SOLUCIONES SEGURAS
CYBERSECURITY
MAGAZINE

Edición No. 17

REVISTA REGIONAL DE CIBERSEGURIDAD

CIBERPANDEMIA

ACTUALIZACIÓN H1 2022

EN ESTA EDICIÓN:

RESUMEN DE CIBERATAQUES DEBIDO AL CONFLICTO RUSIA-UCRANIA

CIBERATAQUES EN COSTA RICA Y PERÚ QUE IMPULSARON UNA RESPUESTA NACIONAL

FOLLINA, VULNERABILIDAD DE DÍA CERO EN MICROSOFT OFFICE

Y MÁS...

2022
VOLUMEN 2

SOLUCIONES SEGURAS
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

Por mucho tiempo hemos hablado de los potenciales peligros que las entidades de nuestra región podían sufrir. A veces no es placentero cuando las predicciones se vuelven realidad, como lo hemos visto en los últimos meses.

Cuando a finales del 2020 comenzamos a hablar del potencial de una ciberpandemia, o cuando hace dos meses hablamos de los impactos geomundiales del conflicto entre Rusia y Ucrania, no podíamos imaginar cómo se vería en nuestra región.

Durante el 2021 vimos un aumento muy significativo de ataques de ransomware exitosos en empresas grandes y pequeñas.

Durante el 2022, hemos visto los ataques a entidades gubernamentales más devastadores en la historia de nuestra región. Y lo peor, es que parece que no han terminado todavía.

Lo hemos dicho previamente, pero ahora toma mayor relevancia: es el momento para hacer una examinación profunda de los sistemas de seguridad que tienen implementados, mejorar la configuración y seguridad de los mismos, y concientizar a todos los usuarios en las mejores prácticas para proteger su identidad y sus accesos. Es también momento de creer en la filosofía de KISS (Keep It Simple), y también de Least Privilege (otorgar el menor privilegio necesario). Piensen en qué es lo que puede pasar en su empresa, y hagan un plan para minorizar ese riesgo y para responder en caso de que realmente se dé.

Aprovechen el tiempo que tienen ahora para planear qué hacer en el futuro. Es lo menos que pueden esperar sus organizaciones del personal de ciberseguridad de la empresa, que cada vez más toman ustedes el rol de los guardianes o protectores del activo más importante: la información.

¡Suerte!

Eli Faskha
CEO

RESUMEN DE CIBERATAQUES
DEBIDO AL CONFLICTO RUSIA-UCRANIA

Debido a los conflictos geopolíticos, específicamente el de Rusia-Ucrania, los profesionales de seguridad deben estar preparados para el aumento continuo de ciberataques y amenazas de red. La ciberpandemia es una realidad y está afectando muchos países. A continuación, veremos las noticias y estadísticas más importantes respecto al impacto del conflicto Rusia-Ucrania en la ciberseguridad:

Grupos de ataque patrocinados por el estado capitalizan la guerra Rusia-Ucrania para el espionaje cibernético

A inicios de año, mientras se desarrollaba la invasión rusa de Ucrania, Check Point Research (CPR) observó que grupos de amenazas persistentes avanzadas (APT) en todo el mundo lanzaban nuevas campañas para atacar a las víctimas con correos electrónicos de phishing selectivo utilizando la guerra como señuelo. El uso del conflicto como carnada no se limita a una región específica, nuestra región no escapa de esta realidad:

Machete APT

Kaspersky reveló públicamente por primera vez a El Machete, un actor de amenazas de habla hispana que se enfoca en los objetivos de América Latina, en 2014 y la actividad del grupo se remonta a 2010. Las actividades del grupo han persistido a lo largo de los años, adoptando la práctica de usar documentos con temas gubernamentales como señuelos, así como el uso de señuelos relacionados con la situación política actual. **A mediados de marzo de este año**, se vio a "El Machete" enviando correos electrónicos de spear-phishing a organizaciones financieras en Nicaragua, con un documento de Word adjunto titulado "Planes oscuros del régimen neonazi en Ucrania. El documento contenía un artículo escrito y publicado por Alexander Khokholikov, el embajador de Rusia en Nicaragua, que discutía el conflicto ruso-ucraniano desde la perspectiva del Kremlin.

Aumento de los ataques cibernéticos tanto en Rusia como en Ucrania, un mes después de la guerra

En un informe anterior, Check Point Research (CPR) observó un aumento en los ataques cibernéticos dirigidos a países de la OTAN que se originaron en direcciones IP chinas.
Un mes después de que comenzara la guerra el 24 de febrero de 2022, tanto Rusia como Ucrania experimentaron aumentos en los ciberataques del 10% y el 17%, respectivamente. CPR también ha observado un aumento del 16 % en los ataques cibernéticos a nivel mundial durante el conflicto actual. CPR comparte datos de ataques cibernéticos para países y regiones de la OTAN y más. CPR postula que los piratas informáticos buscan aprovechar la guerra entre Rusia y Ucrania desde todos los rincones, mientras continúan realizando otros ataques en grandes volúmenes.

En América Latina, el promedio de ataques semanales por organización aumenta un 13% más que antes del inicio de la guerra y un 6% menos que la semana anterior. Durante la guerra, la tasa semanal promedio de ataques aumentó un 9% en comparación con el período anterior a la guerra. Más estadísticas aquí.

Otras Noticias de Interés referentes al tema

Ataques cibernéticos de IP chinas en los países de la OTAN aumentan en un 116%

Check Point Research (CPR) notó un aumento en los ataques cibernéticos provenientes de direcciones IP chinas durante el conflicto actual entre Rusia y Ucrania. Más información.

Criptorecaudación de fondos para Ucrania encontrada en Darknet, utilizada por ciberdelincuentes para fraude

Check Point Research (CPR) notó una tendencia en la que aparecen anuncios que solicitan donaciones a los ucranianos en Darknet. Aunque algunos anuncios son legítimos, muchos son fraudulentos. CPR proporciona ejemplos de ambos. Todos los anuncios solicitan fondos de donación en forma de criptomoneda. Más información.

Ataques cibernéticos a organizaciones gubernamentales fuera de Ucrania aumentan en un 21%

En los primeros tres días de combate, los ataques cibernéticos contra el gobierno y el sector militar de Ucrania aumentaron en un asombroso 196 %. Desde entonces, los ataques cibernéticos contra el gobierno y el sector militar de Ucrania disminuyeron, cayendo un 50 % en los últimos 7 días. CPR sospecha que los piratas informáticos han hecho un cambio para aprovecharse de otros gobiernos centrados en el conflicto.
Más información.

Conti Ransomware Group

Las filtraciones de Conti Ransomware Group pintan la imagen de una empresa emergente tecnológica sorprendentemente normal... más o menos. 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.
Más información.

Noticias falsas sobre ataques cibernéticos se propagaron rápidamente a medida que se intensificaba el conflicto entre Rusia y Ucrania

A medida que se intensificó el conflicto físico entre Rusia y Ucrania, Check Point Research (CPR) advirtió sobre los grupos de hacktivistas que afirman falsamente que ambos lados han realizado ataques cibernéticos exitosos. CPR investigó afirmaciones recientes de tres grupos hacktivistas, AgainstTheWest, KelvinSecurity y Killnet, y demostró que sus afirmaciones eran mentiras. CPR ha desacreditado los presuntos ataques cibernéticos contra el motor de búsqueda más grande de Rusia, Yandex, y otros dos objetivos, una instalación nuclear rusa y un ataque al sitio web de Anonymous.
Más información.

Telegram se convierte en una vanguardia digital en el conflicto

Check Point Research (CPR) rastrea las actividades que suceden en Telegram y comparte una descripción general de las observaciones en Telegram sobre el conflicto actual en Europa del Este. El día que Rusia invadió Ucrania, CPR documentó un aumento de 6 veces en los grupos de Telegram con el tema de la guerra.
Más información.

Cómo el conflicto ucraniano ha polarizado el ciberespacio

En la medida que el conflicto en Europa del Este avanza. La gente en todas partes está decidiendo a quién apoyará. La misma dinámica ocurre en el ciberespacio. Los hacktivistas, los ciberdelincuentes, los investigadores de sombrero blanco o incluso las empresas de tecnología están eligiendo un lado claro, envalentonados para actuar en nombre de sus elecciones.
Más información.

Tendencias de los ataques cibernéticos en medio de la guerra: los números detrás del conflicto

Check Point Research (CPR) publica datos sobre ciberataques observados en torno al conflicto actual en Europa del Este.
Más información.

EVENTO: ¿CÓMO ASEGURAR LOS DATOS PERSONALES DE LOS CLIENTES BANCARIOS?

En los últimos años las instituciones financieras se han convertido en el principal objetivo de los hackers, y asegurar los datos confidenciales que recopilan, procesan y almacenan de clientes, es un desafío importante del sector para garantizar la privacidad y seguridad de las personas y empresas.

Los ciberataques a los bancos a nivel mundial aumentaron un 53% respecto al 2020. En Panamá, el sector banca y finanzas continúa siendo el que más ataques recibe con un promedio de 1736 ataques semanales por organización.

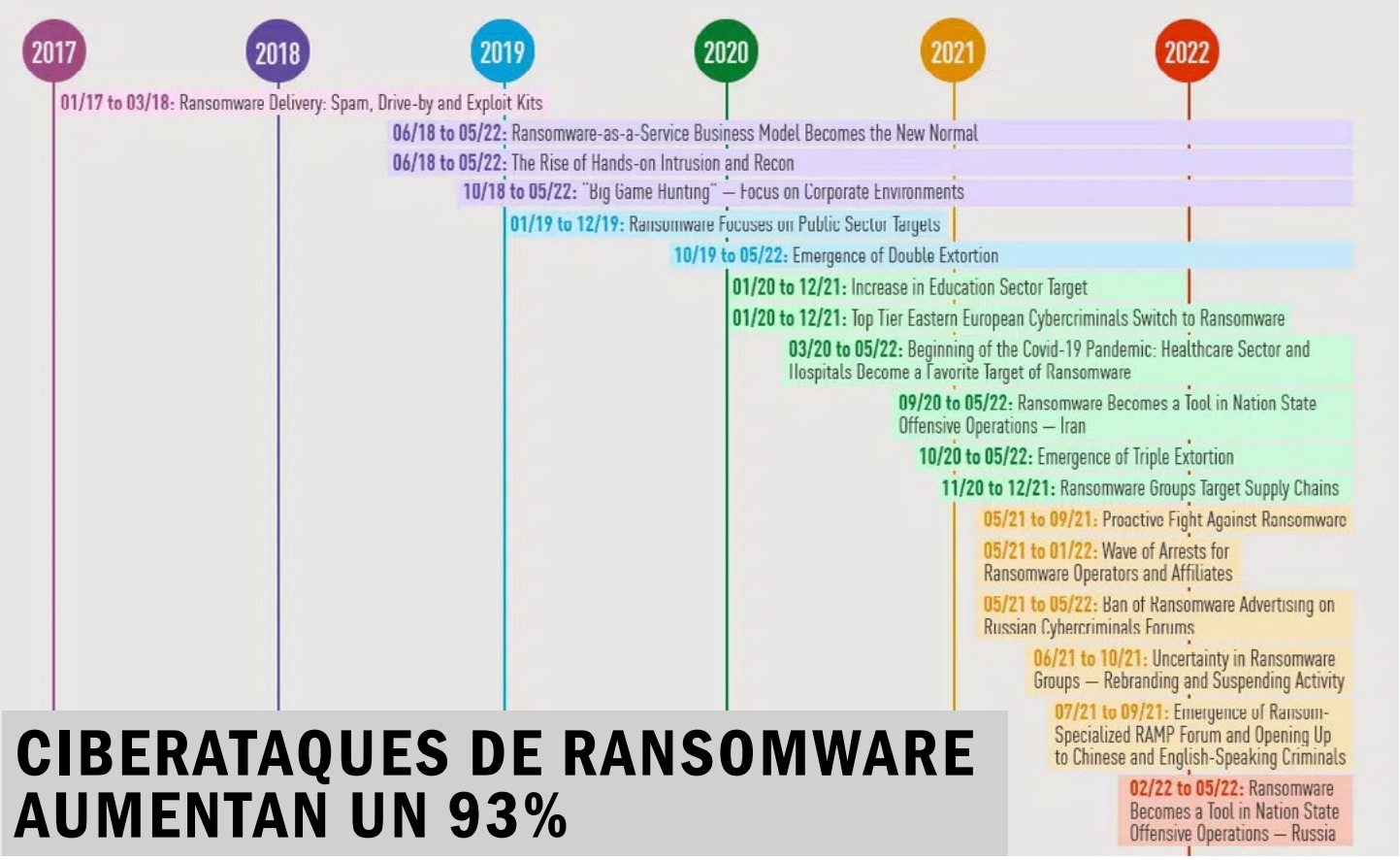
Dada la creciente intensidad y complejidad de las amenazas cibernéticas empleadas por los cibercriminales, ¿Cómo pueden estar seguros los bancos de que su información corporativa y la de sus clientes se mantienen seguras y cumplen con las normas vigentes de protección de datos personales?

En esa línea, Soluciones Seguras, compañía líder en ciberseguridad en Centroamérica, realizó su evento: "Cybersecurity Break", un Conversatorio sobre "Seguridad de los Datos y cumplimiento de las leyes y acuerdos vigentes", junto a sus partners Imperva, Varonis y Thales.

El encuentro, en el que participaron más de 20 entidades del sector financiero panameño, clientes de Soluciones Seguras, tuvo como objetivo ayudarlos a comprender en materia de ciberseguridad, los elementos comunes de la ley 81 que regula la protección de datos personales en la República de Panamá, y el acuerdo No. 001-2022 que establece lineamientos especiales para la protección de datos personales tratados por las entidades bancarias.

Las exposiciones estuvieron a cargo de expertos en seguridad y privacidad de datos, entre ellos Cesar Araque, Regional Sales Director de Imperva, Caribbean, Roque Alvarez, Regional Sales manager de Thales, Eli Faskha, CEO de Soluciones Seguras y Mauro Reluz, Arquitecto de Seguridad en Soluciones Seguras Panamá.

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 y Guatemala, y clientes en otros países de Latinoamérica.



CIBERATAQUES DE RANSOMWARE AUMENTAN UN 93%

Continuando nuestra trayectoria por el estado de la ciberpandemia, Ransomware no escapa de las estadísticas pues es uno de los vectores de ataque más importantes debido a que es usado para extorsión de las víctimas.

- Check Point Research ve un aumento del 93 % año tras año.
- América Latina y Europa vieron el mayor aumento en los ataques de ransomware desde principios de año, con un aumento del 62 % y del 59 %, respectivamente.

Grupo Conti: detrás de las cortinas de la economía del ransomware: las víctimas y los ciberdelincuentes

Los ataques de ransomware van en aumento, pero pocas personas entienden los costos ocultos más allá del pago inicial de extorsión. Esto puede incluir gastos de respuesta y restauración, honorarios legales y costos de monitoreo, por nombrar algunos. CPR se basa en los recientes Conti Leaks, que muestran cómo las pandillas de ransomware son alarmantemente similares a las organizaciones legítimas con estructuras de gestión y políticas de recursos humanos claras. La sofisticación de estos grupos de ransomware incluso se extiende al objetivo de las víctimas y cómo se decide una cifra de rescate, así como las técnicas de negociación que utilizan para obtener la máxima ganancia financiera. Afortunadamente, las organizaciones se están dando cuenta de la amenaza del ransomware al tener un plan claro de respuesta y mitigación. De hecho, la duración de los ataques de ransomware se está reduciendo como resultado.

El grupo Conti ha sido un nombre muy popular este año por sus recientes ataques y actividades. En una investigación realizada por Check Point Research CPR, al analizar los registros de chat del grupo Conti, mostró previamente la sorprendente similitud de Conti con una empresa nueva, con una estructura organizativa, procesos de recursos humanos y responsabilidades estrictas. Con más de 100 empleados, la operación de Conti pudo optimizar toda la operación de ransomware desde una generación automática de carga útil hasta el proceso de negociación de rescate. El equipo de negociación de Conti es responsable de hablar con las víctimas, negociar los pagos de rescate, escribir publicaciones de blog sobre las víctimas en el sitio de filtraciones de Conti y, finalmente, proporcionar el software de descifrado si se cumple con la demanda de rescate. Sus comunicaciones internas arrojan luz sobre el funcionamiento interno de sus procesos de negociación.

Cómo la evolución del ransomware cambió el panorama de las amenazas

De WannaCry a Conti: una perspectiva de 5 años

El ataque de WannaCry cambió la ciberseguridad; hizo olas debido a su gran influencia en el panorama de las ciberamenazas. Como el primer ciberataque multivectorial a escala global impulsado por actores patrocinados por el estado, WannaCry marcó un punto de inflexión en el entorno de ciberseguridad, inspirando a los actores de todo el mundo y afectando todo el panorama de amenazas durante los próximos cinco años hasta ahora. Vea la Línea de tiempo completa.

RADWARE MITIGATES 1.1TBPS DDOS ATTACK

Recurso: Radware Blog, Mayo, 2022
https://blog.radware.com/security/2022/05/radware-mitigates-1-1tbps-ddos-attack/

As more businesses migrate critical resources and applications to the public cloud, attackers are adapting their tactics and techniques to match the scale of public cloud providers. Last week, this trend played out as reality for one of the world's largest service providers when it was hit by a 1.1 Tbps DDoS attack (Figure 1) that lasted approximately 36 hours. Here's how this U.S. provider's story unfolded.

The First Wave

The clock started ticking when this U.S. service provider noticed a service impact. At first, the service provider, which serves millions of businesses worldwide, intended to mitigate the attack using its on-premise solution as it usually does. However, a decision was quickly made to route all traffic through Radware's Cloud DDoS Protection Service when the high-volume, multi-vector attack was too complex to handle locally. Within a few minutes after the first call to Radware's Emergency Response Team (ERT) hotline, the service provider's assets were onboarded to Radware Cloud DDoS Protection Service and mitigation started.

During the first five hours of the attack, traffic peaked at 150 Gbps. The top attack vectors included UDP flood, UDP fragmentation flood, fragmented ACK and PSH flood, and NTP reflection (Figure 2). With UDP flood attacks, the attacker intends to saturate the victim's internet pipes by sending large UDP packets to a single destination or to a random port. With fragmented ACK and PSH flood attacks, on the other hand, the attacker uses very small byte packets to hog the target network's bandwidth using only a moderate packet rate. Radware's ERT security experts worked in collaboration with the new customer to understand normal traffic patterns and immediately applied the relevant mitigation to fully block the first wave of the attack.

Figure 2

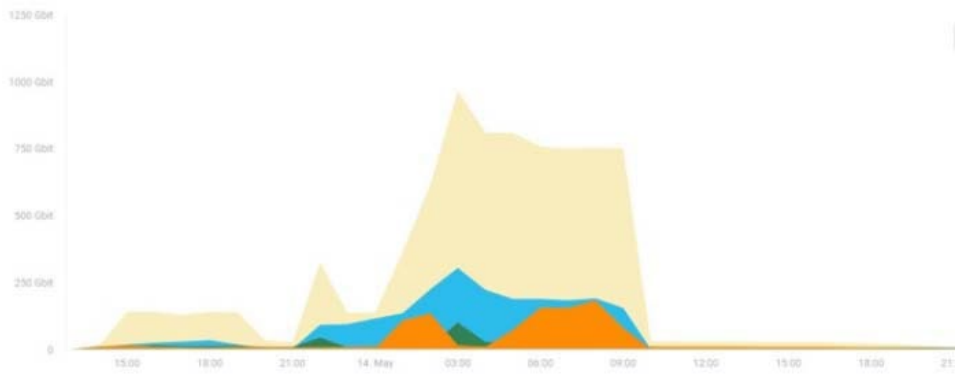


Figure 1

The Second Wave

Six hours into the incident, the second wave of the attack began, with traffic peaking at over 300 Gbps. Based on evidence gathered primarily from indicators of compromise, the attack traffic appeared to have originated primarily from Japan, the United States, Taiwan, and South Korea (Figure 3).

Figure 3

At this point, the unrelenting attack continued. Trying to disrupt service to the provider, approximately 150Gbps of traffic lasted for an additional three hours, before peaking at 1.1 Tbps. The barrage of attack traffic was fully mitigated leveraging the capacity of only four of the scrubbing centers in Radware's global network. The scrubbing centers were located in the United States and EMEA (Figure 4).

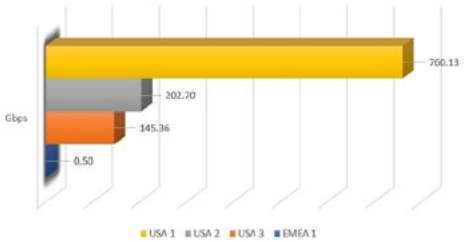


Figure 4

Post Peak

Post peak, approximately 800 Gbps of attack traffic continued for more than nine hours until the attacker's resources were exhausted by Radware's Cloud DDoS Protection mitigation and ERT experts. As of the time of this blog, no hacktivist organization has assumed responsibility for the attack.

Is this just the beginning?

It is impossible to ignore the wave of hyper-volumetric DDoS attacks that have been recorded in 2022. While 2021 saw only a few 1Tbps attacks, attacks of 1Tbps and more are becoming a new reality this year. As bandwidths and resources increase for legitimate businesses, they also increase for threat actors. It is only fair to assume that bad actors can scale as fast and high as their targets. Organizations need to be aware that DDoS attacks are a part of their threat landscape, irrespective of geography or industry.

Radware's Cloud DDoS Protection Services protect organizations of all sizes from a wide variety from sectors, ranging from education, e-commerce, retail, and global financial services to worldwide governments, and leading service providers and carriers. It is safe to say that no organization, regardless of what they do or where they are located, are immune from attack.

“FOLLINA”- VULNERABILIDAD DE DÍA CERO EN MICROSOFT OFFICE

Recurso: Check Point Blog, Junio, 2022
https://blog.checkpoint.com/2022/05/31/follina-zero-day-vulnerability-in-microsoft-office-check-point-customers-remain-protected/

La vulnerabilidad

El 30 de mayo, los investigadores revelaron una vulnerabilidad de día cero en Microsoft Office que, si se explota mediante el uso de un documento de Word malicioso, podría permitir la ejecución de código en la máquina de la víctima.

La vulnerabilidad, ahora denominada “follina”, ve un documento de Word que usa una función de plantilla remota para recuperar un archivo HTML de un servidor remoto y, al usar un esquema de URI de MSProtocol ms-msdt, puede ejecutar un PowerShell.

¿Qué versiones son vulnerables?

Office 2013, 2016, 2019, 2021 y algunas versiones de Office incluidas con una licencia de Microsoft 365 están sujetas a esta vulnerabilidad tanto en Windows 10 como en Windows 11.

¿Cuál es el riesgo en la ejecución remota de código (RCE)?

Los ataques de ejecución remota de código (RCE) permiten a un atacante ejecutar de forma remota código malicioso en una computadora. El impacto de una vulnerabilidad RCE puede variar desde la ejecución de malware hasta que un atacante obtenga el control total de una máquina comprometida.

Los archivos desinfectados sin amenazas mantienen protegidos a los clientes de Check Point

Threat Extraction ofrece archivos desinfectados sin amenazas a los usuarios en tiempo real, proporcionando una postura de alta seguridad mientras se mantiene el flujo comercial. Los archivos adjuntos de correo electrónico y las descargas web que pueden verse afectados por la nueva vulnerabilidad se desinfectan sobre la marcha, entregando contenido seguro a los usuarios sin exponerlos a los riesgos que pueden estar al acecho en el archivo original. Los archivos originales se envían en paralelo a la zona de pruebas de Emulación de amenazas y el usuario puede recuperarlos fácilmente, si no son maliciosos.

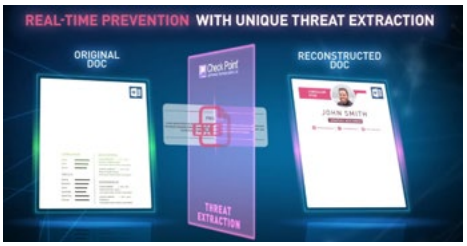
En la práctica, cada archivo recibido por correo electrónico o descargado por un usuario a través de un navegador web se envía a la zona de pruebas de Emulación de amenazas para inspeccionar malware y elementos maliciosos. Los archivos se desinfectan mediante el proceso de extracción de amenazas (tecnología de desarme y reconstrucción de contenido) para entregar contenido desinfectado en milisegundos.

Estas capacidades protegen a los clientes de Check Point mientras usan su Endpoint con Harmony Endpoint, mientras navegan por Internet con Harmony Browse, está disponible a través de nuestra protección de red con Quantum™ Network Security, mientras usan cuentas de correo electrónico con Cloud Email & Collaboration Suite Security, y en dispositivos móviles , por Harmony Mobile.

El 1 de junio, Check Point lanzó nuevas protecciones IPS : la protección ‘Microsoft Support Diagnostic Tool Remote Code Execution (CVE-2022-30190)’ cubre la vulnerabilidad conocida como ‘Follina’

Threat Extraction de Check Point

Las capacidades de Emulación de amenazas están enriquecidas con inteligencia de amenazas alimentada directamente desde Check Point ThreatCloud, el recurso de inteligencia de amenazas más grande del mundo para todas las superficies de TI: nube, red, terminales y dispositivos móviles.



Recomendaciones de mejores prácticas:

Check Point insta a los usuarios a practicar lo siguiente de forma regular:

1. Nunca abra un documento que no espera, incluso si proviene de remitentes conocidos.
2. A menos que exista una clara necesidad, no desactive el modo protegido de los documentos que se originan en Internet o correo electrónico.
3. Absténgase de abrir archivos .rtf que se originen en Internet, incluso en el modo de vista previa.

Microsoft ha publicado una guía de protección y ha asignado CVE-2022-30190 a esta vulnerabilidad.

Los investigadores de Check Point siguen de cerca esta historia en evolución y continuarán informando a medida que haya más información disponible.

Ver en Youtube: Check Point Harmony Endpoint vs. Microsoft Office Exploit “Follina”:

SOLUCIONES SEGURAS Y CHECK POINT PRESENTARON EN EL ISEC INFOSECURITY PANAMÁ LOS DESAFÍOS ACTUALES DE CIBERSEGURIDAD

Ante la acelerada transformación digital que se vive actualmente, Panamá se ha convertido en uno de los principales objetivos de los ciberdelincuentes con un promedio semanal de ciberataques mayor al promedio del resto de Latinoamérica.

Las organizaciones panameñas son atacadas en promedio 1,387 veces por semana en los últimos 6 meses; en comparación con 1054 ataques por organización en las Américas, según el último reporte de inteligencia de amenazas de Check Point, partner de Soluciones Seguras.

Los ciberataques continúan en ascenso como una de las actividades más rentables, y banca y finanzas continúa posicionándose como el sector en el país más atacado, por lo que las organizaciones panameñas deben mantenerse al tanto de las tendencias en amenazas y vulnerabilidades más utilizadas por los cibercriminales a nivel local e internacional.

En esta línea, Soluciones Seguras, compañía líder en ciberseguridad en Centroamérica, participó como patrocinador del ISEC INFOSECURITY TOUR 2022 “A New World Tour”, uno de los eventos más reconocidos en América Latina en lo que refiere a ciberseguridad.

El evento que tuvo lugar en el hotel Sheraton Grand Panamá, y que reunió a profesionales, directivos y proveedores del mundo de la Seguridad de Latinoamérica, se presentaron distintas exposiciones en torno a la seguridad integral de la red para todo tipo de organizaciones. Las mismas estuvieron a cargo de conferencistas expertos en ciberseguridad de compañías líderes de la industria, entre ellas Check Point, partner de Soluciones Seguras, con la exposición “HACKING LIKE A DISNEY VILLAIN”a cargo de Julio Lemus, Security Engineer Panamá - Honduras CCA Check Point.

La presentación ilustró los diferentes tipos de ciberataques a través de las actividades despiadadas realizadas por notorios villanos de Disney, con ejemplos de ataques descubiertos por los investigadores de Check Point a lo largo de los años.

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 las distintas empresas panameñas están en constante aumento. “Es muy importante para nosotros participar en eventos como el Infosecurity Tour 2022, donde se comparte el conocimiento y se pueden unir los esfuerzos para mejorar la ciberseguridad en Panamá y la región”, expresa 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.

SOLUCIONES SEGURAS Y CHECK POINT PARTICIPARON EN EL TECHDAY EN EL ISEC INFOSECURITY COSTA RICA COMO PANELISTAS EXPERTOS

Los ciberataques siguen en ascenso en todo el mundo y Costa Rica no es la excepción. Las organizaciones nacionales son atacadas en promedio 1,464 veces por semana en los últimos 6 meses; en comparación con 1165 ataques por organización a nivel mundial, según el último reporte de inteligencia de amenazas de Check Point, partner de Soluciones Seguras.

omo compañías líderes en ciberseguridad en la región centroamericana, Soluciones Seguras y Check Point, participaron recientemente en los reconocidos eventos TechDay, organizado por la revista ITNOW y el ISEC INFOSECURITY TOUR 2022 “A New World Tour”.

En dichos eventos, que reúnen a profesionales, directivos y proveedores de la industria de tecnología y ciberseguridad, Soluciones Seguras formó parte como patrocinador y Check Point tuvo participación como panelista experto.

La intervención en el TechDay estuvo a cargo de Mauricio Gómez, oportunidad que aprovechó para hablar sobre “La evolución del Rasomware” y cómo ha cambiado el panorama de amenazas, asimismo, brindó recomendaciones para enfrentarlo.

Por su parte, la exposición en el InfoSecurity fue realizada por Ronald Godínez. En esta ocasión se desarrolló el tema de “Estrategia de seguridad Cloud”, abordando aspectos como los desafíos, herramientas y estrategias, para lograr una nube segura.

PODCAST

Entrevista a Eli Faskha

(CEO de Soluciones Seguras)

Impulso Cyber

Conoce a Eli Faskha Fundador y CEO de Soluciones Seguras. Cuenta con más de 20 años de experiencia en el mercado en ciberseguridad. Nos habla de sus inicios en la seguridad y de las exigencias del mercado.
Conecta con Eli en **https://www.linkedin.com/in/eli-faskha/**
Sitio web **https://www.solucionesseguras.com/**

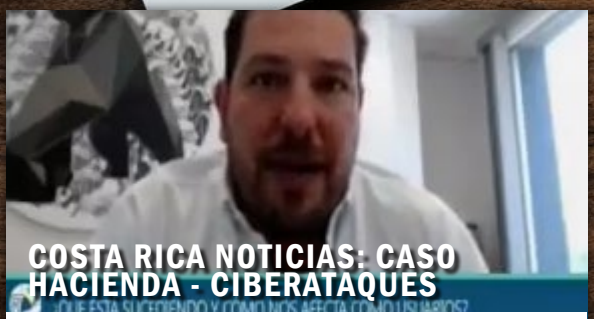
SOLUCIONES SEGURAS EN LAS NOTICIAS

TVN NOTICIAS: AUMENTAN LOS CIBERATAQUES EN PANAMÁ

tvn Noticias

METRO LIBRE: PANAMEÑOS PODRÁN SER BLANCOS DE CIBERCRIMINALES

METRO LIBRE
LA VERDAD DE LA NOTICIA



COSTA RICA NOTICIAS: CASO HACIENDA - CIBERATAQUES

TRECE COSTA RICA NOTICIAS

NEX TV: BANCA Y FINANZAS EL SECTOR CON MAS ATAQUES CIBERNETICOS EN EL PAIS

nex NOTICIAS

FORBES DE CENTROAMÁRICA: EL MINISTERIO DE HACIENDA DE COSTA RICA ENFRENTA UN CIBERATAQUE

Forbes CENTROAMÉRICA

RUMBO ECONÓMICO: ¿CÓMO PREVENIR LOS RIESGOS DE SEGURIDAD EN LA RED?

RE RUMBO ECONOMICO

SOLUCIONES SEGURAS

Empresas Protegidas, Empresas Tranquilas

ESTRATEGIA / NEGOCIOS: CONSEJOS PARA TENER UNA BUENA CONTRASEÑA Y RESGUARDAR LA INFORMACIÓN

E&N

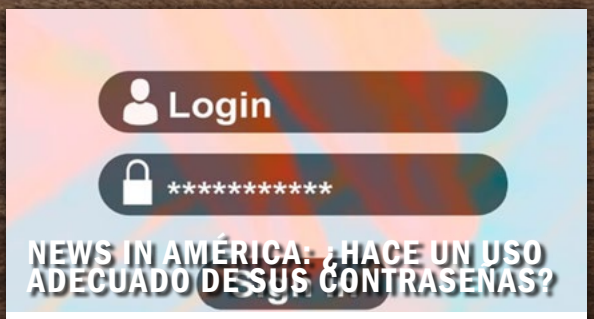
LA PRENSA MARTES FINANCIERO: 1736 CIBERATAQUES SEMANALES POR ENTIDAD BANCARIA SE REGISTRAN EN PANAMÁ

MARTES FINANCIERO
LA REVISTA FINANCIERA DE PANAMÁ

El país es vulnerable a los ataques de ese tipo, por lo que los especialistas sugieren prevención y no solo reacción.

PRENSA LIBRE: PREVÉN UNA GUERRA FRÍA CIBERNÉTICA

PRENSA LIBRE
Periódico líder de Guatemala

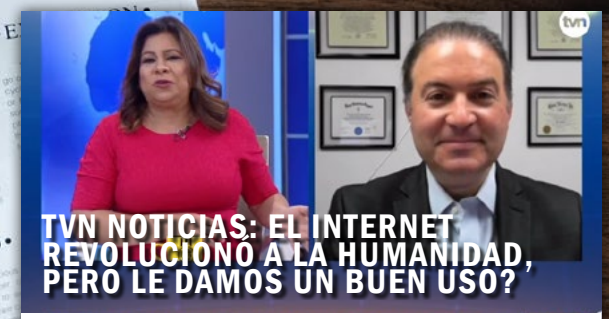


NEWS IN AMÉRICA: ¿HACE UN USO ADECUADO DE SUS CONTRASEÑAS?

newsinamerica.com
PERIODICO DIGITAL
Centroamericano y del Caribe

LA ESTRELLA DE PANAMÁ: LOS CIBERDELITOS AUMENTAN MÁS DEL 50% EN PREPANDEMIA, BANCA Y FINANZAS LOS MAYORMENTE AFECTADOS

LA ESTRELLA DE PANAMÁ 173 AÑOS



TVN NOTICIAS: EL INTERNET REVOLUCIONÓ A LA HUMANIDAD, PERO LE DAMOS UN BUEN USO?

tvn Noticias

CIBERATAQUES EN COSTA RICA Y PERÚ QUE IMPULSARON UNA RESPUESTA NACIONAL

En medio de ataques de ransomware a gran escala en Costa Rica y Perú, supuestamente ambos ejecutados por la infame banda de ransomware Conti, el Departamento de Estado de Estados Unidos emitió un comunicado el 6 de mayo, ofreciendo una recompensa de hasta US$10 millones por información que conduzca a la identificación o ubicación. de personas involucradas en el grupo de ransomware Conti.

Anteriormente, el estado de Costa Rica declaró una emergencia nacional después de los ataques de ransomware Conti que provocaron una fuga de 672 GB de datos pertenecientes a las agencias gubernamentales costarricenses, publicado por el grupo Conti.

El grupo Conti exigió un rescate de 10 millones de dólares al gobierno de Costa Rica, que se negó a pagar.

En Perú, el grupo atacó a "La Dirección Nacional de Inteligencia", la agencia de inteligencia del país, y según una captura de pantalla publicada en Twitter, robó 9,1 GB de datos. La pandilla de ransomware Conti también publicó que están "dando a Perú una ventaja para buscarlos en sus redes, a pesar de que se negaron a cooperar".

Costa Rica vuelve a ser atacado

El pasado martes 31 de mayo de 2022, la Caja Costarricense de Seguro Social, CCSS de Costa Rica fue golpeada por un ataque cibernético presuntamente lanzado por el grupo de ransomware Hive.

El incidente se produce semanas después de un ataque supuestamente realizado por otro grupo de ransomware con sede en Rusia, Conti, dirigido a varias agencias gubernamentales de Costa Rica, incluida la misma agencia de salud. Este ataque se suma a la ya golpeada infraestructura de gobierno debido a los recientes ataques.

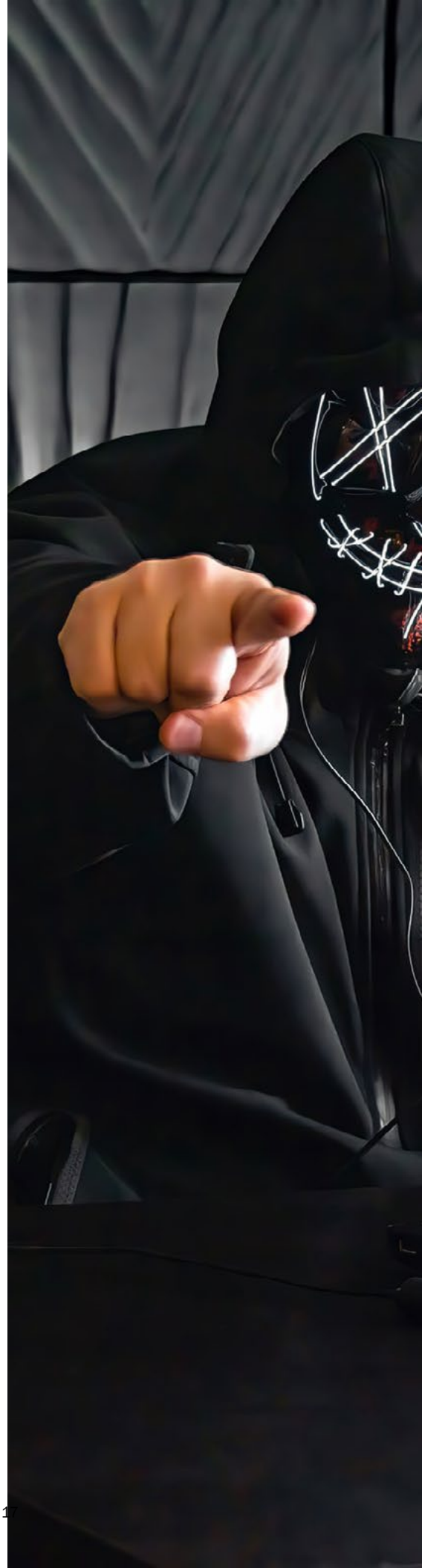
La agencia de salud, Caja Costarricense del Seguro Social, CCSS, en una serie de tuits y durante una rueda de prensa mostrada en su página de Facebook el martes, confirmó que había sido atacada por un ransomware a principios de horas del martes 31 de mayo.

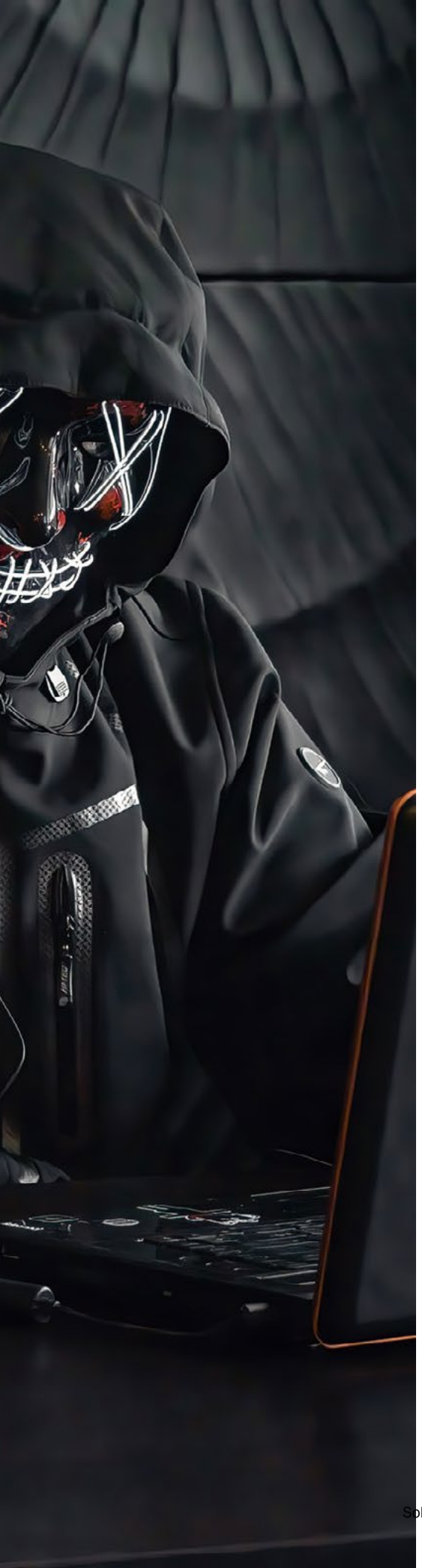
La CCSS en sus tuits dice que una vez detectado el ransomware, la agencia procedió a desconectar los sistemas "para revisar y desde allí trabajar en soluciones inmediatas y levantar los servicios lo antes posible".

Las bases de datos de Edus, Sicere, nómina y pensiones de la agencia no se vieron comprometidas, dice la CCSS en un tuit. Las autoridades gubernamentales están haciendo análisis "para tratar de restablecer los servicios críticos, pero no es posible determinar cuándo estarán en funcionamiento... Estaremos informando oportunamente en el momento en que se restablezcan", indica la CCSS en un tuit.

Una de cada 60 organizaciones es afectada por Ransomware

En los primeros cuatro meses de 2022, Check Point Research (CPR) informa que, en promedio, una de cada 60 organizaciones en todo el mundo se ha visto afectada por un intento de ataque de ransomware cada semana, un aumento interanual del 14 %





Cómo protegerse contra ransomware

La preparación adecuada puede reducir drásticamente el costo y el impacto de un ataque de ransomware. Tomar las siguientes mejores prácticas puede reducir la exposición de una organización al ransomware y minimizar sus impactos:

- **Capacitación y educación para la concientización cibernética:** el ransomware a menudo se propaga mediante correos electrónicos de phishing. Es crucial capacitar a los usuarios sobre cómo identificar y evitar posibles ataques de ransomware. Dado que muchos de los ataques cibernéticos actuales comienzan con un correo electrónico dirigido que ni siquiera contiene malware, sino solo un mensaje de ingeniería social que alienta al usuario a hacer clic en un enlace malicioso, la educación del usuario a menudo se considera una de las defensas más importantes. una organización puede implementar.

- **Copias de seguridad continuas de datos:** la definición de ransomware se explica como malware diseñado para forzar el pago de un rescate como la única forma de restaurar el acceso a los datos cifrados. Las copias de seguridad de datos protegidas y automatizadas permiten que una organización se recupere de un ataque con una pérdida mínima de datos y sin pagar un rescate. Mantener copias de seguridad periódicas de los datos como un proceso de rutina es una práctica muy importante para evitar la pérdida de datos, así como para poder recuperarlos en caso de corrupción o mal funcionamiento del hardware del disco. Las copias de seguridad funcionales también pueden ayudar a las organizaciones a recuperarse de los ataques de ransomware.

- **Aplicación de parches**: la aplicación de parches es un componente fundamental en la defensa contra los ataques de ransomware, ya que los ciberdelincuentes a menudo buscarán las últimas vulnerabilidades descubiertas en los parches disponibles y luego atacarán los sistemas que aún no están parcheados. Como tal, es fundamental que las organizaciones se aseguren de que todos los sistemas tengan aplicados los parches más recientes, ya que esto reduce la cantidad de vulnerabilidades potenciales dentro del negocio para que un atacante las aproveche.

- **Autenticación de usuario**: acceder a servicios como RDP con credenciales de usuario robadas es una técnica favorita de los atacantes de ransomware. El uso de una fuerte autenticación de usuario puede dificultar que un atacante haga uso de una contraseña adivinada o robada.

- **Reduzca la superficie de ataque:** con el alto costo potencial de una infección de ransomware, la prevención es la mejor estrategia de mitigación de ransomware. Esto se puede lograr reduciendo la superficie de ataque abordando:
  - Suplantación de identidad
  - Vulnerabilidades sin parchear
  - Soluciones de acceso remoto
  - Malware móvil

- **Implemente una solución antiransomware**: la necesidad de cifrar todos los archivos de un usuario significa que el ransomware tiene una huella digital única cuando se ejecuta en un sistema. Las soluciones anti-ransomware están diseñadas para identificar esas huellas dactilares. Las características comunes de una buena solución anti-ransomware incluyen:
  - Amplia detección de variantes
  - Detección rápida
  - Restauración automática

RESUMEN DE VULNERABILIDAD CRÍTICA APACHE LOG4J

A finales de diciembre de 2021 publicamos una nota de prensa con los detalles de esta vulnerabilidad crítica y los siguientes pasos que debe realizar para proteger sus sistemas. En esta nota también publicamos el estado de las soluciones de seguridad que representamos en donde las pocas que se vieron afectadas emitieron prontamente una actualización para mitigar la vulnerabilidad.

Sin embargo, a mediados de 2022, aún existen preocupaciones de que esta vulnerabilidad pueda ser explotada en servidores y sistemas. Esto se da principalmente porque, en muchos casos, actualizar sistemas productivos es muy difícil a nivel de planificación y ventanas de mantenimiento. En este artículo resumiremos lo que debe saber de Log4j y las noticias relevantes acerca de esta vulnerabilidad crítica.

Resumen

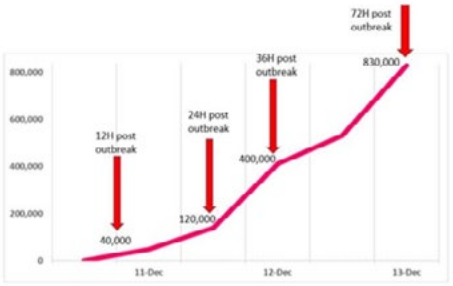
El 9 de diciembre de 2021, se informó de una vulnerabilidad de ejecución remota de código (RCE) en el paquete de registro de Apache Log4j 2 versiones 2.14.1 e inferior (CVE-2021-44228). Unos días después se publicó una nota donde indica que la versión Log4j 2.15 también era vulnerable.

Apache Log4j es la biblioteca de registro de Java más popular con más de 400.000 descargas de su proyecto GitHub. Es utilizado por una gran cantidad de empresas en todo el mundo, lo que permite iniciar sesión en un amplio conjunto de aplicaciones populares.

Aprovechar esta vulnerabilidad es simple y permite a los actores de amenazas controlar los servidores web basados en Java y lanzar ataques de ejecución remota de código. Todos los fabricantes a nivel global activamente validaron y parcharon sus soluciones y sistemas. Más información.

Los números detrás de una pandemia cibernética:

Precisamente un año después de SolarWinds Hack, el innovador ataque a la cadena de suministro que experimentó el mundo, y mientras las organizaciones aún luchan por proteger la cadena de suministro de software del riesgo de terceros, el exploit de vulnerabilidad Apache Log4j sorprendió a los equipos de seguridad. Más información.

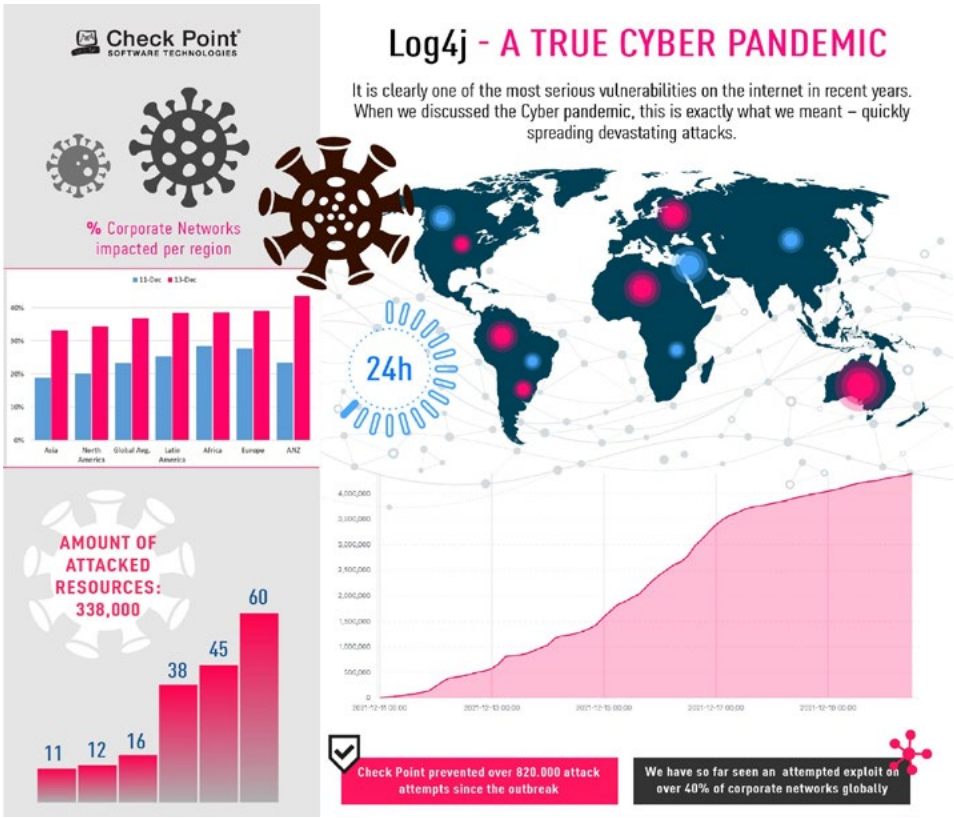


Una inmersión técnica de Log4j en la vida real

Check Point Research detectó recientemente numerosos ataques que explotaban la vulnerabilidad Log4j, que involucraba la minería de criptomonedas. Conozca el comportamiento del malware y cómo funciona, aprovechando la vulnerabilidad de Log4j, descargando la carga útil maliciosa y ejecutando un minero de monedas en el sistema vulnerable. Más información.

Log4j – Una verdadera ciberpandemia

Cuando hablamos de la pandemia cibernética, esto es exactamente lo que queríamos decir. Es claramente una de las vulnerabilidades más graves en Internet en los últimos años. Check Point Research fue testigo de la introducción rápida de nuevas variaciones del exploit original: más de 60 en menos de 24 horas. Ver infografía.



6 BEST PRACTICES FOR SECURING EMPLOYEE WORKSTATIONS EVERYWHERE

Recurso: Cyberark Blog, Mayo, 2022
https://www.cyberark.com/resources/blog/6-best-practices-for-securing-employee-workstations-everywhere

The future of work is "less about a place and more about people's potential," notes a recent Accenture study, which found that 63% of high-growth companies have already adopted "productivity anywhere."

Organizations around the world are fast embracing this hybrid workforce model that puts employee workstations at the edge, far beyond the "walls" of the traditional corporate network. Nearly all our CyberArk Remediation Services team's recent engagements reflect this reality: workstations are now one of the easiest ways for attackers to compromise identities, launch ransomware attacks, exploit privileged credentials and start moving toward sensitive IT systems and exfiltrate confidential data.

By the time incident response experts are engaged, attackers have proliferated throughout the environment. Many organizations believe that deploying endpoint security protections during a cyber attack is like putting storm windows on your house in the middle of a hurricane. Our remediation services engagements have consistently found that organizations can accelerate recovery efforts by implementing the following foundational Identity Security controls at the endpoint before an inevitable attack. These foundational controls include:

1. **Remove local admin rights.** Microsoft Windows, macOS and Linux administrator accounts are used to install and update workstation software, configure system settings and manage user accounts. Attackers target these privileged accounts to disable antivirus software or disaster recovery tools and launch ransomware and other types of malicious software. Moving local admin rights away from standard users and into a secure digital vault with credential rotation is the fastest and simplest step toward hardening employee workstations. It dramatically limits an adversary's reach, while minimizing the impact of unintentional (yet inevitable) employee errors, such as clicking on a phishing link.

2. **Enforce least privilege**. Employees often have a legitimate need to perform an action requiring administrative privileges. Just-in-time privileged access enable workers to perform certain specified tasks, based on policy, at the right time for the right reason — without requiring end-user action or help-desk intervention that can hinder productivity.

3. I**nstitute application control policies.** Blocking ransomware and other attacks at the endpoint requires more than just the ability to allowlist and denylist known applications. Organizations must be able to:

   - "Greylist" applications, such as sandboxing an unknown application and allowing it to run but not access the internet to reduce ransomware risks.
   - Implement advanced conditional policies, so workers can use trusted applications safely. For example, allow Excel to run but prohibit it from launching PowerShell to defend against BazarBackdoor malware.
   - Create comprehensive rules covering specific executables (i.e., by considering a hash, file name, file path) as well as groups of executables (i.e., default-allowing applications that are signed by a specific vendor, have a specific product name associated with them and originate from a designated trusted updater source).

4. **Protect cached credentials.** Credential theft is the No. 1 area of risk for organizations today. Many popular business applications allow credentials to be stored in memory, and many web browsers and password managers cache application and website credentials locally. Once logged in with these stolen credentials, attackers may try to circumvent single sign-on (SSO) solutions as well. Since threat actors can often retrieve cached credentials without ever needing admin privileges, having the ability to automatically detect and block credential harvesting attempts is a crucial endpoint security layer.

5. **Set up traps.** And speaking of detection, endpoint protection tools that support privilege deception functionality — such being able to create fake "honeypot" privileged accounts — can help flag would-be attackers right off the bat.

6. **Monitor privileged activities**. Attackers often fly under the radar, probing defenses and planning their next moves. By proactively monitoring privileged workstation activity, organizations can automatically identify and stop adversaries before they can move laterally, escalate privileges and inflict serious damage. Having complete records of privileged workstation activity is also key in streamlining compliance audits and speeding forensics investigations.

Inadequately protected employee workstations represents a common security gap — one I've seen too many times in my incident response work. If I could offer one piece of advice for organizations looking to shore up security against ransomware and other damaging attacks, it's this: don't wait — behave as if you've just been breached. By following key Identity Security-centric steps to mitigate risk, as well as separating workstations from servers and embracing a layered defense-in-depth strategy, your organization will be better equipped to isolate attacker activity, minimize impact, regain control of your environment and restore trust quickly and efficiently.

SOLUCIONES SEGURAS REALIZA DONACIÓN A LA UNIVERSIDAD TECNOLÓGICA DE PANAMÁ

Con el fin de potenciar el desarrollo de profesionales en tecnología y seguridad de la información en Panamá, Soluciones Seguras, compañía líder en ciberseguridad en Centroamérica se suma al Plan de Equipamiento que ha planteado la Coordinación de Facultad de Ingeniería de Sistemas Computacionales de la Universidad Tecnológica de Panamá UTP en su centro Regional de Chiriquí.

En esta oportunidad y como parte de sus acciones de Responsabilidad Social Empresarial (RSE), Soluciones Seguras a través de Eli Faskha, CEO de la compañía, hizo entrega de equipos para fortalecer las carreras de Redes y Ciberseguridad de la UTP en la sede de Chiriquí.

Durante la entrega, Eli Faskha expresó el interés de la compañía en sumarse a las acciones que la UTP lleva adelante y que benefician a sus estudiantes en su formación profesional para ser líderes en la seguridad, privacidad, protección de datos y las redes.

El correo electrónico continúa siendo el canal más común para ciberataques, y el vehículo de entrega número uno de malware. En la actualidad, más del 90 % de los ataques a organizaciones vienen de un correo malicioso. Un solo email de este tipo puede poner en riesgo a toda la organización además de una pérdida de datos importante.

De acuerdo al último reporte de inteligencia de amenazas de Check Point, partner de Soluciones Seguras, las empresas guatemaltecas son atacadas un promedio de 1,727 veces por semana en los últimos 6 meses; siendo el principal sector atacado el financiero y banca. En los últimos 30 dias, el 86% de los archivos maliciosos en el país se entregaron por correo electrónico.

La transición al trabajo remoto ha traído como consecuencia un aumento en la cantidad de ataques provenientes de correos electrónicos y su tasa de éxito, por lo que la seguridad del correo electrónico es una necesidad para todas las organizaciones

En esa línea, Soluciones Seguras, compañía líder en ciberseguridad en Centroamérica, realizó junto a Check Point. su evento: “Cybersecurity Break”. sobre cómo implementar una seguridad de correo de última generación.

En esta ocasión, la actividad dirigida a clientes de la compañía, fue en un formato de taller de cocina, en el que junto a los expertos de Soluciones Seguras y de Check Point exploraron cómo contener los ataques a correos corporativos entre otras preocupaciones de ciberseguridad.

En el marco del Día Mundial del Internet, Soluciones Seguras, brinda 6 consejos prácticos que permitirán a los usuarios una conectividad más segura.

En la actualidad no es posible imaginar un mundo sin estar conectado a Internet. El acceso a la red ha tomado especial relevancia desde el inicio de la pandemia como herramienta fundamental para trabajar, educarse, realizar transacciones en línea, comunicarse y entretenerse; convirtiéndose en una parte cada vez más vital de nuestra vida cotidiana.

De acuerdo a Statista, portal estadístico internacional, en abril de 2022 el número de usuarios de internet en todo el mundo se situó en cinco mil millones. Específicamente, Panamá cuenta con 2,94 millones de usuarios activos de internet, según cifras de este año. Esto contabiliza que, aproximadamente el 68% de la población tiene algún tipo de conexión a Internet, principalmente por medio de un dispositivo móvil.

"El incremento exponencial del intercambio de datos a través de internet genera nuevas ciberamenazas. Esto convierte a los panameños en un blanco perfecto para que los cibercriminales ataquen. Tomando eso en cuenta, los ciberataques a organizaciones continúan en aumento y sofisticación. Esta tendencia hizo que, en estos últimos 6 meses, Panamá experimentara un promedio de 1.380 ataques semanales por organización, lo que representa un aumento de un poco más del 100% desde abril de 2021. expresa Eli Faskha, CEO de Soluciones Seguras.

Los principales delitos digitales que los usuarios y empresas deben enfrentar son: el robo de datos, phishing, malwares, ataques de ransomware y el cryptojacking, entre otros.

En este contexto, Soluciones Seguras se suma a la celebración del Día Mundial de Internet el próximo 17 de mayo, una fecha que tiene como objetivo resaltar el poder de Internet en el desarrollo de los países. Esta efeméride es aún más relevante en 2022 por ser el momento donde aumentan las demandas de conectividad e incrementan las amenazas cada día.

Con el fin de promover el acceso seguro de los usuarios en internet, Soluciones Seguras, en su compromiso con la seguridad de la información, brinda 6 recomendaciones de ciberseguridad:

- **Actualizar de forma periódica los dispositivos, aplicaciones y programas** para asegurarse de que no han sido infectados por malware. Los fabricantes de software lanzan constantemente actualizaciones y parches de mejora para corregir fallos de seguridad
- **Mejorar la gestión de contraseñas**. Gran parte de la seguridad se establece por medio del acceso controlado a los dispositivos a través de claves de acceso. Es importante que las mismas sean robustas y que contengan combinaciones de números, letras y signos. Se recomienda emplear un gestor de contraseñas y no compartirlas con nadie. Usar múltiples factores de autenticación (SMS, huella digital, reconocimiento facial, o App de autenticación)
- **Evitar las redes públicas**. Al conectarnos a redes WiFi públicas, las operaciones quedan expuestas, vulnerando los datos, tráfico e identidad ante los delincuentes cibernéticos. Si por alguna razón especial debe utilizar este tipo de red, evite realizar transacciones bancarias o consultar datos sensibles. Además, asegúrese de cerrar todas las sesiones una vez que haya finalizado el trabajo y desactivar su dispositivo
- **Cuidado con las redes sociales**. Las redes sociales ofrecen una exposición a su vida personal y privada. Como cualquier plataforma donde se comparten datos, es importante configurar la privacidad y ver hasta qué punto están sus datos expuestos. Nunca acepte conexiones de personas que no conoce, y nunca publique información de identificación personal, como por ejemplo, el lugar donde vive.
- **Instalar un antivirus para evitar posibles amenazas.** Los antivirus son vitales para proteger nuestros dispositivos y computadoras para que estén seguros y actualizados.
- **Manténgase informado**. No hay peor enemigo que la desinformación. Mantenerse actualizado sobre las tendencias globales cibernéticas le brindarán una mejor base de conocimiento para mantener la seguridad cibernética suya o de su empresa.

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.

Soluciones Seguras es patrocinador y participa activamente en las Giras Regionales TECHDAY 2022 "La Gira que promueve la tecnología del futuro" e INFOSECURITY 2022 "A new World Tour"

CURSOS VIRTUALES 2022

CCSA

CHECK POINT

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

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

Check Point Certified

VSX SPECIALIST

Habilidades importantes para implementar seguridad de red virtual

CCCS

CHECK POINT

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

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

SOLUCIONES SEGURAS
TRAINING CENTER

CHECK POINT
PARTNER
ELITE

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 PROTECCION 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