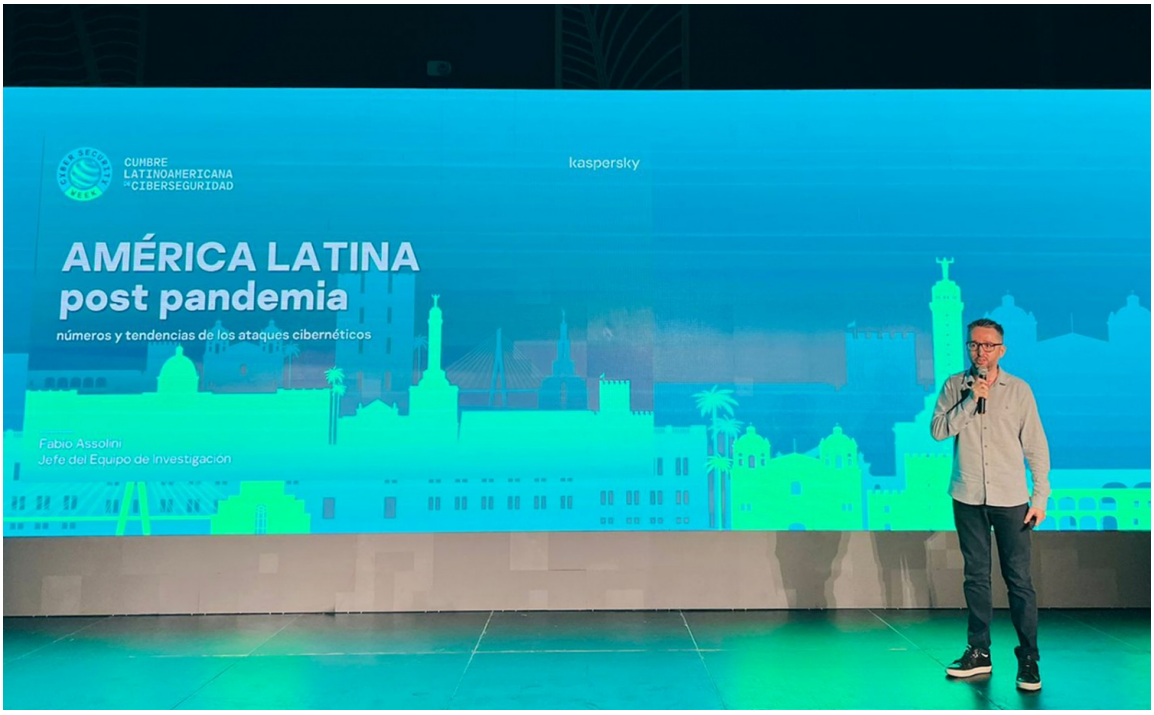
bafing

BOLETÍN
Informativo digital

Nuestra misión es mantenerlo informado con las últimas noticias de investigación, productor y actualidad tecnológica; para mantenerlo al día sobre las tendencias nacionales y globales, con énfasis en la ciberseguridad, eHealth y Smart Buildings.

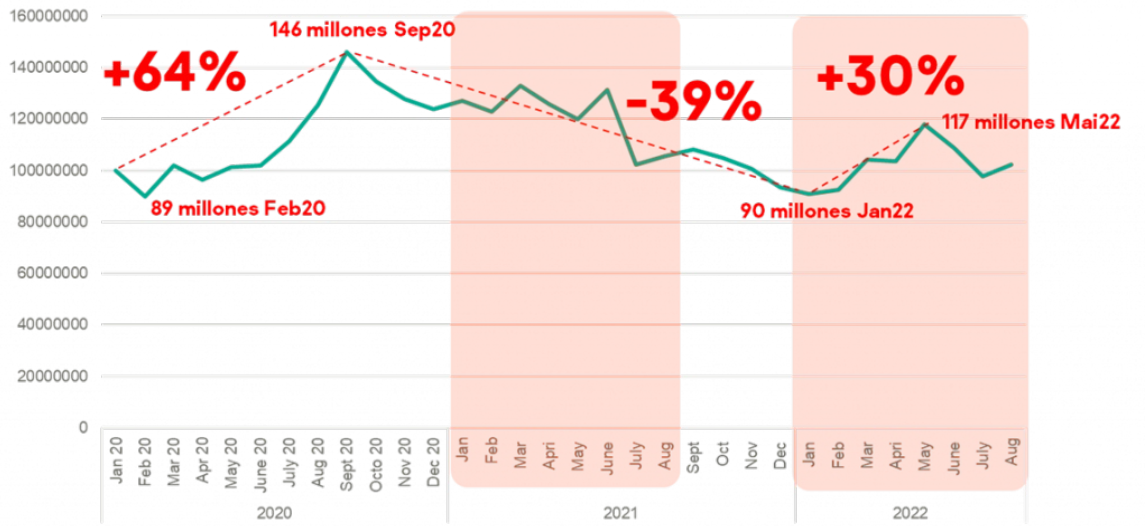
Los ataques financieros crecen en América Latina y aumenta la preocupación por el uso de la piratería

Kaspersky registra más de 2,300 ataques de malware por minuto en la región, mientras las estafas por phishing se disparan en todos los países.



El Panorama de Amenazas de Kaspersky (que analizó datos de enero a agosto de 2021 y el mismo periodo de 2022) reveló que, en 2022, se bloquearon 2,366 ataques de malware y 110 mensajes fraudulentos (phishing) por minuto en América Latina. Los resultados también indican que la región se ha convertido en un importante centro de amenazas financieras a nivel mundial y que el uso de la piratería ha vuelto a ser uno de los principales vectores de infección.

De acuerdo con el estudio, los ciberataques en la región han variado mucho durante la pandemia. Entre enero y septiembre de 2020, se produjo un aumento de 64% en el bloqueo de ataques con malware. Le siguió un descenso del 39% entre septiembre de 2020 y enero de 2022, cuando la actividad maliciosa volvió a los niveles previos a la pandemia. Sin embargo, entre enero y mayo de este año, se registró un aumento del 30%. Considerando los primeros ocho meses de 2022, registramos un total de 817 millones de intentos de ataques en América Latina, lo que representa 2,366 bloqueos por minuto.



Al observar los datos por países, Brasil se destaca como el mercado con más ataques de malware, con 1,554 intentos por minuto o el 65% de todos los bloqueos de la región. Le siguen México con 298 intentos por minuto, Perú con 123 ataques bloqueados por minuto, Colombia y Ecuador con 84, respectivamente, Argentina con 30 y Chile con 28 intentos/minuto. Al detallar las 20 principales amenazas que afectan a los internautas latinoamericanos, la piratería aparece como una de las principales preocupaciones, ocupando siete posiciones de la lista. Le sigue el adware (que muestra publicidad no deseada) en los tres primeros lugares.

> “Desgraciadamente, hemos comprobado que el uso de la piratería continúa siendo uno de los principales vectores de infección. Es decir, un sistema ‘crackeado’ abre las puertas del equipo infectado a otros delincuentes. Aunque puede que esta tendencia sea un reflejo de la crisis económica que afecta a las personas y a las empresas, sobre todo a las más pequeñas, debemos advertir que el ahorro con licencias de software no justifica el riesgo de ser víctima de otras estafas, como el ransomware o el robo de datos financieros”, advierte Fabio Assolini, director del Equipo de Investigación y Análisis de Kaspersky para América Latina.

Continúa leyendo aquí

Fuente: Kaspersky

Kaspersky y Bafing, proponen estrategias de ciberseguridad innovadoras, rumbo al 2023

Bafing y Kaspersky reafirman su compromiso en el desarrollo de la ciberseguridad en el Perú para este 2023.

El pasado lunes 21 de noviembre, un equipo de Kaspersky estuvo en Lima visitando las oficinas de Bafing. Durante su encuentro junto a nuestro CEO, el Ing. Paolo Bisso, y nuestro Gerente comercial, Richard Concha, se propusieron nuevas estrategias en las cuales destacan la visión del futuro de las amenazas persistentes avanzadas. Con ello se definió, por parte de Kaspersky, los cambios que surgirán en el panorama de amenazas el próximo año 2023.

> “Contar con una adecuada preparación es equivalente a contar con una mejor resiliencia y se espera que evaluación del futuro realizada por Kaspersky permita a los defensores fortalecer sus sistemas y bloquear los ataques cibernéticos de manera más efectiva” afirma Paola Barrera, Territory Channel Manager Sur de Latinoamérica en Kaspersky Lab.

Continúa leyendo aquí

Fuente: Bafing

Las 20 contraseñas más usadas en 2022 son también las menos recomendadas

Un informe de 2022 reveló cuáles son las contraseñas más populares a nivel global en 2022 y “password”, “123456” y “123456789” son las tres más utilizada en el mundo.

A diferencia de lo que venía sucediendo, “123456” ya no es la más utilizada, sino que su lugar lo ocupó otra contraseña que constantemente dice presente en este reporte: “password”.

La lista elaborada por NordPass con las 200 contraseñas más comunes surge del análisis de una base de datos de 3TB que contienen contraseñas que quedaron expuestas en incidentes de seguridad. Esta información fue recopilada gracias a la colaboración de investigadores independientes especializados en investigación de incidentes.

Como se puede apreciar en la siguiente imagen, la tabla está ordenada de acuerdo a la cantidad de veces que una misma clave se fue utilizada, incluye el número de veces que estaba presente en la base de datos, y el tiempo en que tardaría en ser descifrada a través de un ataque de fuerza bruta.

RANK	PASSWORD	TIME TO CRACK IT	COUNT
1	password	< 1 Second	4,929,113
2	123456	< 1 Second	1,523,537
3	123456789	< 1 Second	413,056
4	guest	10 Seconds	376,417
5	qwerty	< 1 Second	309,679
6	12345678	< 1 Second	284,946
7	111111	< 1 Second	229,047
8	12345	< 1 Second	188,602
9	col123456	11 Seconds	140,505
10	123123	< 1 Second	127,762
11	1234567	< 1 Second	110,279
12	1234	< 1 Second	106,929
13	1234567890	< 1 Second	105,189
14	000000	< 1 Second	102,636
15	555555	< 1 Second	98,353
16	666666	< 1 Second	91,274
17	123321	< 1 Second	83,241
18	654321	< 1 Second	81,231
19	7777777	< 1 Second	74,233
20	123	< 1 Second	60,795

Otro dato interesante que incluye este reporte es una clasificación de las contraseñas más populares en categorías como deportes, nombres de artistas o grupos musicales, comidas, videojuegos, películas o autos, entre otros. Lo que muestra esto es un patrón que muchas veces siguen las personas a la hora de elegir una contraseña para que sean fáciles de recordar. Sin embargo, esto las convierte en fáciles de predecir. Sobre todo en ataques de fuerza bruta automatizados en los que los cibercriminales utilizan software para probar múltiples combinaciones de direcciones de correo y contraseñas en segundos.

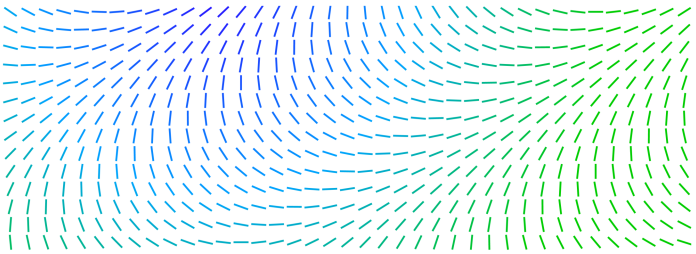
Los resultados demuestran que sigue siendo fundamental concientizar a las personas acerca de la importancia que tiene crear contraseñas largas, difíciles de predecir y que sean únicas para cada cuenta o servicio online. Además, las personas deben saber que todo esto puede lograrse utilizando en la computadora o en el teléfono un administrador de contraseñas, ya que estos servicios contemplan todas estas necesidades. Por último, recordamos a todos la importancia de activar la autenticación en dos pasos en todos los servicios que utilizan para que la seguridad de sus cuentas no dependa únicamente de la contraseña.

Continúa leyendo aquí

Fuente: WeLiveSecurity by ESET

La actividad del ransomware se duplica en la industria del transporte y el envío

Trellix publicó hoy The Threat Report: Otoño de 2022 desde su Centro de Investigación Avanzada, que analiza las tendencias de ciberseguridad desde el tercer trimestre de 2022.



Trellix

We bring security to life.

El informe incluye evidencia de actividad maliciosa vinculada a ransomware y actores de amenazas persistentes avanzadas (APT) respaldados por estados nacionales. Examina la ciberactividad maliciosa, incluidas las amenazas al correo electrónico, el uso malicioso de herramientas de seguridad legítimas de terceros y más. Resultados clave:

La actividad de ransomware en EE. UU. lidera el grupo

Solo en EE. UU., la actividad de ransomware aumentó un 100 % trimestre tras trimestre en transporte y envío. A nivel mundial, el transporte fue el segundo sector más activo. También se detectaron APT en el transporte más que en cualquier otro sector.

Alemania vio las detecciones más altas

Alemania no solo generó la mayor cantidad de detecciones de amenazas relacionadas con los actores APT en el tercer trimestre (29% de la actividad observada), sino que también tuvo la mayor cantidad de detecciones de ransomware.

Actores de amenazas emergentes escalados

El actor de amenazas vinculado a China, Mustang Panda, tuvo los indicadores de amenazas más detectados en el tercer trimestre, seguido por APT29 vinculado a Rusia y APT36 vinculado a Pakistán.

Ransomware Evolved

Phobos, un ransomware que se vende como un kit completo en la clandestinidad ciberdelincuente, ha evitado los informes públicos hasta ahora. Representó el 10% de la actividad global detectada.

Las vulnerabilidades antiguas continuaron prevaleciendo

Las vulnerabilidades de años continúan siendo vectores de explotación exitosos. Trellix observó que las vulnerabilidades del Editor de ecuaciones de Microsoft compuestas por CVE-2017-11882, CVE-2018-0798 y CVE-2018-0802 son las más explotadas entre los correos electrónicos maliciosos recibidos por los clientes durante el tercer trimestre.

Uso malicioso de Cobalt Strike

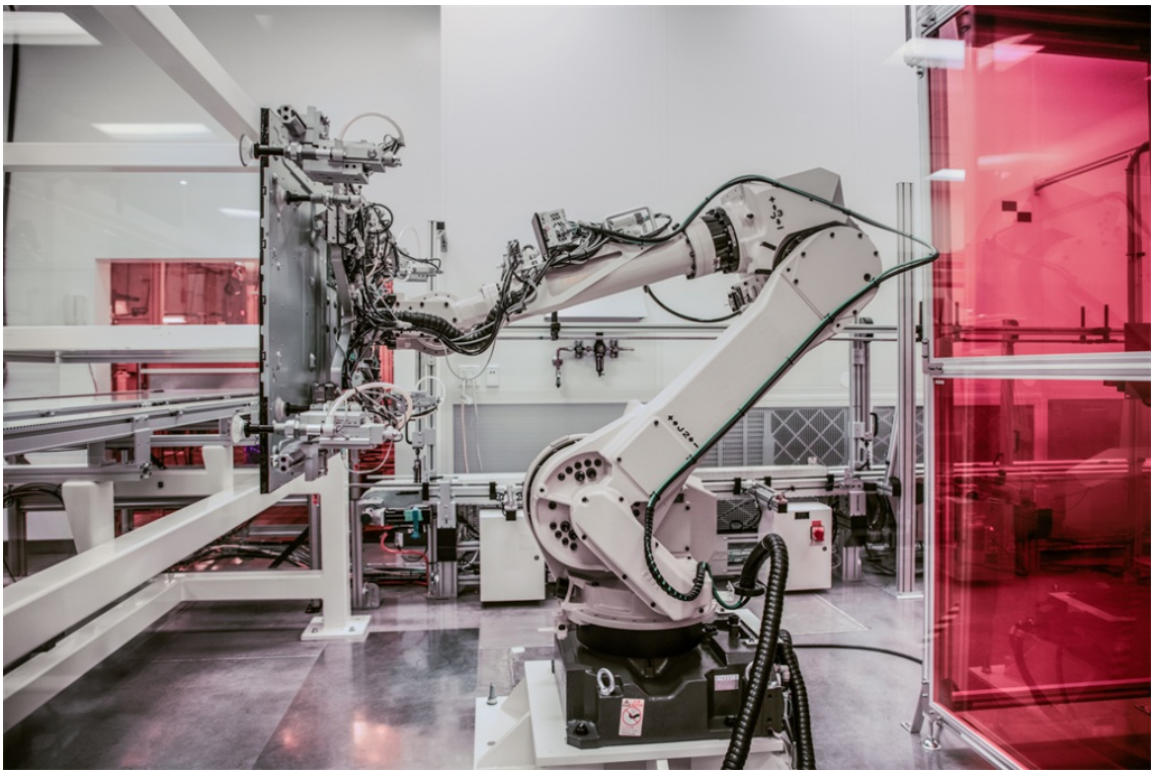
Trellix observó que Cobalt Strike se usó en el 33 % de la actividad de ransomware global observada y en el 18 % de las detecciones de APT en el tercer trimestre. Cobalt Strike, creada para emular escenarios de ataque para mejorar las operaciones de seguridad, es una herramienta favorita de los atacantes que reutilizan sus capacidades con intenciones maliciosas.

Continúa leyendo aquí

Fuente: Trellix

Hacer más con menos: cómo las organizaciones dan forma al futuro con una fuerte postura digital

A pesar de los desafíos económicos y sociales, las organizaciones de todas las industrias continúan adaptándose a la dinámica del mercado en evolución para satisfacer las necesidades de los clientes.



Cisco y Microsoft ofrecen la opción de ejecutar Microsoft Teams de forma nativa en los dispositivos Cisco Room and Desk. 3M ofrece su aplicación Post-It ® en la tienda de aplicaciones Teams, que permite a los usuarios digitalizar notas escritas a mano. Haleon, con sede en el Reino Unido está permitiendo que las personas ciegas o con problemas de visión escuchen las etiquetas de más de 1500 productos de salud de consumo en los EE. UU. y el Reino Unido con Microsoft Seeing AI.

Con una aplicación global reinventada que se ejecuta en Azure, la NBA ofrece a los fanáticos nuevas funciones de personalización, como contenido de pared a pared de cada juego de la NBA y acceso tras bambalinas sin precedentes a jugadores y equipos. Y apenas la semana pasada, el banco global con sede en Suiza UBS anunció que trasladaría más del 50 % de sus aplicaciones a Azure como su principal plataforma en la nube para impulsar aún más la modernización de su patrimonio tecnológico global.

Fue genial conectarme con tantos de ustedes en persona y virtualmente en Ignite, la reunión anual de desarrolladores y profesionales de TI de Microsoft. Si bien los asistentes reconocieron el impacto comercial de los desafíos macroeconómicos actuales, siguen comprometidos con maximizar el valor de sus inversiones digitales mediante la generación de economías de escala con Microsoft Cloud.

Hacer más con menos es más importante que nunca, ya que las organizaciones se enfrentan a la incertidumbre y dan forma al futuro. Las tecnologías impulsadas por la nube, como la inteligencia artificial (IA), el Internet de las cosas (IoT) y el

aprendizaje automático, ofrecen a las organizaciones una agilidad y eficiencia incomparables, aceleran la innovación y hacen que la seguridad sea integral mientras impulsan el crecimiento y avanzan en los compromisos de sostenibilidad.

Judson Althoff, vicepresidente ejecutivo y director comercial.

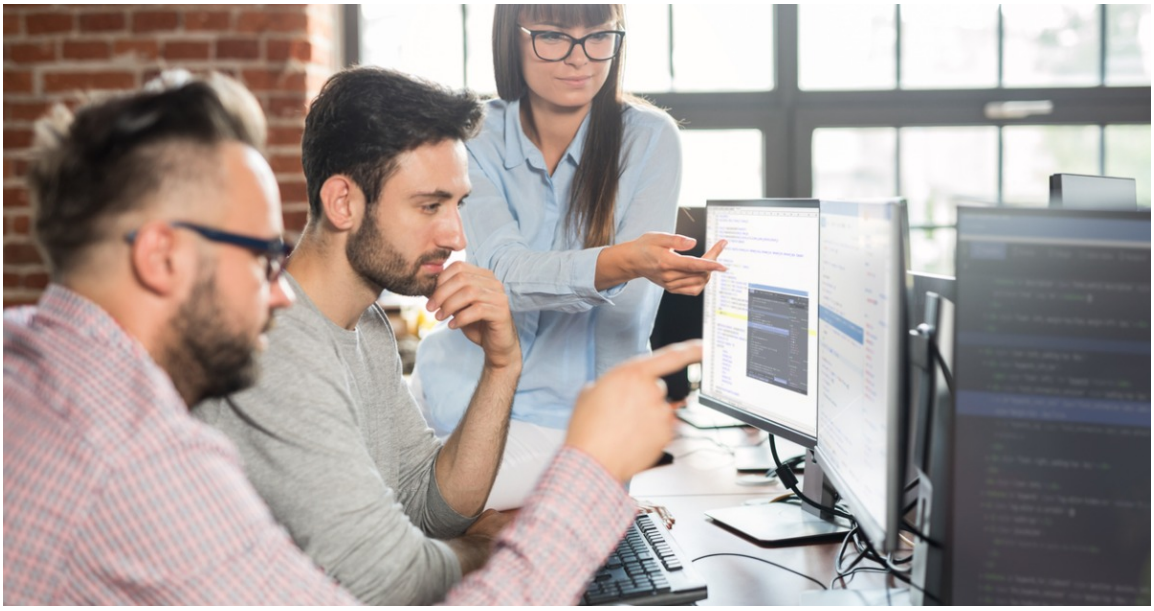
Continúa leyendo aquí

Fuente: Microsoft

---

5 mejores prácticas de higiene de ciberseguridad que todo MSP debe seguir

La ciberseguridad no es un producto sino un viaje. Requiere más que soluciones independientes para brindar la higiene básica de ciberseguridad que las empresas necesitan en el entorno actual.



1. Establece lo que quieres proteger. Los MSP deben ayudar a los clientes a reconocer que tienen múltiples activos y aplicaciones de TI que necesitarán una protección sólida. Eso incluye bases de datos de clientes, sistemas de pago, sistemas de pedidos, herramientas de CRM, interfaces de aplicaciones web, dispositivos móviles e incluso la LAN inalámbrica en el almacén.
2. Cree anillos concéntricos de seguridad alrededor de sus datos. asegúrese de tener una estrategia de defensa en profundidad, a veces llamada "cadena de muerte cibernética". Si por alguna razón su sistema de seguridad de punto final o firewall no detecta algo, ¿qué tiene para detectarlo? Lockheed Martin desarrolló la "cadena de eliminación cibernética" para identificar, prepararse, atacar y destruir un objetivo (en este caso, un ataque cibernético). Su paquete de seguridad debe incluir herramientas que puedan buscar vulnerabilidades, detectar instrucciones, aislar a los atacantes antes de que puedan moverse a través de una red y mitigar el daño.
3. La visibilidad es clave: habilite el monitoreo en tiempo real. Necesita saber si tiene un problema; es por eso que monitorear su entorno es básicamente esencial. Detecte incidentes cibernéticos las 24 horas del día, los 7 días de la semana aprovechando un centro de operaciones de seguridad de primer nivel, que ayudará a mantener a los MSP por delante de posibles amenazas en sus redes y dentro de las redes de los clientes. Este servicio de valor agregado es esencial para prevenir el ransomware y otros tipos de ataques.
4. Reduzca sus tiempos de respuesta. Identificar rápidamente un ataque es una

parte de la ecuación. Los MSP también deben asegurarse de que se alerte al personal adecuado y que los procesos de mitigación entren en acción lo más rápido posible. Cierto nivel de automatización en la solución de seguridad o la solución de monitoreo puede ayudar aquí, pero también es fundamental estructurar las notificaciones y tener un plan de acción. Para un MSP, el tiempo de respuesta será una de las métricas más importantes que usarán sus clientes para medir su valor cuando ocurra un ataque.

5. Estandarizar sobre los marcos aceptados para la ciberseguridad. Siga los estándares de ciberseguridad establecidos, como el marco de ciberseguridad del NIST . Un marco no es una solución en sí mismo, pero proporcionará una manera para que los MSP y sus clientes midan el rendimiento contra esas mejores prácticas y mejoren continuamente.

Continúa leyendo aquí

Fuente: Barracuda

Contáctenos

Central: +511 2259900 anexo 110
Equipo de Marketing: igrandez@bafing.com o al +51 969454618
Command Center y SOC: helpdesk@bafing.com o al +51 971500877

www.bafing.com

Facebook Síguenos **Twitter** Síguenos **LinkedIn** Síguenos

Acerca de Bafing

Somos una empresa con más de 27 años de experiencia en el mercado de Tecnologías que ofrece soluciones muy especializadas en Ciberseguridad, eHealth y Smart Buildings.