SOLUCIONES SEGURAS
CYBERSECURITY
MAGAZINE

Edición No. 16

REVISTA REGIONAL DE CIBERSEGURIDAD

CONFLICTO RUSIA-UCRANIA

Y SU IMPACTO EN LA CIBERSEGURIDAD MUNDIAL PÁG. 3

EN ESTA EDICIÓN:

CIBERATAQUES Y AMENAZAS EN MEDIO DE LA INVASIÓN RUSA DE UCRANIA

COMPAÑÍAS ESTÁN ABANDONANDO OPERACIONES EN RUSIA COMO MEDIDA DE PROTESTA EN CONTRA DEL CONFLICTO

Y MÁS...

2022
VOLUMEN 1

SOLUCIONES SEGURAS
TRAINING CENTER
SOLUCIONES SEGURAS CYBERSECURITY REGIONAL TOUR
SOLUCIONES SEGURAS CYBERSECURITY MAGAZINE

SOLUCIONES SEGURAS CYBERSECURITY MAGAZINE

CONTENIDO

Randol Chen
Soluciones Seguras
Editor de la Revista SS CSM

SOLUCIONES SEGURAS
Empresas Protegidas, Empresas Tranquilas

PALABRAS DE EDICIÓN

Si hay algo que los últimos años nos han enseñado, es que es imposible predecir el futuro y que el mundo está en constante cambio. Después de los dos años más inesperados y donde la forma de relacionarse y trabajar cambió, llega una guerra que todavía no sabemos qué efectos traerá.

Pero sabemos que, en la Era de la Información, los datos, los sistemas y las redes, son más importantes que nunca, y que los ataques no paran. El trabajo de ciberseguridad es así, constante, cambiante, importante.

A veces oímos solamente de los ataques y los problemas. Pero por cada ataque exitoso, hay cientos de defensas que pararon otros ataques. En este mundo, que no existan noticias, son buenas noticias (no news is good news).

Por eso tomo este tiempo para agradecer a los diferentes equipos de tecnología y ciberseguridad que tienen el reto de mantener seguros sus sistemas, un trabajo difícil y muchas veces sin el agradecimiento que se debería. Y por supuesto, reconocer al excelente equipo de ingenieros en Soluciones Seguras, siempre dispuestos a ayudar.

Hasta nuestra próxima edición... veamos qué cosa nueva nos trae el mundo entonces...

Gracias!

Eli Faskha

CEO

CONFLICTO RUSIA-UCRANIA
Y SU IMPACTO EN LA CIBERSEGURIDAD MUNDIAL

Mientras el conflicto Rusia-Ucrania continúa, se siente el impacto global y regional a nivel de ciberseguridad. Y es que los ciberdelincuentes estarán siempre al tanto de las noticias que estén haciendo tendencias para moverse en ese entorno. En este artículo analizaremos los diversos impactos que ha tenido el conflicto en la ciberseguridad a nivel mundial. Iniciaremos con el hacktivismo que es el que más ruido está causando, pero no necesariamente el más peligroso, y es que los ataques silenciosos y dirigidos también están al acecho. Esto sumado a la larga lista de las compañías que están dejando sus operaciones en de forma temporal, parcial o general en Rusia, lo que está llevando a temas más peligrosos como el estudio de legalizar la piratería en terreno ruso.

HACKTIVISMO, RECLAMACIONES CUESTIONABLES Y GUERRA DE CRÉDITOS

Según el Research Team de Check Point, los hacktivistas que apoyan a Rusia o Ucrania por razones ideológicas aplican como uno de los jugadores más activos en el ciberespacio durante la guerra en Ucrania. Actualmente cuentan como el grupo de mayor ruido, pero no necesariamente el de mayor daño. Mientras que, en el pasado, los éxitos de los hacktivistas se concentraron principalmente en áreas de ejecución de ataques DDoS y piratería o desfiguración de pequeños sitios web de organizaciones no importantes, durante la última semana varios grupos de hacktivistas afirmaron haber tenido éxito en apuntar a organizaciones de alto perfil. Los hacktivistas reclamaron dos tipos de ataques:

- Ataques DDoS
- Hackear redes de organizaciones sensibles o de alto perfil con el objetivo de filtrar los datos y/o interrumpir las operaciones

Si bien la mayoría de las afirmaciones sobre los ataques DDoS parecen ser relativamente confiables y fue posible confirmar que algunos de los sitios web que se afirmaron que habían sido atacados en realidad no estaban disponibles, la situación es más complicada con respecto a las entidades que supuestamente fueron violadas. Si bien no es fácil confirmar las afirmaciones de esos grupos, la investigación de Check Point revela que muchas de las afirmaciones son falsas, y que las capturas de pantalla y los datos de las redes presuntamente violadas son antiguos, se publicaron anteriormente en el pasado o simplemente son insignificantes. en muchos casos.

Esta tendencia es relevante para ambos lados, mientras se pudo ver que algunas afirmaciones del grupo KillNet en el lado pro-ruso son cuestionables, así como las afirmaciones de los grupos AgainstTheWest y KelvinSecurity en el lado pro-ucraniano. Para conocer más detalles siga este enlace.

ACTIVIDAD PELIGROSA EN LA RED

Mientas los hacktivistas buscan hacer ruido a nivel global para manipular la opinión pública, existen otros tipos de atacantes a nivel mundial que aprovechar la situación para cometer los típicos crímenes cibernéticos cómo:

- Exfiltración y robo de datos
- Robo de cuentas bancarias
- Infección de equipos para ampliación de botnets
- Robo de Cuentas (Account Takeovers
- Chantajes/rescates (Ransomware)

Estos ataques son realizados generalmente a través de campañas de correo electrónico o portales de noticias donde se alega entregar contenido urgente o importante relevante al conflicto en Ucrania. Incluso se han visto campañas por Whatsapp donde se alega distribuir videos de último momento que son enlaces a sitios maliciosos donde se realiza la entrega del malware que causará el daño en su equipo. Debe ser cauteloso con el contenido que recibe, sobre todo a través de redes sociales o chats.

COMPAÑÍAS DEJANDO RUSIA HA POTENCIADO A UN ENEMIGO PELIGROSO

De forma paralela a los ciberataques, numerosas compañías de alto prestigio han empezado/realizado su retirada de operaciones de Rusia. Y es que, además de la necesidad de cumplir con las sanciones occidentales contra Rusia, las empresas son cada vez más conscientes de los riesgos potenciales para su reputación al continuar con sus negocios habituales en el país, mientras que algunas han citado sus propios estándares de responsabilidad corporativa para retirarse. También están expresando su preocupación por la difícil situación de los ucranianos a medida que la guerra cobra un número cada vez mayor de civiles, con más de 2 millones de personas que han huido de Ucrania desde la invasión rusa del país, según las Naciones Unidas. Para ver un listado detallado de las principales compañías que han dejado Rusia, le invitamos a leer el artículo: “COMPAÑÍAS QUE HAN DEJADO RUSIA DEBIDO AL CONFLICTO”, en esta edición.

Y la preocupación a nivel mundial en temas de ciberseguridad ha surgido debido a que Rusia ha respondido a estas sanciones con el deseo de suavizar las leyes de derechos de autor, lo que conlleva específicamente a la legalización del uso de contenido protegido por derechos de autor, como video juegos, películas, programas de televisión, entre otros. Y ha avanzado más rápido de lo esperado, porque según los medios locales en Rusia (City A.M.), el gobierno ruso ahora ha anunciado que las empresas rusas no tienen la obligación de pagar a los titulares de patentes por el uso de la propiedad intelectual, de cualquier país que haya sancionado al país. Esto ha legalizado efectivamente la piratería en todo el país.

La preocupación en temas de ciberseguridad radica en que todo el software o contenido pirateado, ha sido manipulado o alterado por fuentes desconocidas que han roto los medios de autenticación y seguridad que se le han aplicado. Por lo que no hay garantía de que no vengan con piezas de software maliciosos incrustados.

La legalización de la piratería en este país conlleva a un drástico aumento en la movilización de contenido alterado que será potencialmente peligroso si llega a equipos que pertenecen a una compañía. Incluso el mismo usuario puede perder acceso a sus cuentas personales, incluyendo las bancarias.

CIBERATAQUES, FRAUDES Y NOTICIAS FALSAS: LOS CIBERDELINCUENTES Y HACKTIVISTAS APROVECHAN TELEGRAM PARA ACTIVIDADES RELACIONADAS CON EL CONFLICTO

CHECK POINT Recurso: Check Point Blog, Marzo, 2022
https://blog.checkpoint.com/2022/03/02/telegram-becomes-a-digital-forefront-in-the-conflict/

Destacados

- En medio del conflicto entre Rusia y Ucrania, el volumen de usuarios se multiplicó por cien diariamente en los grupos relacionados con Telegram, alcanzando un máximo de 200 000 por grupo.
- Los grupos de ataques cibernéticos anti-rusos que se crearon recientemente están creciendo de manera constante todos los días, llegando a más de 250 000 usuarios por grupo.
- Se sospecha que algunos grupos disfrazados de recaudación de fondos para Ucrania son fraudulentos
- Los grupos independientes de fuentes de noticias pasan por alto a los agentes de noticias y "transmiten" firmemente "hechos" sin editar.

Background

El conflicto entre Rusia y Ucrania está cerrando su primera semana, y recientemente surgieron números crecientes de ciberataques relacionados. Recientemente, Check Point Research (CPR) publicó datos sobre ciberataques contra el gobierno y el sector militar de Ucrania, que aumentaron en un asombroso 196 % en los primeros tres días de combate. Los ataques cibernéticos a organizaciones rusas aumentaron en un cuatro por ciento. CPR también advirtió sobre el envío de correos electrónicos fraudulentos para engañar a las personas que buscan donar a Ucrania desde el extranjero.

Desde el estallido del conflicto el 24 de febrero, los investigadores de CPR han estado monitoreando de cerca la creciente actividad que se gestiona en Telegram. CPR vio alrededor de 6 veces más grupos relacionados con el conflicto que el día anterior a la invasión. En este informe, brindamos cierta visibilidad a lo que parece ser un frente de guerra propio.

Los hacktivistas cibernéticos están eligiendo Telegram para transferir mensajes, armas cibernéticas y herramientas, y están "apuntando" a los atacantes a objetivos rusos relevantes. Desde el comienzo de la guerra, hemos visto la creación de decenas de grupos diariamente. Algunos grupos cuentan con más de 250.000 usuarios. CPR estima que alrededor del 23% de los grupos observados en Telegram intentan unir a piratas informáticos, profesionales de TI y otros "fanáticos" de TI para atacar objetivos rusos en el ciberespacio. Estos grupos se utilizan para coordinar el ataque, decidir objetivos y compartir resultados, incluso ofreciéndose a ayudarse unos a otros hacia la meta. Los ataques DDoS se volvieron muy comunes como arma cibernética, con atacantes antirrusos que apuntan a los objetivos que prefieren y solicitan a los usuarios del grupo que los sigan.

Por ejemplo, el grupo Anna está llamando a sus seguidores a atacar objetivos

rusos a través de DDoS., SMS o ataques basados en llamadas.

SIGA ESTE ENLACE PARA VER EL INFORME COMPLETO

Cómo mantenerse protegido contra el fraude y el ciberdelito mientras usa Telegram

Como cualquier software de comunicación en línea, los usuarios deben permanecer atentos y cuidadosos con la información publicada en Telegram. Para mantenerse protegido, Check Point recomienda lo siguiente:

- No presione enlaces que tengan orígenes desconocidos para usted, especialmente en tiempos de crisis y circunstancias extremas. Los delincuentes pueden aprovechar y explotar la situación para intentar robar credenciales, detalles privados y otra información personal mediante el envío de malware o enlaces de phishing.
- Cuidado con las solicitudes sospechosas. Si un mensaje de una fuente desconocida hace una solicitud que parece inusual o sospechosa, esto podría ser evidencia de que es parte de un ataque de phishing.
- Enviar dinero a fuentes desconocidas que solicitan asistencia a menudo puede resultar en fraude. Tenga cuidado con quién se está comunicando y qué tipo de información se le pide que proporcione. Para donaciones financieras siempre vaya a los sitios oficiales de organizaciones reconocidas
- Consuma fuentes de noticias y busque la "verdad" de fuentes confiables en las que pueda confiar.

CPR continúa monitoreando la evolución de la situación en el conflicto, e informaremos en consecuencia.

CIBERATAQUES Y AMENAZAS EN MEDIO DE LA INVASIÓN RUSA DE UCRANIA

radware Recurso: Radware Blog, Febrero, 2022
https://www.radware.com/security/threat-advisories-and-attack-reports/cyberattacks-and-threats-amidst-russian-invasion-in-ukraine/

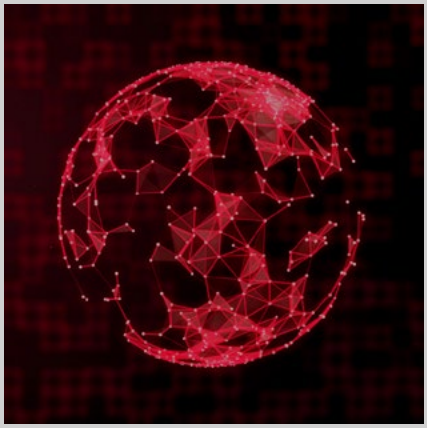
En su aviso especial, Radware comparte información basada en información pública sobre amenazas y ataques en torno a la acción militar especial del Kremlin contra Ucrania.

Actualmente, los ataques se limitaron a objetivos directamente relacionados con el conflicto y nuestros servicios de seguridad en la nube no tienen indicadores significativos de un cambio en los patrones de ataque que puedan atribuirse a este evento. La amenaza más importante para las organizaciones es convertirse en colateral en una guerra de poder librada por activistas patrióticos.

Las amenazas y los ataques potenciales que podrían seguir a medida que los conflictos se intensifican entre naciones o entre comunidades en línea no son diferentes de las amenazas que las organizaciones han enfrentado por parte de los hacktivistas y los operadores de ransomware en los últimos meses. Las organizaciones de todo el mundo deben seguir reforzando su resiliencia en materia de seguridad cibernética, ahora más que nunca.

Puntos destacados del informe:

- Las tropas rusas invadieron Ucrania el 24 de febrero, en un intento de derrocar al gobierno ucraniano, después de que Estados Unidos y la OTAN rechazaran la demanda de Rusia de excluir a Ucrania de la OTAN.
- La OTAN apoya plenamente la soberanía, la integridad territorial y el derecho de Ucrania a la autodefensa de Ucrania y condenó la invasión.
- Los miembros de la alianza de la OTAN no pueden y no irán a la guerra con Rusia a menos que uno de sus miembros sea atacado, esto se aplica tanto a los conflictos en línea como fuera de línea.
- Justo antes de que comenzara la invasión, los objetivos de Ucrania fueron atacados por un malware de limpieza.
- Los ataques DDoS en Ucrania fueron informados y atribuidos a Rusia por el gobierno de EE. UU. y el NCSC (Reino Unido)
- Anonymous declaró la guerra a Rusia y se atribuyó la responsabilidad de los ataques DDoS contra objetivos financieros y gubernamentales rusos.
- Los operadores de ransomware Conti y CoomingProject publicaron mensajes anunciando su apoyo del gobierno ruso
- Lockbit publicó una "Declaración oficial sobre la amenaza cibernética a Rusia" diciendo que no participa en conflictos internacionales y que "solo está interesado en el dinero por su trabajo inofensivo y útil".
- Un canal de Telegram está reagrupando a más de 180 000 miembros pro-ucranianos que están dispuestos a difundir contenido y atacar a quienes atacan a Ucrania, con el apoyo del Viceprimer Ministro de Ucrania.
- Geobloqueo supuestamente desplegado por Rusia en un intento de mitigar posibles ataques
- Asesoramiento para organizaciones de todo el mundo



En este aviso especial, Radware comparte una colección de información pública sobre amenazas y ataques en torno a la acción militar especial del Kremlin contra Ucrania. La información se basa en desarrollos recientes en línea, influenciados por y en apoyo del conflicto fuera de línea.

LEA LA ALERTA COMPLETA

SOLUCIONES SEGURAS EN LAS NOTICIAS

TELETICA: CONSEJOS PARA EVITAR SER VÍCTIMA DE LA CIBERDELINCUENCIA

TELETICA.com

TVN NOTICIAS: BRINDAN RECOMENDACIONES PARA EVITAR CIBERDELITOS Y LA PROTECCIÓN DE DATOS PERSONALES

tvn Noticias

LA PRENSA MARTES FINANCIERO: ¿CUÁLES SON LOS RIESGOS EN LÍNEA PARA NIÑOS Y ADOLESCENTES Y CÓMO PROTEGERLOS?

MARTES FINANCIERO
LA REVISTA FINANCIERA DE PANAMÁ

ESTRATEGIA Y NEGOCIOS: CRÍMENES CIBERNÉTICOS AUMENTARON EN LAS CADENAS DE SUMINISTRO

E&N

NEWS IN AMERICA: HACKERS UTILIZAN CONFLICTO RUSIA-UCRANIA PARA EL AUMENTO DE CIBERATAQUES

newsinamerica.com
PERIODICO DIGITAL
Centroamericano y del Caribe

EL CAPITAL FINANCIERO: HACKERS UTILIZAN CONFLICTO RUSIA-UCRANIA PARA EL AUMENTO DE CIBERATAQUES

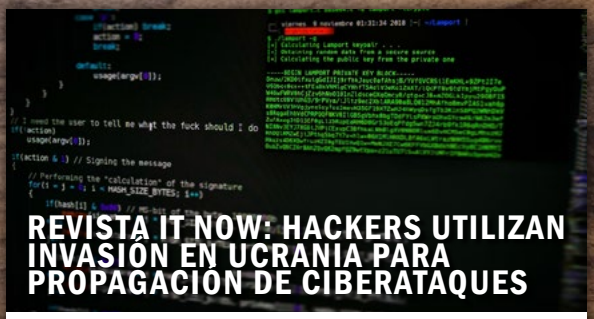
ElCapital
FINANCIERO.COM

SOLUCIONES SEGURAS

Empresas Protegidas, Empresas Tranquilas

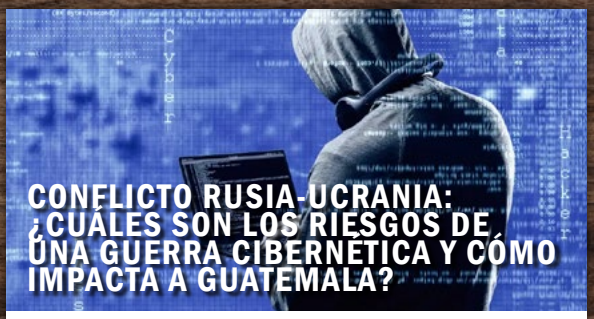
TELEMETRO: CIBERDELINCUENTES APROVECHAN GUERRA PARA SOLICITAR DONACIONES FALSAS

telemetro.com



REVISTA IT NOW: HACKERS UTILIZAN INVASIÓN EN UCRANIA PARA PROPAGACIÓN DE CIBERATAQUES

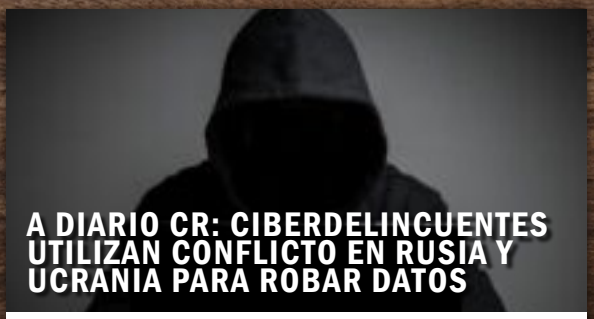
IT NOW



CONFLICTO RUSIA-UCRANIA: ¿CUÁLES SON LOS RIESGOS DE UNA GUERRA CIBERNÉTICA Y CÓMO IMPACTA A GUATEMALA?

PRENSA LIBRE

Periódico líder de Guatemala



A DIARIO CR: CIBERDELINCUENTES UTILIZAN CONFLICTO EN RUSIA Y UCRANIA PARA ROBAR DATOS

aDiarioCR.com

TELEDIARIO: DÍA DE LA PROTECCIÓN DE DATOS PERSONALES

Telediario

EPP NEWS: ELI FASKHA TOMA POSESIÓN COMO PRESIDENTE DE LA CCIAPI

EEP NEWS

COMPAÑÍAS ESTÁN ABANDONANDO OPERACIONES EN RUSIA COMO MEDIDA DE PROTESTA EN CONTRA DEL CONFLICTO

Bajo la presión de inversores y consumidores, muchas empresas occidentales han comenzado a deshacer sus inversiones, cerrar tiendas y pausar las ventas en Rusia.

Los envíos de automóviles se detuvieron. La cerveza dejó de fluir. McDonald's cerró las ventas de Big Macs. Los buques de carga abandonaron las escalas en los puertos y compañías petroleras están cortando sus oleoductos.

La invasión rusa de Ucrania está provocando que algunas de las marcas más conocidas del mundo, desde Apple hasta Disney e Ikea, abandonen abruptamente un país que se ha convertido en un paria mundial.

A continuación, compartimos un listado de las empresas que han detenido sus operaciones de forma temporal, parcial o indefinida en territorio ruso:

COMBUSTIBLES FÓSILES

- **BP**. Empresa de energía, que se autodenomina el mayor inversor extranjero de Rusia, dijo el 27 de febrero que abandonaría su participación de casi el 20% en la empresa estatal rusa de petróleo y gas Rosneft. La medida podría costarle entre 14,000 y 25,000 millones de dólares, según Reuters.
- **Equinor**. Compañía de energía más grande de Noruega anunció el 28 de febrero que comenzaría a retirarse de sus empresas conjuntas en Rusia, valoradas en alrededor de $1,200 millones. "Todos estamos profundamente preocupados por la invasión de Ucrania, que representa un revés terrible para el mundo", dijo en un comunicado Anders Opedal, presidente y director ejecutivo de Equinor.
- **ExxonMobil** dijo el 2 de marzo que se retiraría de un proyecto clave de petróleo y gas, Sakhalin-1, y detendría cualquier nueva inversión en Rusia. La firma no proporcionó un cronograma para su retiro del proyecto, que opera en nombre de un consorcio internacional.
- **Shell** dijo el 28 de febrero que dejaba su empresa conjunta con la empresa estatal Gazprom y ponía fin a su participación en el gasoducto Nord Stream 2, ahora suspendido, construido para transportar gas natural a Europa Occidental. La medida podría costarle a la empresa aproximadamente 3,000 millones de dólares en activos. El martes, el gigante energético dijo que dejaría de comprar petróleo y gas natural rusos y cerraría sus estaciones de servicio y otras operaciones en Rusia.

AUTOMÓVIL Y AVIONES

- **Airbus y Boeing**. Los fabricantes de aviones Boeing y Airbus dejaron de suministrar repuestos y servicios a las aerolíneas rusas. Boeing suspendió operaciones importantes en Moscú y cerró temporalmente su oficina en Kiev. Además, Boeing dijo que había suspendido la compra de titanio de Rusia.

- **Caterpillar**. El fabricante de equipos pesados dijo el 9 de marzo que detendría la fabricación rusa, citando interrupciones en el suministro y la guerra en curso.
- **Ferrari**. El fabricante de automóviles de lujo dijo el 8 de marzo que suspendería la producción de vehículos para el mercado ruso hasta nuevo aviso. "Ferrari está junto a todos los afectados en Ucrania por esta crisis humanitaria en curso", declaró el director ejecutivo Benedetto Vigna.
- **Ford Motor Company**. Ford también suspendió sus operaciones en Rusia y dijo que donaría dinero para los refugiados ucranianos. "Dada la situación, hoy informamos a nuestros socios de JV que suspenderemos nuestras operaciones en Rusia, con efecto inmediato, hasta nuevo aviso", dijo Ford el 1 de marzo.
- **Harley-Davidson** detuvo los envíos de motocicletas a Rusia y dijo que sus pensamientos "continúan por la seguridad del pueblo de Ucrania".
- **Mercedes-Benz** suspendió las exportaciones de automóviles y furgonetas a Rusia y cesó su fabricación allí a última hora del 2 de marzo.
- **Renault**, uno de los principales actores en el mercado automotriz de Rusia, detuvo temporalmente las operaciones en su planta de Moscú a principios de marzo.
- **Toyota** detuvo la producción en su planta de San Petersburgo que fabrica los modelos RAV4 y Camry a partir del 4 de marzo.
- **El Grupo Volkswagen**, cuyas marcas de automóviles incluyen Audi, Ducati, Skoda y Porsche, dijo el 3 de marzo que detendría la producción en dos fábricas en Rusia y detendría las exportaciones al país de inmediato. Los trabajadores rusos afectados recibirían vacaciones pagadas de la empresa, dijo VW.
- **Volvo Cars** de Suecia dijo que detuvo las entregas debido a los "riesgos potenciales asociados con el comercio de material con Rusia", incluidas las sanciones occidentales.

BIENES DE CONSUMO

- **Adidas**. El fabricante alemán de ropa deportiva suspendió las operaciones en las tiendas y en línea en Rusia, diciendo que apoya a quienes piden la paz. La medida sigue a la interrupción de las operaciones rusas por parte de sus rivales Nike y Puma.
- **Airbnb**. dijo el 3 de marzo pasado que había detenido todas las operaciones en Rusia y su aliado cercano Bielorrusia.
- **Walt Disney** dijo el 10 de marzo que detendría todos los negocios en Rusia, incluidas las licencias de contenido y productos, los cruceros de Disney y los recorridos de National Geographic.
- **H&M** dijo el 2 de marzo que "detendría temporalmente todas las ventas en Rusia". Todas sus tiendas en Ucrania han sido cerradas por razones de seguridad, dijo H&M.
- **Ikea**. La compañía sueca de muebles dijo que cerraría todas sus tiendas rusas y pausaría el abastecimiento de Rusia y Bielorrusia, un aliado de Rusia.
- **Sony** ha "suspendido todos los envíos de software y hardware, el lanzamiento de Gran Turismo 7 y las operaciones de PlayStation Store en Rusia", según un comunicado tuiteado por un reportero de CNBC.

ALIMENTOS Y BEBIDAS

- **McDonald's** dijo el 8 de marzo que cerraría temporalmente sus 850 restaurantes en Rusia.
- **Coca-Cola**, PepsiCo y Starbucks se hicieron eco de McDonald's en cuestión de horas, todas suspendiendo las ventas en Rusia. Pepsi, sin embargo, dijo que continuaría vendiendo productos lácteos, fórmula infantil y otros productos esenciales.
- **Nestle**. El grupo de alimentos envasados más grande del mundo dijo el 9 de marzo que había suspendido todas las inversiones de capital en Rusia.

TECNOLOGÍA

- **Alphabet**. Google ha bloqueado los canales de medios estatales rusos de sus plataformas, incluidos YouTube y la tienda Google Play, así como pausado los anuncios de YouTube en Rusia. También suspendió Google Pay para los clientes de los bancos rusos afectados por las sanciones, lo que significa que los clientes de esos bancos no podrán utilizar el sistema de pago móvil.
- **Apple** dijo que dejaría de vender su iPhone y otros dispositivos populares dentro de Rusia. Apple no tiene tiendas en el país, pero si vendidos a través de muchos minoristas externos.
- **Dell Technologies** ha "suspendido" las ventas tanto en Ucrania como en Rusia.
- **Meta**. La compañía anteriormente conocida como Facebook bloqueó el acceso a los puntos de venta controlados por el estado ruso en toda la Unión Europea después de que "recibiera solicitudes de varios gobiernos y de la UE", dijo el jefe de políticas de la compañía, Nick Clegg, el 28 de febrero.
- **Netflix** dijo el 6 de marzo que "dadas las circunstancias sobre el terreno, hemos decidido suspender nuestro servicio en Rusia".
- **Spotify**. Anunció que cerraría su oficina en Rusia "indefinidamente", pero continuaría ofreciendo su servicio de música y podcasts en el país, aunque sin contenido de los medios afiliados al estado ruso.
- **TikTok** ha bloqueado los canales de medios estatales rusos de la plataforma, incluidos RT y Sputnik.

¿CUÁLES SON LOS PRINCIPALES DESAFÍOS DE CIBERSEGURIDAD EN EL SECTOR FINANCIERO PANAMEÑO?

Ante la acelerada trasformación digital impulsada por la pandemia, el sector financiero se ha convertido en uno de los principales objetivos de los ciberdelincuentes. A nivel mundial, los bancos fueron atacados en promedio 700 veces por semana durante el año pasado, un aumento del 53% respecto al 2020.

Desde estafas de phishing y ataques de denegación de servicio, hasta ataques sofisticados por parte de actores de estados-nación, las amenazas cibernéticas dirigidas a los bancos están en constante aumento.

Panamá no escapa de esa situación. De acuerdo al último reporte de inteligencia de amenazas de Check Point, partner de Soluciones Seguras, el sector banca y finanzas del país se ha convertido en el blanco perfecto de los hackers y es el sector que más ciberataques recibe. Es así que una organización del sector es atacada en promedio 1415 veces por semana en los últimos 6 meses.

Los principales países de origen de estas amenazas son: Panamá (43%), Estados Unidos (28%), Ecuador (24%), Rusia (1%) y otros no identificados (4%).
A medida que el panorama de las amenazas cibernéticas continúa evolucionando, las organizaciones del sector financiero deben comprender cuales son los riesgos cibernéticos a los que se enfrentan al ser una de las industrias con mayores índices de digitalización.

En esa línea, Soluciones Seguras, compañía líder en ciberseguridad en Centroamérica, participó activamente en el **II Congreso Internacional de Ciberseguridad y Prevención de Fraudes**, evento organizado por la Asociación Bancaria de Panamá.

El encuentro congregó a representantes de la banca local, con el propósito

de actualizarlos sobre las principales tendencias tecnológicas, y compartir las mejores prácticas de prevención y soluciones para mitigar los riesgos.

Las ponencias estuvieron a cargo de expertos nacionales e internacionales del más alto nivel, entre ellos Eli Faskha, CEO de Soluciones Seguras y experto en ciberseguridad, quien impartió la conferencia: "**Consideraciones de Ciberseguridad más importantes para el 2022**".

"Es para nosotros muy importante de participar en eventos como este, donde se comparte el conocimiento adquirido y se pueden unir los esfuerzos para mejorar la seguridad de uno de los sectores más importantes de la economía panameña. La gran participación de los asistentes y los temas que se presentaron muestra que la industria esta anuente a los retos y con planes de mejoramiento continuo", expresó Eli Faskha.

En el área de exhibición, expertos de Soluciones Seguras recibieron a los participantes del encuentro quienes pudieron conocer las soluciones y servicios de ciberseguridad que permiten superar los desafíos más difíciles de la actualidad con el más alto nivel de seguridad para su red, nube, usuarios y acceso.

Los participantes pudieron interactuar, resolver dudas y obtener más información específica para sus necesidades puntuales.

Acerca de Soluciones Seguras. Con 20 años de experiencia en la gestión de seguridad de redes, aplicaciones y telecomunicaciones, Soluciones Seguras es la compañía líder en ciberseguridad en Centroamérica. Con un equipo de profesionales del más alto nivel, certificados por los fabricantes más reconocidos de la industria de seguridad, es el Centro Regional de Entrenamiento Autorizado Check Point número uno en la región. Cuenta con operaciones en Panamá, Costa Rica, Guatemala y El Salvador, y clientes en otros países de Latinoamérica.

INFORME DE SEGURIDAD DE 2022 DE CHECK POINT: SE REVELA LA MAGNITUD DE LA CIBERPANDEMIA MUNDIAL

El Informe de seguridad cibernética de 2022 descubre las tendencias clave de seguridad cibernética de 2021, incluido un "frenesí" de ataques a la cadena de suministro y una mayor interrupción de la vida cotidiana. La Educación y la Investigación se revelaron como el sector más objetivo.

Desde el ataque 'SolarWinds' a principios de año, que presentó un nivel completamente nuevo de sofisticación y propagación, hasta diciembre y la afluencia de explotaciones de vulnerabilidad 'Apache Log4j', el Informe de seguridad cibernética 2022 revela el ataque clave vectores y técnicas presenciadas por Check Point Research (CPR) durante 2021.

Los aspectos más destacados del informe de seguridad cibernética de Check Point 2022 incluyen:

- Los ciberataques contra redes corporativas aumentaron un 50% en 2021 respecto a 2020
- Educación e investigación fue el sector más atacado, con organizaciones que enfrentaron un promedio de 1,605 ataques semanales.
- Los proveedores de software experimentaron el mayor crecimiento año tras año, con un aumento del 146%

El Informe de seguridad cibernética de 2022 brinda una descripción detallada del panorama de amenazas cibernéticas y recomendaciones sobre cómo prevenir la próxima pandemia cibernética. Estos hallazgos se basan en datos extraídos de ThreatCloud Intelligence de Check Point Software entre enero y diciembre de 2021, y destacan las tácticas clave que utilizan los ciberdelincuentes para atacar a las empresas.

FILTRACIONES DE CONTI RANSOMWARE GROUP PINTAN LA IMAGEN DE UNA EMPRESA EMERGENTE TECNOLÓGICA SORPRENDENTEMENTE NORMAL... MÁS O MENOS

Recurso: Check Point Research Team, Marzo, 2022
https://research.checkpoint.com/2022/leaks-of-conti-ransomware-group-paint-picture-of-a-surprisingly-normal-tech-start-up-sort-of/

Probablemente haya oído hablar del grupo de ransomware Conti. Después de su surgimiento en 2020, acumularon al menos 700 víctimas, donde por "víctimas" nos referimos a corporaciones de "peces gordos" con millones de dólares en ingresos; a diferencia de la operación de ransomware promedio de su vecindario, a Conti nunca le importó extorsionar a su suegra por las fotos de sus vacaciones. Durante un tiempo, Conti fue el rostro del ransomware, junto con su compañero de pandilla REvil, hasta este febrero, cuando las autoridades rusas arrestaron a 14 agentes de REvil, lo que dejó a Conti efectivamente solo en su posición como una operación de ransomware de la liga principal. En ese momento, esto fue aclamado con cautela como una señal de buena voluntad por parte de Rusia; algunos pensaron que posiblemente los rusos finalmente se negarían a tolerar los ataques incesantes e irreverentes que se originaban en suelo ruso y tenían como objetivo las oficinas corporativas occidentales. escuelas y hospitales. Ahora, un mes después y dos semanas después de la guerra en toda regla entre Rusia y Ucrania, esta visión utópica no parece tan probable.

El 25 de febrero de 2022, Conti emitió una declaración de pleno apoyo al gobierno ruso, junto con una severa advertencia dirigida a cualquiera que pudiera considerar tomar represalias contra Rusia a través de la guerra digital.

"WARNING"

The Conti Team is officially announcing a full support of Russian government. If any body will decide to organize a cyberattack or any war activities against Russia, we a re going to use our all possible resources to strike back at the critical infrastructures of an enemy.

2/25/2022 55 0 [0.00 B]

Unas horas más tarde, alguien en lo más alto de la cadena de Conti debe haberse dado cuenta de que esta declaración podría ser contraproducente y se modificó para quedar de la siguiente manera:

"WARNING"

As a response to Western warmongering and American threats to use cyber warfare against the citizens of Russian Federation, the Conti Team is officially announcing th at we will use our full capacity to deliver retaliatory measures in case the Western w armongers attempt to target critical infrastructure in Russia or any Russian-speaking region of the world. We do not ally with any government and we condemn the ongoi ng war. However, since the West is known to wage its wars primarily by targeting civ ilians, we will use our resources in order to strike back if the well being and safety of peaceful citizens will be at stake due to American cyber aggression.

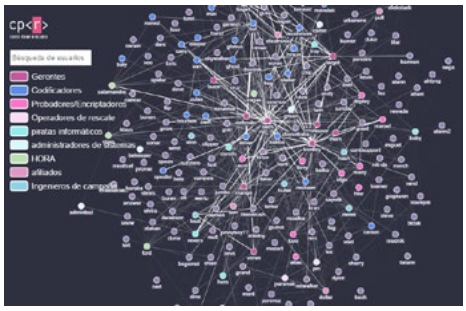
2/25/2022 410 0 [0.00 B]

Según la famosa cita de la Dra. Maya Angelou, "Cuando alguien te muestre quiénes son, créele la primera vez". Mucha gente estaba enfadada y no le importaba la aclaración. Para consternación de Conti, una de estas personas tenía los medios para actuar de manera significativa sobre su ira.

Apartir del 27 de febrero, apareció una nueva cuenta de Twitter con el nombre de "ContiLeaks", y comenzó a hacerle a Conti lo que solían hacer a las corporaciones que no pagan. Presuntamente un investigador de seguridad ucraniano, ContiLeaks publicó un enorme registro que contenía cientos de miles de mensajes de Jabber y Rocket. Chat que Conti había utilizado para la comunicación interna. Esto condujo a una verdadera fiebre del oro de investigadores que se sumergieron en la enorme pila de mensajes y compartieron sus resúmenes, hallazgos y observaciones; seríamos negligentes si no mencionáramos la serie en profundidadde publicaciones de blog publicadas por Brian Krebs, quien leyó la filtración completa y la destiló en una lista de conclusiones, un sacrificio que no debe darse por sentado.

Decimos eso porque el conjunto de datos en cuestión es simplemente enloquecedor de leer. En primer lugar, como se señaló anteriormente, es enorme. Una vez que superas eso, hay muchos otros problemas. Faltan algunos de los mensajes. Algunos de los mensajes no son claros. Algunos de los mensajes fueron encriptados con OTR (Mensajería Off-the-Record). Algunos de los mensajes contienen jerga rusa que no sobrevive a la traducción automática.

Aún así, con todo lo dicho anteriormente, estos mensajes ofrecen una visión sin precedentes de las operaciones de Conti Corporation. Y es una corporación, para todos los efectos; hay un departamento de recursos humanos, un proceso de contratación, oficinas fuera de línea, salarios y pagos de bonos. Si no fuera por la inminente amenaza de prisión, podrías confundir a Conti con una startup tecnológica normal.



Vea el informe completo aquí donde se profundiza en el funcionamiento interno del grupo Conti, sorprendentemente parecido a una startup.

HACKERS UTILIZAN CONFLICTO RUSIA-UCRANIA PARA EL AUMENTO DE CIBERATAQUES

Al igual que en Europa del Este, se está llevando a cabo una batalla de desinformación y un aumento en los ataques cibernéticos por parte de grupos llamados "hacktivistas" para aprovechar a realizar robo de datos o campañas de malware.

Los ciberdelincuentes, además de realizar ataques a las redes de organizaciones sensibles o de alto perfil con el objetivo de filtrar los datos y/o interrumpir sus operaciones, también se han aprovechado de la guerra entre Rusia y Ucrania para enviar ataques más extensos con el fin de engañar o estafar a las personas o introducirse a una red corporativa.

En medio del contexto actual, los estafadores están haciendo de las suyas con una gran cantidad de correos electrónicos fraudulentos, o mensajes solicitando ayuda para los refugiados o para la resistencia ucraniana.

Los atacantes envían un email con sentido de urgencia incitando al usuario a hacer clic en un enlace que direcciona a un sitio web con la idea de donar a la causa. Sin embargo, estos son utilizados para instalar software malicioso (malware) en el dispositivo para robar información, o bien abrir un archivo para instalarle en el mismo un código malicioso. También emplean las llamadas telefónicas o mensajes de voz o texto falsos de fuentes falsas con el objetivo de robar información confidencial de la compañía.

Estas y otras amenazas a la seguridad de la información continuarán en aumento, principalmente con temas de "moda" que se vitalizan o atraen a una gran cantidad de personas. Así mismo, países como Panamá, los ciberataques avanzan pues no se tiene el acompañamiento de la ciberseguridad necesaria. Por ejemplo, una organización panameña es atacada un promedio de 1,102 veces por semana en los últimos 6 meses, siendo los sectores banca - finanzas y gobierno los más afectados. El vector de ataque para archivos maliciosos más utilizado por los ciberdelincuentes es el correo electrónico, lo que representa que en Panamá el 85% de estos archivos fueron entregados vía email en los últimos 30 días, de acuerdo al último reporte de inteligencia de amenazas de Check Point.

El año pasado se produjo una gran cantidad de ataques dirigidos a infraestructura crítica que provocaron una gran interrupción en la vida cotidiana y, en algunos casos, incluso amenazaron el sentido de seguridad física de las personas y empresas. Es por esto que, ante la coyuntura internacional y la situación de la guerra, los expertos de Soluciones Seguras recomiendan las siguientes acciones, tanto para empresas como para personas o familiares:

- **Cuidado con las noticias falsas**. Evite y tenga cuidado con la información errónea que se propagará

- **Verifique el enlace que obtiene**. Siempre busque y verifique los enlaces que recibe. ¿Son prestados de algún otro lugar? ¿Está conduciendo a una página copiada? ¿Contiene encriptación o certificados de seguridad? Al navegar por sitios que requieren de la utilización de credenciales, validar siempre que se encuentre en el sitio con certificado digital seguro y confiable indicado con un candado al lado de la URL y que la misma comience con https (certificado de seguridad) y no http.

- **Prestar atención a los correos electrónicos de restablecimiento de contraseña no solicitados**. Si recibe uno de estos, visite siempre el sitio web directamente sin hacer clic en los enlaces adjuntados.

- **Contraseñas seguras y robustas:** cerciórese que las contraseñas contengan combinaciones de números, letras y signos, y que haya una contraseña diferente en cada cuenta que utilice.

- **Instalar un antivirus para evitar posibles ataques**. Cuando utilice internet, principalmente fuentes abiertas de WiFi, es primordial tener que tanto sus computadoras como dispositivos móviles estén seguros y actualizados.

- **Nunca comparta sus credenciales o información con otras personas**. Los ciberdelincuentes utilizan diferentes estafas para intentar robar accesos a sistemas empresariales o información personal como datos bancarios, tarjetas de crédito, contraseñas u otra información confidencial.

BLUEPRINT PARA ASEGURAR SU RED

Si desea mejorar la postura de seguridad de su red, pero no sabe cómo empezar, esta guía es para usted. Aquí podrá encontrar las áreas clave y recomendaciones que debe considerar dentro de su estrategia de ciberseguridad.

Acerca de la Guía

El propósito de esta guía es brindar una descripción general de las áreas que debe tomar en cuenta al momento de implementar o revisar la postura de ciberseguridad de su entidad. De modo que no pase por alto alguna pieza crítica del rompecabezas a la hora de revisar o armar su arquitectura de seguridad de redes.

Con este enfoque, deseamos proporcionarle herramientas que le permitan conocer un listado de verificación de alto nivel para garantizar que se hayan abordado los componentes de seguridad más importantes, ya sea que estos sean o no elegidos dentro de la arquitectura.

Esta guía le brinda una referencia para cualquier red, esto se logra al reflejarse contra un listado de niveles que le permitirá conocer la ubicación y madurez de su red en temas de ciberseguridad.

También proporcionará el conocimiento de que una seguridad de red efectiva no es solo una colección de piezas. Debe ser una serie de herramientas entrelazadas planificadas para minimizar la exposición de la red corporativa.

Áreas a Proteger

Todas las áreas y posibles controles de seguridad deben ser parte de su análisis y estrategia de ciberseguridad. Cada posible acceso o superficie de riesgo debe evaluarse para determinar el valor de riesgo de no implementarse un mecanismo de seguridad. Este análisis generalmente viene dado al considerar el costo de una solución versus el costo de recuperar los datos, así como el costo de no disponer del servicio durante el tiempo de recuperación.

Durante la lectura de la guía explorará a fondo las áreas que están involucradas en la seguridad junto a los riesgos que surgen en torno a ellas y como puede ir incorporándolas dentro de su estrategia de ciberseguridad.

Madurez y Niveles de Seguridad

Finalmente, una arquitectura de seguridad completa debe disponer de muchas soluciones de seguridad. Muchas veces los clientes se sienten confundidos porque no saben por dónde comenzar. Por ello, hemos definido los Niveles de Seguridad, que le permitirán revisar de forma ordenada las soluciones revisadas durante la guía, siguiendo un orden de madurez de red.

¿No sabe por dónde comenzar a asegurar su red?

Descargue Gratis Nuestro
Blueprint de Ciberseguridad

CURSOS VIRTUALES 2022

CCSA

Check Point Certified

SECURITY ADMINISTRATOR

Conceptos y habilidades necesarias para gestionar las operaciones diarias de ciberseguridad utilizando la tecnología de Check Point

CCSE

Check Point Certified

SECURITY EXPERT

Habilidades avanzadas para proteger y mantener eficazmente la seguridad de las redes de su empresa

> CURSOS VIRTUALES DISPONIBLES
Contáctenos para obtener más información

CCVS

Check Point Certified

VSX SPECIALIST

Habilidades importantes para implementar seguridad de red virtual

CCCS

Check Point Certified

CLOUD SPECIALIST

Gestione las soluciones de Check Point CloudGuard IaaS dentro de su entorno de seguridad en la nube

CCTA

Check Point Certified

TROUBLESHOOTING ADMINISTRATOR

Conceptos y habilidades necesarias para solucionar problemas

> CURSOS VIRTUALES DISPONIBLES
Contáctenos para obtener más información

Consúltenos para obtener más información:
entrenamiento@solucionesseguras.com
www.solucionesseguras.com

PROTECCIÓN DE REDES, ENDPOINTS Y MOVILES

Check Point ofrece la más reciente protección de seguridad de redes en una plataforma integrada. Con protección para su centro de datos, empresa, móviles, estaciones de trabajo y oficina en el hogar, Check Point tiene una solución para usted.

SEGURIDAD Y SERVICIOS DNS, DHCP & IPAM

Consolide los servicios DNS, DHCP & IPAM en una sola plataforma, administrada centralmente. Para DNS externos elimine la interrupción del servicio DNS mediante una defensa automatizada contra ataques volumétricos basados en DNS y exploits.

PROTECCIÓN DE BASE DE DATOS Y APLICACIONES WEB

Soluciones de auditoría y protección a datos críticos mediante protección de Bases de Datos, además de protección para aplicativos web (WAF). Brindando una protección completa lo más cerca de la fuente de información.

MITIGACIÓN DE ATAQUES | ENTREGA DE APLICACIONES

Soluciones para seguridad, disponibilidad, balanceo y rendimiento de infraestructura y aplicaciones web. Sistema Mitigador de Ataques para protección perimetral y alta disponibilidad en sus aplicaciones web manteniéndolas seguras y optimizadas.

SEGURIDAD DE CUENTAS PRIVILEGIADAS

CyberArk es líder y experto en seguridad de cuentas privilegiadas. Gestión de privilegios, análisis de amenazas privilegiadas y registro de sesiones. Las contraseñas privilegiadas se mantienen en una bóveda segura.

VISIBILIDAD Y CONTROL DE ACCESO A LA RED

Solución de seguridad heterogénea que puede ver dispositivos, controlarlos y organizar respuestas de amenazas en instalaciones cableadas e inalámbricas, centros de datos, campus, nube y tecnología operativa sin agentes.

IPS Y PROTECCIÓN AVANZADA PARA REDES Y SERVIDORES

Soluciones que frecen alta tecnología en prevención de intrusiones para proteger contra toda la gama de amenazas en cualquier lugar de su red y servidores en ambientes físicos, virtuales y en la nube.

FILTRADO DE CONTENIDO Y ARCHIVADO DE DATOS

Barracuda le birnda una única fuente para proteger todos sus vectores de amenazas, incluidos el correo electrónico, sitios web, aplicaciones web, y el rendimiento de la red, ya sea en el sitio o en la nube.

MONITOREO DE RENDIMIENTO DE REDES Y SERVIDORES

El monitoreo de su infraestructura completa desde una solución centralizada todo-en-uno. Es de rápida implementación brindando alertas proactivas y vistas instantáneas, permitiendo resolver incidencias de red lo más rápido posible.

ANÁLISIS DE EVENTOS DE DISPOSITIVOS DE SEGURIDAD

Plataforma con integración profunda a dispositivos críticos, con automatización pre-cargada e instrucciones de remediación fácil de leer que proveen herramientas valiosas al equipo.

SISTEMA INMUNE DE LAS EMPRESAS

Detección de amenazas en tiempo real, visualización de la red y capacidades avanzadas de investigación en un solo sistema unificado.

SIEM BASADO EN LA NUBE | ANÁLISIS DE VULNERABILIDADES

Solución SIEM basado en la nube con User Behavior Analytics y Deception Technology (HOneypot). Además de solución para análisis de vulnerabilidades.

LA ATENCIÓN QUE USTED NECESITA

El Soporte de Soluciones Seguras con Atención de Emergencias 24x7 le da protección completa y el servicio que usted espera de un líder en ciberseguridad de redes.

RECONOCIDOS POR LA INDUSTRIA

Hemos recibido múltiples reconocimientos por los fabricantes y mayoristas líderes que representa.

EMPRESAS PROTEGIDAS, EMPRESAS TRANQUILAS

SÍGUENOS EN NUESTRAS REDES SOCIALES

SOLUCIONES SEGURAS
Empresas Protegidas, Empresas Tranquilas

CHECK POINT PARTNER ELITE

ACERCA DE SOLUCIONES SEGURAS

Con 20 años de experiencia en la gestión de seguridad de redes, aplicaciones y telecomunicaciones, Soluciones Seguras es la compañía líder en ciberseguridad en Centroamérica. Nuestra reputación se ha creado en base al excelente servicio que ofrecemos, el total conocimiento de las líneas que manejamos, y los productos líderes que representamos.

PERSONAL EXPERTO Y CERTIFICADO

Somos un equipo de profesionales del más alto nivel, certificados por los fabricantes más reconocidos de la industria de seguridad.

CENTRO REGIONAL DE ENTRENAMIENTO AUTORIZADO

Centro Regional de Entrenamiento Autorizado Check Point número uno en la región, con profesionales expertos que forman parte del equipo de desarrollo del contenido de los entrenamientos.

SOLUCIONES SEGURAS TRAINING CENTER

LÍDER EN CIBERSEGURIDAD EN CENTROAMÉRICA

PRESENCIA REGIONAL

SOLUCIONES SEGURAS EN PANAMÁ

Edificio 237, 2do piso
Ciudad del Saber, Panamá
Tel: +507 317-1312
Fax: +507 317-1320
info@sseguras.com

SOLUCIONES SEGURAS EN COSTA RICA

Edificio Atrium piso 3.
Escazú, San José, Costa Rica
Tel: +506-4000 0885
Fax: +506-4001 5822
infocr@sseguras.com

SOLUCIONES SEGURAS EN GUATEMALA

Edificio Zona Pradera
Torre IV, Nivel 6, Oficina 608
Boulevard Los Próceres 24-69.
Tel: +502 2261-7101
infogt@sseguras.com

SOLUCIONES SEGURAS EN EL SALVADOR

Edificio Vittoria, 5to Nivel,
Calle El Mirador 4814
San Salvador, El Salvador
Tel: +503 2206-6929
infosv@sseguras.com

Alianzas

SOLUCIONES SEGURAS

Empresas Protegidas, Empresas Tranquilas

Panamá | Costa Rica | Guatemala | El Salvador

www.solucionesseguras.com

SOLUCIONES SEGURAS CYBERSECURITY MAGAZINE