Ransomware: El Gran Enemigo De Latinoamérica

by Marcelo Ruiz, Consulting Director

En Colaboración Con

CROWDSTRIKE

A Frost & Sullivan White Paper

Powering clients to a future shaped by growth

FROST & SULLIVAN

CONTENIDO

Entendiendo el Ransomware y la Nueva Tendencia de Raas (Ransomware as a Service)

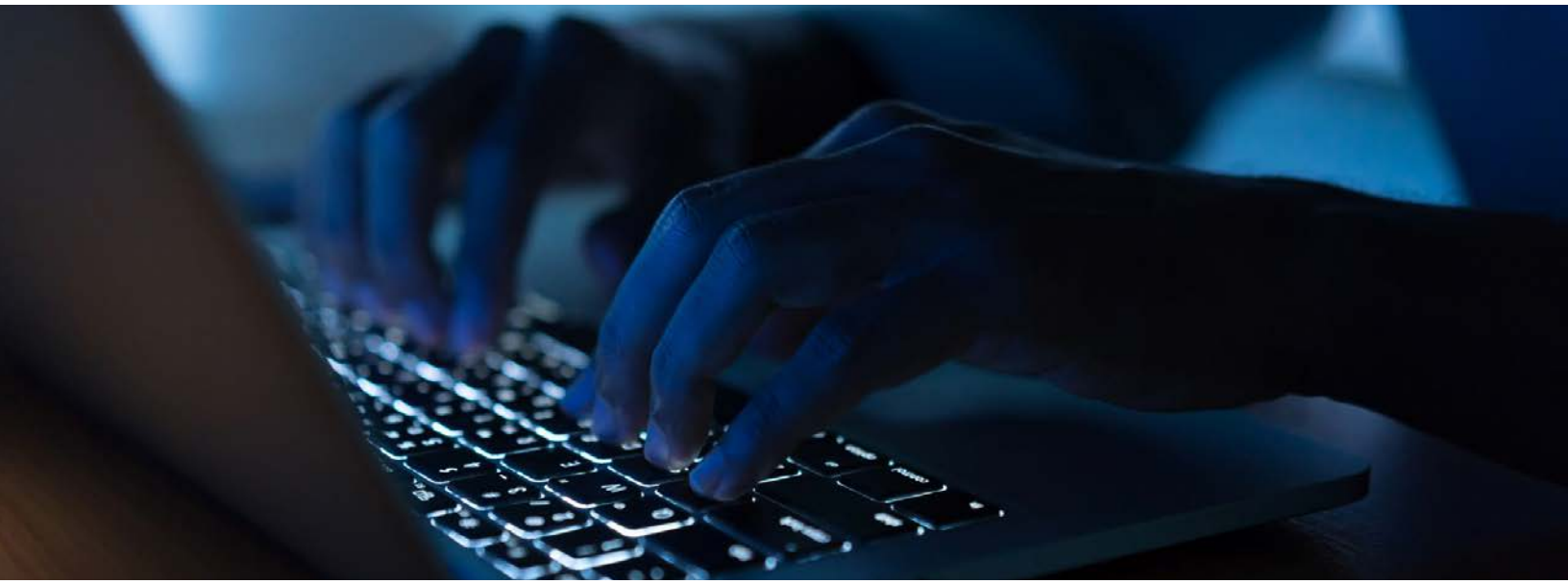
Entendiendo el Ransomware

El malware es un software malicioso que infecta los dispositivos informáticos personales. Puede afectar la disponibilidad, integridad y confidencialidad de los datos. El Ransomware es una variante de la familia de malware, donde puede cifrar maliciosamente los archivos en un dispositivo informático tras la infección, lo que afecta la disponibilidad de datos. Cuando un usuario intenta abrir un archivo cifrado, aparece una ventana emergente que informa a la víctima que los archivos han sido encriptados, exigiendo posteriormente un rescate, generalmente a pagar en criptomonedas, a cambio de liberar la clave de descifrado.

El Ransomware se considera uno de los tipos de ciberataques más comunes y de mayor crecimiento en América Latina, especialmente en el segmento de pequeñas y medianas empresas, incluido los gobiernos estatales y locales los cuales suelen ser más vulnerables a los ataques cibernéticos. Lo anterior no descarta a las grandes organizaciones que también son foco de ataque para obtener grandes pagos.

La siguiente es una lista de factores claves que hicieron que el Ransomware sea popular como arma preferida de los ciberdelincuentes:

- La tendencia de las empresas hacia el modelo de teletrabajo para acceder a redes corporativas a través de conexiones remotas.
- El Ransomware induce al mayor impacto y miedo en las víctimas, provoca la interrupción de operaciones comerciales y afecta la reputación de las organizaciones.
- Las víctimas que aceptan pagar por el descifrado de archivos fomentan más ataques de este tipo.
- Falta de buenas prácticas de ciberseguridad en las organizaciones, principalmente la baja adopción de soluciones para respaldo de la información.



RaaS (Ransomware as a Service)

El Ransomware as a Service es un tipo de servicio, con la diferencia de que en vez de ofrecer programas legítimos para usar en nuestro trabajo, lo que ofrecen son kits de malware para llevar a cabo un ataque de Ransomware. Es decir, un hacker o grupo de hackers desarrollan un virus Ransomware (capaz de encriptar todos o casi todos los archivos de una empresa o uno en particular y denegar su acceso a ellos hasta recibir un rescate a cambio) y lo ponen a la venta en la Web Oscura (Dark Web), de manera que cualquier persona, sin necesidad de tener grandes conocimientos técnicos, puede comprarlo y utilizarlo contra el objetivo que haya elegido. El Ransomware as a Service seguirá siendo tendencia entre los ciberdelincuentes y una preocupación más para muchas empresas.

Un grupo de Ransomware que ha tenido mucha actividad en el 2021 es Avaddon según un artículo publicado por el Diario Económico y de Negocios El Financiero de México; Avaddon es un Ransomware as a Service (RaaS) donde se han registrado varias empresas afectadas de todos los sectores en América Latina en países tales como Brasil, México, Chile, Colombia, Perú y Costa Rica principalmente. Algunos de los mecanismos de acceso inicial que estuvo utilizando este Ransomware fueron correos de phishing con archivos adjuntos en formato ZIP que contienen un archivo javascript malicioso. Estos correos incluían un mensaje en el cuerpo del correo que buscaban despertar la curiosidad del usuario, como una supuesta foto o similar.

Asimismo el grupo de cibercriminales Neshta ha tenido una dinámica importante en América Latina realizando ataques focalizados, este Ransomware está infectado con el código malicioso Neshta, donde se adhiere a archivos ejecutables para evitar ser detectado, según el blog del portal Virus Bulletin. El último grupo de Ransomware que ha se ha identificado es Atomsilo, donde hicieron su primer ataque en Brasil en una empresa farmacéutica, según blog del portal de tecnología infochannel.info.

Situación de Ransomware y tendencias en América Latina

En América Latina

Más del 80% de las empresas en América Latina no están preparadas, para contraatacar un ataque cibernético.

En el 2021 se dan las Primeras iniciativas de Cooperación Internacional de investigación contra el Ransomware, promovido por organismos multilaterales y gobiernos.

En América Latina crece el número de ataques de Ransomware, con ataques más focalizados donde piden rescates de mayor valor, junto a una mejor planeación logrando más eficacia en el ataque. Los ciberatacantes de Ransomware han adicionado nuevos métodos en varias fases de la amenaza que van desde su creación y mutación para no ser detectados hasta los ataques de denegación de servicio (DDoS) como nueva modalidad extorsiva.

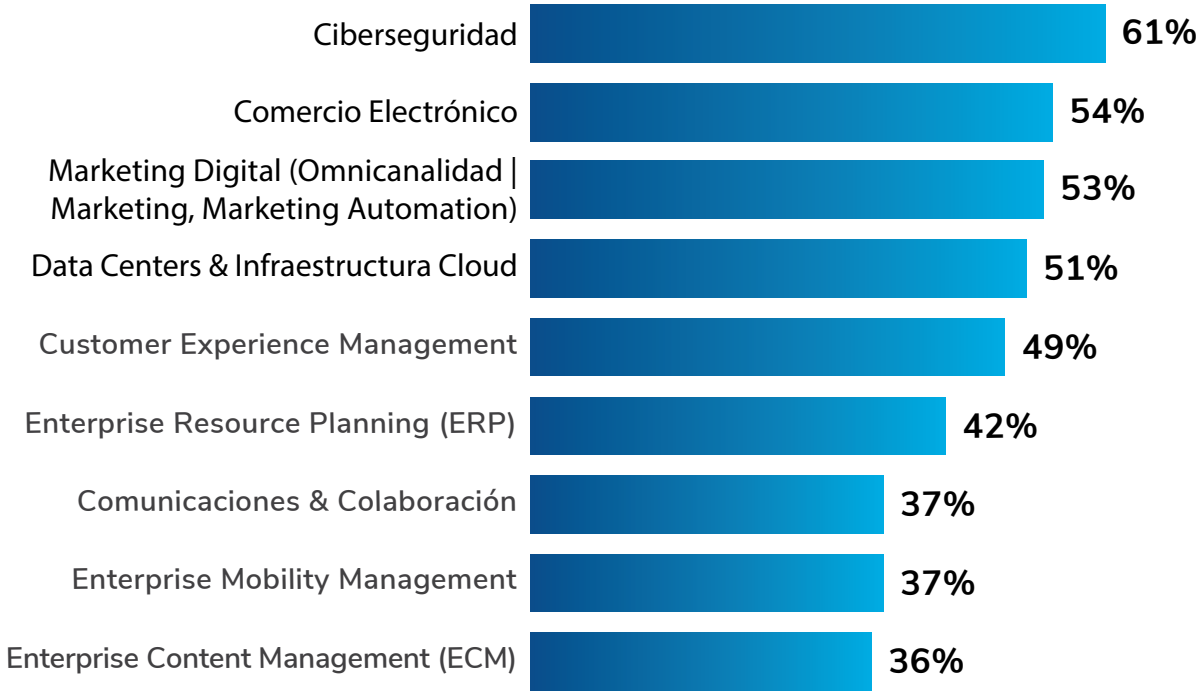
Las principales verticales foco de ataque en la región son principalmente gobierno, educación, financiero, salud, logística y servicios.

De acuerdo a un estudio realizado por Frost & Sullivan enfocado a Decisores de IT, el tema de ciberseguridad es la prioridad de inversión en los próximos 2 años, donde la tendencia es ataques más focalizados y sofisticados en América Latina.

Priorización de Futuras Inversiones en TIC - LATAM

EXHIBIT 1: Nivel de Prioridad de las Empresas en Inversiones TIC en los próximos 2 años: LATAM, 2020

Cuota Superior (Prioridad Alta)



Base: Todos los encuestados en América Latina (n=468).
P22. Durante los próximos dos años, ¿cuál es el nivel de prioridad en su organización para las inversiones en las siguientes soluciones?

Estudio: IT Decision Makers Latam 2020 – Frost & Sullivan

De acuerdo con el Informe global de Fraude e Identidad 2021, realizado por DataCrédito Experian desde junio de 2020 hasta enero de 2021 en diferentes países de América del Norte, América Latina, Europa y Asia-Pacífico, en Latinoamérica se generó un incremento en los reclamos fraudulentos, conocidos como auto-fraude o fraude amistoso, y del cibercrimen, como consecuencia del deterioro de la situación económica, donde más del 80% de las empresas no están preparadas, para contraatacar un ataque cibernético.

Entre lo que se venía incrementado y lo que se disparó en estos dos últimos años, solo el Ransomware ha crecido seis veces más de lo que venía reportando antes de la pandemia, según KPMG.

Según un reporte de la Cepal (Comisión Económica para América Latina y El Caribe), Estado de la ciberseguridad en la logística de América Latina y Caribe", se triplicaron los incidentes en las cadenas logísticas de la región, donde los países más afectados son Brasil, Chile, Argentina, México, Perú, Panamá, Uruguay, Colombia, Ecuador y República Dominicana.

La Organización de Estados Americanos (OEA) ha promovido una serie de Webinars en el 2021 sobre los desafíos y cooperación internacional ante el Ransomware, dirigido a fiscales, investigadores y servidores públicos que se encuentren a cargo de investigar, perseguir y sancionar cibercriminales en América Latina y el Caribe, donde comparten sus experiencias investigando casos de Ransomware. Recientemente, el presidente de Estados Unidos, Joe Biden, solicitó acelerar la cooperación internacional contra el Ransomware y la ciberdelincuencia y detener el uso de las criptomonedas, con la participación de 30 países, donde los países que participaron de América Latina fueron Brasil, México, Colombia y República Dominicana.

Algunos Países de la Región

En 2021, el ataque con mayor crecimiento en México fue el Ransomware y menos del 50% de las organizaciones cuentan con personal capacitado para enfrentarlo.

México

Según la revista Contacto en su artículo “En 2021 el ataque con mayor crecimiento en México fue el Ransomware” donde describe esta tendencia de la siguiente manera:

- En México, el costo promedio de remediación para las organizaciones por un ataque de Ransomware es de USD $470 mil dólares y si se paga el rescate, es de USD $940 mil dólares.
- En 2021, el ataque con mayor crecimiento en México fue el Ransomware y menos del 50% de las organizaciones cuentan con personal capacitado para enfrentarlo.
- Según la Unidad de Investigación SILIKN, el costo para eliminar un sistema de Ransomware puede superar los USD $80 mil dólares para las grandes corporaciones (Enterprise) y USD $55 mil dólares para pequeñas y medianas empresas (PyMEs). En México, el 66.9% de las PyMEs cierran sus operaciones o quiebran seis meses después de haber sufrido un ataque cibernético.
- En México, más de la mitad de las organizaciones privadas y públicas (52.8%) sufrieron un ataque de este tipo durante 2020. Se calcula que durante el 2020 se presentó un ataque de Ransomware cada 14 segundos y para el 2021, fue de cada 10 segundos.
- En México el sector Gobierno ha sido víctima de ataques principalmente entes del gobierno relacionados con la Economía, Finanzas e Impuestos del país y del sector petrolero. Estos casos se caracterizan por una mayor sofisticación y grado de eficacia de los atacantes, ya que usan inteligencia artificial donde han dirigido los ataques con una mayor probabilidad de éxito.

Brasil

Brasil es el quinto país del mundo con mayores ataques cibernéticos y con la mayor cantidad de grupos de Ransomware activos.

Brasil es el quinto país del mundo con mayores ataques cibernéticos y con la mayor cantidad de grupos de Ransomware activos. Según un estudio de un fabricante global de software el Ransomware en Brasil crece 30% y genera daños para las empresas por $ 32,4 billones de reales.

Los principales ataques de Ransomware en Brasil han sido enfocados a los sectores de gobierno, financiero, industria, energía y logística.

En Brasil son conocidos los casos de Ransomware al sector Gobierno especialmente a entes Judiciales y Ministerios donde roban datos críticos y sensibles del sector público, donde el esquema más común es que ataquen los servidores con Ransomware, el cual bloquea el acceso a todos o partes de los documentos, públicos, judiciales, contratos, información administrativa, datos de salud entre otros. Donde algunos entes estatales quedaron fuera de servicio. Los piratas informáticos exigen un pago para liberarlos. No hay información de que se haya pagado algún rescate por parte de las diferentes entidades estatales.

Colombia

Colombia ocupa el tercer lugar en cibercrimen, dentro del top 5 de fraudes, mientras que en lo referente a ataques cibernéticos el país es el sexto de América Latina con más casos detectados.

En Colombia, la Policía Nacional publicó un informe en 2020 que analizaba el crimen cibernético en el año 2019. En primer lugar, el estudio estimaba que el costo del Ransomware en Colombia era de USD 1,1 millones de dólares, correspondiente al 30% de todos los ataques de este tipo de amenaza en América del Sur. Se estima que para Perú es del 16%, México 14%, Brasil 11% y Argentina 9%.

Colombia ocupa el tercer lugar en cibercrimen, dentro del top 5 de fraudes, mientras que en lo referente a ataques cibernéticos el país es el sexto de América Latina con más casos

detectados y que ha llegado a registrar 198 millones de casos, generando pérdidas por USD 6.179 millones de dólares, según un estudio de Datacredito Experian.

En Colombia una empresa multinacional tuvo un ataque de Ransomware. La empresa opera en Latinoamérica y de los 72 servidores que le fueron secuestrados, 58 están localizados en Colombia.

El ataque fue lanzado desde México, utilizando el computador de un empleado en El Salvador, al que tuvieron acceso mediante phishing (páginas web falsas). El empleado utilizó el computador de su hijo para conectarse a tareas de oficina, en tiempos de pandemia. Los ciberdelincuentes mexicanos, autores del ataque original, vendieron el secuestro a otro grupo, que permaneció durante dos meses en la red de esta compañía realizando labores de recolección de información, mediante la aplicación de diversas herramientas para obtener datos sensibles de la compañía, donde procedieron a la extorsión.

Los atacantes exigieron cuatro millones de dólares, que debían ser pagados en criptomonedas en el plazo de una semana, o divulgarían la información empresarial sensible. Tenían datos de los clientes de esta enorme compañía que, si llegaran a divulgarse, le traerían serias consecuencias económicas, puesto que la empresa tiene sede en Europa y la conocida ley de protección de datos europea impone severas sanciones.

No fue necesario pagar el rescate, porque un grupo de expertos logró vencer a los cibercriminales. Encontraron la puerta de acceso que los atacantes estaban utilizando, la bloquearon, mejoraron la seguridad perimetral y recuperaron gran parte de la información, luego de varios días de tensión.

Chile

Cerca del 50% de las organizaciones en Chile cree que fue víctima de al menos un ciberataque durante el 2021.

Según estimaciones de la empresa de seguridad gerenciada NovaRed cerca del 50% de las organizaciones en Chile cree que fue víctima de al menos un ciberataque durante el 2021.

Los sectores con mayores ataques de Ransomware en Chile son financiero, gobierno, educación, industria, retail y salud respectivamente.

Los últimos grupos de Ransomware que han atacado a Chile son Prometheus y LockBit 2.0.

En Chile es conocido un caso de ataque de Ransomware a una importante Universidad, principalmente a la Intranet y a las aulas virtuales.

La Universidad dio una serie de recomendaciones a su comunidad para evitar ser afectados por el ataque informático. Entre éstas se incluyen los posibles archivos infectados a eliminar, como parte del proceso para identificar si el equipo está infectado con el archivo Rainmeter.ex o Rainmeter.dll y respaldar toda la información en un disco duro externo, así como no acceder a las redes de la universidad. El ataque externo fue controlado y no pagaron rescate.

En otros países de América Latina como Argentina, es conocido un ataque de Ransomware a una importante entidad del gobierno, donde los ciberdelincuentes secuestraron información y solicitaron un rescate de USD 2 millones de dólares, que posteriormente incrementaron a USD 4 millones de dólares al cumplirse el primer plazo. Al negarse a pagar, la información fue publicada en la Web Oscura (Dark Web).

Caso Global de Ataque y Mejores Prácticas de Mitigación contra el Ransomware

Caso de Éxito Global - EMPRESA SIG, Sector de la Construcción.

SIG empresa global líder en soluciones de construcción, recibió un ataque GandCrab, el cual impactó a más de 600 dispositivos. La empresa se vio obligada a cerrar parte de su operación de un país, que representa casi el 30% de los de los ingresos totales.

Afortunadamente, dos dispositivos estaban protegidos con soluciones CrowdStrike, y esto fue clave para derrotar el ataque. Se mantuvieron seguros, detectaron el ataque y se alertó de la situación. Esto permitió a la empresa tomar medidas para evitar que el Ransomware se difundiera más ampliamente.

Varios meses antes del incidente del Ransomware, el equipo de seguridad de la empresa de soluciones de construcción había comenzado una evaluación para determinar si su cultura e infraestructura de ciberseguridad existentes todavía eran apropiadas para protegerse contra la creciente amenaza de ataques, especialmente para los usuarios finales, que se consideraban objetivos principales. En esos momentos, la empresa contaba con varios productos antivirus para terminales.

La evaluación resultó en la decisión de reforzar la estrategia de ciberseguridad de la empresa, con un enfoque en la protección de endpoints. Inicialmente, el equipo de seguridad de la empresa consideró mejorar la seguridad de los endpoints utilizando su centro de operaciones de seguridad (SOC), pero descartó este esquema debido a los recursos de TI limitados y al cumplimiento de una estrategia reciente para construir sólidas alianzas con proveedores. Donde se eligió a CrowdStrike por su probada capacidad de servicio gestionado, su reputación y la calidad de respuesta durante el proceso de licitación.

El equipo de TI de la empresa de soluciones de construcción se dedicó a reconstruir los componentes clave de la infraestructura, como el Directorio Microsoft Active y dispositivos de creación de imágenes en ubicaciones de sucursales para volver a las operaciones comerciales normales.

El evento permitió demostrar al resto del negocio que la empresa ahora tenía la capacidad de detectar tal amenaza y destacó la razón por la que estaban poniendo CrowdStrike a la vanguardia del plan de respuesta a incidentes. CrowdStrike había demostrado, de manera muy real la situación y de una manera muy tangible: su capacidad para identificar con precisión los ataques y evitar que se propaguen.

Para resolver la situación, uno de los miembros del equipo de TI de la empresa sugirió probar qué tan bueno es CrowdStrike consiguiendo que resolviera el problema. En 30 minutos, CrowdStrike tenía 450 de los 600 dispositivos en funcionamiento y protegidos. Fue una hazaña increíble dado que acababa de pasar 24 horas tratando y fallando de solucionar el problema del ataque.

El ataque de Ransomware en este país reforzó el valor de CrowdStrike y muy rápidamente Falcon Complete estaba protegiendo todos los terminales de la empresa. La amenaza también llevó a la empresa a utilizar la capacidad de evaluación del compromiso de los servicios CrowdStrike para investigar el "por qué, el cómo y el impacto del ataque GandCrab y para garantizar que se pusieran en marcha medidas para evitar la repetición de cualquier amenazas similares".

Mejores Prácticas de Mitigación Contra Ransomware

Frost & Sullivan recomienda establecer una práctica de controles preventivos, de detección y de remediación contra el Ransomware, en personas, procesos y tecnología. A continuación se describen las mejores prácticas líderes del ecosistema de ciberseguridad:

Controles Preventivos	Controles De Detección	Remediación
Análisis de vulnerabilidades y gestión de parches	Detección de Endpoints	Control de acceso a la red (NAC)
Protección de Endpoints	Sistemas de Detección de Intrusión (IDS)	Forense y erradicación de malware
Desinfección de archivos	Sistemas de Engaño	Copia de seguridad y recuperación
Lista blanca de aplicaciones	Detección de Factor Humano	Descifrado
Seguridad de red - Gateways de seguridad integradas		
Correo electrónico y seguridad web - Gestión segura de contenido		
Análisis avanzado de malware basado en la red		
Segmentación de la Red		
Mitigación del Factor Humano		

Recomendaciones y Conclusiones

Algunas Recomendaciones de Frost & Sullivan

- Las empresas deben contar con un plan y una estrategia de ciberseguridad en las que se destacan políticas de configuración de acceso remoto, de contraseñas seguras, copias de seguridad y actualización de software. Lo anterior acompañado de soluciones de prevención de Ransomware con machine learning y con análisis de amenazas automatizado y predictivo.
- Realización de capacitaciones de concientización en seguridad, principalmente para que todos los empleados entiendan los riesgos de abrir enlaces, sitios web y archivos adjuntos sospechosos desde equipos corporativos, y aprendan buenas prácticas sobre el uso de contraseñas complejas y únicas.
- Implementar y hacer cumplir una política del uso de una conexión segura (usando una VPN) para acceder a cualquier recurso de la empresa de forma remota.
- Realizar copias de seguridad (Back-ups) de sus datos de manera regular, guardándolas en archivos offline (sin conexión a Internet) o en servicios basados en la nube seguros y confiables para evitar que sus datos sean vulnerados.
- Nunca hacer clic en enlaces sospechosos ni abrir archivos adjuntos de fuentes desconocidas.

Aplicar el nuevo marco de seguridad llamado Zero Trust que requiere que todos los usuarios, ya sea dentro o fuera de la red de la organización, estén autenticados, autorizados y validados continuamente para la configuración y postura de seguridad antes de que se les otorgue o conserven el acceso a las aplicaciones y los datos. Zero Trust asume que no existe un borde de red tradicional. Las redes pueden ser locales, en la nube o híbrida con recursos en cualquier lugar y trabajadores en cualquier lugar.

Evolución del Ransomware en el 2022

En el 2021, el Ransomware evolucionó al incluir el pago de extorsión basado en la recuperación de información robada. Durante 2022, este fenómeno involucrará tipos diferentes de activos, tales como Internet de las Cosas (IoT), así como la extracción de información privilegiada de personas. Es muy posible que los datos robados sean regresados a sus propietarios poco a poco en el tiempo, según sean los términos de pago acordados.

Conclusiones

El Ransomware tiene seis efectos principales en las organizaciones: Interrupción de la producción, la entrega de productos o servicios a los clientes; pérdida de datos comerciales sensibles o información protegida; costos directos de reparación, recuperación o el posible pago de un rescate; costos asociados a los litigios, a menudo demandas colectivas; sanciones legales y reglamentarias y daños a la reputación. Donde es importante que las organizaciones tengan un plan y estrategia de ciberseguridad y preparar a las organizaciones para una respuesta temprana a un incidente cibernético donde si no se puede evitar, que se pueda reaccionar rápido.

Descargo de Responsabilidad Frost & Sullivan y Sobre CrowdStrike

Descargo de Responsabilidad

Durante los últimos 60 años, Frost & Sullivan ha realizado estudios de mercado y estrategia con el fin de crear un flujo de oportunidades de crecimiento innovadoras para empresas, gobiernos e inversores, que les permiten maximizar el potencial económico, conocer las megatendencias emergentes y visualizar un futuro basado en el crecimiento sostenible.

El crecimiento es un viaje. Somos su guía.

Este es un Whitepaper de Frost & Sullivan en colaboración con CrowdStrike. Estas páginas contienen solo información general y no abordan ninguna circunstancia o requisito particular. Frost & Sullivan no ofrece garantías, representaciones o compromisos (expresos o implícitos) sobre el contenido de este documento; incluyendo, sin limitación, cualquiera en cuanto a la calidad o idoneidad para un propósito particular o cualquiera que la información proporcionada sea precisa, completa o correcta.

Este documento se basa en investigaciones secundarias y sitios web operados por terceros sobre los cuales Frost & Sullivan no tiene control.

www.frost.com

Sobre CrowdStrike

CrowdStrike Holdings, Inc. (Nasdaq: CRWD), líder global en ciberseguridad, está redefiniendo lo que es seguridad en la era de nubes con una plataforma de protección de endpoint y workload desarrollada desde cero para detener las brechas.

La arquitectura de agente exclusiva y ligera de la plataforma CrowdStrike Falcon® impulsa la inteligencia artificial (IA) hacia una escala en nube y ofrece protección y visibilidad en tiempo real a toda la empresa, evitando ataques en endpoints y workloads en la red o fuera de ella.

Alimentado por el Threat Graph® propietario de CrowdStrike, CrowdStrike Falcon captura en tiempo real aproximadamente 1 billón de señales de alta fidelidad por día en tiempo real en todo el planeta, avivando una de las plataformas de datos más avanzadas del mundo en seguridad.

Con CrowdStrike, los clientes se benefician de mejor protección, mejor rendimiento y tiempo de valor inmediato entregado por la plataforma Falcon nativa para nube.

Solo hay una cosa a recordar sobre CrowdStrike:

Nosotros detenemos brechas.

www.crowdstrike.com/latam/

latam@crowdstrike.com

FROST & SULLIVAN

Growth is a journey. We are your guide.

For over six decades, Frost & Sullivan has provided actionable insights to corporations, governments and investors, resulting in a stream of innovative growth opportunities that allow them to maximize their economic potential, navigate emerging Mega Trends and shape a future based on sustainable growth.

Contact us: Start the discussion