digital

Panorama
Infraestructura Crítica
2023

digital

Panorama de Infraestructura Crítica 2023

TLP:RED

No divulgar, restringido solo a participantes.

TLP:AMBER

Divulgación limitada, restringida a la organización de los participantes y sus clientes.

TLP:GREEN

Divulgación limitada, restringida a la comunidad.

TLP:CLEAR

Divulgación sin restricciones.

En este panorama, se abordan los desafíos que enfrenta la infraestructura crítica a nivel global, con especial atención en América Latina y Chile. La ciberseguridad se vuelve esencial para proteger sectores vitales como energía, telecomunicaciones, finanzas y más, buscando comprender las tácticas de los ciberdelincuentes y establecer un marco sólido de protección a escala mundial.

Se destaca la importancia de considerar las leyes y regulaciones específicas, como la Ley chilena N° 21.542, así como la creciente dependencia de tecnologías de la información en infraestructuras críticas en todo el mundo.

El panorama examina amenazas en América Latina y Chile desde 2022 y casos a nivel global, analizando incidentes y estadísticas. Además, se enfoca en soluciones basadas en mejores prácticas de ciberseguridad y la colaboración público-privada para aumentar la resiliencia en el entorno digital en todas las regiones. El objetivo es fortalecer la protección de estos activos vitales en un contexto global y garantizar el funcionamiento seguro y eficiente de nuestras sociedades en todas partes.

Chile

No es necesario ir muy lejos para observar cómo la infraestructura crítica de nuestro país ha sido impactada en diversas ocasiones, como en el emblemático caso que sacudió a una entidad bancaria en el año 2018. En este incidente, un grupo de ciberactores de origen norcoreanos consiguió (según comunicados oficiales) sustraer alrededor de US$10 millones a través de transacciones autorizadas. Este evento representó tan solo una de las múltiples incidencias atribuidas a estos sofisticados ciberactores que, entre 2014 y 2023, han afectado a instituciones financieras en al menos 13 países. Se sospecha que los ingresos obtenidos se emplean en el desarrollo de tecnología nuclear y de misiles en Corea del Norte. Asimismo, en 2020 el ransomware REvil (también conocido como Sodinokibi) afectó a otra entidad bancaria nacional, esta entidad mantuvo la mayoría de sus sucursales cerradas durante al menos cuatro días, provocando una indisponibilidad generalizada en sus sistemas y servicios al cliente.

A raíz de estos incidentes, la Comisión de Economía acordó solicitar al ejecutivo la aplicación de la máxima urgencia al mensaje en segundo trámite que establece normas sobre delitos informáticos, derogando la ley N° 19.223 y modificando otros cuerpos legales con el objetivo de adaptarlos al convenio de Budapest.

En 2022, el grupo de hackers conocido como Guacamaya filtró, el 19 de septiembre, cerca de 400.000 correos electrónicos de organizaciones de las FF. AA. en Chile.

Del mismo modo, en el transcurso de este año 2023, dos organizaciones ligadas al sector financiero de nuestro país han sufrido las acciones de un presunto ciberactor chileno, de alias "Kung_Liao". Este individuo primero impactó en una organización, explotando sus sistemas mediante una vulnerabilidad de inyección SQL, para luego continuar con la segunda organización, donde el atacante publicó una supuesta shell obtenida a través de SQLMap y compartió el presunto endpoint vulnerable.

Continuando con las actividades del ciberactor "Kung_Liao", este también atacó a una organización del rubro de la tecnología y ciberseguridad en Chile, publicando un acceso a la infraestructura de Microsoft de la organización afectada, exponiendo información de usuarios corporativos y otros.

Adicionalmente, para el rubro de la tecnología y ciberseguridad en Chile, a principios de abril se dió a conocer un ataque ransomware por parte del grupo Medusa afectando a una organización chilena dedicada a la ciberseguridad, donde los ciberactores publicaron más de 1 TB de información de la organización afectada.

En la última semana de mayo de 2023, se reveló que una organización de las FF. AA. de Chile, fue objetivo del grupo de ransomware Rhysida. Los ciberatacantes publicaron en su sitio de filtraciones aproximadamente 360.000 documentos, afirmando que esta cantidad solo representa el 30% de la información sustraída.

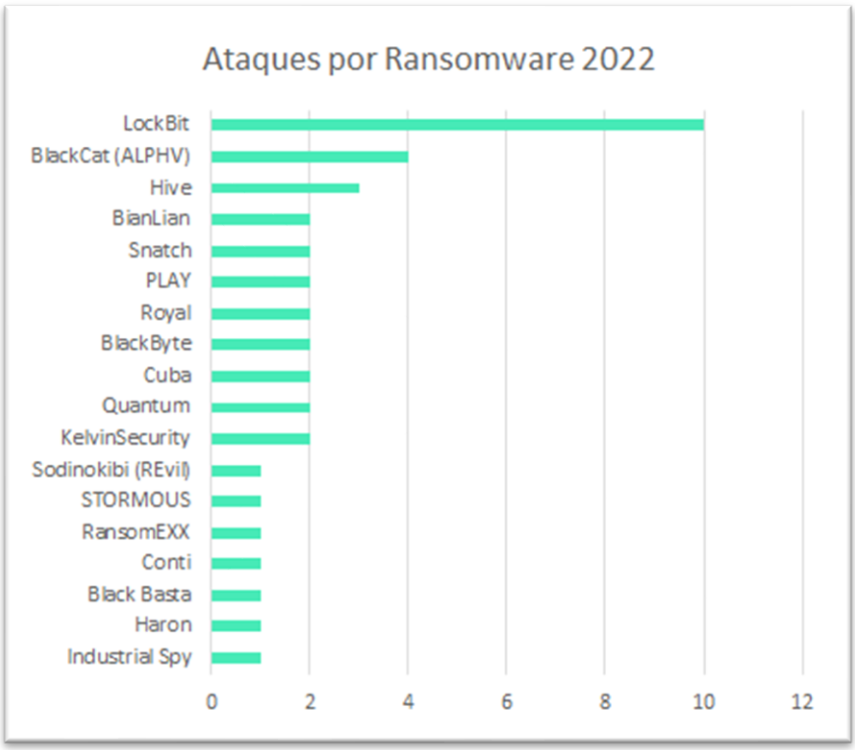
Para concluir, a mediados de septiembre de 2023 un proveedor de telecomunicaciones con operaciones en 17 países de Latinoamérica fue afectado con ransomware, paralizando varios portales entre ellos gubernamentales, afectando diferentes organizaciones tanto en Colombia, Chile, Argentina y Panamá.

Ataques de Ransomware

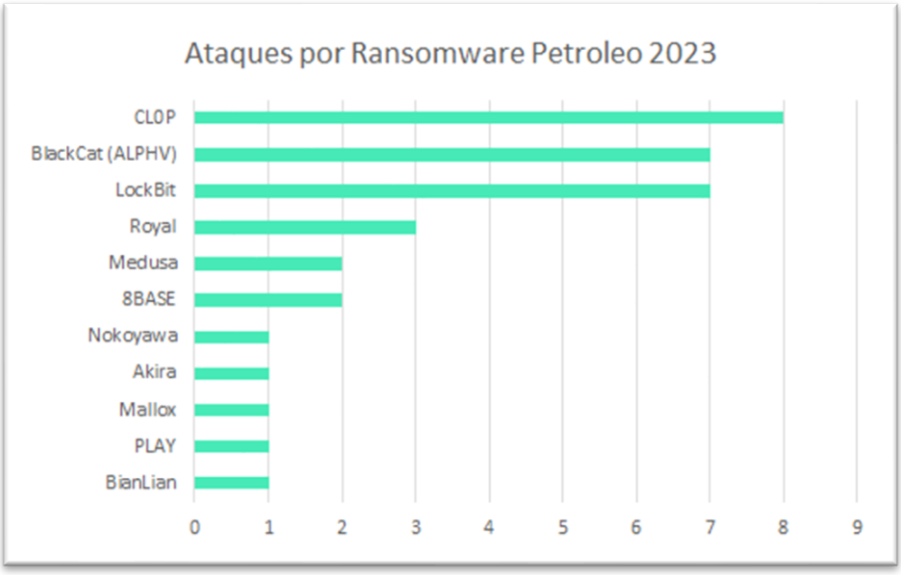
Industria Petrolera

Desde enero 2022 hasta agosto 2023, se han identificado un total de 74 ataques de ransomware dirigidos a la industria del petróleo a nivel global. Estos incidentes son un recordatorio de la vulnerabilidad que poseen las infraestructuras críticas frente a las amenazas cibernéticas.

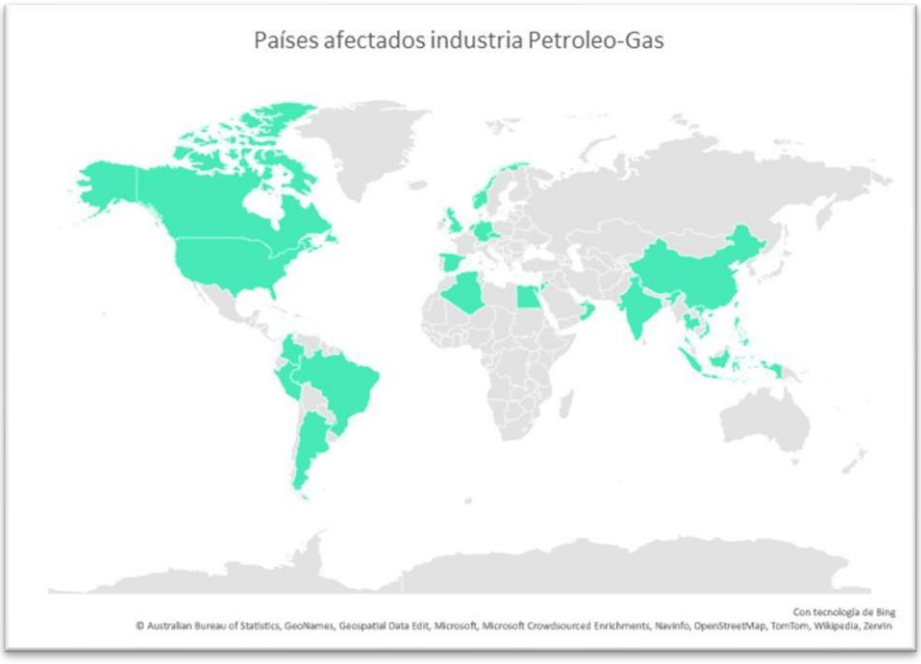
En 2022, se registraron 40 de estos ataques, un número significativo que pone de relieve la creciente tendencia de los ciberdelincuentes a apuntar a sectores vitales para la economía y el funcionamiento de las sociedades. Cada uno de estos ataques no solo implicó costos económicos significativos en términos de rescate potencial y pérdida de ingresos, sino que también, pudo haber tenido serias repercusiones en la seguridad energética y la estabilidad de las operaciones diarias.



En lo que va de 2023, la industria ha sido golpeada por 34 ataques adicionales. Este dato alarmante subraya la necesidad de que las empresas del sector petrolero, y de infraestructuras críticas en general, refuercen sus medidas de ciberseguridad. Esto incluye la implementación de firewalls avanzados, la actualización regular de software y hardware, la capacitación de empleados en ciberseguridad, y la colaboración con entidades gubernamentales y privadas en materia de ciberinteligencia para anticiparse a posibles amenazas.



Estos ataques, y la creciente sofisticación de estos, subrayan la necesidad de una robusta ciberinteligencia que pueda prever, detectar y contrarrestar estas amenazas. Las empresas e instituciones deben estar preparadas para reaccionar rápidamente a los incidentes de seguridad, minimizar el daño y recuperarse con la mayor eficacia posible. Esta necesidad se hace cada vez más evidente en la medida en que la ciberseguridad en las infraestructuras críticas se convierte en una cuestión no sólo de seguridad empresarial, sino de seguridad nacional e internacional.



En nuestra región, el año 2022 evidenció la vulnerabilidad de la industria del petróleo y gas frente a las amenazas cibernéticas, con 4 organizaciones que sufrieron ataques de ransomware. Este tipo de incidentes no sólo interrumpe las operaciones, sino que también puede tener graves repercusiones en términos de seguridad energética y pérdida de confianza de los inversores y clientes.

Mientras tanto, en lo que va del 2023, ya se conocen 2 organizaciones más que han sido afectadas en esta industria para LATAM. Este panorama resalta la creciente amenaza que los ataques de ransomware representan para las infraestructuras críticas en nuestra región.

2023

- Organización: GRUPOVANTI
  - País: Colombia
  - Ransomware: Cl0p
  - Fecha: 23-03-2023
- Organización: PAN AMERICAN ENERGY S.L. SUCURSAL ARGENTINA
  - País: Argentina
  - Ransomware: Hive
  - Fecha: 04-03-2023

2022

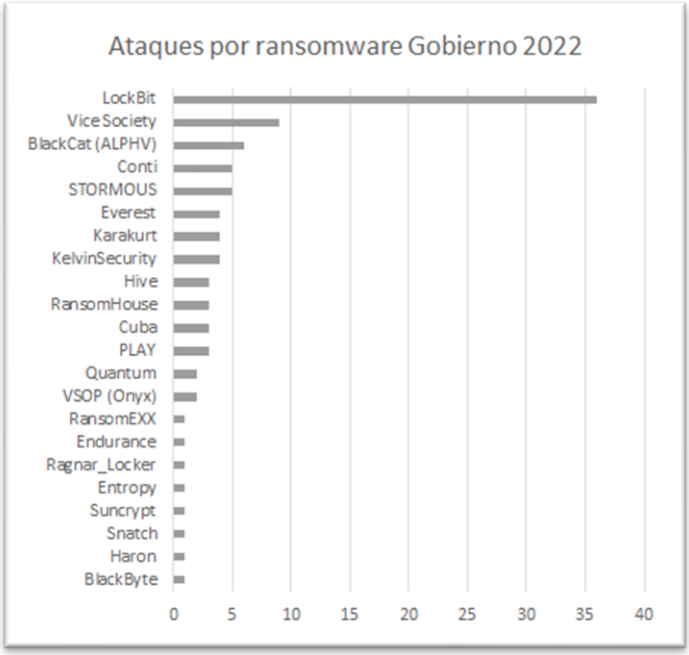
- Organización: Zeus Energy S.A.C
  - País: Perú
  - Ransomware: LockBit
  - Fecha: 21-03-2022
- Organización: webnordeste.com.br
  - País: Brasil
  - Ransomware: LockBit
  - Fecha: 24-09-2022
- Organización: independence.com.co
  - País: Colombia
  - Ransomware: LockBit
  - Fecha: 14-09-2022
- Organización: eneva.com.br
  - País: Brasil
  - Ransomware: LockBit
  - Fecha: 05-09-2022

Es imperativo que las organizaciones en la industria del petróleo y gas de América Latina incrementen sus esfuerzos para fortalecer su postura de ciberseguridad, incluyendo la adopción de una estrategia de ciberinteligencia robusta. Esta debería incluir la detección y respuesta temprana a las amenazas, la formación continua de su personal en prácticas de seguridad cibernética, la adopción de tecnologías de ciberseguridad actualizadas y la cooperación con otras organizaciones y autoridades para compartir información sobre amenazas y mejorar la resiliencia de toda la industria.

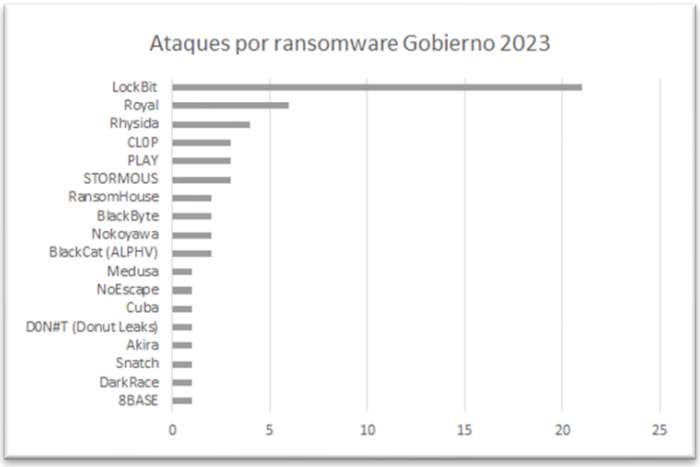
Gobierno

Las entidades gubernamentales también han sido el blanco de significativos ataques cibernéticos durante el periodo analizado. En total, se han detectado 153 ataques de ransomware conocidos, un indicador alarmante de la creciente amenaza que este tipo de ataques representa para los órganos de gobierno.

En 2022, se registraron 97 de estos ataques, evidenciando la persistencia y el alcance de las amenazas cibernéticas hacia las instituciones gubernamentales. Este elevado número refleja la necesidad de que las autoridades gubernamentales tomen medidas decisivas para proteger sus sistemas y redes.

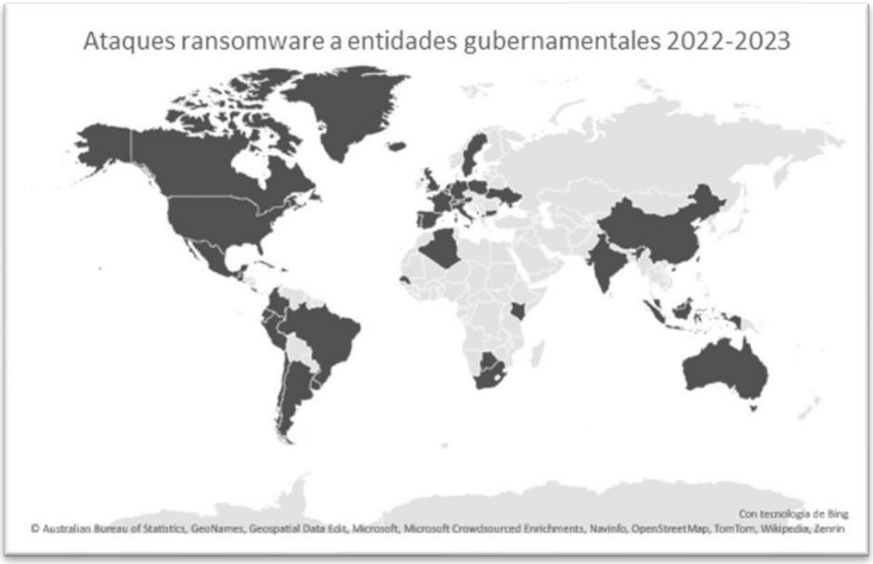


En lo que va de 2023, se han registrado otros 56 ataques a entidades gubernamentales. Este patrón sugiere que las amenazas de ransomware seguirán siendo una preocupación importante para los gobiernos en el futuro cercano.



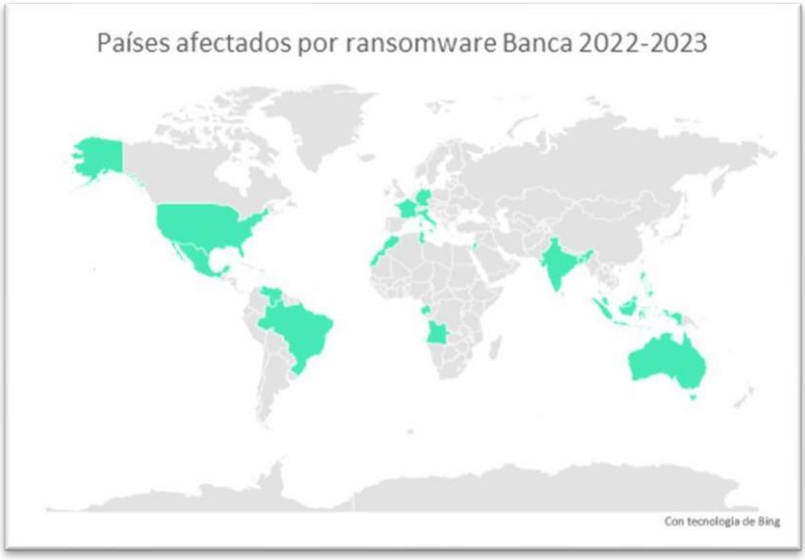
Es esencial que las entidades gubernamentales refuercen sus medidas de seguridad cibernética y adopten estrategias de ciberinteligencia para anticipar, prevenir y responder a estos ataques. Esto incluye no solo medidas defensivas, como la instalación de software de seguridad actualizado y la realización de auditorías de seguridad regulares, sino también medidas proactivas, como la formación de personal en las mejores prácticas de ciberseguridad y la colaboración con expertos en ciberinteligencia para identificar y neutralizar las amenazas antes de que puedan causar daño.

La protección de la infraestructura crítica gubernamental contra los ciberataques es un aspecto esencial de la seguridad nacional, y es fundamental que se hagan todos los esfuerzos necesarios para mantener la integridad, disponibilidad y confidencialidad de los sistemas y redes gubernamentales.

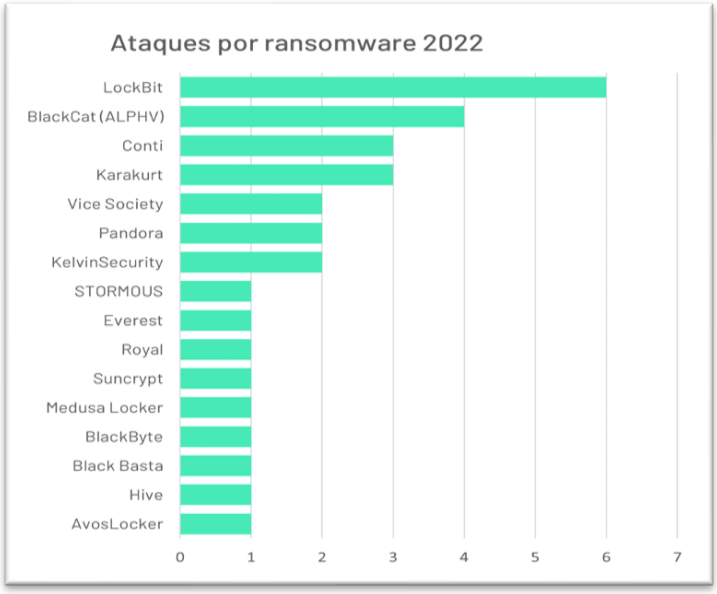


Entidades Bancarias

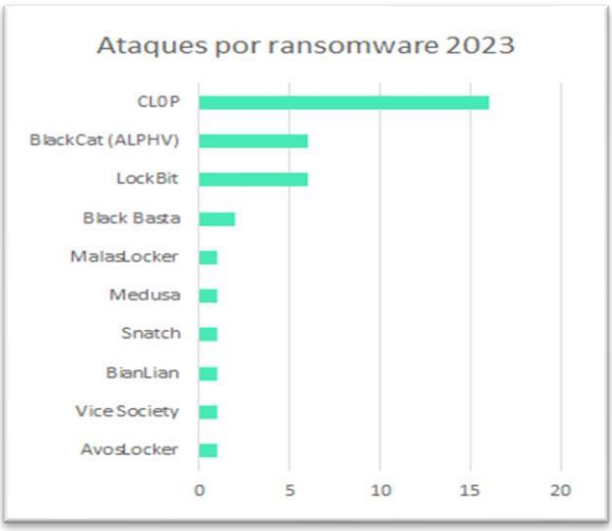
Las entidades bancarias, vitales para la economía global, no han sido inmunes a las amenazas cibernéticas. Durante el periodo que abarca esta investigación, se registraron 67 ataques de ransomware, afectando con mayor incidencia a los Estados Unidos.



En 2022, se reportaron 31 de estos ataques, un número preocupante que demuestra la creciente amenaza que los ciberdelincuentes representan para el sector financiero. Cada uno de estos ataques puede causar interrupciones significativas en los servicios bancarios, pérdidas financieras directas e indirectas y daños a la reputación de las instituciones afectadas.



En lo que va de 2023, se han registrado 36 ataques adicionales superando la cifra del año anterior en dos trimestres. Este ritmo constante de ataques subraya la importancia de que las instituciones financieras implementen medidas de ciberseguridad efectivas y robustas, así como estrategias de ciberinteligencia para detectar, prevenir y responder a estas amenazas.



La adopción de tecnologías avanzadas de ciberseguridad, el establecimiento de protocolos de respuesta a incidentes, la capacitación de los empleados en seguridad cibernética y la colaboración con los gobiernos y otras instituciones financieras para compartir información sobre las amenazas pueden ayudar a proteger a las entidades bancarias de futuros ataques de ransomware.

Estos ataques ponen de manifiesto la necesidad de una mayor inversión en ciberseguridad por parte de las entidades bancarias, así como de un enfoque más estratégico y proactivo para combatir las amenazas cibernéticas.

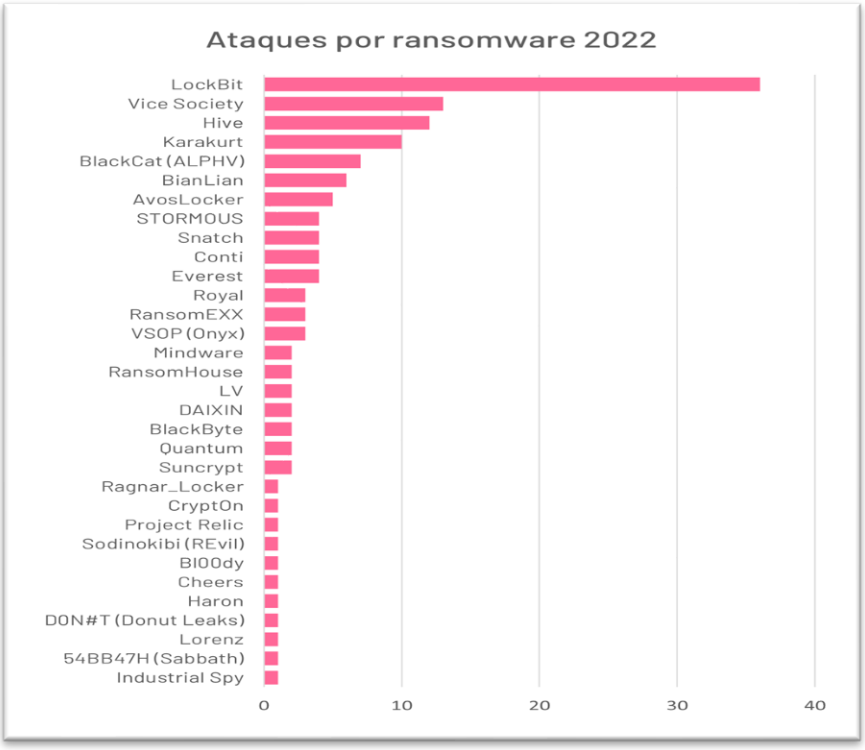
A pesar de que la lucha en el terreno de la ciberinteligencia es ardua y exige constantes y considerables esfuerzos, su importancia no puede ser subestimada. Esto se debe a la intensa atracción que el ciberespacio ejerce sobre los actores maliciosos, quienes buscan obtener recompensas de alto rendimiento. Estos beneficios les permiten no solo mejorar la sofisticación de sus ataques, sino también, en algunos casos, financiar programas de carácter tan serio como los nucleares.

Recientes estimaciones han puesto de manifiesto un hecho inquietante: se sugiere que Corea del Norte genera cerca del 50% de sus ingresos a través de ciberataques. Las entidades financieras constituyen sus principales objetivos, aunque actualmente las redes blockchain también están siendo explotadas. Estos ciberdelincuentes logran sustraer enormes cantidades de criptomonedas de manera anónima, lo que complica aún más la tarea de rastrear y prevenir dichas amenazas en la infraestructura crítica.

Salud

Desde enero 2022 hasta agosto 2023, el sector de la salud ha sufrido de manera considerable las embestidas de los ataques de ransomware. Se han detectado 292 ataques de este tipo, lo que resalta la vulnerabilidad de una industria esencial para el bienestar de todas las sociedades.

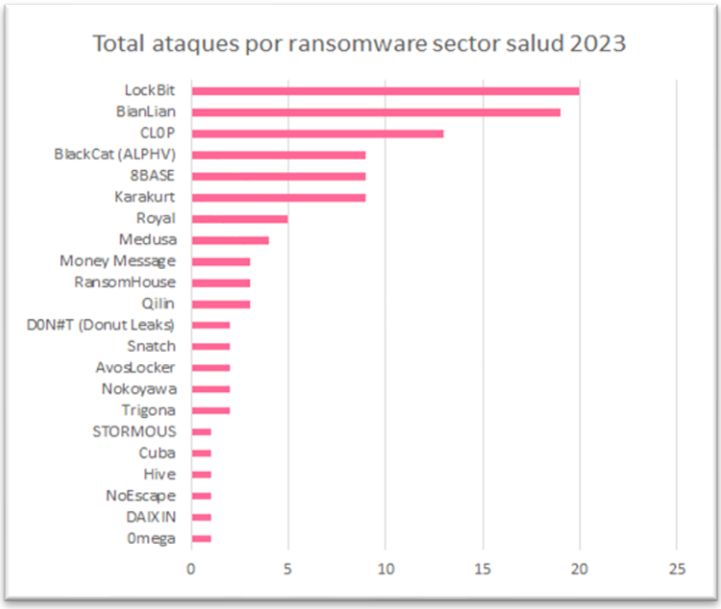
En el año 2022, se registraron 139 de estos ataques, cada uno de ellos no solo puede interrumpir los servicios de atención médica vitales, sino que también puede poner en peligro la privacidad de los datos del paciente, lo que tiene implicaciones éticas y legales significativas.



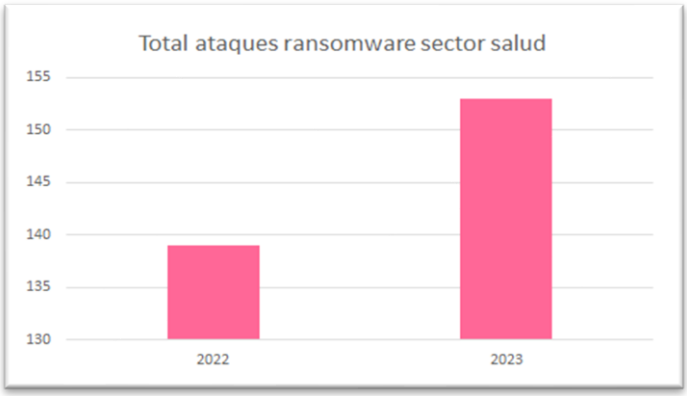
Es vital reconocer los límites éticos dentro del ámbito de la ciberseguridad, especialmente cuando se trata de infraestructura crítica. Aunque algunos ciberactores han declarado que las organizaciones de salud no están en su punto de mira, la realidad puede resultar diferente. Incluso se ha visto a operadores de ransomware cómo LockBit disculparse y proporcionar claves de descifrado gratuitas a las entidades afectadas por sus afiliados.

Sin embargo, no se puede ignorar la dura realidad: la mayoría, si no todos, los actores de ransomware han comprometido alguna vez una entidad dentro del sector sanitario. Esta afirmación se ve respaldada por el gráfico a continuación, que pone de manifiesto la prevalencia de estos incidentes de seguridad. A pesar de las aparentes garantías, la amenaza persiste, subrayando la necesidad imperante de una ciberinteligencia robusta para proteger nuestra infraestructura esencial.

Para lo que va del 2023, ya se han registrado otros 153 ataques, lo que pone de manifiesto que el sector de la salud sigue siendo un objetivo atractivo para los ciberdelincuentes. Aunque algunos grupos de ciberactores, como LockBit, han prometido no atacar hospitales y han llegado incluso a pedir disculpas por hacerlo, el sector de la salud sigue siendo uno de los más afectados en comparación con otras infraestructuras críticas.



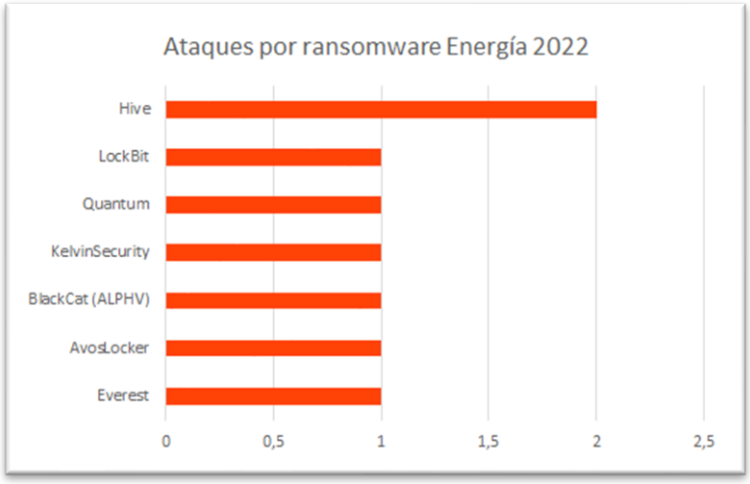
Es esencial que las organizaciones de salud refuercen su ciberseguridad e inviertan en ciberinteligencia para anticiparse y responder a estas amenazas. Además de contar con una infraestructura de TI segura y actualizada, las organizaciones de salud necesitan tener un plan de respuesta a incidentes que se pueda activar en caso de un ataque de ransomware. Este plan debe incluir medidas para recuperar los sistemas y los datos afectados, comunicarse con los pacientes y las autoridades pertinentes, y aprender de cada incidente para evitar que se repita en el futuro.



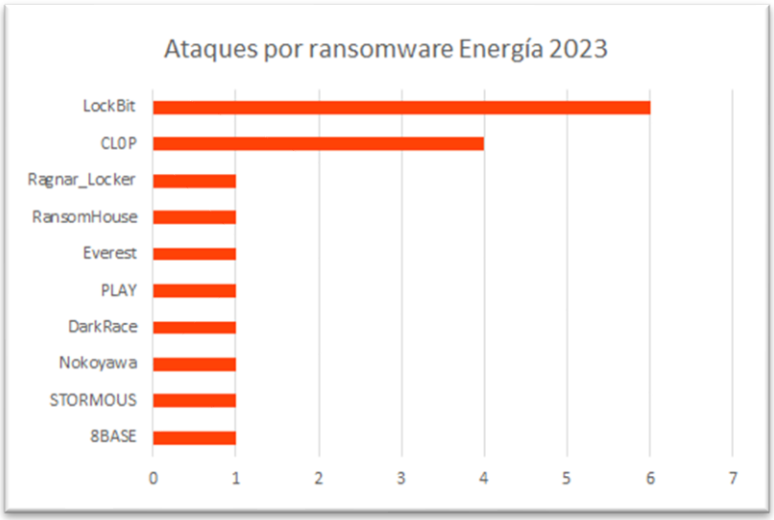
La protección del sector de la salud contra las amenazas cibernéticas es de suma importancia, y se requiere de un enfoque integral y proactivo para garantizar la seguridad y la resiliencia de este sector vital. Del total de los ataques para este sector se registran 13 en Latinoamérica siendo Brasil el país más afectado con 8 ataques, seguido con 3 en Colombia y 1 ataque para Argentina y México.

Energía

El sector energético, que constituye una infraestructura crítica para cualquier nación, también ha sido objetivo de ataques de ransomware durante el periodo analizado. Se han registrado un total de 26 ataques conocidos, poniendo en evidencia la necesidad de medidas de seguridad cibernética robustas en esta industria.



Durante el 2022, se reportaron 8 ataques de ransomware, mientras que en lo que va de 2023 ya se han registrado 18 ataques adicionales. Este patrón demuestra que los ciberdelincuentes están cada vez más enfocados en la infraestructura crítica, y el sector energético no es una excepción.



Es importante destacar que solo uno de estos ataques ha tenido lugar en nuestra región, específicamente en Argentina. Sin embargo, este hecho no debe dar lugar a la complacencia. La interconexión global de las infraestructuras energéticas y la creciente sofisticación de los ciberataques significa que ninguna región está exenta de estas amenazas.

Las organizaciones del sector energético deben tomar en serio la amenaza que representan los ciberataques y deben tomar medidas proactivas para proteger sus sistemas y redes. Estas medidas deben incluir una sólida estrategia de ciberinteligencia que permita detectar y responder a las amenazas de manera oportuna, así como la formación de su personal en prácticas seguras de ciberseguridad y la adopción de tecnologías avanzadas de ciberseguridad.

En última instancia, la seguridad cibernética en el sector energético no es solo una cuestión de proteger los activos de la empresa, sino también de garantizar la continuidad de los servicios energéticos y proteger la seguridad nacional. Por lo tanto, es esencial que se realicen inversiones adecuadas en la protección cibernética de las infraestructuras energéticas.

Es fundamental destacar que se conocen más de 600 ataques de ransomware dirigidos a diversas infraestructuras críticas, lo que subraya la importancia de proteger estos sectores vitales. Los ransomware, debido a su capacidad destructiva y sus impactos adversos, plantean un riesgo significativo tanto para individuos como para organizaciones.

Este tipo de malware avanzado tiene la capacidad de cifrar archivos y sistemas, bloqueando el acceso a información crucial y paralizando las operaciones. Los costos asociados con los ransomware no se limitan al rescate financiero que exigen; también pueden ocasionar daño a la reputación, pérdida de datos insustituibles y la interrupción de servicios esenciales.

Desde 2022 hasta la fecha, el grupo de ransomware más activo en el ataque a organizaciones clasificadas como infraestructura crítica ha sido LockBit, con 155 organizaciones comprometidas a nivel mundial. En nuestra región, este grupo ha sido responsable de 16 ataques conocidos a infraestructuras críticas.

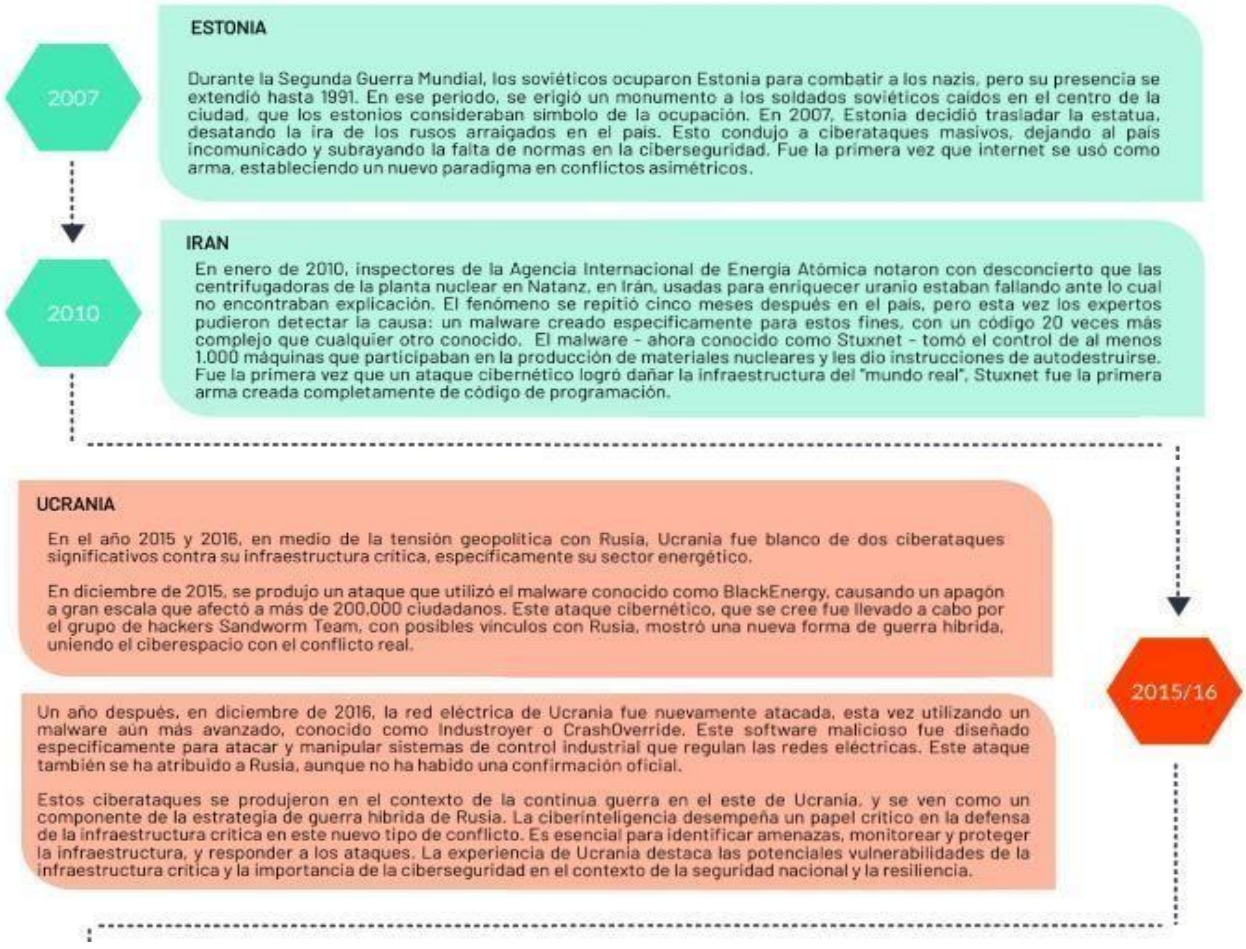
Las múltiples y variadas Tácticas, Técnicas y Procedimientos (TTP´s) utilizados por afiliados de LockBit son un recordatorio de la sofisticación de los actores de amenazas y la necesidad de una ciberdefensa dinámica y proactiva. Esto incluye el monitoreo constante de las redes, la formación regular de los empleados, y la adopción de medidas de seguridad como la autenticación de dos factores, las copias de seguridad periódicas de los datos y el mantenimiento actualizado de los sistemas y el software.

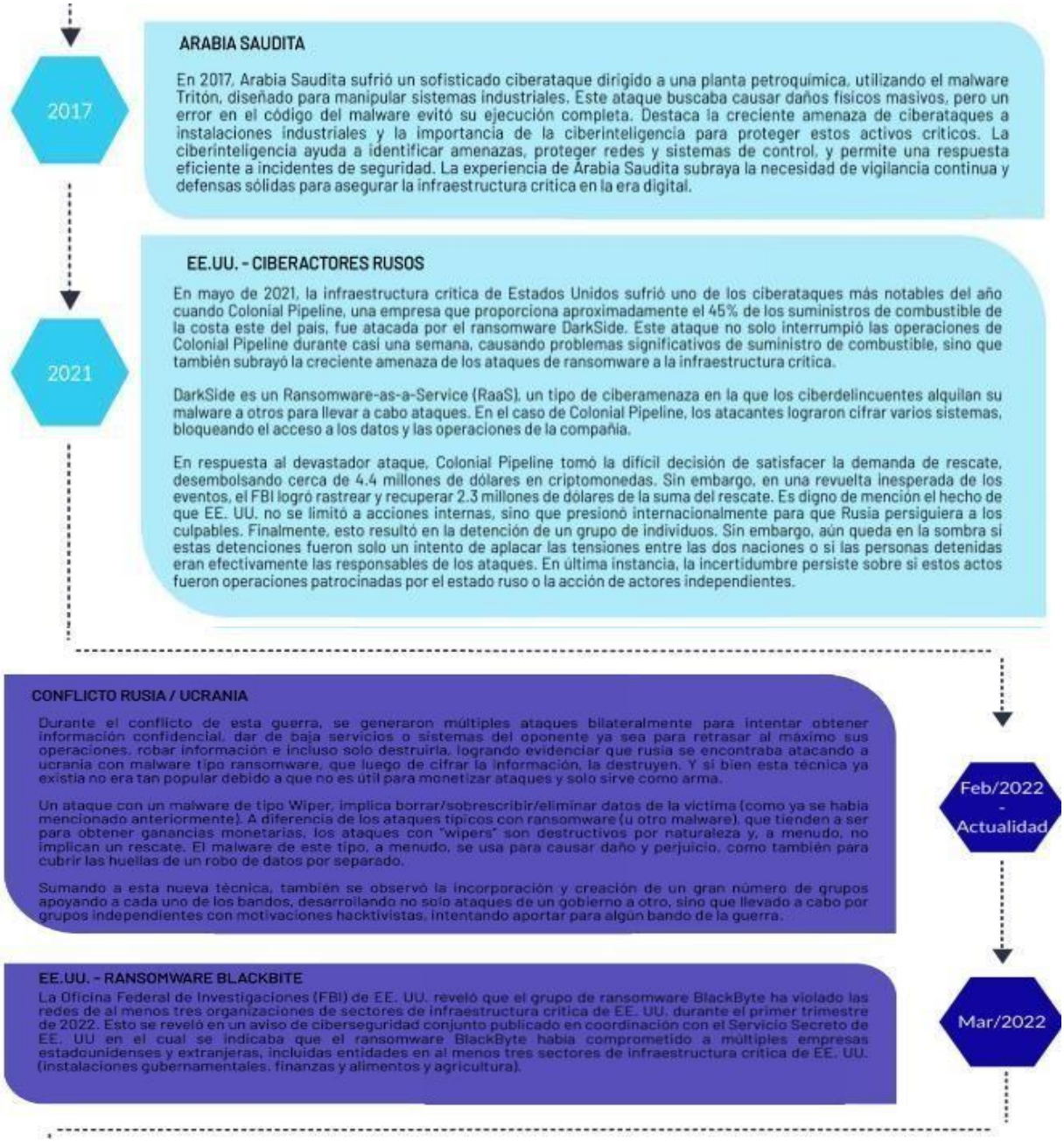
Además, es vital una respuesta rápida y efectiva a los incidentes para minimizar el daño. Los equipos de respuesta a incidentes de seguridad informática (CSIRT) deben estar preparados para actuar rápidamente en caso de un ataque, identificando el problema, conteniendo el daño, eliminando la amenaza y restaurando los sistemas a su estado normal.

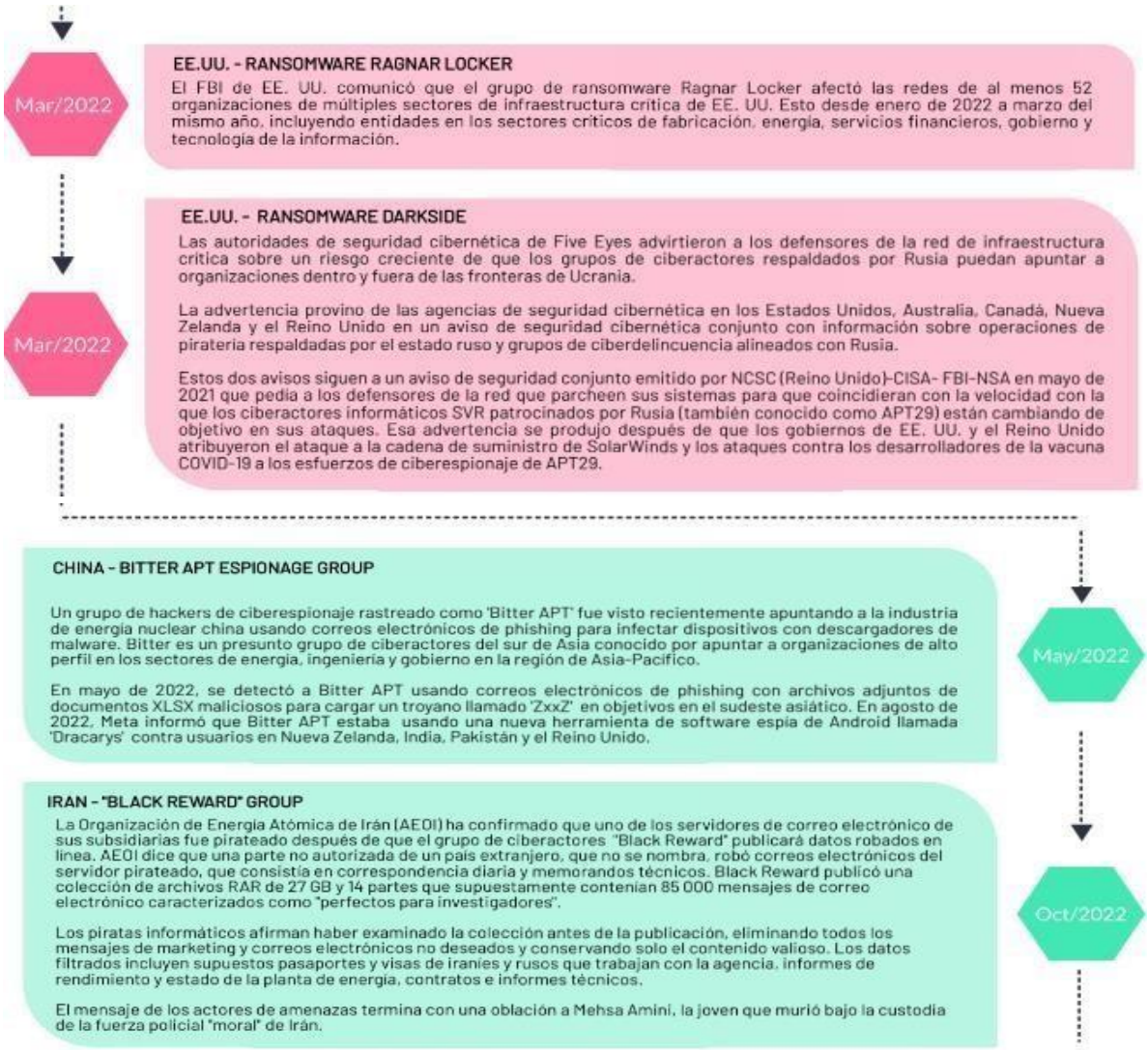
Historia

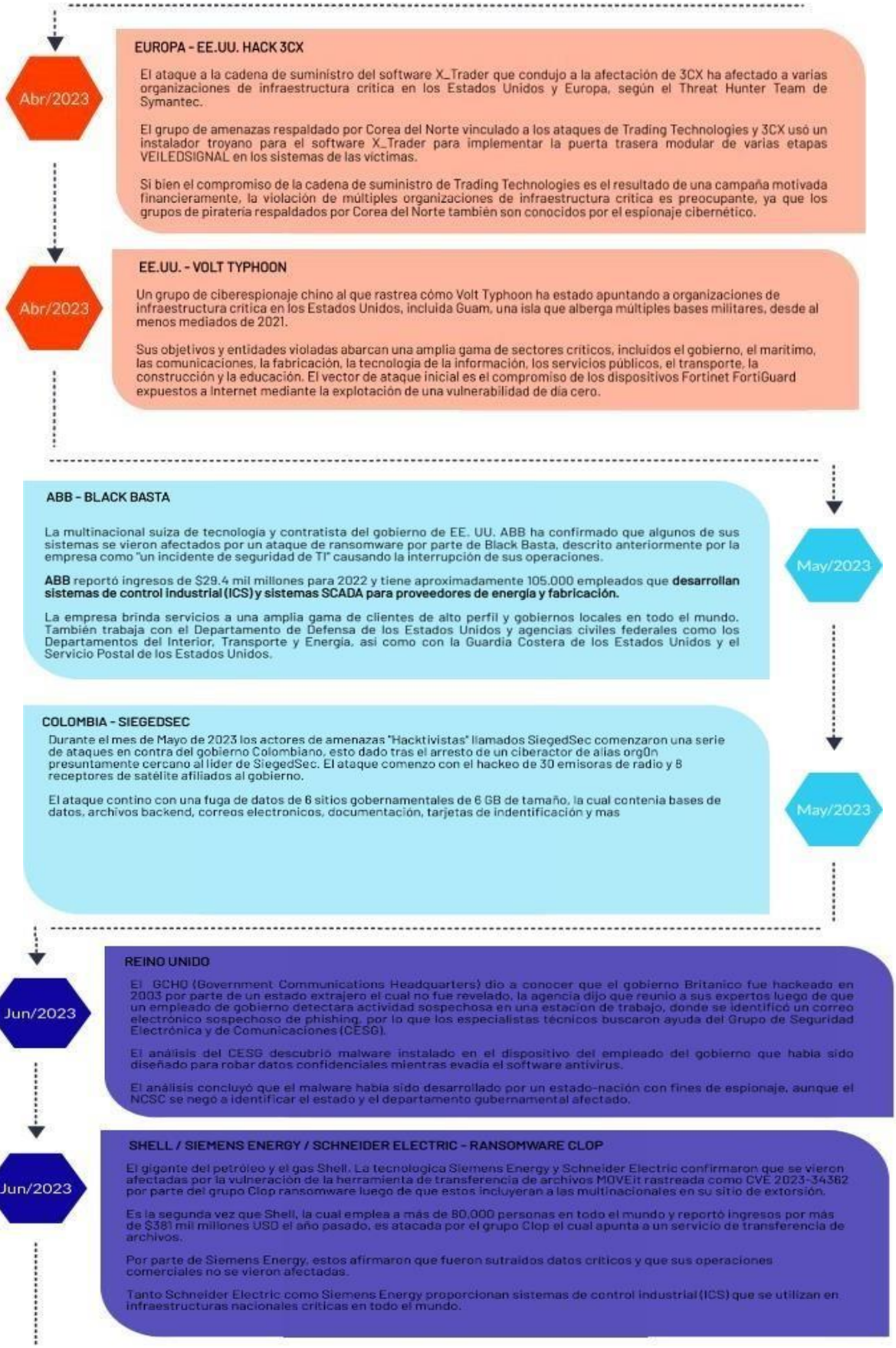
Durante las últimas décadas hemos visto los impactos disruptivos que genera este tipo de ataques en las sociedades, casos memorables como el de Estonia (2007), Irán (2010), Ucrania (2015/2016), Arabia Saudita (2017), EE.UU. (2021/22/23), no deben pasar desapercibidos.

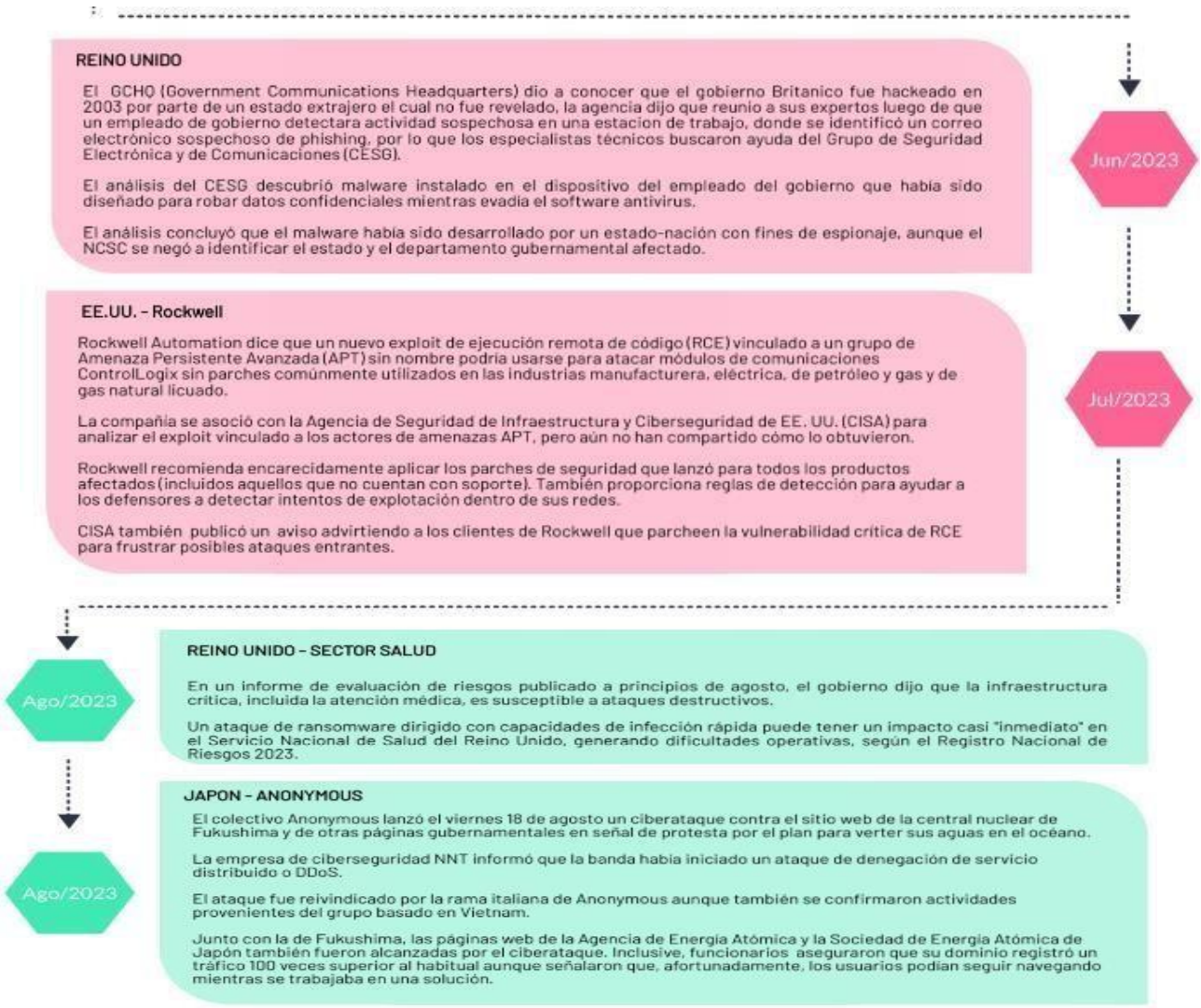
Estos casos ilustran la vulnerabilidad de las infraestructuras críticas a los ciberataques y subraya la importancia de la ciberinteligencia en la detección y respuesta a estas amenazas. La ciberinteligencia puede proporcionar información valiosa sobre las amenazas emergentes, ayudar a predecir y prevenir ataques, y proporcionar una guía estratégica para la respuesta y recuperación después de un ataque.











¿Cómo avanzamos en materias de resguardo de infraestructura críticas en Chile?

En abril de 2023 el senado aprobó legislar el proyecto de Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información, En su Artículo 1, el proyecto de Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información establece los principales objetivos de la norma:

En primer lugar, determinar la institucionalidad, los principios y la normativa general que permitan estructurar, regular y coordinar las acciones de ciberseguridad de los organismos del Estado. Y también entre estos y los particulares.

Asimismo, la norma persigue fijar los requisitos mínimos que contribuyan a prevenir, contener, resolver y dar respuesta a los incidentes de ciberseguridad.

De igual manera, tiene como fin precisar las atribuciones y obligaciones de los organismos del Estado, así como los deberes de las instituciones privadas, y los mecanismos de control, supervisión y responsabilidad ante infracciones.

Creación ANCI

En el articulado de la Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información cabe destacar el papel de la ANCI. Entre otras funciones, será la encargada de identificar a los operadores de importancia vital y servicios esenciales.

Además, la ley obligará a que los organismos del Estado y las instituciones privadas sean más proactivos ante los incidentes de seguridad cibernética. Para ello, la agencia establecerá protocolos y estándares diferenciados en función del tipo de organización.

Del mismo modo, todas las entidades públicas y privadas, con excepción de aquellas eximidas por la ANCI, deberán reportar al CSIRT nacional, en un plazo de tres horas, los ciber incidentes que puedan tener efectos significativos. Y también informar de su plan de acción. Por otro lado, se les prohíbe realizar pagos si son víctimas de ataques de ransomware.

Finalmente, a la agencia se le atribuye la regularización, fiscalización y sanción de las acciones de seguridad informática de los organismos de la Administración del Estado y de las instituciones privadas.

Apreciación

Dado que estamos en un mundo cada vez más globalizado, esta interconectividad también las expone a una serie de amenazas cibernéticas, como ataques cibernéticos, intrusiones maliciosas y sabotajes digitales. Un ataque exitoso contra una infraestructura crítica puede tener consecuencias devastadoras, desde la interrupción del suministro de servicios básicos hasta el colapso de la economía y la puesta en peligro de la seguridad nacional. Por lo tanto, la implementación de medidas sólidas de ciberseguridad, que incluyan la protección de redes, sistemas y datos sensibles, así como la detección temprana de amenazas y la respuesta efectiva, es esencial para salvaguardar estas infraestructuras críticas y garantizar la continuidad de las operaciones vitales para el bienestar de la sociedad.

Además, se debe establecer una cultura de concienciación sobre la ciberseguridad entre el personal que opera y mantiene las infraestructuras críticas. La educación y la capacitación en temas de seguridad cibernética son vitales para garantizar que todos los empleados comprendan los riesgos asociados y sepan cómo detectar y responder ante posibles amenazas. Esto incluye prácticas de higiene digital, como el uso de contraseñas fuertes y actualizadas regularmente, así como la verificación de la autenticidad de los correos electrónicos y los enlaces antes de hacer clic en ellos.

Asimismo, es crucial establecer protocolos claros y procedimientos de respuesta ante incidentes de seguridad. Contar con un plan de acción detallado y bien estructurado permite una respuesta rápida y eficiente ante cualquier intento de violación o intrusión. La implementación de mecanismos de monitorización y registro de actividad también es esencial para detectar y responder a posibles amenazas de manera oportuna.

En resumen, mejorar la ciberseguridad en infraestructuras críticas implica una combinación de medidas técnicas, educativas y organizativas. Con una evaluación de riesgos efectiva, concienciación del personal, protocolos de respuesta claros y un mantenimiento riguroso de los sistemas, es posible fortalecer las defensas y proteger adecuadamente estos activos vitales contra las constantes amenazas cibernéticas.

Acciones inmediatas:

- Redes de segregación: Asegúrese de que su infraestructura crítica esté segregada de otras redes y sistemas, utilizando firewalls o separaciones físicas, para limitar el acceso y aislarla de potenciales amenazas.
- Monitoreo de Red Constante: Use sistemas de detección y prevención de intrusiones (IDS/IPS) y monitoree constantemente el tráfico de red para detectar anomalías o comportamientos inusuales.
- Implementar una Estrategia de Defensa en Profundidad: Esta estrategia implica múltiples capas de defensa con la idea de que si una capa es penetrada, la siguiente capa estará allí para detener o detectar el ataque.
- Gestión de Vulnerabilidades: Realizar una evaluación regular de las vulnerabilidades y llevar a cabo pruebas de penetración de forma periódica para detectar y corregir cualquier debilidad en la infraestructura.
- Plan de Respuesta a Incidentes: Diseñar y mantener un plan de respuesta a incidentes que defina claramente los roles y responsabilidades, los procedimientos de comunicación y las acciones a tomar en caso de un incidente de seguridad.
- Gestión de Acceso a los Sistemas Críticos: Es importante asegurar que sólo el personal autorizado tenga acceso a los sistemas críticos. Esto puede lograrse mediante la implementación de controles de acceso físico y lógico.

- Políticas de Seguridad de la Información: Las políticas de seguridad deben estar actualizadas y deben ser revisadas y actualizadas periódicamente para reflejar cualquier cambio en la organización o en el panorama de amenazas.
- Pruebas de Recuperación: No solo es importante tener copias de seguridad, sino también probar regularmente los procedimientos de recuperación para garantizar que se pueden restaurar los datos y sistemas críticos en caso de un incidente.
- Automatización de la Seguridad: Implemente soluciones de seguridad que utilicen la automatización para detectar, prevenir y responder a las amenazas en tiempo real.
- Integrar Inteligencia de Amenazas: Utilice la inteligencia de amenazas para estar al tanto de las amenazas emergentes y adaptar su estrategia de seguridad en consecuencia.
- La seguridad en la ciberinteligencia no es un estado sino un proceso continuo de mejora y adaptación. Estas recomendaciones pueden ser de ayuda, pero siempre es crucial tener en cuenta las particularidades de cada infraestructura y organización.