51 incidencias de ransomware desde el primero de enero hasta el 30 de noviembre de 2022.

Chile ocupa el séptimo lugar con 8 incidencias, representando casi un 5% de las incidencias en la región.



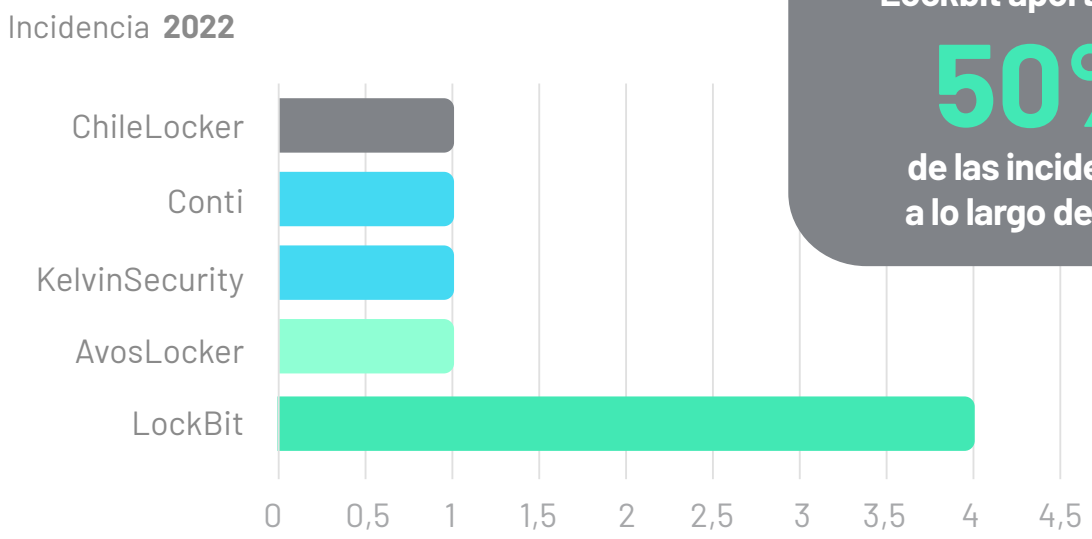
Incidencia de **Ransomware en Chile 2020 hasta el 2022**



De los 29 actores identificados en Latinoamérica, sólo 12 han cometido actos delictivos en Chile, tomando una relevancia para la ciberseguridad del país.

El principal responsable de vulnerar sistemas de seguridad **en Chile es Lockbit, que se perfila como la mayor amenaza para este 2023.**

Cantidad de **Ransomware en Chile**



El ransomware Lockbit aportó con el

50%

de las incidencias a lo largo del 2022

Ciberactores ligados al uso de Ransomware en Chile.

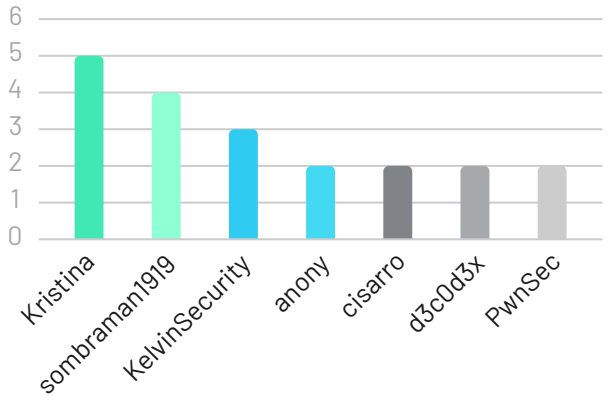
Los ciberactores de data leaks se presentan en la Deep y Dark Web (DDW) bajo diferentes seudónimos o alias, para ocultar su identidad mientras llevan a cabo sus proyectos de filtración de datos. Existe una amplia variedad de actores que se han visto involucrados en casos de filtración de información en LATAM.

Uno de los mayores eventos de data leak vinculados a LATAM en el último tiempo, además del renombrado caso de Pandora Papers, tiene que ver con **el grupo Guacamaya. Este grupo ha realizado filtraciones como actos de hacktivismo, poniendo en riesgo la seguridad de diferentes organismos estatales.**

Aunque no existe claridad sobre sus integrantes, la evidencia sugiere que podrían tener operadores de nacionalidad chilena, quienes se han adjudicado el haber vulnerado servidores de correo electrónico de diferentes organismos gubernamentales y privados dentro de la región.

En el caso específico de Chile, diversos actores, mediante distintos alias, han protagonizado filtraciones de información relacionada al país. Entre los alias más recurrentes, destacan Kristina, sombraman19191 y KelvinSecurity, los que han generado un total de 12 incidencias a nivel nacional.

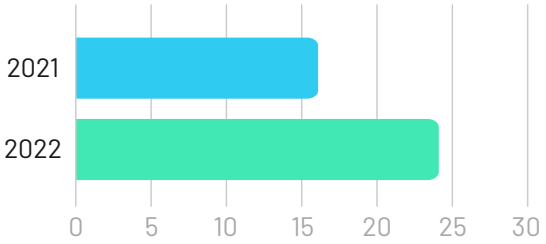
Cantidad de **filtraciones por Alias 2021-2022**



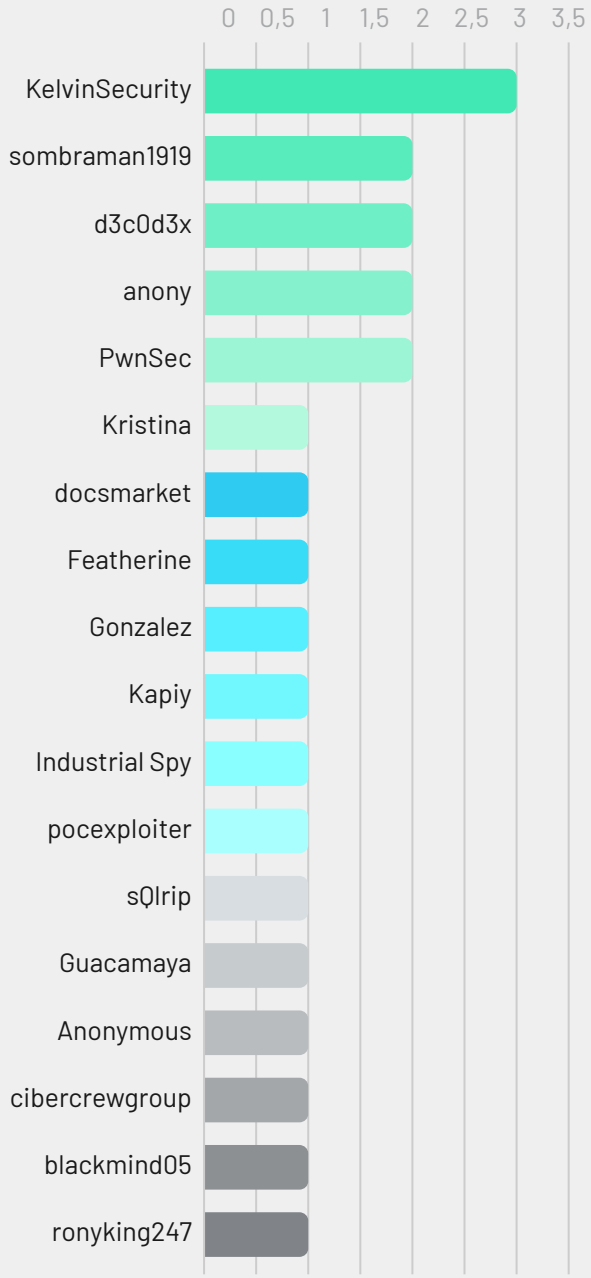
A lo largo del 2021, el alias Kristina tomó un rol protagónico en el panorama de data leaks nacional, siendo responsable de cinco filtraciones. Sin embargo, **en el 2022** cedió espacio para la aparición de **KelvinSecurity, se ha convertido en la amenaza más prolífica actualmente con tres filtraciones en el año.**

La aparición de todos estos actores ha provocado un crecimiento significativo en el número de casos de data leaks que el país ha presenciado durante los últimos años. De mantenerse el ritmo de crecimiento actual que ha llevado hasta ahora, **se estiman cerca de 36 incidentes en relación a filtraciones que involucran organizaciones chilenas para el año 2023.**

Comparativa de filtraciones de datos **relacionados a Chile durante años 2021 y 2022**



Cantidad de **filtraciones por Alias 2022**



Ciberactores ligados al uso de phishing en Chile y LATAM

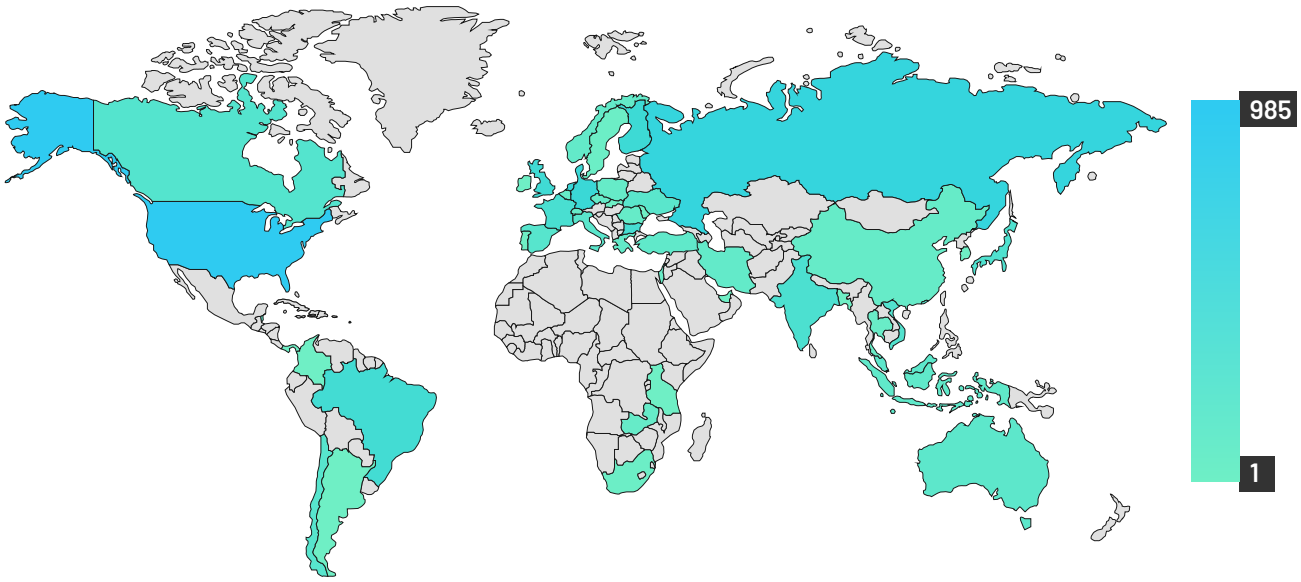
Las campañas de engaño bajo técnicas de phishing han experimentado un crecimiento acelerado que les ha valido atención a nivel global, donde Chile no ha sido la excepción.

Identificar a los actores relacionados con el phishing no resulta una misión simple, sobre todo por la gran oferta de hosting gratuitos o de bajo costo de los cuales estos actores se sirven para llevar a cabo sus operaciones para no ser ubicados.

De esta manera, aunque nuestros registros señalan que la gran mayoría de las IP's donde se alojan las campañas de phishing dirigidas a Chile y LATAM se geolocalizan principalmente en Estados Unidos, es difícil asegurar que hayan empezado efectivamente ahí, ya que es en este país donde se encuentra la gran mayoría de los hosting a nivel mundial.

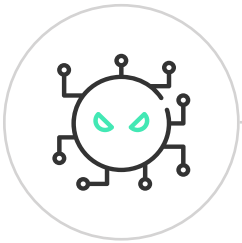
De cualquier manera, aunque las nuevas medidas de muchos ciberdelincuentes les ayudan a ocultar su ubicación e identidad, este mapa permite comenzar a armarse una idea sobre la forma en que se distribuyen y organizan las campañas de phishing que han impactado a nuestro país.

Geolocalización de IP **donde se aloja el phishing**



CAPÍTULO 2.

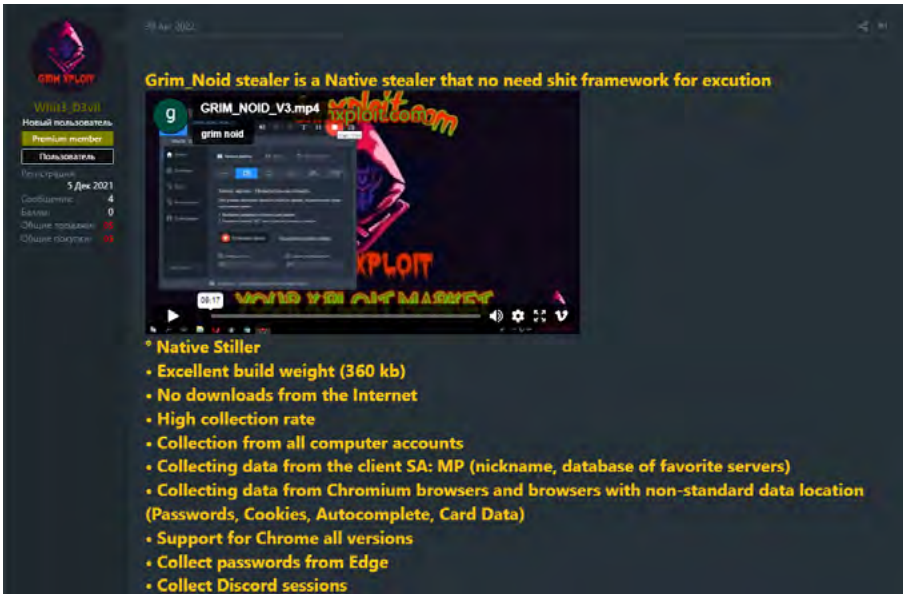
ROBO DE INFORMACIÓN, CÓMO SE PRODUCE Y QUÉ EFECTOS TIENE



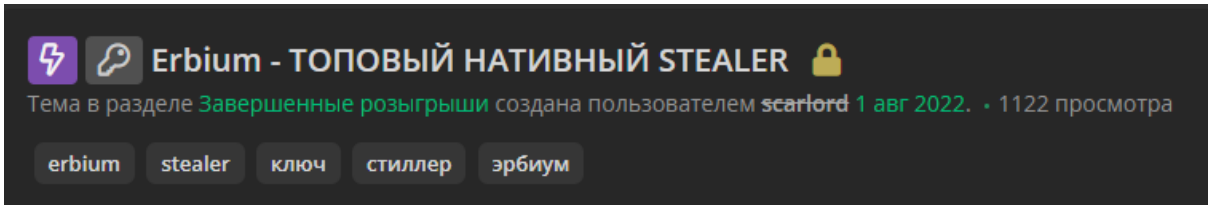
La gran mayoría de los robos de información se lleva a cabo bajo un mismo proceso, que utiliza varias familias de malware para cada caso y operación. Sin embargo, los métodos más frecuentes son la propagación de malware de la familia Dropper e Infostealer.

Mientras Dropper maximiza el volumen de malware descargado en el equipo, Infostealer se centra en secuestrar la mayor cantidad de información posible, para luego implantar nuevas cargas útiles (*payload*) y continuar con el ataque. Una vez que se logra permanencia en la red objetivo sin ser detectado, sea por cualquiera de los dos métodos, se procede a generar un movimiento lateral. Esta táctica busca comprometer la mayor cantidad de equipos posible y elevar privilegios hasta, por ejemplo, alcanzar un Active Directory, posición desde la que pueden controlar e infectar toda la red.

En este punto, el actor malicioso comienza a exfiltrar información relevante de la víctima, para hacerse con ella y posteriormente desplegar un malware de mayor capacidad como ransomware o wiper, realizar extorsiones a cambio de un beneficio, filtrar información (data leak) o alguna otra acción, según sean sus objetivos.



Foro underground donde se **ofrece a la venta Infostealer Grim_noid**



Foro underground donde **se ofrece a la venta Infostealer Erbium**

Tipos de Data leak

Podemos reconocer tres tipos principales de data leak:

- **Data leak corporativo**

Este tipo de filtraciones de información aplica tanto para corporaciones como para redes sociales y/o plataformas ampliamente utilizadas, que requieran el registro y la confianza de personas que ingresan información personal.

El data leak corporativo suele estar principalmente originado por ransomware y negociaciones fallidas que, por no pago de rescate, terminan en la divulgación de información que luego es rápidamente consumida por los usuarios. En este tipo de filtraciones, suelen incluirse registros de usuarios de active directory.

Por otra parte, el dump de bases de datos de sitios web es otro fenómeno de filtración de información corporativa, que suele ser

enfocado al secuestro de tarjetas y accesos bancarios. Adicionalmente, existen ataques enfocados en el secuestro de credenciales, lo cual resulta atractivo para cibercriminales, ya que pueden ofrecerlas a la venta.

- **Data leak por vulnerabilidades**

Tiene gran similitud con el data leak corporativo, ya que en este último también se suelen explotar vulnerabilidades perimetrales o configuraciones deficientes, con la finalidad de acceder a sistemas de terceros o la utilización de técnicas como el phishing.

Resulta bastante común que los ataques dirigidos exploten vulnerabilidades de software para concretar la infección (Macros, Follina) o involucren la explotación activa de vulnerabilidades en algún punto de la intrusión.

- **Data leak a usuarios individuales**

En Chile y Latinoamérica, este tipo de filtraciones se realiza, principalmente, por infección con malware del tipo infostealer y se suele distribuir por medio de troyanos en softwares fraudulentos ofrecidos en internet. Una vez que el intruso entra en el equipo víctima, roba la mayor cantidad de información posible. Esto puede incluso permitirles un perfilamiento detallado del usuario y terminar en casos de suplantación de identidad.

En 2022, los data leak más comunes en nuestro país correspondían a usuarios individuales que, mediante la infección de malware infostealer, comprometen accesos organizacionales, permitiendo que sus credenciales (para diferentes plataformas) sean ofrecidas en internet de forma gratuita o pagada.

Este tipo de robo de credenciales por infostealer se mantiene como tendencia a nivel global. Sin embargo, existen otros servicios alojados fuera de Chile que han sufrido casos de data leak masivos, como es el caso del gigante tecnológico Twitter.

› 2.1. Panorama de Amenazas (Ransomware y Malware)

Malware

El panorama de malware en Latinoamérica cuenta con bastantes amenazas significativas. Entre las más activas, se destacan Emotet, Frombook, XMRig y AgentTesla.

- **Emotet**

Es el malware con mayor actividad a nivel mundial. Está activo desde el año 2014 y es operado por el grupo TA542, quien constantemente actualiza, desarrolla y modifica sus TTP´s para evadir su detección. Modificar los IoC´s es una tarea fácil y bastante común dentro de las familias de malware, pero para cambiar las TTP´s se requiere gran expertiz y desarrollo. Esto pone en evidencia las grandes capacidades de TA542, que incluso mantiene segmentaciones geográficas en sus redes de bots, denominadas desde Epoch1 a Epoch6.

Las campañas de este malware se han extendido por regiones variadas y se han identificado casos donde la distribución estaba siendo dirigida específicamente a Chile. Investigaciones han logrado evidenciar la presencia de campañas dirigidas a suplantar correos electrónicos de entidades gubernamentales del país, mediante documentos ofimáticos con macros maliciosas, que comienzan la descarga y ejecución de malware adicional en el sistema afectado.

- **FormBook**

Es un troyano con capacidades de infostealer disponible como malware-as-a-service (MaaS). Normalmente, se distribuye a través de correos electrónicos con datos adjuntos maliciosos y se puede utilizar para robar distintos tipos de información.

Este malware tiene funciones de robo avanzadas, como las capacidades de extraer información almacenada y registrada de un usuario, buscar, ver e interactuar con archivos, tomar capturas de pantalla y recibir órdenes directas mediante C&C.

- **XMRig:**

Es un software de minería de código abierto, completamente legal, que facilita el acceso a la criptominería de Monero, una criptomoneda difícil de rastrear. Esto ha ayudado a ciberdelincuentes a mantener un mayor anonimato.

Se vió por primera vez el 26 de mayo de 2017 y ha sido adoptado en campañas maliciosas para añadir nuevas funcionalidades de criptominería a su malware. Dentro de los que utilizan a XMRig se encuentran VictoryGate y la botnet Phorpiex, quienes se dedican a distribuir este minero en todos los equipos que infectan.

- **AgentTesla:**

Es un infostealer que se conoce desde el año 2014 y, desde sus inicios, ha sido ligado al robo de datos y credenciales. Este malware es distribuido principalmente mediante correo electrónico con archivos adjuntos maliciosos.

Hasta hoy, sigue vigente y se le considera un actor muy peligroso, gracias a su capacidad de adaptación con nuevas variantes y módulos que permiten hacerse con credenciales de aplicaciones descargadas, navegadores web, clientes VPN, FTP o de correo electrónico.

Según registros, la mayor actividad se encuentra orientada hacia el malware del tipo infostealer, el cual representa un negocio altamente lucrativo que genera víctimas a diario. Su funcionamiento tiene grandes ventajas en comparación a un ataque directo, ya que permite otorgar accesos iniciales a plataformas restringidas con mayor facilidad, tiene un menor porcentaje de detección, menos actividad en la infraestructura del atacado y logra operar en un tiempo más acotado.

Ransomware

Datos y estadísticas internas señalan que los últimos dos años han estado marcados por la prosperidad y el crecimiento continuo del ransomware en Latinoamérica y, particularmente, en Chile. Estos ataques se han vuelto un panorama cada vez más habitual en toda la región. En el país, el año 2021 cerró con un total de 12 víctimas conocidas y hasta noviembre de 2022 se contabilizaron ocho de este tipo.

Cantidad **Ransomware en Chile**

Año 2020 Año 2021 Año 2022

El alcance mediático de estos casos suele relacionarse con el avance de las negociaciones entre las víctimas y los actores maliciosos. Dependiendo de cuántos beneficios estén logrando obtener estos últimos, tomarán medidas para hacer más o menos públicos los datos robados.

Si las negociaciones o extorsiones no están resultando beneficiosas para los ciberdelincuentes, suelen exponer a las víctimas de manera pública. Esto también puede ocurrir si el afectado cuenta con capacidades de restauración suficientes para mitigar el impacto, de manera parcial o total, evadiendo con esto el proceso de extorsión.

Por otra parte, existen escenarios donde se dan a conocer a las víctimas por un breve periodo de tiempo o son revelados de forma parcial, con el fin de presionarlas a pagar el rescate. En "el mejor de los casos", si las negociaciones están cumpliendo bien las aspiraciones de los victimarios, puede que no se publique el caso y éste permanezca desapercibido para la comunidad.

Presencia en Chile

Entre los casos altamente mediáticos ocurridos en nuestro país, destacan los que afectaron a instituciones de gobierno. Se ha notado también un incremento en las bandas de ransomware que antes operaban en otras regiones y ahora han comenzado a dejar un gran número de víctimas en el país, como es el caso de LockBit.

Esta última es una de las bandas de ransomware más activas del momento y cuenta con el registro histórico de víctimas más alto, superando con creces los números de Conti (APT Ruso). **Entre 2020 y 2022, LockBit (Online) lidera el listado de amenazas con mayor número de incidencias, seguido de Prometheus** (Offline), Conti (Offline), BlackByte (Online) y Spook (Offline).

› 2.2. Panorama de Phishing

El phishing es un fraude que se realiza suplantando la identidad de una persona u organización. Sus procedimientos se reinventan continuamente y están en un constante proceso de perfeccionamiento para evitar el reconocimiento de los atacantes. Dentro de sus principales objetivos destacan el robo de contraseñas, tarjetas de crédito, datos financieros y hasta la usurpación de identidad en redes sociales, entre otros.

Además, el phishing se utiliza como un medio de distribución de malware, lo que ha marcado una tendencia en los últimos años, ya que su efectividad es trágicamente alta. Se ha convertido en una potente herramienta de ejecución de diferentes amenazas, desde infostealer hasta ransomware y malware del tipo RAT.

Para conseguir estos distintos fines, se utilizan técnicas como: **Browser in the browser, Google Captcha y Crypto-scan.**

- **Browser in the browser (BITB)**

Este es un recurso que fue detectado por primera vez en el año 2020, pero que se ha popularizado durante el pasado 2022. Permite insertar una ventana emergente en un sitio web y desplegar campos de login falsos para sustraer los datos del usuario. Estas ventanas son muy difíciles de detectar para un ojo inexperto, ya que el sitio fraudulento se las arregla para ser idéntico al original, inclusive en su URL. La diferencia fundamental es que no corresponde a un sitio web en sí, sino que a una ventana dentro de otra ventana (Browser in the Browser).

Esta técnica se popularizó luego de que en sitios como GitHub se publicaran plantillas para ejecutar este tipo de ataque, reduciendo drásticamente el nivel de sofisticación para su despliegue. Para detectar un fraude de este tipo, es importante considerar que las ventanas comunes de un navegador pueden moverse dentro de la pantalla, maximizar y minimizar, mientras que aquellas alojadas como emergentes sólo pueden moverse dentro de la ventana donde se alojan.

- **Google CAPTCHA**

Algunos ciberdelincuentes han comenzado a utilizar CAPTCHA y reCAPTCHA de Google (también conocido como la función "No soy un robot") para ocultar algunas de sus campañas de phishing, utilizando técnicas de evasión para escapar de la detección de los rastreadores de seguridad automatizados.

Investigadores de Unit 42 de Palo Alto han informado que "las URL maliciosas protegidas por CAPTCHA se están multiplicando". Esto resulta preocupante, ya que indica que, por medio de reCAPTCHA, los ciberdelincuentes logran bloquear el contenido de sus páginas de phishing y evitan que los servicios de escaneo de URL detecten el contenido malicioso. Así, logran otorgar un aspecto legítimo a sus páginas de inicio de sesión y conseguir que las víctimas ingresen sus datos.

- **Crypto-scam**

Este tipo de ataques se realiza en el sector de las criptomonedas. Primero, los actores maliciosos suelen realizar campañas de suplantación de identidad o de secuestro de cuentas verificadas de redes sociales. Así, utilizan luego la reputación de una persona legítima y reconocida en el rubro, con el fin de que usuarios menos experimentados se vean involucrados en uno o más de los siguientes engaños:

1. Se insta al usuario para que transfiera de forma voluntaria su dinero a una billetera virtual maliciosa, con la premisa de que será multiplicado rápidamente.

2. Se invita a la víctima a comprar criptomonedas de proyectos falsos, que prometen altas rentabilidades, pero son inexistentes.

3. Se convence al usuario de firmar un SmartContract en donde, sin saberlo, entrega la totalidad de sus fondos a los delincuentes.

Registros y tendencias de Phishing

De acuerdo con el portal PhishStats, entre las estadísticas globales que es posible obtener del procesamiento de millones de registros, destacan los siguientes términos:

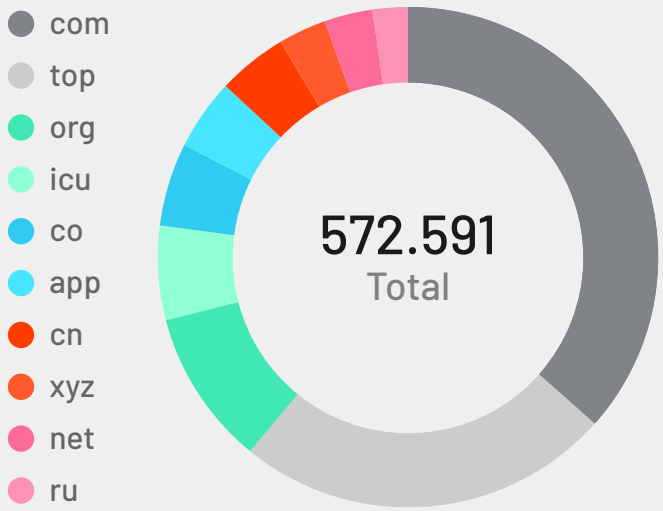
TOP TLD's

Corresponde a los Top Level Domain más utilizados para campañas de phishing. Entre estos, el dominio .com, abarca aproximadamente un 37% de los hallazgos, seguido por .top con un 24.5% y .org con un 10%.

A partir de este dato, es llamativa la facilidad que tienen los ciberactores para conseguir los dominios .com. Es de conocimiento general que, para poder obtenerlos, es necesario realizar una compra. Esto entrega una trazabilidad con los operadores, en caso de que se lleve a cabo una investigación. Sin embargo, los delincuentes implementan mecanismos de una larga cadena de delitos para sortear este registro, como, por ejemplo:

- La implantación de phishing en sitios webs legítimos que son vulnerables y que ya cuentan con un TLD conocido.
- El uso de tarjetas bancarias obtenidas en el mercado negro para poder adquirir los dominios deseados sin entregar datos personales reales.
- La utilización de un web hosting gratuito con dominios conocidos.

Top 10 TLDs - año en curso



Volumen de Phishing histórico

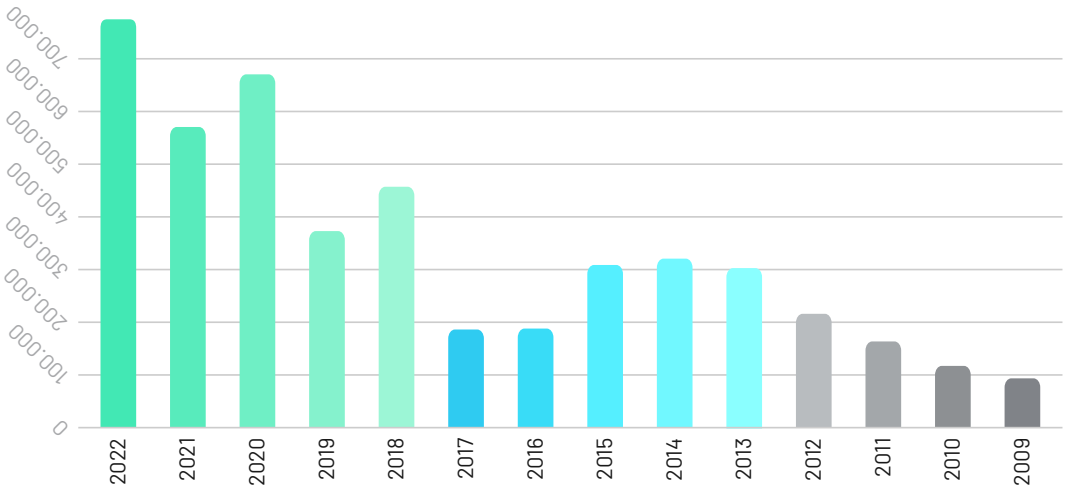
De acuerdo a los datos obtenidos desde la misma fuente, es posible observar que el año 2022 fue el año con mayor cantidad de sitios fraudulentos registrados, seguido por el año 2020. Este último, gracias a la aparición del COVID-19, se volvió un escenario favorable para la difusión de enlaces maliciosos. A pesar de que se puede esperar un alza en el corto y mediano plazo, la tendencia en los años anteriores (2020, 2021 y 2022) ha mostrado que los volúmenes de phishing histórico han sufrido de alzas y bajas.

HTTP v/s HTTPS

Los atacantes se ven en la necesidad de adaptarse constantemente a los nuevos procesos de seguridad implementados en internet, para que sus campañas sean más convincentes y efectivas. Para ello, deben adoptar nuevas estrategias que les permitan obtener certificados de seguridad en sus sitios web, entre las que se destacan:

- La utilización de web hosting gratuitos que cuentan con certificados HTTPS.
- La implantación de sitios fraudulentos en sitios vulnerables que cuentan con certificados ya adquiridos.
- La suplantación de tarjetas bancarias para la adquisición de nuevos certificados seguros.
- Los ataques a entidades certificadoras (CA).

Búsquedas de **URL por año**



*2022 actualizado al 30 Noviembre son 780.170 (incremento del 138% con respecto a 2021)

Los datos muestran que, en la actualidad, **la cantidad de sitios de phishing con certificados de seguridad es comparable con los que no los poseen.** El año 2020 marcó un registro histórico donde las webs con HTTPS superaron a las menos seguras.

Un caso reciente

Empleando las técnicas descritas, distintos ciberactores han ejecutado campañas de phishing a nivel global. Entre ellos, podemos destacar el caso de Earth Preta:

- **Earth Preta - Spear-Phishing**

Durante 2022, se ha observado al APT Earth Preta (AKA Mustang Panda y Bronze President), originario de China, realizando campañas de ciberespionaje mediante spear-phishing, con un enfoque mundial. Se ha dirigido específicamente hacia áreas de la educación, gobiernos, fundaciones y sectores de investigación, demostrando que es una técnica transversal para operaciones de diferentes envergaduras y motivaciones.

Su principal vector de ataque es la ingeniería social, apelando al usuario, quien usualmente resulta ser el eslabón más débil de la cadena de seguridad.

2.3. Panorama de Data leaks

Dos conceptos, cuya diferencia resulta fundamental para comprender en detalle la manera en que se ha desarrollado este panorama, son **data breach** y **data leak**:

- **Data breach**

Corresponde al robo de datos de organizaciones que contienen malas prácticas en términos de seguridad, como configuraciones erróneas o deficientes, las cuales exponen datos sensibles de forma pública, sin siquiera saberlo.

- **Data leak**

Es el robo de datos a organizaciones, por medio de un ciberataque que compromete parte de su infraestructura. Estos, por lo general, son de alta relevancia y permiten sustraer información confidencial.

Dentro de estas fugas de datos, ya sean por ataques premeditados o por daño colateral resultante de un ataque, se obtiene una amplia variedad de información. Entre los datos más comunes, se encuentran:

1. **Direcciones de correo electrónico.**
2. **Contraseñas.**
3. **Nombres.**
4. **Números de teléfono.**
5. **Direcciones IP.**
6. **Nombres de usuario.**
7. **Direcciones físicas.**
8. **Fechas de nacimiento.**
9. **Géneros.**
10. **Compras.**
11. **Ubicaciones geográficas.**
12. **Perfiles en las redes sociales.**
13. **Estado civil.**
14. **Ocupaciones.**
15. **Números de cuentas bancarias.**

La información robada, comúnmente, se ofrece en foros de DDW o en los canales de Telegram de cada operador. Los precios que se le asignan varían según diferentes modalidades de venta, dependiendo de si se ofrece la totalidad o una parte de los datos, del número de clientes y de si contienen datos de ubicación geográfica.

Por otra parte, el valor de compra de la información filtrada depende también del tipo de información que se oferte, los cuales se estiman de forma general en:

Entre 25 y 65 USD c/u

Valores de cuentas de **RRSS secuestradas**

Entre 20 y 30 USD c/u

Valores de **tarjetas de crédito clonadas**

Entre 25 y 35 USD c/u

Valores de **cuentas bancarias hackeadas**

Entre 80 y 120 USD c/u

Cuentas bancarias con saldo superior a **$2.000 USD**

Entre 10 y 50 USD c/u

Cuentas de **Paypal o Western Union**

Registros y tendencias

Es común pensar que las grandes filtraciones de datos no suelen afectarnos, menos aún cuando ocurren lejos de nuestro país de residencia. Sin embargo, esta idea presenta un sesgo importante, ya que no contempla los servicios que utilizamos en internet. Al participar de diferentes servicios globales en la red, podemos haber sido afectados por una filtración masiva sin saberlo.

Un ejemplo significativo de este problema fue una de las publicaciones más recientes, ocurrida en 2021, que expuso registros de usuarios de Facebook en todo el mundo. De estos usuarios, cerca de siete millones corresponden a Chile. Este episodio se ubica entre los 15 data leak más grandes conocidos a día de hoy y filtró más de 500 millones de registros a nivel global.

Top 15 Data Leak de compañías **con mayor cantidad de registros históricos**

1. Yahoo - 2013 — 3.000.000.000
2. River City Media Spam List - 2017 — 1.373.430.309
3. Aadhaar - 2018 — 1.100.000.000
4. Whisper Secret-sharing app - 2022 — 900.000.000
5. First American Corporation - 2019 — 885.000.000
6. Verifications.io - 2019 — 763.117.241
7. Onliner Spambot - 2017 — 711.477.622
8. LinkedIn Scraped Data - 2021 — 700.000.000
9. CAM4 Adult Site (10.88 miles de millones de registros) - 2020 — 693.067.857

10

Data Enrichment Exposure From PDL Customer - 2019

622.161.052

11

Facebook - 2019

540.000.000

12

Facebook - 2021

509.458.528

13

Syniverse - 2021

500.000.000

14

Yahoo - 2014

500.000.000

15

Friend Finder Networks - 2016

412.214.295

Por otra parte, de entre las organizaciones responsables de coleccionar la mayor cantidad de registros tomados de Data breach, se ha podido identificar a 5 principales. El ranking es liderado por la organización de ciberdelincuentes COMB21, con más de 3 mil millones de registros históricos.

Top 5 colecciones de Data Breach con **mayor cantidad de registros históricos**

Puesto	Organización	Año	Breach
1	COMB21	2021	3.279.064.312
2	Collection #1-5	2019	2.200.000.000
3	16 hacked websites	2019	617.000.000
4	Exploit.In (unverified)	2017	593.427.119
5	Anti Public Combo List (unverified)	2017	457.962.538

En este escenario, se sospecha que los actores maliciosos están utilizando estas tácticas como base de conocimiento para desarrollar otros métodos de ataque. Por ejemplo, analizan las contraseñas más usadas, con el fin de encontrar patrones para dar con otras adicionales. Las reutilizan o toman como base su formato de creación, para así romper otras contraseñas con mayor eficiencia.

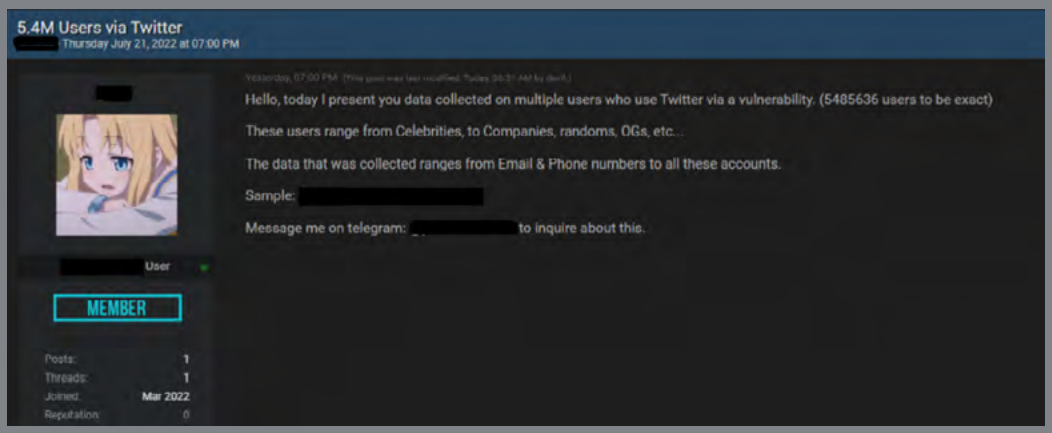
Gracias a estas bases de conocimiento, se han creado diccionarios con las contraseñas más comunes, como por ejemplo “Rockyou2021”, que permiten generar ataques de fuerza bruta mediante el uso de ellas.

Casos recientes

La filtración de datos ha protagonizado distintos ataques a grandes corporaciones y presenta en la actualidad una amenaza importante. De entre los casos más mediáticos se destacan los sufridos por Twitter, Meta, Microsoft y algunas organizaciones gubernamentales latinoamericanas.

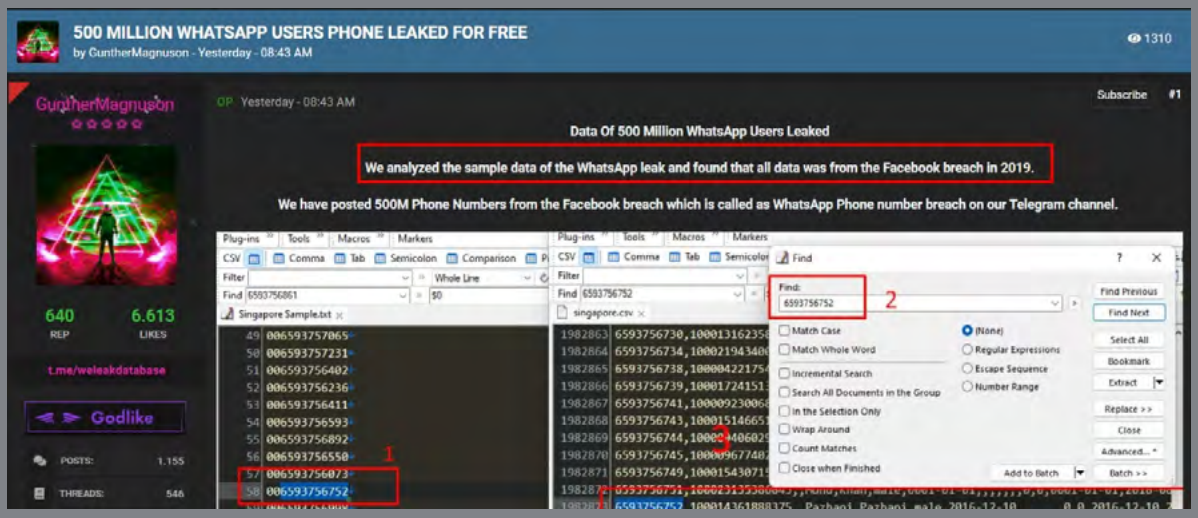
- **Twitter**

En 2022, una masiva filtración de datos, principalmente de correos electrónicos y números de teléfono, tuvo como víctimas a usuarios de la plataforma Twitter. Entre ellos se contaban distintas personalidades, como celebridades, compañías, organizaciones y usuarios comunes. La información filtrada se vendía en el canal de Telegram del ciberactor responsable.



- **Whatsapp**

Los ciberdelincuentes no siempre cobran por las filtraciones de la información, como es el caso del data leak sufrido por usuarios de WhatsApp, que entregó datos de más de 500 millones de personas. Según los mismos anunciantes, corresponde a información del data leak ocurrido en Facebook en 2019. Al pertenecer a la misma compañía que Facebook "Meta", facilitó el acceso a la plataforma y es de esperarse que permita vincularse con usuarios de Instagram.



- **Microsoft**

Uno de los eventos más relevantes del presente año corresponde al data leak vinculado al gigante Microsoft, que ha sido nombrado como **BlueBleed**. Este ataque se logró gracias a una mala configuración de un servidor expuesto hacia Internet, lo que posibilitó el acceso no autenticado a datos de transacciones comerciales entre la compañía y clientes potenciales. Igualmente, permitió acceder a la planificación, implementación y provisión de servicios de Microsoft, entregando así información de clientes de la propia empresa.

Organizaciones gubernamentales en LATAM y Chile

En el ámbito público, uno de los mayores eventos de leaks de datos vinculados a LATAM, fue ejecutado por el grupo Guacamaya a través de su operación fuerzas represivas. Este grupo actúa bajo causas relacionadas con el respeto a comunidades indígenas y a la naturaleza, posicionándose en contra de la sobreexplotación del territorio, tanto ante gobiernos locales como extranjeros.

De acuerdo a las evidencias obtenidas, han vulnerado servidores de correo electrónico de diferentes organismos gubernamentales y privados de Latinoamérica. Además, se estima que podrían tener operadores de nacionalidad chilena.

Entre las víctimas publicadas bajo las operaciones del grupo, se identifican las siguientes:

- **Fuerzas Armadas de Chile, Colombia, Perú y El Salvador.**
- **Secretaría de la Defensa Nacional de México (6 TB - SEDENA).**
- **Policía Nacional Civil de El Salvador (4 TB, @pnc.gob.sv).**
- **Quiborax Chile.**

CAPÍTULO 3.

PANORAMA DE VULNERABILIDADES

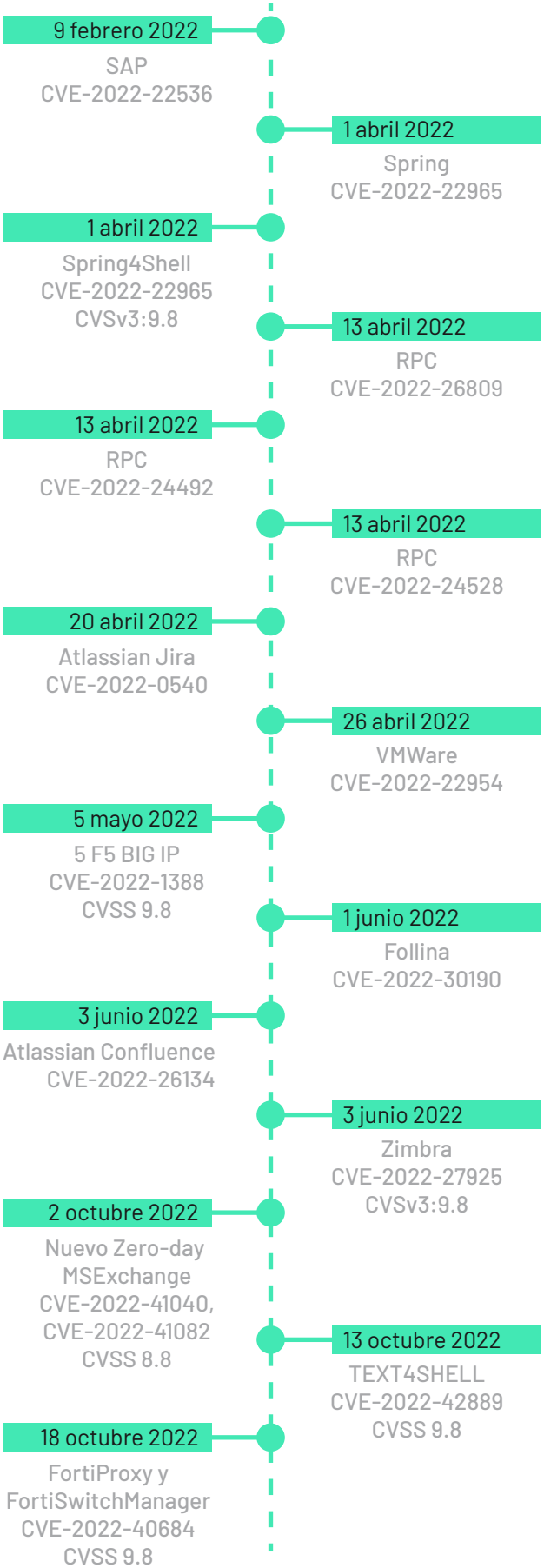
Con el paso del tiempo surgen nuevas vulnerabilidades críticas que podrían comprometer los sistemas de una organización y durante el año 2022 se han detectado varias. Aunque cada una de ellas ya cuenta con sus parches disponibles, el trabajo de monitoreo y parchado debe realizarse de forma continua y programada, contemplando todos sus activos digitales.

Las organizaciones más proactivas suelen generar procesos de parchado dentro de la primera semana del descubrimiento de la vulnerabilidad, pero existen otras que funcionan bajo el lema de "si funciona no se toca", de manera que evitan tomar medidas hasta que es demasiado tarde. Esta postura llega a venir incluso de la alta dirección, lo que revela graves falencias en sus políticas de seguridad.

Esto último se ve con más frecuencia en organizaciones pequeñas, ya que no cuentan con los recursos para mantener sus sistemas seguros. Por consiguiente, se convierten en objetivos interesantes de ataque, ya que podrían formar parte de la cadena de suministro de organizaciones más grandes y permitir a los ciberdelincuentes acceder a ellas.

Tendencias y casos recientes

Debido al gran impacto que ha causado su alta exposición y facilidad de explotación en los últimos años, es posible enumerar las siguientes vulnerabilidades críticas que han puesto en alerta máxima a administradores de sistemas para este 2023:



Se espera que las técnicas para explotar estas vulnerabilidades comiencen pronto a ser utilizadas, si es que no lo están siendo ya, por actores maliciosos, quienes buscan conseguir accesos iniciales a redes corporativas. Esta actividad les permitirá ahorrar tiempo en la preparación y ejecución de sus campañas.

Por lo mismo, es necesario conocer en detalle las vulnerabilidades más recientes y así poder identificarlas:

- **F5 BIG IP (CVE-2022-1388) - CVSS 9.8**
  Esta vulnerabilidad puede permitir que un atacante no autenticado ejecute comandos arbitrarios del sistema, para crear o eliminar archivos y deshabilitar servicios. Actualmente, se emplea por familias de malware para lograr un compromiso inicial mediante la instalación de Backdoor.

- **POC (CVE-2022-1388)**

Esta vulnerabilidad puede permitir que un atacante, no autenticado y con acceso de red, entre al sistema BIG-IP a través del puerto de administración y/o direcciones IP propias, ejecute comandos arbitrarios, genere o elimine archivos y deshabilite servicios.

- **Nuevo Zero-day MSExchange (CVE-2022-41040, CVE-2022-41082) CVSS 8.8**

Esta es una vulnerabilidad crítica de Microsoft Exchange (2013, 2016 y 2019), que está siendo explotada activamente a través de dos vulnerabilidades Zero-Day. Esto les ha permitido acceder al servidor de correo electrónico y allí cargar backdoors, maniobra que les faculta de movimientos laterales y la carga de webshells, para ejecutar comandos de forma remota.

- **TEXT4SHELL (CVE-2022-42889) - CVSS 9.8**

Es una reciente vulnerabilidad de gravedad crítica. Está presente en algunas versiones de la biblioteca Apache Commons Text y posibilita la ejecución de código de forma remota (RCE). Se ha denominado como el nuevo Log4J, pese a que existan diferencias en su modo de explotación.

- **FortiProxy y FortiSwitchManager (CVE-2022-40684) - CVSS 9.8**

Una omisión de autenticación en FortiOS y FortiProxy puede permitir que un atacante no autenticado realice operaciones en la interfaz administrativa a través de solicitudes de HTTP o HTTPS especialmente diseñadas.

Pese a que esta vulnerabilidad ya haya sido alertada a Fortinet y cuente con un parche disponible, se tiene registro de que ha seguido siendo activamente explotada por actores maliciosos al menos hasta octubre de 2022.

CAPÍTULO 4.

INFRAESTRUCTURA CRÍTICA Y CLOUD SECURITY

"Los ataques a la infraestructura crítica deben tratarse como un problema de seguridad nacional similar al terrorismo"
DoJ USA (octubre de 2021)

A inicios de 2022, producto del conflicto bélico entre Rusia y Ucrania, un nuevo escenario digital se originó, marcado por constantes ciberataques a la infraestructura crítica de ambos países. Los alcances de esta situación no han cesado y, por el contrario, han terminado por propagarse hacia el resto del mundo.

El último año ha sido testigo de la aparición de distintas campañas de los grupos delictivos involucrados, que ya se encuentran presentes en Chile. Estos grupos se enfocan en afectar distintos servicios indispensables para el funcionamiento de cualquier sociedad.

La siguiente gráfica detalla los puntos claves en la infraestructura crítica de un país:

Infraestructuras críticas de un país, según CISA

Sector químico	Instalaciones comerciales	Comunicaciones	Manufactura crítico
Base industrial de defensa	Servicios de emergencia	Tecnologías de la información	Salud y salud pública
Servicios financieros	Agroalimentario	Sistemas de transporte	Agua y saneamiento
Instalaciones gubernamentales	Sector de control de presas	Reactores nucleares, Materiales y Residuos	Sector energético

Casos históricos a nivel global

Más allá de los hechos recientes, lamentablemente, los ciberataques a la infraestructura crítica no son una novedad. Hace algunos años que se han registrado distintos eventos notables que sirven como guía para comprender más cabalmente este problema. Entre ellos, se destacan:

Año: 2014
Malware: Stuxnet

País afectado: Irán

Descripción: un ataque a la planta de enriquecimiento de uranio, generando un sobrecalentamiento que no indicó ninguna alerta en los paneles de monitoreo.

Año: 2015
Malware: BlackEnergy

País Afectado: Ucrania

Descripción: mediante phishing, se accedió a ICS (sistemas de control industrial) para apagar estaciones eléctricas y que eventualmente fueran destruidas.

Año: 2016
Malware: Industroyer

País Afectado: Ucrania

Descripción: un malware que podía ser adaptado y utilizado para atacar cualquier infraestructura crítica como Luz, Agua y Gas.

Año: 2017
Malware: NotPetya

País afectado: Ucrania (principalmente)

Descripción: un ransomware destructivo, que no buscaba pago por rescate. Principalmente ataca a Ucrania pero, por error o a propósito, se extendió por toda Europa.

Año: 2021
Malware: Tofsee

País afectado: Estados Unidos

Descripción: los atacantes accedieron a los sistemas de una planta de tratamiento de agua en una ciudad de Florida y modificaron los niveles químicos de hidróxido de sodio. Sin embargo, pudo ser contenido antes de afectar el consumo humano.

Año: 2021
Malware: Ransomware Darkside

País afectado: Estados Unidos

Descripción: ataque de ransomware a una de las compañías de distribución de petróleo más grandes de EE. UU. llamada Colonial Pipeline.

Año: 2022
Malware: HermeticWiper, HermeticWizard, HermeticRansom, IsaacWiper, DoubleZero, WhisperGate

País afectado: Ucrania

Descripción: desde el inicio de la guerra, surgen múltiples amenazas catalogadas como Wiper, que se centran en el borrado y destrucción de información más que el secuestro de ésta.

Panorama mundial actual e industrias afectadas

En el último tiempo, nuevas formas de amenaza se han sumado a los casos anteriores y generan alerta en distintos países. Durante el año 2022, la división de ciberseguridad del FBI emitió un comunicado que informa sobre el aumento de ataques contra infraestructura crítica en Estados Unidos.

Para este informe, se centraron en víctimas de múltiples sectores, incluidos servicios financieros, fabricación crítica e instalaciones gubernamentales. Los afectados reportaron fallas de seguridad en las instalaciones de Microsoft Exchange, que se consideran como el vector probable de intrusión.

En otros países, los actores maliciosos han tenido por objetivo principal grandes industrias como la del petróleo, las telecomunicaciones y entidades bancarias.

Ataques Industria Petrolera

Organización	Amenaza
PetroVietnam (Vietnam)	Ransomware: Snatch Fecha: 09-02-2022
Petrolimex (Vietnam)	Ransomware: BlackByte Fecha: 05-02-2022
Edgo (Jordania)	Ransomware: Cuba Fecha: 04-02-2022
KCA Deutag (Reino Unido)	Ransomware: RansomEXX Fecha: 28-01-2022
AL-SOOR FUEL MARKETING COMPANY K.S.C.P (Kuwait)	Ransomware: Snatch Fecha: 30-12-2021
Solaris Management Consultants (Canadá)	Ransomware: BlackCat (ALPHV) Fecha:29-12-2021
Divestco Geoscience Inc (Canadá)	Ransomware: AvosLocker Fecha: 25-12-2021
Kangean Energy Indonesia (Indonesia)	Ransomware: BlackByte Fecha: 19-12-2021

Ataques Industria de Telecomunicaciones

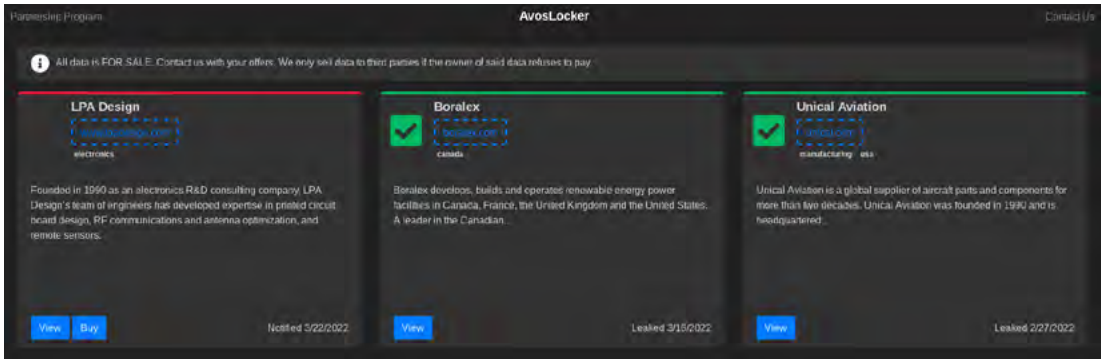
A1 HRVATSKA en Croacia sufre leak con información de 200.000 clientes.
Vodafone Ucrania sufre una pérdida masiva de conectividad en servicio de telefonía e internet móvil.
Vodafone Portugal sufre un ataque (aparente DDoS) que interrumpió sus servicios 4G y 5G en todo el territorio.

Ataques Entidades bancarias

Privatbank y Oschadbank, los principales bancos estatales de Ucrania, sufren DDoS interrumpiendo sus servicios.
Los principales bancos de Canadá: Royal Bank of Canada, BMO, Scotiabank and Canadian Imperial Bank of Commerce, sufren interrupción de sus servicios, limitando el retiro de dinero en cajeros automáticos.
Investigadores de Mandiant advierten sobre posibles ciberataques globales por parte de Rusia a industrias bancarias.
Nueva Zelanda lanza un comunicado a la banca local advirtiendo de posibles efectos colaterales del conflicto Rusia - Ucrania.

Amenazas en Chile

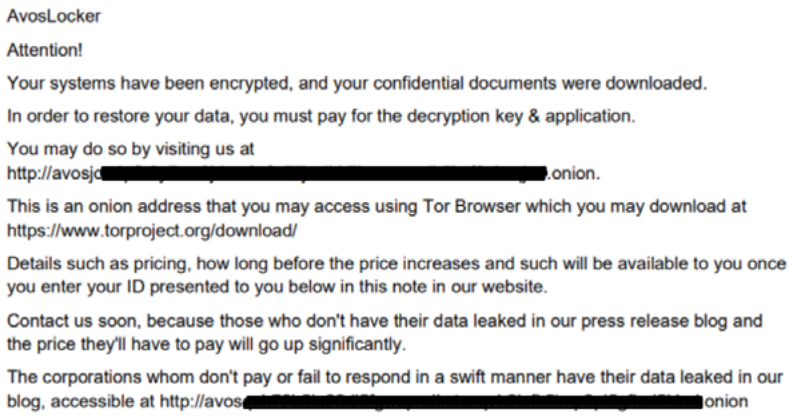
Una de las amenazas que ha estado presente en territorio nacional es el ransomware Avoslocker, que comprometió una organización con presencia en Chile y otros países. Su campaña se relaciona con un ataque de infraestructura crítica dirigido a compañías en Estados Unidos, que tiene alta probabilidad de extenderse a otras naciones aliadas o simpatizantes del país.



Sitio de Leaks AvosLocker

Ransomware AvosLocker

Es una familia de ransomware relativamente nueva, que fue observada por primera vez en julio de 2021. Esta familia aumenta sus ataques mientras adopta nuevas tácticas para evadir el software de seguridad. Desde que apareció por primera vez, habría mejorado sus técnicas de ataque destinadas a explotar vulnerabilidades que sirven como vector de entrada.


AvosLocker

Attention!

Your systems have been encrypted, and your confidential documents were downloaded.

In order to restore your data, you must pay for the decryption key & application.

You may do so by visiting us at
http://avosjc[redacted].onion.

This is an onion address that you may access using Tor Browser which you may download at
https://www.torproject.org/download/

Details such as pricing, how long before the price increases and such will be available to you once you enter your ID presented to you below in this note in our website.

Contact us soon, because those who don't have their data leaked in our press release blog and the price they'll have to pay will go up significantly.

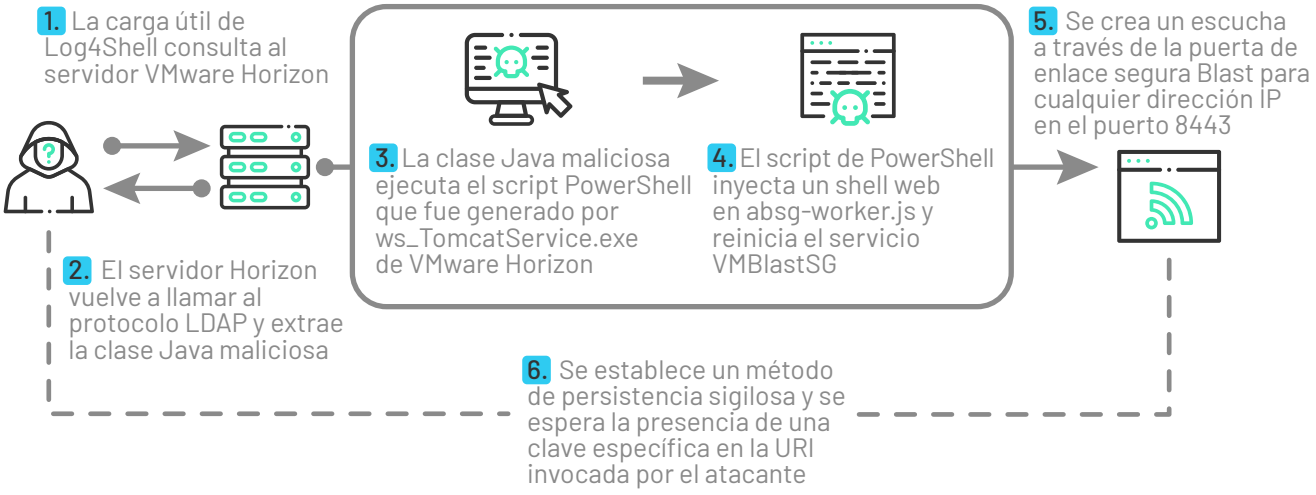
The corporations whom don't pay or fail to respond in a swift manner have their data leaked in our blog, accessible at http://avos[redacted]onion

Nota de rescate Ransomware AvosLocker

El sitio público de filtraciones de este ransomware enumera a sus víctimas según cumplan los compromisos y negociaciones para el pago del rescate. Entre ellas se encuentran organizaciones de todas partes del mundo: Reino Unido, Alemania, España, Bélgica, Turquía, Emiratos Árabes Unidos, Canadá, Siria, Arabia Saudita, China y Taiwán.

Actualización de AvosLocker apunta a servidores VMware.

Según boletines de cybersecure, la última variante de AvosLocker tiene un componente de Linux que se dirige a los servidores del hipervisor VMware ESXi, obligando a terminar cualquier ejecución de máquina virtual, para luego cifrar los archivos de la VM.



**Fuente: Campaña AvosLocker contra servidores VMware*

Investigaciones han indicado que los atacantes obtienen credenciales de administrador, necesarias para habilitar ESXi Shell o acceder a los servidores por medio de la adquisición de dumps relacionados a infecciones con malware de la familia infostealer. Además, las evidencias señalan que gran parte de las víctimas suelen ser administradores de sistemas a cargo de estas tecnologías.

El aumento de los ataques a infraestructura crítica, complementado por la creciente expertiz que estos ciberactores han podido adquirir, permite tener mayor claridad sobre cuáles son los objetivos trazados por estos grupos y esperar un significativo aumento de este tipo de operaciones.

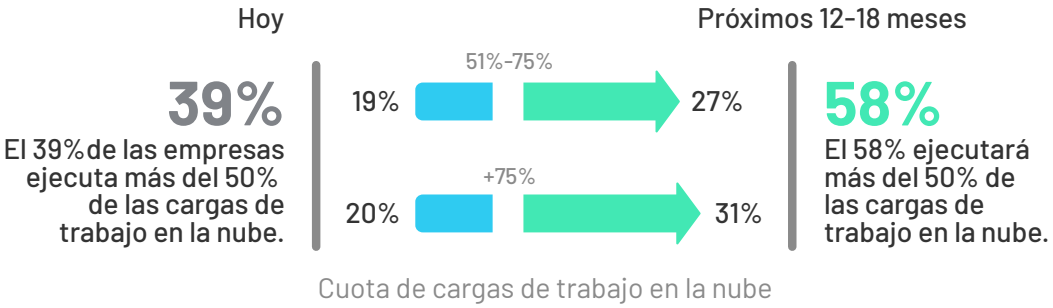
Por esto, es fundamental mantener un constante monitoreo de este tipo de actividades, ya que los atacantes combinan diferentes técnicas para reconocer blancos de gran valor y consolidar sus ataques.

Credenciales obtenidas en el sitio de dumps Infostealer

CAPÍTULO 5.

CLOUD SECURITY

La pandemia y los distintos hitos sociales de los últimos años han incentivado una rápida adopción de tecnologías Cloud. Esta acelerada migración a la nube proyecta que, para los siguientes 12 a 18 meses, **casi el 60% de las organizaciones alojarán más de la mitad de sus cargas de trabajo en cloud, frente al 39% actual.**



Cuota de cargas de trabajo en la nube

Aplicaciones en la Nube

El corazón de la transformación digital ofrece aplicaciones alojadas en una infraestructura comprendida de cuatro pilares principales.

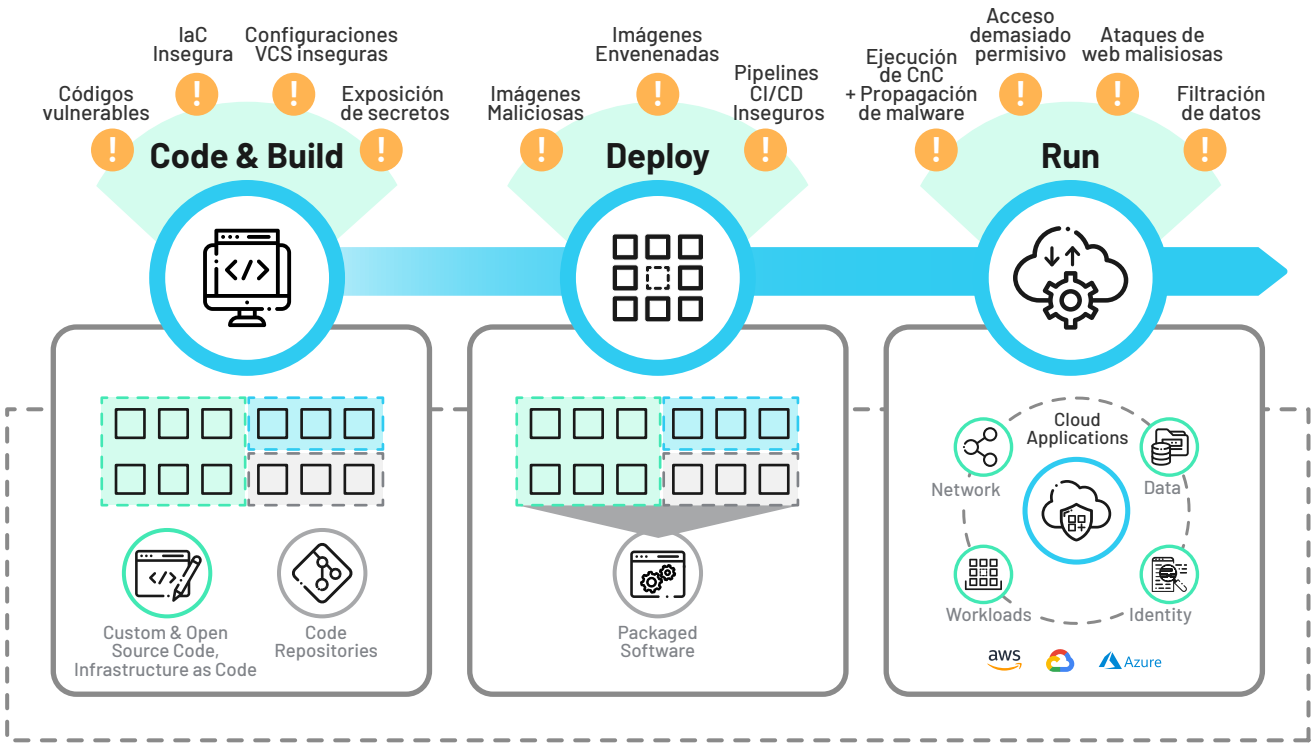
1. Redes elásticas.
2. Cargas de trabajo dinámicas - Host, Container, Serverless.
3. Identidades complejas.
4. Almacenamiento de datos en crecimiento.

Estos cuatro pilares entregan beneficios como:

- Capacidad de escalar hacia arriba o abajo rápidamente.
- Self-service, eficiencia operativa.
- Mejor utilización de recursos.

Amenazas de seguridad

Pese a sus grandes beneficios, las aplicaciones en la nube están sujetas a varios riesgos y vulnerabilidades que se distribuyen en sus distintas etapas, desde la confección del código hasta el tiempo de ejecución:



Los profesionales en ciberseguridad advierten que las mayores amenazas en este ámbito se deben a las configuraciones mal realizadas en cada proveedor de servicios e infra Cloud, que producen brechas de seguridad no configuradas. Otras brechas significativas son las APIs e interfaces inseguras y filtración de datos sensibles, las cuales son provocadas principalmente por accesos no autorizados, hacking de cuentas, servicios o tráfico, compartir datos a externos y ciberataques patrocinados por actores extranjeros.

62%

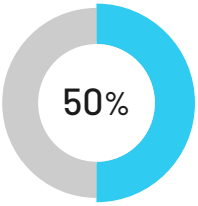
Configuración deficiente de la plataforma de la nube

54%

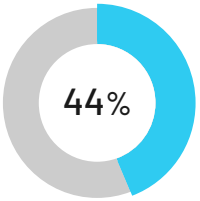
Interfaces inseguras/APIs

51%

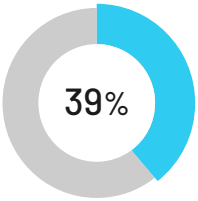
Filtración de datos sensibles



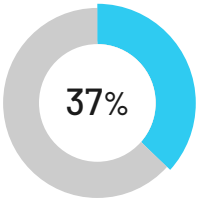
Accesos no autorizados



Hacking de cuentas,servicios o tráfico



Datos compartidos de forma externa



Ciberataques patrocinados por extranjeros

Barreras a la adopción

Hoy en día, las empresas están ejecutando múltiples estrategias para adoptar nuevos procedimientos en la nube, ya sean multi-cloud, híbridas o privadas. Sin embargo, su adaptabilidad presenta ciertas barreras que dificultan su adopción y necesitan de soluciones y mejoras en los principales puntos críticos
Entre estos puntos, podemos destacar la falta de pericia y equipo calificado, los incumplimientos legales y regulatorios y, finalmente, problemas en la seguridad de los datos que pueden derivar en filtraciones.

40%

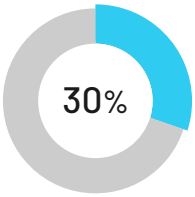
Falta de personal y recursos calificados

33%

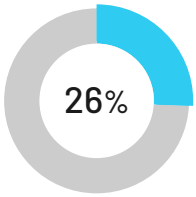
Cumplimiento legal y regulatorio

31%

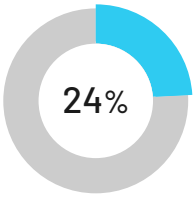
Seguridad de datos, pérdida y riesgo de filtraciones.



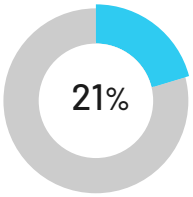
Integración con ecosistema IT existente



Miedo al bloqueo por parte del proveedor

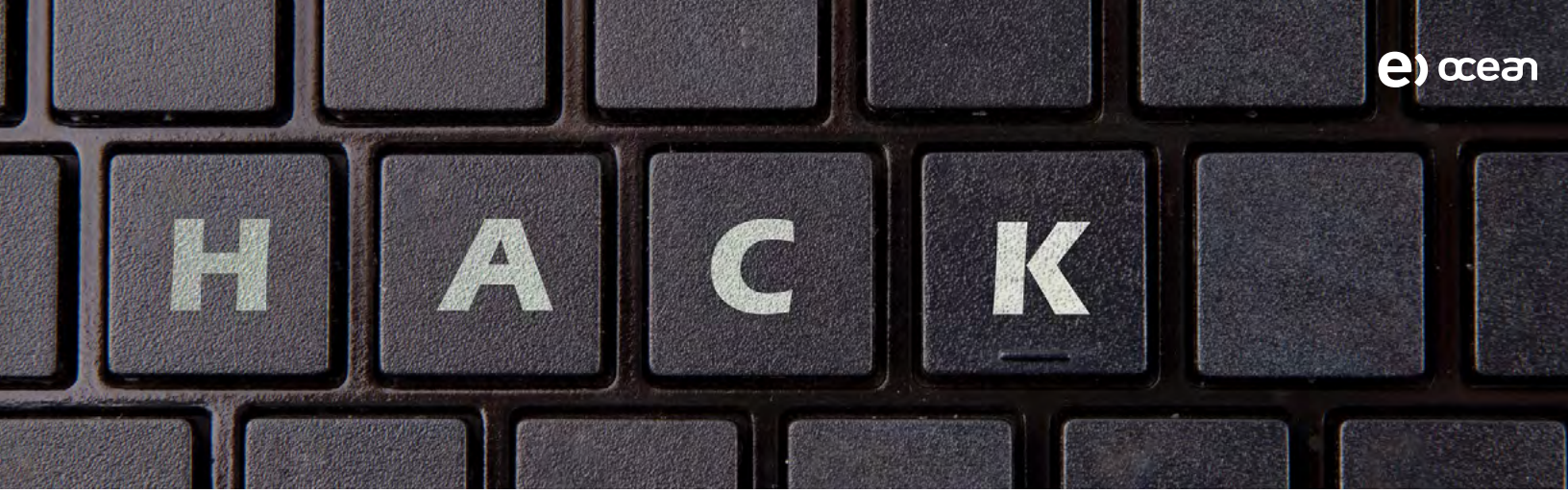


Riesgos generales de seguridad



Pérdida de control

La diversidad de entornos también puede contribuir a la complejidad operativa y de seguridad.

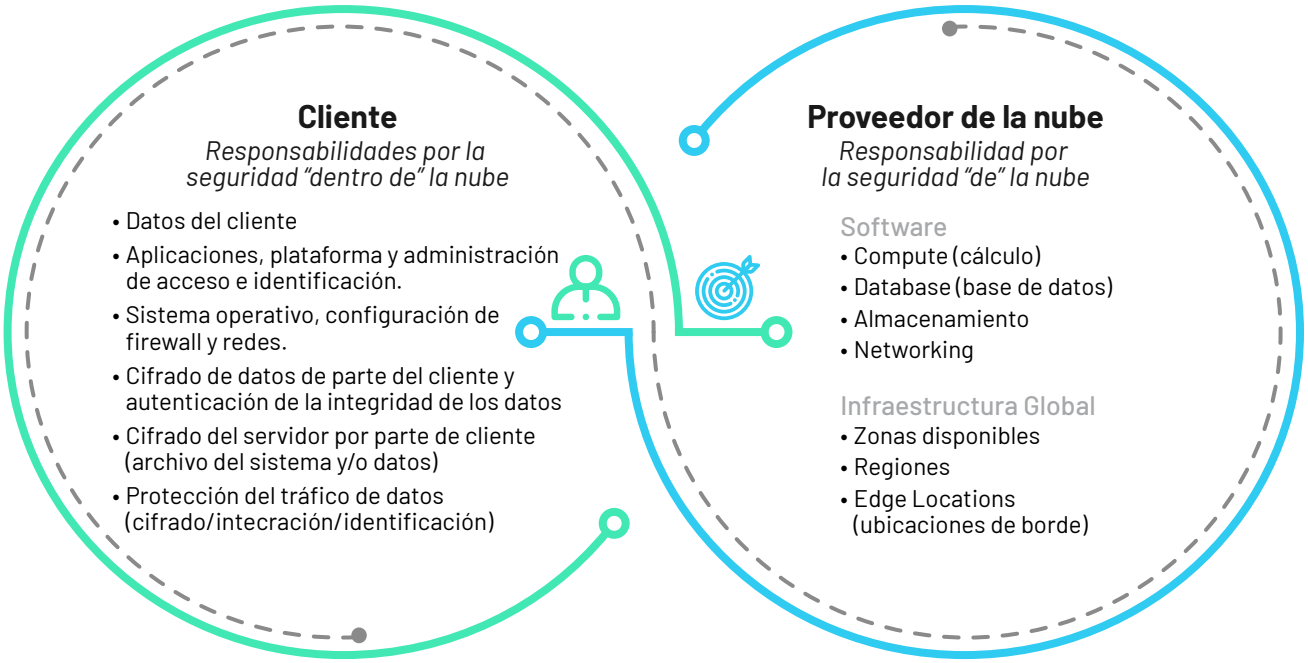


Modelo de responsabilidad

Para mitigar estas amenazas, lo primero es conocer nuestra responsabilidad compartida de seguridad en la nube pública. A partir de este punto, ya se pueden identificar configuraciones erróneas y deficientes por cada una de las partes.

"Una brecha de seguridad que proviene de una mala configuración, es nuestra propia responsabilidad"

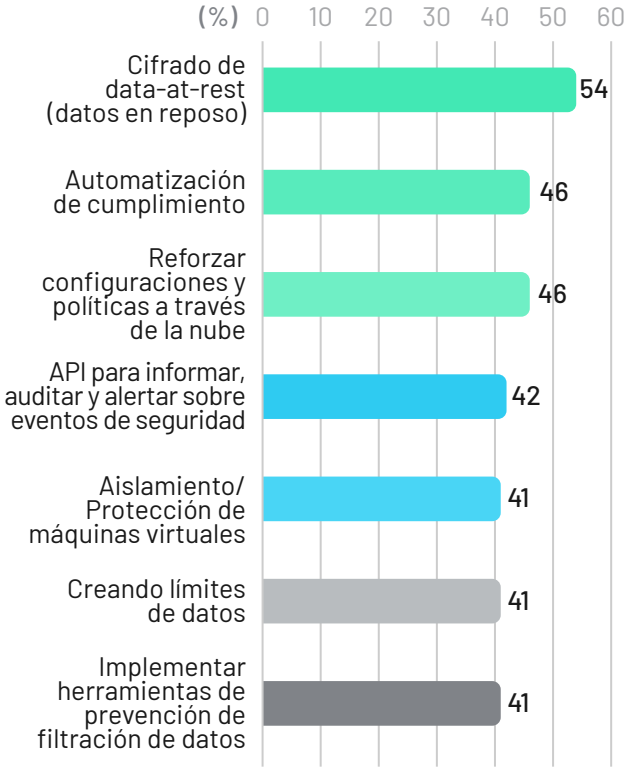
Flujo de responsabilidad entre cliente y proveedor



Mejorando la seguridad del Cloud

Compañías de distintos tamaños están buscando formas de mejorar la seguridad en cloud públicos, dando un mayor énfasis a controles de seguridad más críticos, con el fin de aumentar la confidencialidad.

En este ámbito se está dando prioridad al cifrado de data-at-rest, automatización de cumplimiento y reforzando configuraciones y políticas a través de la nube.



Estrategia Zero Trust

Para mitigar las amenazas en cloud, actualmente las compañías están considerando el modelo Zero Trust (confianza cero), con el fin de alojar sus activos en la nube pública. Este considera capas de protección desde el mundo TI, pero con mayor visibilidad dentro de todo el stack, desde el acceso hasta la aplicación y los datos.
Un 69% de empresas encuestadas en LATAM afirmó considerar que la confianza cero es particularmente importante para el acceso a la nube, cifra que resultó similar a nivel global. Por otro lado, un 48% de las empresas en la región aseguró que zero trust daba forma a su estrategia de seguridad en la nube en gran medida, superando ampliamente al promedio mundial del 34%.

Estas cifras muestran una evidencia del progreso hacia la conciencia y adopción de confianza cero en la nube en países latinoamericanos.

Al igual que sus contrapartes globales, las empresas de LATAM están adoptando estrategias de confianza cero y están comenzando viajes de confianza cero.

CAPÍTULO 6.

HERRAMIENTAS/TECNOLOGÍAS PARA LA TOMA DE DECISIONES

"Las expectativas son peligrosas cuando son altas y sin forma".
Lionel Shriver

Actualmente, existe una mayor consciencia a nivel directivo sobre los riesgos latentes en ciberseguridad, lo que ha elevado las expectativas a la hora de prepararse y responder a este relevante desafío.

Llevar los controles de ciberseguridad a un nivel de estrategia es clave en un contexto que presenta:

- Amenazas cada vez más sofisticadas.
- Superficie de ataque en expansión, casi infinita.
- Captura, desarrollo y retención de talento.

Automatización de la ciberseguridad

Debido a que los cibercriminales operan desde hace ya algunos años automatizando sus ataques, para las organizaciones resulta imprescindible implementar una defensa adecuada a esta realidad que considere:

1. Acelerar y mejorar la respuesta a incidentes.

2. Aumentar la visibilidad y el control sobre todos los eventos de seguridad.

3. Implementar métricas críticas de seguridad en tiempo real.

4. En tareas complejas, apoyar la intervención humana de remedición.

5. Automatizar el control de falsas alertas.

Servicios de detección y respuesta de amenazas avanzadas.

A medida que aumenta exponencialmente el volumen, variedad y sofisticación de las amenazas, las organizaciones se esfuerzan por mantener a sus equipos de seguridad SOC (Security Operations Center) dotados de personal y recursos altamente calificados.

En este escenario, los proveedores de Detección y Respuesta Gestionada (MDR) comienzan a tomar relevancia, ya que brindan una alternativa eficiente de servicios llave en mano, diseñados para mejorar las defensas y minimizar los riesgos de incidentes en un entorno empresarial.

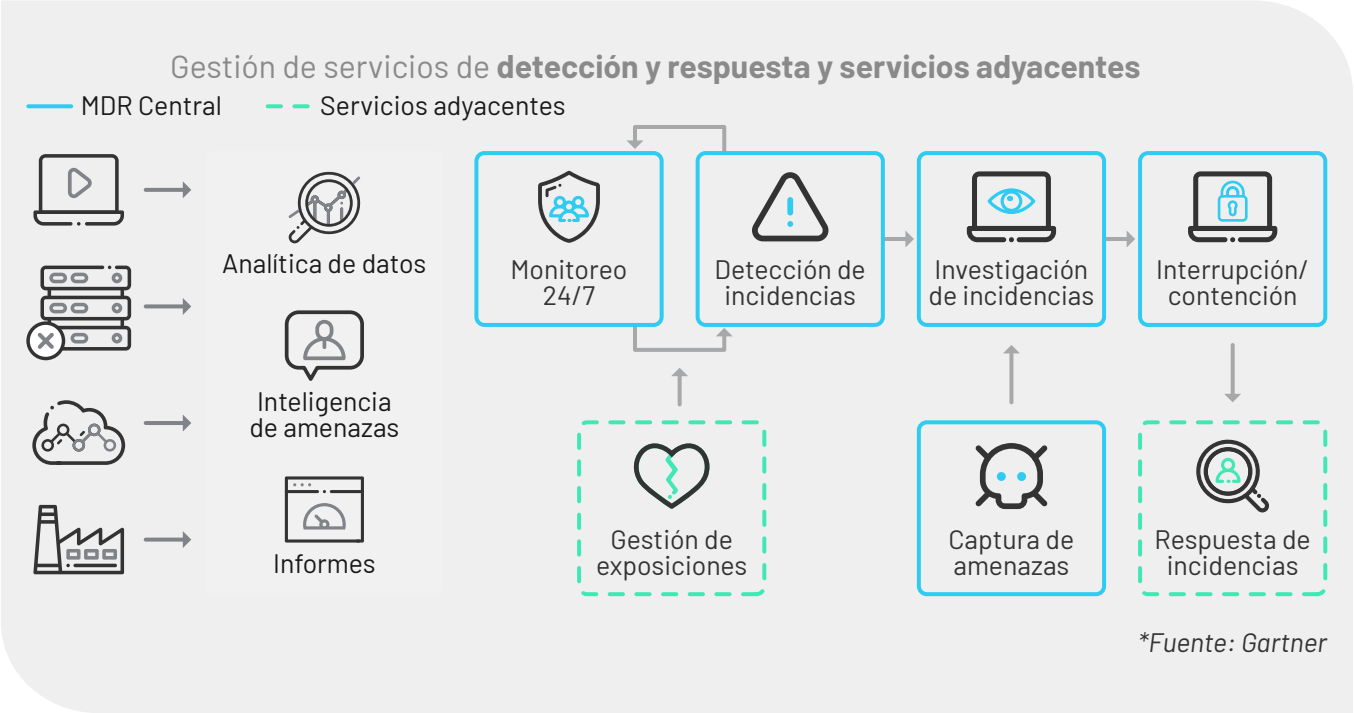
- **Servicios MDR**

Permiten a las organizaciones detectar, analizar, monitorear, investigar y responder rápidamente ante amenazas, fusionando la pericia de profesionales altamente especializados con tecnología de vanguardia y bases de datos globales avanzadas.

Es ideal para quienes que buscan lo último en productos de seguridad que integran herramientas de detección y respuesta extendida (XDR) y orquestación (SOAR).

Según Gartner, para el año 2025, el 50% de las organizaciones empleará los servicios de MDR para las funciones de monitoreo, detección y respuesta de amenazas. Esto se debe a que brindan inteligencia de amenazas avanzada y retroalimentan con información proactiva a los equipos de seguridad ya existentes en una organización.

Esto permite la visibilidad de distintas dependencias, como estaciones de trabajo, granja de servidores, red interna y servicios en la nube.



Fuente: Gartner

Los servicios MDR:

- Recopilan registros, datos e información relevante que ayuda a determinar comportamientos anormales.
- Mejoran los niveles de detección y reducen el tiempo de permanencia (Dwell Time).
- Aportan valor al cumplimiento normativo, ya que entregan informes completos y la retención de registros en una amplia gama de regulaciones y estándares.

Como resultado, un servicio MDR pone a disposición de una compañía un equipo de seguridad altamente especializado, sin tener que incurrir en los gastos que implica capacitar en estas herramientas.

ocean + paloalto NETWORKS CORTEX XDR

Detección y Respuesta Gestionada (MDR)

Enfoque holístico proactivo que actúa **sobre todas las fuentes de datos**

Reduce tiempos de detección y contención de meses **a horas/minutos**

Equipo experto local, reduce tiempos de respuesta y costos

Gestión Integral de Riesgos

Hoy nuestro portafolio cuenta con una sección dedicada a la gestión integral de riesgos que pone a la automatización en el centro.

Gestión Integral de Riesgos

Servicios Gestionados de Detección y Respuesta (MDR)

Contención de ataques 24/7 con:

- Monitoreo continuo
- Búsqueda proactiva de amenazas
- Clasificación de alertas
- Investigación de servicios de respuesta de incidentes entregados por expertos

Servicios CSOC NG

Descentralizar y gestionar la automatización de las operaciones de seguridad

- NG-SIEM
- XSOAR
- XSIAM
- XDR Agent/ Dataleak
- Threat Hunting
- Equipo de Respuesta a Incidentes

Servicios CSOC NG

Descentralizar y gestionar la automatización de las operaciones de seguridad

- XDR Agent/ Dataleak
- Threat Hunting
- Equipo de Respuesta a Incidentes
- NG-SIEM
- XSOAR
- XSIAM

CAPÍTULO 7.

RECOMENDACIONES DE SEGURIDAD: PRE Y POST MORTEM

Dado el panorama actual en amenazas de robo de información, tanto a nivel global como en Chile, es importante que la alta dirección de empresas comprenda y se haga cargo de la seguridad como una inversión y una medida para el resguardo de sus operaciones.

Pasar por alto este escenario, puede significar:

- Asumir el costo de millones de dólares sólo en la fase de mitigación.
- La extorsión con filtración de datos para sustraer dinero.
- Disminución de la productividad o paralización de la operación por efecto de un ataque.
- Daño a la imagen y reputación corporativa.
- Socios, proveedores y colaboradores podrían eliminar las relaciones, por amenaza de su propia seguridad.

› Recomendaciones de ciberseguridad pre y post mortem

En un mundo lleno de soluciones de seguridad, el crecimiento de microservicios, contenedores y servicios cloud ha terminado por aumentar la aparición de nuevos riesgos y amenazas. Cada línea, entre cientos que componen un código, podría contener un error y generar una vulnerabilidad o falla de seguridad.

Por otra parte, el crecimiento de microservicios, contenedores y servicios cloud ha terminado por aumentar la aparición de nuevos riesgos y amenazas. A esto se suma la falta de rigurosidad en las configuraciones o escasez de control en cuentas sin uso por largos periodos de tiempo, que pueden significar vectores de ataque futuro.

Estas nuevas amenazas son cada vez más fáciles de ejecutar y más complicadas de resolver. Es responsabilidad de cada empresa tomar esta información y transformarla, de forma proactiva, en un cambio hacia mejores prácticas cotidianas. Parte de esta tarea es hacer de la ciberseguridad un conocimiento transversal.

A nivel de gerencia, resulta fundamental que quienes componen el c-level comprendan cabalmente lo que ocurre y puedan hacer de esta información un lenguaje accesible para todos. De esta manera, todas las personas que componen una organización pueden tomar conciencia en su vida privada y dentro de su núcleo familiar.

Para generar una cultura de protección en ciberseguridad, especialmente si no se ha adoptado aún un modelo o framework, es importante contar con lo siguiente antes de enfrentar un incidente:

Una matriz de decisiones entre la visibilidad de la superficie de ataque y el nivel de intrusión.

- Actualizaciones trimestrales del listado de la infraestructura crítica y el núcleo del negocio.

- Realizar el levantamiento funcional del estado de la redundancia y coordinar pruebas de operación.

- Utilizar framework, como controles CIS, para realizar el hardening del ingreso de nuevos equipos de trabajo.

- Efectuar un proceso maduro de alta y baja de colaboradores, así como también la destrucción de información y el envío de la misma.

- Emplear herramientas de mitigación, como Virtual Patching, cuando el sistema no permita el parchado.

- Asegurar la actualización constante de la matriz de contactos y proveedores para mantener la continuidad de las actividades durante un incidente.

- Asegurar que los externos cumplan con políticas de seguridad al momento de interactuar con sus servicios.

- Mantener distancia cero entre los equipos de monitoreo, infraestructura, arquitectura, ciberseguridad, administración y riesgos.

- Poseer un equipo de respuesta preparado ante incidentes, que genere ciclos de entrenamiento constantes.

- Establecer ciclos de vida para los indicadores asociados al negocio.

- Ejecutar pruebas de escritorio, tanto para incidentes de ciberseguridad como para planes de recuperación de disponibilidad.

- Establecer y realizar entrenamientos de recuperación de información en escenarios reales.

- Modelar constantemente el plan director de ciberseguridad. Agregar nuevas fases para proyectos que busquen solventar brechas de seguridad.

- Destinar un 20% del presupuesto de ciberseguridad a incidentes no controlados.

- Actualizar y gestionar automáticamente el inventario de activos.

- Tener un equipo de inteligencia personalizado acorde al negocio.

- Atraer y retener talentos, sobre todo los formados en el negocio de la empresa.

Para estar a la vanguardia de los nuevos vectores de ataque existentes, es necesario contar con un plan de pruebas periódicas que permita conocer el nivel de exposición real de la organización. Así, es trascendental implementar ciclos de revisiones, cuya frecuencia de ejecución dependerá del nivel de riesgo que posea cada organización.

Estas prácticas logran reducir los costos de mitigación y aseguran mantener un nivel de seguridad aceptable en los aplicativos. En ese sentido, no se trata tanto de curar la enfermedad, sino de fortalecer el sistema

inmune para evitar futuras fallas. Dentro de las principales actividades que se recomiendan, para establecer una línea base y protegerse de futuros ataques informáticos, se encuentran:

- Análisis de superficie de ataque.
- Verificación de vulnerabilidades.
- Revisión de aplicaciones web y móviles.
- Ejercicios de ingeniería social.
- Comprobación de requerimientos.
- Análisis de código estático.
- Revisiones de dependencias.
- Análisis de código dinámico.

Para poder evitar los vectores de ataque producidos por **configuraciones poco rigurosas y cuentas sin uso por largos periodos,** es necesario proteger las actividades alojadas en la nube ante eventos maliciosos, como la denegación de servicio (DoS) o la denegación de servicio distribuido (DDoS).

Estos ataques, cuando superan el ancho de banda de la víctima, no pueden ser detenidos por cuenta propia y requieren de la ayuda de un partner tecnológico que proteja el servicio y permita la continuidad de sus operaciones.

Por último, para **casos de ataques aplicativos,** es de suma importancia contar con lo siguiente:

- Levantamiento de servicios publicados, tomando en consideración sistema operativo, aplicación, lenguaje de programación y bases de datos utilizadas.

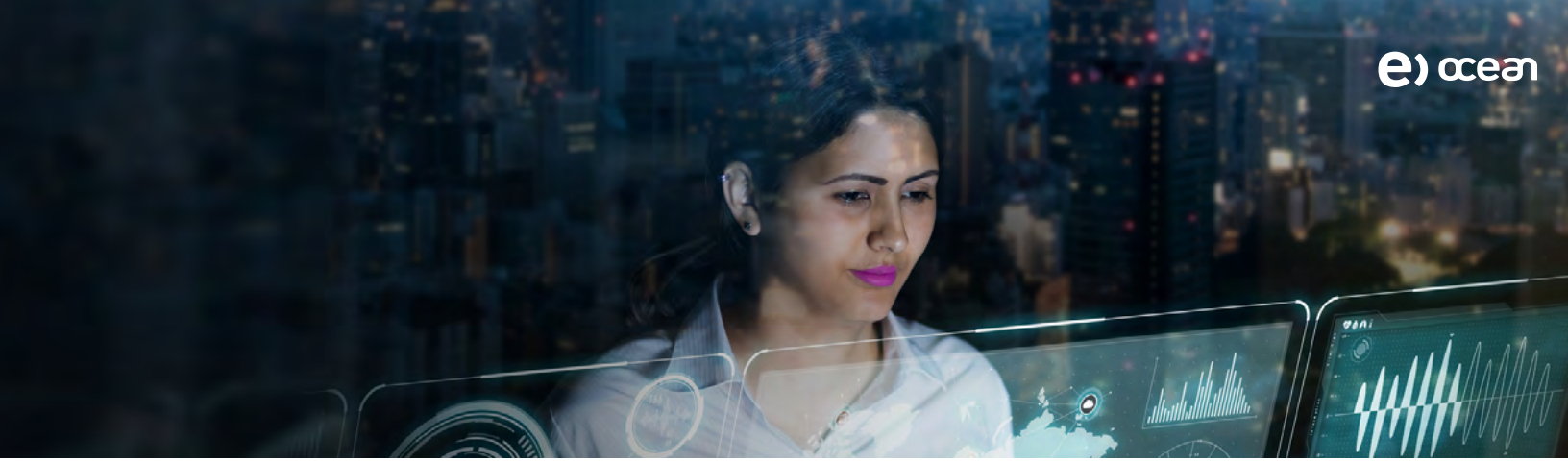
- Establecer una línea base de seguridad, tanto con la encriptación como con las cabeceras y protecciones sobre ataques aplicativos conocidos. Para esto es indispensable contar con equipamiento WAF para la protección.

› Pre-Mortem (Prevención)

La única manera de direccionar de forma adecuada los recursos disponibles para la prevención de ciberataques es partir por identificar los High Target Value de una organización. A través de ellos, se pueden analizar los riesgos que conlleva su exposición y entender qué es lo que hay que proteger y de qué manera hacerlo.

- **Proteger el acceso**

La configuración deficiente de servidores es una de las principales causas de acceso de atacantes. Por lo mismo, es necesario contar con profesionales capacitados para actualizar, parchar y



segmentar adecuadamente los sistemas y servicios, así como también monitorear de forma constante los registros de activos mediante tecnologías SIEM.

Para garantizar la seguridad, un sistema de administración de identidad y acceso (IAM) se describe generalmente en cuatro procesos principales:

- **Identificación:** creación de una cuenta o ID que represente de manera única al usuario, dispositivo o proceso en la red, junto con una contraseña compleja.
- **Autenticación:** probar que el sujeto es lo que dice ser al momento de acceder al recurso.
- **Autorización:** determinar qué derechos posee el sujeto sobre cada recurso y garantizar su cumplimiento.
- **Accounting (Registros):** realizar un seguimiento del uso autorizado de un recurso o uso de derechos por parte de un sujeto y alertar cuando se detecta un ingreso o uso no autorizado.

› Educar al personal

Para complementar cualquier estrategia de seguridad, practicar la concientización y formación de los usuarios es el método más eficaz para bloquear el malware. Una buena educación de ciberseguridad resulta clave para prevenir ataques de ingeniería social como el phishing. Estos ataques desencadenan descargas de malware y secuestros de credenciales, pudiendo lanzar por la borda los demás esfuerzos de seguridad.

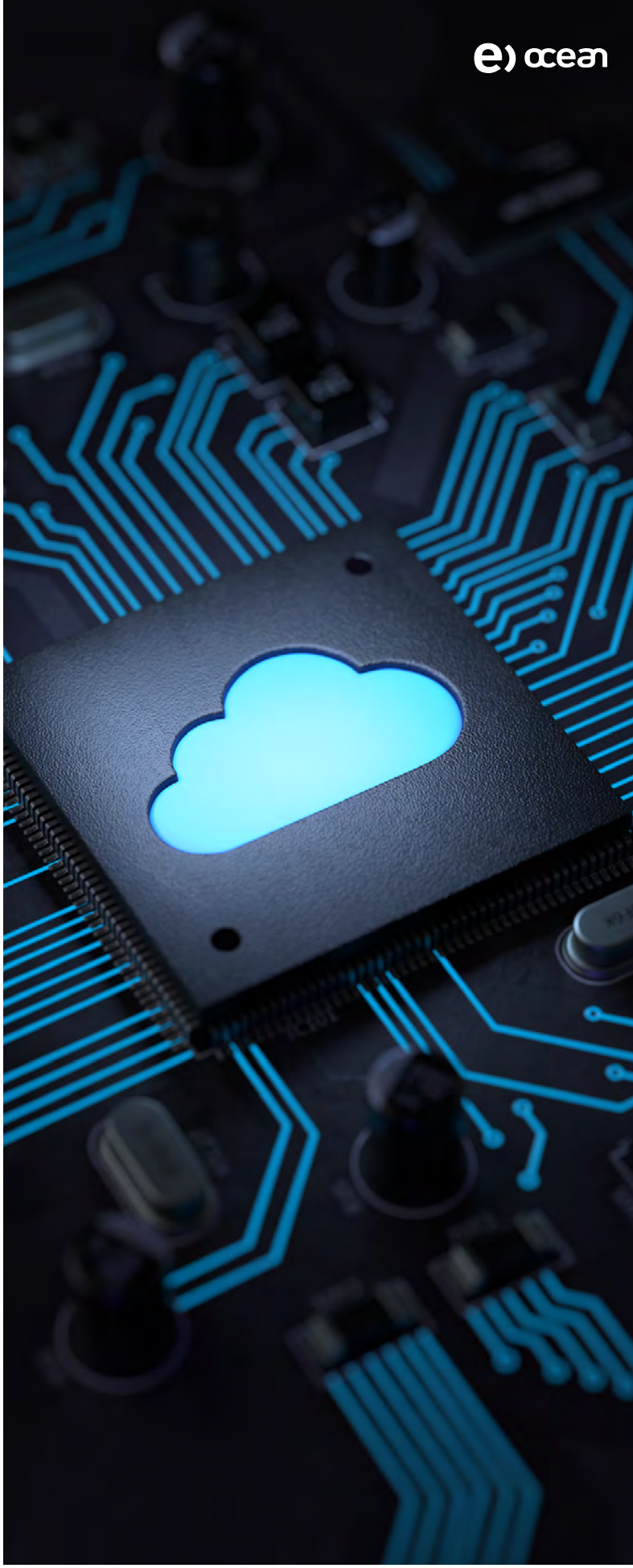
Por esta razón, ya no basta pensar en contraseñas complejas con más de 14 caracteres, pues los infostealer permiten extraerlas en texto plano, directamente desde los terminales comprometidos. Sólo con una concientización cabal, que abarque a todos los usuarios, se puede mantener la seguridad del acceso.

Defensa en profundidad

Sumado a los consejos mencionados, es aconsejable implementar un enfoque de defensa en profundidad en capas, que incluya protección contra malware, parches oportunos, seguridad de DNS, cifrado y copia de seguridad.

Según datos de Microsoft, sólo el 22% de sus clientes empresariales en Azure Active Directory (AD) han adoptado una solución multifactorial para proteger sus cuentas, pese a que hasta un 98% de los ataques se pueden prevenir usando reglas básicas de higiene y seguridad como:

- Habilitar 2FA.
- Utilizar Antimalware modernos y licenciados.
- Aplicar mecanismos de seguridad Zero-Trust.
- Mantener actualizaciones periódicas.
- Conservar una adecuada protección de datos.



Post-Mortem (Mitigación)

Si un ataque ya se ha llevado a cabo de forma exitosa, igualmente habrá que tomar una serie de medidas de mitigación que permitan reducir lo más posible los daños. Estos son algunos de los puntos a considerar:

- Aislar el equipo o la red comprometida y deshabilitar las cuentas o accesos comprometidos.
- Conocer si el usuario afectado corresponde a un proveedor conocido y si cuenta con un equipo, para actuar de acuerdo con sus protocolos de contención de amenazas.
- Indagar en logs obtenidos de plataformas de seguridad como WAF, FW, SIEM, AV u otras, para realizar un análisis e identificación detallados de la amenaza.
- Auditar equipos afectados para identificar las amenazas y rastrearlas en otros activos de la organización mediante la obtención de IoC (indicadores de compromiso) o IoA (indicadores de amenaza) principalmente vinculados a los TTP del atacante.

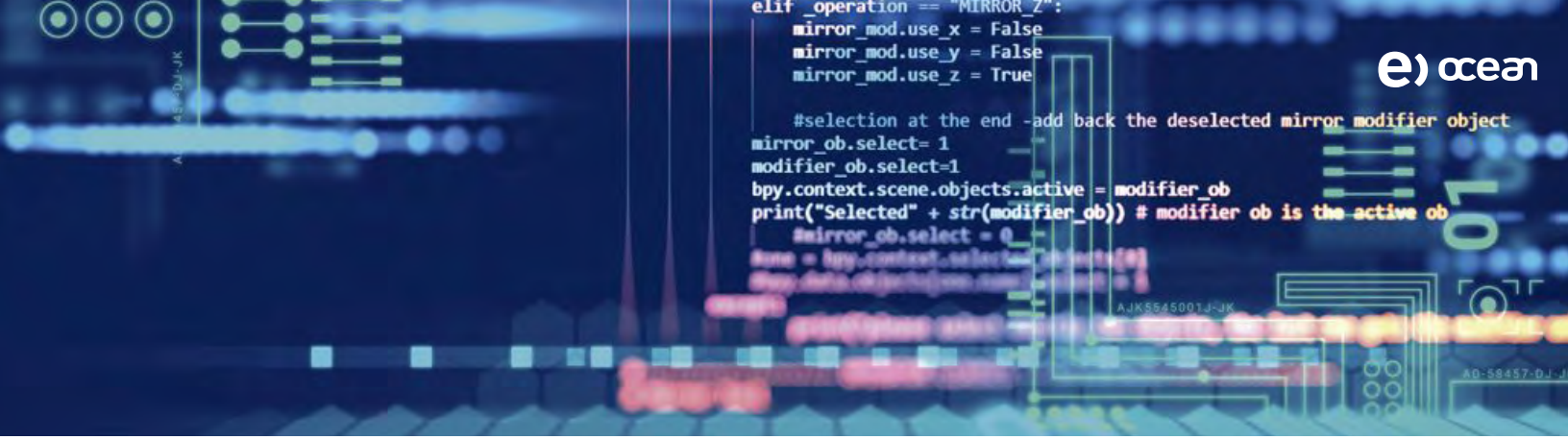
CAPÍTULO 8.

PREDICCIONES Y APRENDIZAJES CLAVE PARA EL 2023

Aprendizajes de 2022

La gran mayoría de los ataques informáticos, aparte del hacktivismo y el ciberespionaje, buscan recompensas monetarias, a la vez que afectan la imagen y confianza de una organización. Esto indica que la reputación se relaciona directamente con la seguridad digital, siendo el usuario el principal vector de ataque y de entrada para el compromiso de una red.
Al respecto de los hallazgos del año 2022, se destacan las principales tendencias:

- **Phishing:** líder en tendencia, ya que continúa siendo altamente efectivo para propagación de malware, estafas y suplantación de identidad.
- **Ransomware:** se encuentra en una curva de crecimiento importante, que mediante filtraciones y rivalidades internas han liberado Builders de forma pública. Estos permiten la proliferación de nuevos grupos que, sin tener un amplio conocimiento de desarrollo, pueden tomar estas herramientas y levantar sus propias operaciones delictivas.
- **Ataques a infraestructura crítica:** pueden traer consigo consecuencias físicas y reales a un gran número de personas, debido a que la integración de IT/OT es un plano complejo de resguardar.
- **Dataleak y databreach:** brindan una gran puerta de entrada para lograr accesos iniciales, por lo que deben ser constantemente monitoreados por dispositivos perimetrales. Además, es necesario revisar, segmentar y asegurar los servidores de bases de datos internos y de clientes, que podrían ser utilizadas para ataques de mayor envergadura.



Predicciones para 2023

Ciberguerra

En el actual episodio entre Rusia y Ucrania, la ciberguerra ha jugado un papel importante. La tecnología se utiliza para deshabilitar servicios críticos de un país (DDoS, Defacement), para el espionaje (APT's) o simplemente para hacer daño al enemigo (Ransomware Wiper). Estos ataques, siempre limitados por el factor del tiempo, aunque suelen buscar extraer información de la contraparte, tienen como primera prioridad afectar a la víctima y hacerle daño de forma rápida, crítica y específica.

Estas tácticas son difíciles de visibilizar y cuantificar, lo que se traduce en que entidades internacionales sean incapaces de presentar sanciones, por la falta de evidencia obtenida y un escaso entendimiento de los sucesos. Por esta misma razón, esta actividad se ha visto incluso fuera del contexto de los conflictos bélicos de manera cada vez más frecuente.

Bypass, captura o fatiga de 2FA

La masiva adopción del 2FA en la protección de accesos ha impuesto una gran barrera para los delincuentes. Estos se han visto obligados a destinar tiempo, recursos y desarrollo para crear nuevas herramientas y/o mecanismos que permitan capturar este valioso código. Sin él, ninguna credencial de acceso con la que puedan contar será útil.

Esta medida ha resultado ser la más segura en cuanto a protección de accesos y ya se trabaja en mecanismos de 3FA y 4FA, que utilizan diferentes bases de conocimiento del usuario para confirmar su identidad y validar el acceso. Así, se pueden complementar las credenciales de acceso tradicionales con condicionantes como un código de autenticación secundario, datos biométricos y geolocalización.

Sin embargo, se puede esperar que los actores maliciosos sigan trabajando para superar estas barreras.

Por ello, ya existe **el acceso password-less**, que elimina el hecho de memorizar largas y complejas contraseñas y hace que, según cifras de Microsoft, sea un 99% más difícil de comprometer

un equipo. A nivel global, la adopción de este método va en alza y para 2023 se espera que siga aumentando, alcanzando un valor de mercado de 18,5 millones de dólares en comparación a los 15.6 en 2022.

Phishing crypto

Este ecosistema y su tecnología son relativamente nuevos. Su principal uso es el movimiento de dinero y cuenta con elevadas recompensas a quienes logren vulnerar los sistemas. Dado su potencial, existen múltiples actores y APT's en el rubro, tales como Lazarus, que han robado miles de millones de dólares en breves periodos de tiempo, aprovechando el anonimato que brinda esta tecnología.

Pese a sus ventajas, este tipo de delitos enfrenta una barrera para el lavado de dinero. Al realizar la conversión de criptomonedas a Fiat (dinero corriente), por ser sumas muy grandes, difícilmente pasan desapercibidos. Las entidades bancarias cuentan con capacidades de rastreo de flujos de dinero que identifican esas grandes cifras y al individuo que ha realizado la operación.

Por otra parte, además del robo de dinero, el sector crypto ha evidenciado la distribución de malware por parte de criptomineros como XMRig. Esta práctica ha sido bastante utilizada en el despliegue de diferentes familias de malware que buscan monetizar al máximo sus ataques. La situación va en alza y se esperan nuevos incidentes a futuro.

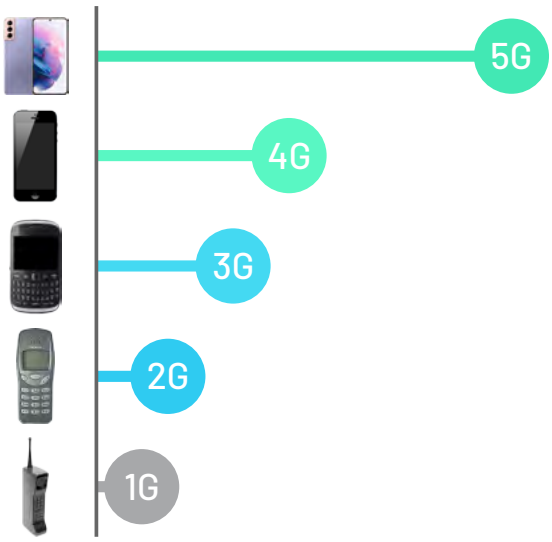
Ransomware y Dataleak

Durante los últimos años, estos ataques han mostrado una tendencia al alza y debido a su continuo desarrollo se esperan nuevas incidencias a futuro. Estas estrategias han causado grandes pérdidas monetarias en el sector público y privado de diversas naciones, así como la fuga de información comercial y estratégica de múltiples organizaciones a nivel global. En una sociedad donde la información ha adquirido un inmenso valor, los responsables de este tipo de ataques no escatiman en gastos para lograr sus objetivos. Por este motivo, la seguridad digital tiene cada vez mayor relevancia.

CAPÍTULO 9.

CÓMO ENFRENTAR LOS DESAFÍOS DE CIBERSEGURIDAD EN 5G

En cada generación de la red móvil han ido aumentando las acciones que se pueden realizar desde un celular. En el caso del 5G, en comparación con el 4G, se reduce la latencia en hasta 50 veces y aumenta la velocidad en hasta 10 veces. Además, puedes conectar, al mismo tiempo, todos los dispositivos que posean dicha conectividad: celulares, computadores, autos, buses, refrigeradores, hospitales, relojes y hasta ampolletas inteligentes, posibilitando la conexión de ciudades completas.



Sin embargo, junto a los grandes beneficios que ofrece a las personas y organizaciones la incorporación de nuevas tecnologías, se abren también nuevos desafíos en el ámbito de la ciberseguridad.

1. Reducir la superficie de ataque

Existen nuevos desafíos de seguridad que crecen a medida que se fusionan tecnologías de Cloud, Datos e IoT, lo que ha resultado especialmente riesgoso para las infecciones relacionadas con ransomware. Más aún, el 32% de los operadores mundiales sitúan la mayor superficie de ataque como un desafío clave (Trend Micro and GSMA Intelligence Report 2021).

¿Cómo reducir la superficie ataque?
Empresas y agencias gubernamentales fiscalizadoras deben invertir en planes de ciberseguridad sustentables, con estructuras capaces de atender las vulnerabilidades en la superficie de la red de manera preventiva.

2. Protocolos de seguridad en dispositivos IoT

No tener protocolos claros con respecto a la fabricación de estos dispositivos puede producir carencias de seguridad. Esto se vuelve un importante factor de riesgo para cualquier organización que los utilice, ya que son un punto de acceso interesante para ataques Botnet o DDoS, entre otros.
En 2018, la actividad de las botnet's IoT representó 78% de los eventos de detección de malware en los ISP, cifra que, según proyecciones de Knowhoy Distrelec, aumentará con la integración de 5G.

¿Cómo enfrentar estas amenazas?
Es crucial que exista una instrucción en todos los niveles de una empresa sobre cómo emplear productos IoT de forma segura, privilegiando la adquisición de modelos que establezcan mínimos estándares de seguridad.

3. Expansión del trabajo remoto

Las modalidades híbridas y el teletrabajo se verán potenciadas con el paso del tiempo, consolidando entornos laborales en la nube. Más aún, se estima que, sólo en Estados Unidos, 36,2 millones de personas trabajarán de forma remota para 2025, un aumento del 87% comparado con el escenario previo a la pandemia (Beekeeper Digital Wokforce).

Sin embargo, esto implica también la apertura de otro frente de riesgo, puesto que una conexión en tiempo real también significa un riesgo de una potencial pérdida de datos en tiempo real.

¿Cuáles son las medidas para mitigar las brechas de seguridad en la nube?

- Privilegiar el acceso mínimo al entorno organizacional y otorgar permisos exclusivos por roles.
- Emplear claves con doble autenticación y el uso de una VPN.
- Realizar un monitoreo constante para identificar amenazas, evitar rupturas y accesos no autorizados.

4. Integrar conocimientos en el uso del 5G

El mayor reto para las compañías radica en la falta de herramientas y conocimientos respecto de esta nueva tecnología, dificultando el enfrentamiento a las vulnerabilidades que ésta trae.

Así lo afirma el Trend Micro and GSMA Intelligence Report 2021, estudio en el que el 48% de los encuestados declaró la falta de preparación como el desafío más grande en la adopción del 5G.

¿Cómo prepararse para el 5G?

Las empresas y organizaciones que migren a la nueva red móvil deben apoyarse en **partners especialistas en 5G** y en las tecnologías que lo rodean, considerando ecosistemas de IoT, cloud y seguridad, entre otros.

CAPÍTULO 10.

NUESTROS SERVICIOS

La constante transición y expansión de organizaciones hacia un entorno digital está impulsando nuevas tendencias de ciberseguridad. Los procesos comerciales en la nube, la migración hacia el teletrabajo, el ransomware sofisticado, los ataques a la cadena de suministro digital y las vulnerabilidades profundamente arraigadas han expuesto importantes brechas tecnológicas y carencias de habilidades y conocimiento.

Para abordar estas amenazas, **los directores de seguridad de la información (CISOs)** y **líderes de seguridad y gestión de riesgos (SRM)** tienen la labor de transmitir y compartir sus roles con estrategas corporativos que gestionen el riesgo cibernético.

Nuestras recomendaciones

Los responsables del riesgo cibernético enfrentan un escenario crítico, ya que la huella digital de las compañías se está expandiendo y el control centralizado de ciberseguridad va quedando obsoleto. Por esto, recomendamos replantear el rol que cumplen los líderes de ciberseguridad en las organizaciones de hoy.

Los **SRM** están atrapados en un entorno de amenazas cada vez más agresivo y la visión de los **CISOs** dificulta su intervención con el Departamento de Tecnología de la unidad de negocios. Para resolver estos desafíos de manera exitosa, primero hay que replantear algunos conceptos de liderazgo que, actualmente, no tienen el enfoque correcto:

Concepto erróneo de liderazgo	Replanteamiento
"El CISO previene las infracciones"	"Un lider facilita la gestión de riesgos"
"El riesgo cibernético es un problema de seguridad"	"El riesgo cibernético es un riesgo empresarial/organizacional"
"La seguridad es un obstáculo para la velocidad"	"La seguridad permite productos ágiles y seguros"

Nuestros servicios y soluciones

Así como recomendamos replantear el rol del Líder de Ciberseguridad con una perspectiva estratégica, recomendamos recurrir a servicios y soluciones desarrolladas por expertos, en concordancia con las tendencias de ciberseguridad y gestión de riesgo para 2023.

Estas soluciones permiten preparar y enfrentar, con herramientas de estándares mundiales, los antiguos y nuevos riesgos de la digitalidad.

La estrategia es **tan relevante como la tecnología**

Cybersecurity Mesh
Rediseñar el perímetro con una visión de malla (identidad) **SASE + Zero Trust**

- Arquitectura SASE
- ZTNA
- CASB accesos SAAS Cloud

Visibilidad Consolidada
Buscar nuevas estrategias de detección con observabilidad **extendida**

- Soluciones XDR (MDR)
- Threat Hunting

NG SOC
Descentralizar la operaciones y buscar la **Automatización**
Automatización SOAR

- **Threat Intelligence Platform/Management**

Inteligencia de Amenazas
Proyectar el estado de la Ciberseguridad, complementar con operaciones de **CiberInteligencia** de amenazas.

- Nivel Cyberexposición
- **Servicios de CiberInteligencia**
- CSPM (Postura Cloud)
- BAS

NG Seguridad para Aplicaciones
Proteger las Aplicaciones desde **múltiples** dimensiones, desde su proceso de desarrollo, tiempo de ejecución y publicación

- WAAP+DDoS
- WSCC
- **RASP**

Gestión de Identidades
Gestión universal de usuarios privilegiados **Multiplataforma**.

- Sistema de control de usuarios privilegiados
- **PAM**

Conclusiones

El cierre del año 2022 nos ha dejado una serie de alertas y enseñanzas de las cuales debemos aprender para preparar el desarrollo de este nuevo año.

De acuerdo a las estadísticas y a los casos de estudios realizados, se estima que para este 2023 tendremos en la región un aumento significativo de casos de dataleak, coronando el incremento que este fenómeno ha experimentado en los últimos años.

Ya en el segundo semestre de 2022, hemos presenciado el impacto y consecuencias de las filtraciones, tanto en Chile como en otros países de Sudamérica.

Por otra parte, la amenaza de infostealer también continuará creciendo y afectando a distintas empresas. Su función principal es el robo de la mayor cantidad de información de un usuario, exponiendo así a las organizaciones a la filtración de información crítica que ponga en riesgo su credibilidad, y a la consecuente extorsión que estos datos permiten.

Además, al igual que todos los años, la explotación de vulnerabilidades continuará en aumento, producto de la constante transformación digital y del avance en el desarrollo de aplicaciones en la nube. Ante la mayor exposición que estas innovaciones provocan, resulta más necesario que nunca continuar avanzando en metodologías de desarrollo seguro, que puedan evitar errores desde la fase inicial en el ciclo de vida.

Por su parte, el ransomware es una amenaza que se encuentra en descenso en nuestra región, apreciación de inteligencia obtenida de las investigaciones e incidencias en el último periodo. Sin embargo, la extorsión a la que este malware nos ha acostumbrado a recibir será igualmente presentada por otros tipos de ataques, que se enfocarán en el chantaje y amenaza a distintas personas y organizaciones.

Finalmente, es un hecho que el aumento en ataques a redes OT en EE.UU. y Europa continúa aumentando año a año. Ante el creciente protagonismo y amplitud que toman todas estas formas de amenaza, ¿cuáles son los planes de acción que estamos abordando dentro de las organizaciones? Y, aún a mayor escala, ¿cómo estamos trabajando en la región sobre este tipo de ataques?

Hoy resulta fundamental definir con claridad qué acciones estamos ejecutando o qué tipo de regulaciones estamos cumpliendo para crear una línea base de seguridad en estas redes.

El crecimiento de estas amenazas es real y observable a lo largo del tiempo, tal como queda en evidencia a través de los estudios y reportes que hemos desarrollado en los últimos años. Para poder hacer frente a este avance y preparar a las organizaciones con medidas realmente efectivas, la visibilidad e integración de tecnología y servicios es fundamental en la toma de decisiones de las organizaciones.

En este esfuerzo colectivo, las organizaciones y sus directivos deben valerse de los aprendizajes del 2022 para desarrollar un mayor nivel de consciencia y preparación, y así poder enfrentar y reaccionar a tiempo, evitando que el año 2023 se vea protagonizado por grandes pérdidas.

Eduardo Bouillet Carroza
Director del Centro de Ciberinteligencia

Sobre los Autores

El presente informe del estado de la ciberseguridad es confeccionado por la unidad especializada de ciberseguridad de Entel Ocean y su centro de ciber inteligencia (CCI)

Autores del Informe:

Cyril Delaere
Gerente de la unidad
de Ciberseguridad

Eduardo Bouillet Carroza
Director del Centro de
Ciberinteligencia

Jonathan Armijo Catalán
Especialista Senior Operación
Ciberinteligencia

Luis Elola
Experto en Ciberseguridad

Equipo Ciber Inteligencia:

Joaquín Miranda Gajardo
Ingeniero Operación
Ciberinteligencia

Inés Von Borries Reyes
Ingeniero Operación
Ciberinteligencia

Lorena Pérez Contreras
Ingeniero Operación
Ciberinteligencia

Marco Arancibia Ocampo
Ingeniero Operación
Ciberinteligencia

CAPÍTULO 11.

GLOSARIO DE TÉRMINOS

2FA: Doble Factor de Autenticación.
AD: Active Directory.
APT: Advanced Persistent Threat (Amenaza persistente avanzada).
AV: Antivirus.
BackDoor: Puerta Trasera.
BITB: Browser In The Browser.
C&C: Command and Control (Mando y control).
CA: Autoridad Certificadora.
CaaS: Cybercrime as a Service (Cibercrimen como servicio).
CAPTCHA: Prueba pública de turing completamente automatizada para diferenciar a la computadora de los humanos.
CISA: Agencia de Ciberseguridad y Seguridad de la Infraestructura.
CVE: Common vulnerabilities and exposures (Vulnerabilidades y exposiciones comunes).
CVSS: Common Vulnerability Scoring System (Sistema de puntuación para los CVE).
Databreach: Robo de datos de organizaciones debido a malas prácticas en configuraciones de seguridad.
Dataleak: Robo de datos mediante un ciberataque que ha comprometido parte de la infraestructura de una organización.
DDoS: Acrónimo de denegación de servicio distribuida. Técnica que utiliza numerosos hosts para realizar el ataque.
DDW: Dark o Deep web.
DNS: Sistema de nombres de dominio.
DoS: Denegación de servicio.
Dwell Time: Tiempo de permanencia.
Framework: Esquema o marco de trabajo que ofrece una estructura base.

FTP: Protocolo de transferencia de archivos.
FW: Firewall.
HaaS: Hacking as a Service (Hacking como servicio).
Hostings: Alojamiento web.
HTTP: Protocolo de transferencia de hipertexto.
HTTPS: Protocolo seguro de transferencia de hipertexto.
HUMINT: Inteligencia que proviene de la información obtenida y facilitada por fuentes humanas.
IAM: Gestión de identidad y acceso.
ICS: Abreviación de sistema de control industrial. Es un sistema de información usado para controlar procesos industriales como la fabricación, el manejo de productos, la producción y la distribución.
IoA: Indicadores de amenaza.
IoC: Indicadores de compromiso.
IT: Tecnología de la Información.
Leak: Fuga de información.
MaaS: Malware as a service (Malware como servicio).
MDR: Detección y respuesta gestionada.
OT: Tecnología de las operaciones.
PoC: Prueba de concepto.
RaaS: Ransomware as a service (ransomware como servicio).
RAT: Remote Access Trojan (troyano de acceso remoto).
RRSS: Redes Sociales.
SIEM: Security Information and Event Management (correlacionador de eventos).
SOAR: Security Orchestration, Automation and Response (herramienta de seguridad, orquestación y respuesta automatizada).
SOC: Security Operations Center (centro de operaciones de seguridad).
SSL: Secure Sockets Layer (seguridad de la capa de transporte).
TLD: Top Level Domain.
TTP: Tácticas, Técnicas y Procedimientos.
VM: Virtual Machine (máquina virtual).
VPN: Red Privada Virtual.
WAF: Web Application Firewall.
XDR: Herramienta de Detección y Respuesta Extendida.
Zero-Day: Vulnerabilidad de software, totalmente desconocida tanto para el fabricante del software, como para los motores de detección de amenazas.

ocean

entelocean.com /entelocean /entelocean