SOLUCIONES SEGURAS
CYBERSECURITY
MAGAZINE

Edición No. 19

REVISTA REGIONAL DE CIBERSEGURIDAD

MUNDIAL DE FÚTBOL Y
AMENAZAS CIBERNÉTICAS

EN ESTA EDICIÓN:

CYBERSECURITY REGIONAL TOUR 2022
PANAMÁ, COSTA RICA, GUATEMALA

CÓMO REDUCIR EL RIESGO DE
SER VÍCTIMA DE RANSOMWARE

PROYECTO
NO-MORE-RANSOM

Y MÁS...

2022
VOLUMEN 4

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

Hola queridos lectores, gracias otra vez por darnos un tiempo de su día para leer esta revista que con mucho esmero publicamos para ustedes.

El mes de diciembre siempre es un mes especial, y este creo que aún mas de lo normal.

Primero, llegan las fiestas de fin de año, que son momentos para compartir en familia y con amigos, para reflexionar sobre el año que hemos tenido y ponernos metas para el próximo año. ¡Le deseamos lo mejor a todos en este año venidero 2023!

Hace poco menos de 1 mes, realizamos después de casi 3 años nuestro Cybersecurity Regional Tour en Panamá, Costa Rica y Guatemala, que fue un completo éxito. Casi 200 participantes en los diferentes países pudieron compartir con nosotros y con nuestros socios de negocios tardes llenas de valiosa información y amenas veladas. Personalmente me sentí sumamente honrado de ver a tantas personas que no veía por casi 3 años, y conocer a muchas nuevas, incluyendo nuevo personal de Soluciones Seguras que ha seguido creciendo en todos los países. Mi agradecimiento otra vez a todo el personal de la empresa, a todos los fabricantes que nos acompañaron en estos eventos, y por supuesto a nuestros usuarios que son al final el motivo por el que todos estamos aquí.

Pero hay otro tema interesante este mes: El Mundial de Futbol Catar 2022. Aunque admito que no sigo de cerca el deporte, no hay forma de evitar emocionarse viendo a los mejores equipos del mundo jugando por ser el mejor. Pero lo que más me ha llamado la atención es la cantidad de sorpresas que se han dado. Equipos y países considerados como los mejores del mundo, con estrellas reconocidas que ganan cientos de millones de dólares, han sido vencidos por equipos en juegos que a veces son difíciles de creer. ¿Y por qué saco a relucir esto? Porque la analogía con la ciberseguridad es muy potente:

Aún el mejor equipo, con los mejores jugadores y el mayor presupuesto, a veces es sorprendido por grupos pequeños que juegan muy bien ese día, o cuando el equipo dejo una puerta abierta que no debería. Todo puede pasar (y muchas veces pasa). A nosotros como expertos en ciberseguridad también nos puede pasar, por lo que siempre tenemos que estar atentos y tener planes de contingencia. Los mejores equipos pueden sufrir derrotas, pero lo importante es la reacción y que una derrota no afecte a la empresa a mediano ni largo plazo. Al final todos somos humanos, errores existen, pero lo importante es aprender de ellos.

No los dejo sin antes desearles un año 2023 lleno de felicidad, éxitos, mucha salud, ¡y que disfruten en compañía de sus seres queridos!

¡Suerte!

Eli Faskha

CEO

SOLUCIONES SEGURAS CYBERSECURITY REGIONAL TOUR 2022

Soluciones Seguras, compañía líder en ciberseguridad en Centroamérica, realizó su evento anual de cierre de año: “Cybersecurity Regional Tour 2022” en Panamá, Costa Rica y Guatemala, junto a sus socios de negocios y clientes. En este evento regional, realizado en el marco de la celebración del Día Internacional de la Seguridad de la Información, se presentaron las soluciones de ciberseguridad que ayudarán a afrontar los desafíos más difíciles en el campo digital, con conferencias y panelistas expertos en defensa.

En cada parada del Cybersecurity Regional Tour se contó con la participación de clientes, directivos, gerentes de distintas empresas del área púbica y privada; quienes pudieron conocer de primera mano las tendencias en protección de la infraestructura de TI, integridad, privacidad, así como las nuevas tecnologías para prevención de amenazas.

El tour inició en Ciudad de Panamá el 15 de noviembre del 2022 con la especial presencia del ex-portero de la selección local, Jaime Penedo; quién compartió con los presentes su experiencia en el campo de fútbol y haciendo referencia a la importancia de tener una estrategia de defensa para prevenir escenarios inesperados. Siguió el 16 de noviembre en San José, Costa Rica, y el 17 de noviembre en Ciudad de Guatemala.

Así mismo, los expertos de Soluciones Seguras, junto a las principales empresas aliadas, también presentaron el panorama de cómo evolucionarán las ciberamenazas en el 2023 y las opciones para hacer frente a la gran complejidad de ataques.

Al finalizar la jornada de actualización, Soluciones Seguras, en agradecimiento a sus clientes, socios de negocio, invitados especiales y colaboradores ofreció su tradicional cóctel de fin de año, donde los invitados disfrutaron de una noche acompañada de cócteles, buena música, entretenimiento, y sorteos.

Con casi 200 participantes, el Cybersecurity Regional Tour cierra con gran éxito el año 2022, para iniciar el 2023 y hacer frente a los retos para minimizar los riesgos de ciberseguridad durante el próximo año.

¡GRACIAS POR SER PARTE DEL ÉXITO DEL SOLUCIONES SEGURAS CYBERSECURITY TOUR 2022!

MUNDIAL DE FÚTBOL Y AMENAZAS CIBERNÉTICAS

El desarrollo de la Copa del Mundial de Fútbol Qatar 2022, inevitablemente, atrae la atención de los ciberdelincuentes y otros actores de amenazas, quienes, como se ha visto una y otra vez, son expertos en apropiarse de eventos significativos e incorporarlos en sus campañas maliciosas.

Investigación

El equipo de investigación de Digital Shadows Photon ha estado rastreando amenazas cibernéticas que surgen alrededor de la Copa del Mundo durante los últimos 90 días utilizando un sistema de alerta especialmente creado. Descubrieron que, en términos generales, las amenazas al evento se pueden organizar en cuatro categorías: protección de marca, amenaza cibernética, protección física y fugas de datos. De estos, la mayor parte de la actividad observada se relaciona con la categoría de amenazas cibernéticas.

Los actores de amenazas motivados financieramente a menudo colocan URL maliciosas que falsifican estos eventos en sitios fraudulentos, con la esperanza de maximizar sus posibilidades de estafar a los usuarios de Internet desprevenidos para obtener una ganancia rápida e ilícita. Entre algunos descubrimientos relevantes del equipo se encuentran: más de 170 dominios que se hacen pasar por propiedades en línea oficiales de la Copa Mundial, muchos de ellos sitios web de phishing destinados a robar los datos de sus víctimas; 53 aplicaciones móviles maliciosas, utilizadas para instalar adware, robar datos y credenciales, e instalar cargas de malware adicionales (payloads); y docenas de páginas de redes sociales fraudulentas, algunas de las cuales se utilizan para difundir estafas piramidales o marketing de afiliados dudosos.

La investigación también señaló la posibilidad de una actividad cibernética más sofisticada en torno a la Copa del Mundo. Por ejemplo, durante su investigación, el equipo encontró varios anuncios de registros de datos sin procesar que habían sido robados mediante el malware Redline. Redline es un ladrón de información que se utiliza para recopilar pares de credenciales, datos de autocompletado e información de tarjetas de crédito de los navegadores web de sus víctimas. También puede recopilar otros datos técnicos sobre el sistema comprometido.

Algunos de los registros parecen estar relacionados con los activos de la Copa Mundial. Dicha información podría usarse para apoderarse de las cuentas de las víctimas y realizar más actividades maliciosas.

El grupo indica también que observaron docenas de páginas de redes sociales que se hacen pasar por activos pertenecientes a la Copa del Mundo Qatar 2022. La mayoría de estas páginas albergan contenido inofensivo; sin embargo, también se identificaron varias páginas de Facebook que explotan la marca y los logotipos de la Copa Mundial de Qatar 2022 para difundir estafas como esquemas piramidales, entre otros. Las páginas de redes sociales no son la única preocupación cuando se trata de robo de marcas y logotipos. También se puede suplantar a VIP y ejecutivos para realizar ataques de ingeniería social.

Análisis de suplantación de identidad

Los ataques de phishing se encuentran entre los ataques de ingeniería social más comunes y los actores de amenazas los usan ampliamente en organizaciones deportivas internacionales. En general, los ataques de phishing son bastante dañinos porque el nivel de conciencia de seguridad cibernética de la sociedad es bajo. Este daño aumenta exponencialmente en organizaciones con muchos fanáticos entusiastas, como la Copa Mundial de la FIFA. Los ataques de ingeniería social tienen como objetivo obtener información personal o privada, acceso y credenciales utilizando técnicas de manipulación aprovechando el error humano.

Hay muchos tipos de ataques de ingeniería social, pero los actores de amenazas utilizan con mayor frecuencia las técnicas de phishing. Los ataques de phishing están diseñados para robar las contraseñas de las víctimas, la información de identificación personal (PII) u otros datos confidenciales mediante el envío de mensajes falsos que ofrecen boletos gratis, obsequios, obsequios, descuentos u otros artículos atractivos. Los ataques de phishing pueden ocurrir a través de SMS, publicaciones en redes sociales, correos electrónicos, etc.

Los actores de amenazas suelen utilizar dos estrategias al crear dominios de phishing:

Typosquatting:

Su objetivo principal es engañar a la víctima para que visite sitios web maliciosos con cambios menores en los nombres originales de los sitios web. Durante los eventos de FIFA, se pueden ver dominios creados usando typosquatting. Ej. fifawordcup2022 (cambiando la "L" por "D") ó fifa2022 (usando la letra O en vez del número 0).

Dominios genéricos de nivel superior (TLD):

Otra táctica de phishing es utilizar un dominio de nivel superior diferente a los tradicionales (.com, .org, .gov, etc.), pero con las mismas palabras claves que utiliza la organización. Ej. fifa2022[.]pro, fifa2022[.]online, fifaworldcup2022[.] world, etc.

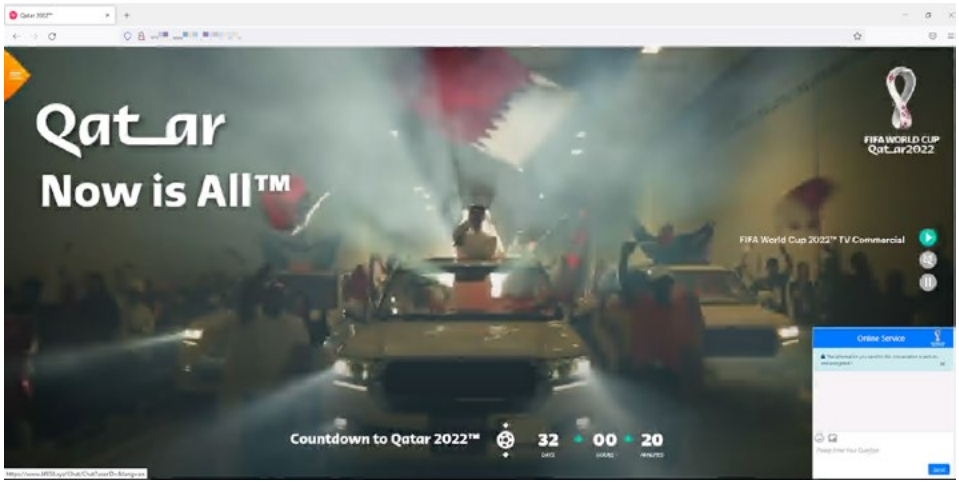
Conclusión

En definitiva, la Copa Mundial de la FIFA 2022 en Qatar será blanco de ciberdelincuentes de alto nivel, como cualquier otro evento de gran magnitud. En este sentido, todos los espectadores y organizaciones participantes en el evento deben tomar precauciones para protegerse de los riesgos cibernéticos.

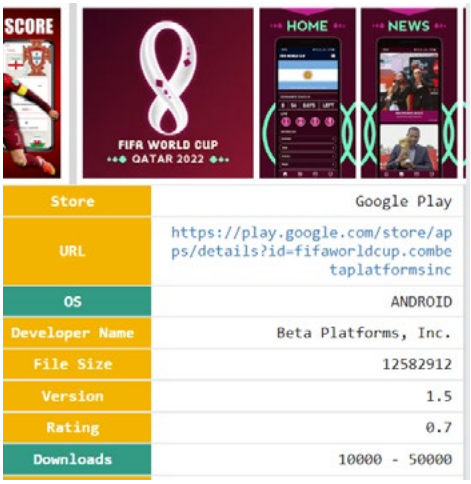
El país anfitrión, Qatar, estableció un Comité Nacional de Seguridad Cibernética en 2013. En 2014, publicaron un documento de Estrategia Nacional de Seguridad Cibernética, abordando planes de acción, implementaciones e identificando posibles amenazas en el panorama cibernético de Qatar. Qatar se ha posicionado para tener sólidos controles de seguridad cibernética a lo largo de los años para garantizar la seguridad cibernética del evento.

Como otro objetivo de las amenazas cibernéticas potenciales, todos los espectadores de este evento deben ser conscientes de los siguientes puntos:

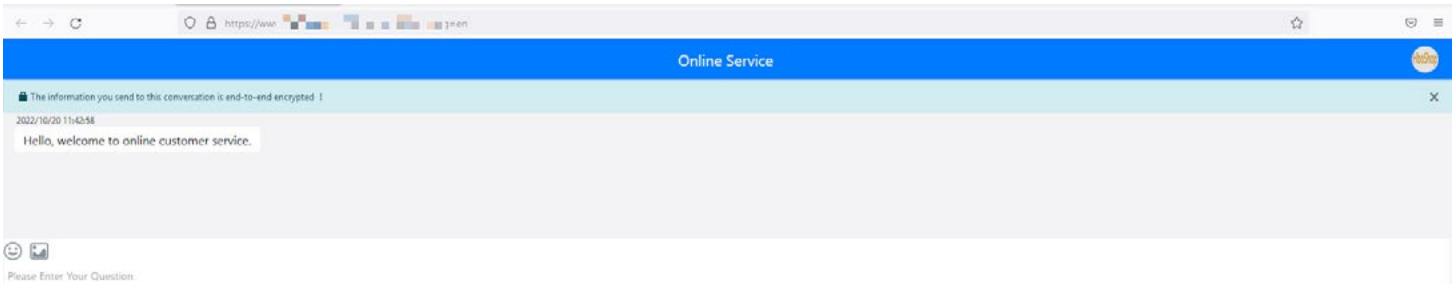
- Mantener la higiene general de la seguridad cibernética (Usar software actualizado, antivirus, etc.)
- Conocer las numerosas estrategias de ingeniería social que emplean los ciberdelincuentes.
- Ser consciente de la comunicación digital y los enlaces a sitios web relacionados con la Copa del Mundo, especialmente no hacer clic en correos electrónicos sospechosos y enlaces a sitios web con temas de la Copa del Mundo;
- No utilizar credenciales, contraseñas o información de tarjetas de crédito en sitios o plataformas donde no esté seguro de la seguridad.
- A medida que se desarrolla el evento de la Copa Mundial de la FIFA 2022, se prevé que las actividades de amenazas cibernéticas aumenten aún más y, especialmente, aumentarán las campañas de phishing con temas de torneos y los nombres de dominio falsos.



Dominio phishing impersonando el sitio de Qatar 2022 con alta calidad.



Apps Maliciosas en Google Play



Chatbox malicioso en los sitios phishing

¡ALERTA CVE! OPENSSL CVE-2022-3786 AND CVE-2022-3602: X.509 EMAIL ADDRESS BUFFER OVERFLOWS

radware

Recurso: Radware Blog, Noviembr, 2022
https://blog.radware.com/security/alert/2022/11/cve-alert-openssl-cve-2022-3786-and-cve-2022-3602-x-509-email-address-buffer-overflows/

Overview

After a week of speculation about OpenSSL vulnerabilities, the OpenSSL project disclosed two new CVEs to address buffer overrun vulnerabilities in its cryptographic library that could trigger crashes or lead to remote code execution (RCE).

Here is an overview of both vulnerabilities and mitigation techniques organizations should consider.

Vulnerabilities

- CVE-2022-3602 is a 4-byte stack buffer overflow that could trigger crashes or be leveraged for RCE.
- CVE-2022-3786 is a buffer overflow that can trigger a denial-of-service (DoS) state through crashes.
- OpenSSL version 3.0.0 through 3.0.6 are affected by both vulnerabilities.
- Both vulnerabilities are caused by incorrect constraint checking of the email address field during the validation of X.509 client certificates.
- The vulnerabilities could potentially be exploited via malicious TLS certificates
- Because OpenSSL 3.0 was only recently FIPS certified (August 23, 2022), many vendors that have FIPS certifications are using OpenSSL version 1.x, which is not affected by the vulnerabilities.
- The vulnerability only affects services and client implementations that perform X.509 certificate validation through the OpenSSL cryptographic library.

Risk

Several non-trivial conditions need to be met for successful exploitation. Modern application runtimes contain stack overflow protections, and as such, the risk for RCE or DoS is low, though not zero.

At the time of publication, there are no public proofs-of-concept available or reports of exploitation in the wild for either of these flaws.

To impact web services, the maliciously crafted certificate would have to be signed by the web services' CA certificate. Without obtaining a valid CA certificate, the client certificate validation will be stopped higher up in the certificate chain. Client applications can be impacted when visiting servers using maliciously crafted certificates. Though expected to be very slim, there might be a risk for RCE on the client side. A server certificate must be signed by a valid CA, so unless a legitimate server was compromised or the client was tricked into browsing a malicious server, there should not be an immediate risk.

Impacted Software & Devices

Any application or device, from messaging clients and web browsers on desktop and mobile, network attached storage (NAS) devices and security gateways, up to server software and online services that leverage OpenSSL 3.x and provide certificate-based authentication.

Mitigations

- Update to OpenSSL version 3.0.7
- Contact your product vendors and update any software or appliances leveraging OpenSSL version 3.0.0 up to 3.0.6
- If no certificate validation is required, disabling certificate validation will mitigate the vulnerability.
- If timely updating is not possible, the following steps will alleviate the urgency of patching:
  - fronting the affected services
  - disabling certificate validation in the service
  - moving the certificate validation to a reverse proxy running an unaffected or patched version of OpenSSL

More Information

OpenSSL Vulnerabilities:
https://www.openssl.org/news/vulnerabilities.html

OpenSSL Security Advisory:
https://www.openssl.org/news/secadv/20221101.txt

OpenSSL QA:
https://www.openssl.org/blog/blog/2022/11/01/email-address-overflows/

Radware Product Exposure(s)
Product status for CVE 2022-3602
Product status for CVE 2022-3786

"QRISHING", LA NUEVA MODALIDAD DE ESTAFA CIBERNÉTICA EN EL MARCO DE QATAR 2022

QRishing o Phishing a través de códigos QR es la nueva forma de ataque poniendo en riesgo a los fanáticos del Fútbol. Mientras los fanáticos del fútbol disfrutan la Copa Mundial Qatar 2022, los ciberdelincuentes aprovechan este importante evento para estafar y robar información sensible.

Esta fiesta deportiva hace que los delincuentes digitales creen nuevas estrategias según las tendencias de compra de productos (como las postales del álbum) o servicios relacionados al Mundial. También lo hacen con mensajes indicando al usuario que ha ganado premios de una u otra campaña mundialista.

Una de las modalidades de estafa que más se ha presentado en el marco de Qatar 2022 es el QRishing o Phishing a través de códigos QR. Esta forma de ataque consiste en implantar códigos falsos y cuando el usuario lo escanea se dirige a un sitio web ilusorio que le pide las credencias; de esta forma los ciberatacantes roban los datos de pago, duplican tarjetas o suplantan la identidad de las víctimas.

"Los ciberataques están en constante evolución y cada vez son más las formas en que recibimos notificaciones fraudulentas, por esta razón, es importante que las personas comprendan que nadie está exento de ser víctima de QRishing o cualquier otra forma de robo. Es fundamental estar informados de estas tendencias para saber cómo proceder y no caer en el cibercrimen" indicó Joey Milgram, Gerente General de Soluciones Seguras en Costa Rica.

¿Cómo evitar el QRishing y otras estafas en línea?

Estar informado y prevenido le permitirá disfrutar del evento más importante del balompié mundial. A continuación, los expertos de Soluciones Seguras le brindan algunos consejos importantes para no caer en el QRishing:

- Desactive la opción de accesar automáticamente a las páginas que dirigen los códigos QR.
- Utilice aplicaciones que le permitan verificar el URL ligado al código QR antes de abrirlo.
- Si tiene dudas de la procedencia del código QR, mejor no ingrese y realice una doble verificación del sitio web.
- Al realizar pagos o transacciones de dinero con código QR, compruebe la operación de forma inmediata con el comprador o vendedor.
- Si el código QR se encuentra en un objeto físico, compruebe que no haya sido manipulado con adhesivos o stickers colocados sobre el código real.
- Instale una solución que identifique cuando se trata de acceder a sitios de Phishing.

El QRishing no es la única forma en que su información está en riesgo o su privacidad se pueda ver comprometida. Según un reporte de Check Point, partner de Soluciones Seguras, particularmente en Costa Rica, se ha registrado un promedio de 1291 ataques semanales, en los últimos seis meses. Las industrias más atacadas siguen siendo MSP (Proveedores de servicio), Gobierno y Educación.

Por ello, también se recomienda:

- Esté atento a situaciones atípicas. Los ciberataques pueden llegar con cualquier excusa: sorteos, premios, descuentos, movimientos inusuales en sus cuentas bancarias, encuestas, falsas ofertas laborales, entre otras.
- Los links por medio de mensajes de texto, redes sociales y correos electrónicos son las vías más recurrentes que usan criminales de la red para hacer caer a sus víctimas. Nunca abra estos enlaces sin estar seguro de que son confiables.
- Si está conectado a una red pública, evite ingresar a sitios donde manipule sus datos sensibles como números de tarjetas, usuarios, contraseñas, claves.
- Realice compras o pagos solo por canales oficiales o plataformas de eCommerce verificadas.
- Instale un software de seguridad en sus dispositivos tecnológicos, con el fin de que estos puedan detectar malware en aplicaciones o nuevas descargas.
- No ingrese a páginas como la del banco desde los buscadores; ingrese manualmente la dirección URL para asegurarse de acceder al sitio real.

Sin importar desde qué parte del planeta disfruta de Qatar 2022, sea precavido e implemente todos los filtros de ciberseguridad, para que esta fiesta del fútbol no se torne un amargo recuerdo.

CUIDADOS AL REALIZAR COMPRAS EN LÍNEA EN ESTE FIN DE AÑO

Estadísticas

- **Check Point Research encontró un fuerte aumento en los sitios web relacionados con compras falsas en el período previo a las ventas del Black Friday.**
- **El 17 % de todos los archivos maliciosos distribuidos por correo electrónico en noviembre estaban relacionados con pedidos/entregas y envíos.**
- **Desde principios de este mes, el 4% de todos los nuevos sitios web relacionados con las compras resultaron ser maliciosos.**

En la región se puede decir que noviembre es el pico del periodo en donde surgen nuevos sitios phishing y ciber-amenazas en el entorno relacionado con las compras de fin de año, y esto es porque las tiendas inician su periodo de publicidad, asique es buen momento para ir atrapando clientes desprevenidos. Sin embargo, desde noviembre las compras y transacciones no hacen más que ir en aumento hasta diciembre, incluso extendiéndose hasta el día 24 de diciembre debido imprevistos de último momento.

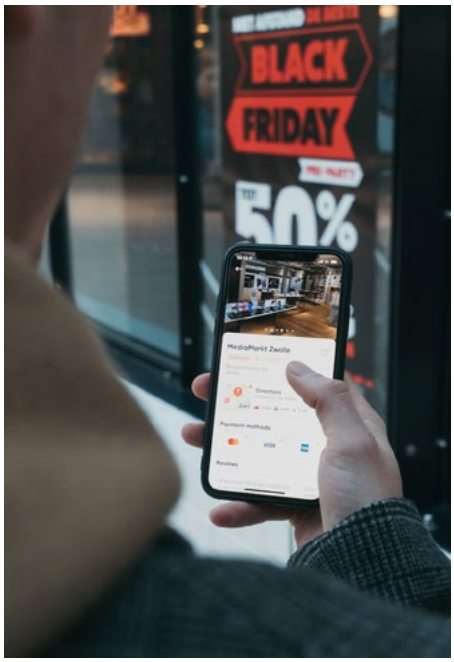
Según Adobe, en Estados Unidos, el gasto en vacaciones en línea se acercará a los 210.000 millones de dólares este año, un aumento interanual del 2,5 %. Sin embargo, mientras los consumidores se preparan para conseguir la mejor oferta, los ciberdelincuentes se aprovechan de las mentes distraídas al lanzar sus propias compras "especiales" en forma de campañas de phishing y sitios web falsos.

En artículos anteriores hemos conversado sobre el Phishing y es que ha sido el tipo de ataque más popular debido a su alta efectividad al tomar desprevenidas a las víctimas. Los mensajes de phishing están diseñados para manipular a un usuario para que realice una acción, como descargar un archivo malicioso, hacer clic en un enlace sospechoso o divulgar información confidencial. Un phisher (actor malicioso que utiliza la técnica de phishing) puede usar canales públicos, como las redes sociales, para recopilar información de antecedentes sobre su objetivo. Estas fuentes se utilizan para recopilar detalles como el nombre del objetivo, el cargo y la dirección de correo electrónico, así como sus intereses y pasatiempos. El phisher puede usar esta información para crear un mensaje de spam personalizado.

Evite las estafas y disfrute de compras, pero sin bajar la guardia

Los ciberdelincuentes están aprovechando al máximo el espíritu navideño. Por eso es importante que todos tomen precauciones adicionales para disfrutar de una experiencia de compra en línea más segura. Aquí hay seis formas en que puede mantenerse seguro en estas compras de fin de año:

- Compre siempre de una fuente auténtica y confiable: antes de realizar una compra, es importante autenticar el sitio que estamos utilizando para realizar la compra. Entonces, en lugar de seguir un enlace enviado por correo electrónico o mensaje de texto, vaya directamente al sitio buscándolo en su navegador seleccionado y localizando la promoción usted mismo. Esos pocos pasos adicionales garantizarán que no haga clic en ningún enlace fraudulento y que pueda realizar su compra con confianza.
- Esté alerta a los nombres de dominio similares: muchos sitios web fraudulentos a menudo usan un nombre de dominio similar a la marca que está tratando de replicar, pero con letras adicionales o errores ortográficos. Para asegurarse de no entregar su información bancaria a los estafadores, preste atención a las URL, ¿hay algo habitual o desconocido? Al tomarse un minuto para buscar señales de que un sitio web puede ser fraudulento, puede identificar rápidamente su legitimidad.
- Ojo con las ofertas 'demasiado buenas para ser verdad': a menudo, las estafas de phishing prometen descuentos extremadamente buenos en artículos muy populares. Si recibe una oferta que parece ser demasiado buena para dejarla pasar, no se apresure a comprarla antes de que se agote, ya que es probable que sea una estafa. En su lugar, verifique que el vendedor sea auténtico consultando otros sitios web para ver si ofrecen descuentos similares.
- Siempre busque el candado: una forma rápida de ver si un sitio web es seguro es mirar si la URL comienza con HTTPS. Este es un indicador de que cumple con los estándares de seguridad internacionales y, por lo general, va acompañado de un candado para reflejarlo. La ausencia de estos signos podría indicar que no es confiable y debe evitarse.



- Utilice seguridad en su equipo: si bien vemos un aumento en los correos electrónicos fraudulentos durante los períodos de compras populares, los ciberdelincuentes utilizan correos electrónicos de phishing durante todo el año. Es por eso que todos deberían buscar implementar soluciones de seguridad de correo electrónico para evitar que lleguen a nuestras bandejas de entrada en primer lugar.
- Tenga cuidado con los correos electrónicos de restablecimiento de contraseña: con muchos preparando sus cestas y cargando su información de pago en sus cuentas para hacer el pago más rápido, los piratas informáticos también buscarán formas de ingresar a las cuentas de compras de las personas. Como resultado, los consumidores deben tener cuidado con los correos electrónicos de restablecimiento de contraseña que podrían ser fraudulentos. Si recibe uno, siempre visite el sitio web directamente (no haga clic en los enlaces) y cambie su contraseña.

¿ESTÁS REUTILIZANDO CONTRASEÑAS EN TODAS LAS PLATAFORMAS WEB? ¡PIENSA OTRA VEZ! LAS BASES DE DATOS DE CREDENCIALES ROBADAS SON UN MERCADO CLANDESTINO FLORECIENTE

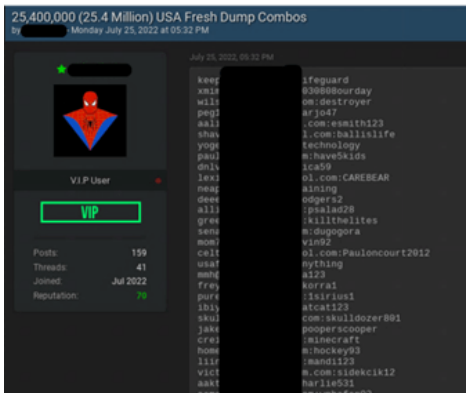
Recurso: Check Point Research, Antoine Korulski & Adi Goldshtein Harel, Noviembre, 2022
https://blog.checkpoint.com/2022/11/01/are-you-re-using-passwords-across-web-platforms-think-again-stolen-credentials-databases-are-a-flourishing-underground-market/

When you think about your social media accounts – let's say your Facebook password – does it have anything in common with your LinkedIn or bank account password? Does it have the same password as your corporate account? If so, you are not alone! According to a Google survey, at least 65% of participants re-use their passwords across multiple accounts and web services

As every service, website, and social media account requires a password, many people find it easier to reuse the existing ones instead of reinventing new ones, especially since it is difficult to manage and memorize multiple passwords. This is particularly true as, due to security policies, passwords are by necessity becoming more and more complex. Although most of the population understands the risk and knows that one shouldn't reuse passwords, most of us continue reusing passwords for both corporate and personal accounts.

Some people use password managers, which are considered safe, to help them store their credentials. However, these tools are not bulletproof as seen in August 2022 when LastPass was breached for a second time. On that note, in a survey from 2022, another password manager service, Bitwarden, found that 84% of the service consumers use the same password across multiple business and personal platforms.

It's not surprising that cybercriminals immediately saw an opportunity presented by people's generally lax behavior regarding password reuse and created a flourishing underground market of databases obtained from breached websites.



As most cybercriminals do not care about the origins of the credential pair, they create "combo lists", huge compilations of many stolen databases that are just lists of email addresses and passwords. Many of those are lists of corporate email accounts with passwords that were used on 3rd party services. The largest combo list of all time, called RockYou2021, was published in 2021 and contained more than 8 billion unique sets of email accounts and passwords.

Credential Stuffing Attacks – How do threat actors leverage stolen credentials and combo lists?

Credential stuffing is a type of cyberattack in which the attackers collect stolen account credentials, typically consisting of lists of usernames and/or email accounts and the corresponding passwords. They then use the credentials to gain unauthorized access to user accounts through large-scale automated login requests directed against a Web application.

Credential stuffing is one of the most common techniques to take over user accounts, including emails, banking accounts, social media, and corporate accounts.

The Underground Perspective

As soon as cybercriminals understood the big business potential of stolen passwords, they started focusing their efforts on hacking different websites and services that are not of great value by themselves – but are lucrative because of the user credentials they contain.

The NIST password storage guidelines require that passwords be salted with at least 32 bits of data and hashed with a one-way key derivation function. However, even in 2022, many websites don't comply with this policy, and some even store passwords as plain text records.

The cybercriminals who hack these websites are not necessarily the ones who most effectively use them. Many flourishing underground communities and markets were created around buying and selling stolen data and credentials. Valuable sets of credentials, that provide administrator-level access to an organization, can cost up to $120K in the underground, with an average of $ 3K for administrator sets, and while many sets of credentials are sold in the underground forums, many are also given for free.

In just the last six months, in one of the prominent English-speaking underground communities, more than 3,500 threads concerning stolen databases were opened, and more than 1,500 threads about combo lists that include just email accounts and passwords. Each one of these databases can include millions or even hundreds of millions of credential sets.

While those databases and combo lists include a high percentage of webmail credential sets whose exposure poses only a low risk to the corporation, they also include many sets of corporate email accounts with passwords that employees use to register on 3rd party websites. This is the Holy Grail for the cybercriminals, the most valuable quarry of them all. When the same password is used across personal and business accounts, the damage potential of a cyber-attack increases as criminals can access multiple accounts when just one is breached, and the organizations' vulnerability to cyber-attacks increases. These accounts and applications lie beyond the visibility and protection of business IT teams.

In many cases, cybercriminals also separate the combo lists according to country, to make it much more convenient to use.

MAXIMIZACIÓN DE LA UTILIDAD DEL TIEMPO

Muchas veces se menciona de como maximizar dinero, utilidades, el valor de las cosas materiales pero muy poco se habla de la maximización de la utilidad del tiempo.

El tiempo representa nuestro principal activo en la vida y la inversión más valiosa. Cada persona o empresa es el producto de la inversión de su tiempo, hoy somos el resultado de la forma en que hemos invertido el tiempo en el pasado; mañana seremos el resultado de la forma en que invirtamos hoy nuestro tiempo.

El tiempo mediante un aprovechamiento eficaz hace la diferencia entre un logro o un desacierto o bien entre un éxito y un fracaso.

Cada año que pasa el tiempo invertido o tiempo perdido va moldeando nuestras empresas; muchas empresas que promueven que sus colaboradores estudien, se especialicen en su área y busquen la eficacia en la labor del personal van a recibir utilidades de esa inversión del tiempo.

Todos tenemos los mismos 365 días por año, pero la maximización de la utilidad del tiempo varia de empresa a empresa.
La administración del tiempo se puede definir como una manera de ser y una forma de vivir.

Si se malgasta, se derrocha algo muy valioso. Para aprender a valorar el tiempo y a planificar es imprescindible:

- Identificar metas, objetivos y prioridades.
- Planificación del tiempo.
- Adaptar la planificación del tiempo.
- Seleccionar las estrategias más idóneas para alcanzar las metas, los objetivos y las prioridades.

ALGUNAS DE LAS CARACTERÍSTICAS DEL TIEMPO SON:

- Puede ser un enemigo que vencer o un aliado si lo logramos organizar.
- Puede ser un recurso escaso, si no se controla en función de las prioridades que se le asignen a las actividades diarias de la empresa.
- No se puede comprar.
- No se puede atrapar, detener o regresar.
- El más importante de los recursos, ninguna acción humana se puede realizar sin tiempo
- Un recurso limitado; hagamos lo que hagamos se nos acaba, podemos controlar nuestras acciones, pero no el tiempo
- No se puede ahorrar, acumular, ni prestarse.
- El tiempo que dediquemos a cada actividad de nuestra agenda debe ser proporcional a su importancia, lo ideal es que la sumatoria de los beneficios tienen que ser mayores a la sumatoria de los costos y la sumatoria de los riesgos.

Es importante saber que los ciberdelincuentes aprovechan su tiempo y trabajan 24/7 buscando sistemas vulnerables en los cuales cuando logran su cometido, la empresa atacada va a sufrir una pérdida de imagen con sus clientes, pérdida de información junto con mucho tiempo en reconstruirla y pérdida parcial o total de su operación entre otras cosas.

Para mitigar esos riesgos y maximizar la utilidad del tiempo, es muy importante que las empresas estén protegidas en aspectos externos, internos, monitoreo de redes, seguridad de los usuarios, seguridad de datos sensitivos y seguridad de nube con soluciones líderes en el mercado.

Wagner Gamboa Fuentes
Gerente Regional de Operaciones
Soluciones Seguras Panamá

2023 CYBERSECURITY PREDICTIONS FROM CYBERARK LABS

Recurso: Cyberark Blog, Noviembre, 2022
https://www.cyberark.com/resources/blog/2023-cybersecurity-predictions-from-cyberark-labs

It's been an eventful 2022 and, based on what our CyberArk Labs team is observing, 2023 will introduce yet another chapter of cybersecurity threats and challenges, along with some new opportunities for vigilant defenders. Here are six of our cybersecurity predictions for the coming year:

1. Web3 on the Blockchain Promises Enhanced Privacy — and Bigger Payouts

Today, more than four out of 10 consumers feel unable to protect their personal data, and many have taken action. This widespread push for greater data transparency and personal control will only grow stronger in 2023, accelerating global momentum for Web3 (aka Web 3.0) on the blockchain. But as technology infrastructure becomes more decentralized, the financial application attack surface will expand significantly, while security practices in this new frontier lag. Threat actors will use this to their advantage to target crypto exchanges and susceptible bridges to the world "off the chain," drawing inspiration from the $615 million Ronin cryptocurrency heist of 2022.

2. Geopolitical "Winter is Coming," Along with Increased Attacks on Critical Infrastructure

Our first predicted trend may be exacerbated by the continued conflict in Ukraine, as certain criminal groups ramp up financially motivated attacks and — banking on the promise of massive payouts — shift their gaze in decentralized infrastructure's direction. Meanwhile, winter is rapidly approaching Eastern Europe, and we can expect attacks on critical infrastructure to spike as temperatures plummet, driving global energy prices up even higher.

3. What's Old Will Be New Again as Threat Actors Revisit Familiar Tricks

Since Log4j sent shockwaves around the world, speculation on when the other shoe will drop has been constant. But the next "big thing" isn't likely to be a massive zero day — especially as prices for these coveted vulnerabilities reach upwards of $10 million on darknets and other underground marketplaces, and well-resourced groups and nation-states compete fiercely. Most threat actors will use alternative ways to infiltrate organizations and move laterally toward their targets. And at the end of the day, why would they spend so much cash on a specialized exploit or time contriving new methods when old tricks like phishing, credential theft and social engineering, or one-day kernel-level or memory corruption exploits work just fine?

4. Forget New Year's Diets — Your Cookies Will Be Too Irresistible

The good news is most organizations no longer view multifactor authentication (MFA) as a "nice to have" for their business applications, meaning most users must input both a username/password combo and complete a secondary authentication challenge before establishing a web session. The bad news is attackers are getting more sophisticated in snagging session cookies — which establish access to these third-party applications — to bypass both primary authentication and MFA and hijack accounts. As organizations continue to adopt more SaaS applications and consolidate them on the browser, session cookies will become even more critical and more vulnerable. With Genesis Store and other marketplaces specializing in stolen session cookies growing in popularity, threat actors will seek ways to further automate and scale these session hijacking attacks to boost profitability next year.

5. A Silver Lining in the Commoditized Credential Age

2023 is the year to begin a career in cybercrime, thanks to the commoditization of the credential. Would-be attackers who

lack the skills (or time) can simply browse on a marketplace, fill their carts with cheap lists of stolen credentials and cookies or off-the-shelf ransomware, phishing and exploit kits and check out — no attack legwork required. In this environment, MFA and two-factor authentication won't be enough. Yet there will be a silver lining for security teams that take a defense in depth approach — one that could swing the pendulum in their favor. Rushing to get rich quick, many cybercriminals will make rookie mistakes or create far too much noise on the network, foiling their plans. For instance, pushing 20 authorization requests in rapid succession as part of an MFA bombing attempt will show up in the victim organization's logs and raise major red flags.

6. Carbon Credits Will Take Center Stage in Multi-Million-Dollar Schemes

On the heels of the COP27 Climate Conference in Egypt where carbon credits took center stage, opportunistic cyber attackers will increase efforts to manipulate the murky and largely unregulated voluntary carbon market (VCM). While carbon credits continue to grow in popularity with companies and governments working to reduce emissions and offset their own output, we can expect to see more multi-million-dollar schemes to steal and sell emission-trading rights in the next 12 months.

Infoblox Q3 2022 Cyber Threat Intelligence Report

Infoblox se complace en publicar esta edición del tercer trimestre de 2022 de nuestro Informe trimestral de inteligencia sobre ciberamenazas. Publicamos estos informes durante el primer mes de cada trimestre natural.

Este informe del tercer trimestre de 2022 destaca de manera especial e introductoria la investigación original de Infoblox Threat Intelligence Group (TIG) sobre la puntuación de reputación de dominios de nivel superior (TLD) y cómo esta información puede ayudar a las organizaciones a evaluar amenazas potenciales.

DESCARGAR EL INFORME

CURSOS VIRTUALES 2023

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 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.

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.

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.

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.

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.

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.

SOLUCIONES DE CIFRADO Y SEGURIDAD DE SERVIDORES Y DATOS

Soluciones que frecen seguridad de servidores y datos mediante mecanismos de cifrado, enmascaramiento y tokenización. Además provee de auditoría y control de acceso a datos sensitivos.

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.

FILTRADO DE CONTENIDO Y ARCHIVADO DE DATOS

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.

DEFENSA DISEÑADA PARA AMENAZAS AVANZADAS

Solución que le muestra no solo a dónde van los intrusos, sino dónde han estado. Brinda visibilidad completa en la nube, el centro de datos y la IoT, incluso cuando el tráfico está cifrado.

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.

MONITOREO DE RENDIMIENTO DE REDES Y SERVIDORES

Monitoreo completo de su infraestructura. De rápida implementación brindando alertas proactivas y vistas instantáneas, permitiendo resolver incidencias de red lo más rápido posible.

Asegure, evalúe y analice su código fuente en tiempo de desarrollo. Mitigue vulnerabilidades en su código de manera más rápida y sencilla.

Plataforma de capacitación y concientización de usuarios. Establezca sus metas y deje que Smartfense haga el resto.

Plataforma con integración profunda a dispositivos críticos, pre-cargada de instrucciones de remediación fácil de leer.

Descubra su nivel de compromiso en minutos. Mida el compromiso con rapidez y presición.

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 representamos.

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