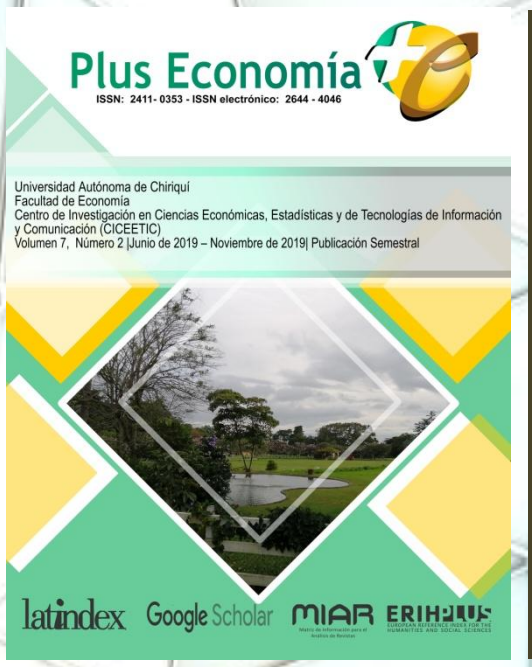
- Revista Plus Economía
- ISSN: 2411-0353
- ISSN electrónico: 2644-4046
- pluseconomia@unachi.ac.pa
- Centro de Investigación en Ciencias Económicas, Estadísticas y de Tecnologías de Información y Comunicación, CICEETIC
- Universidad Autónoma de Chiriquí (UNACHI)
- República de Panamá



Picado, Francisco.

Estado del internet y la seguridad cibernética.

Vol. 7, Núm. 2, Junio 2019 – Noviembre 2019

pp. 37-45

Consultor empresarial para soluciones de ciberseguridad, Costa Rica.

+ | ESTADO DEL INTERNET Y LA SEGURIDAD CIBERNÉTICA

Mgtr. Francisco Picado | Project Manager en el área de Ciberseguridad | Especialista en proyectos de integración en paquetes de seguridad | Consultor empresarial para soluciones de cibserseguridad, Costa Rica | email: elprofe_79@hotmail.com

Recibido: Septiembre de 2019 **Aceptado:** Noviembre de 2019

RESUMEN

La vida hoy en día no se puede concebir sin el uso del Internet. Es necesario, el mundo simplemente no puede continuar sin el avance de la tecnología y la interconectividad que tanto ha beneficiado a la humanidad, ya no se trata únicamente de ingresar a un navegador web y visitar un sitio web, ahora se trata de socializar, de hacer compras en línea, de evitar filas en los bancos, de ver películas en demanda, eventos en tiempo real y muchos otros servicios que están disponibles para el colectivo. El presente artículo tiene como objetivo educar a la población acerca del avance de la tecnología y sembrar conciencia de los riesgos que también implica el uso de todos estos dispositivos que forman parte de esta gran red mundial que conocemos bajo el nombre del Internet.

Palabras claves: Estado del Internet, Ciberseguridad, Internet de las Cosas, Ciberataques.

ABSTRACT

Today, the life without the use of the Internet cannot be conceived. It is a necessity, it is not possible to continue evolving as a society without the technology and the interconnectivity that comes along with it, nowadays, the use of the Internet is not only about going into a browser and visit a website, it is all about social media, online shopping, bank account transactions, video on-demand, real time events and many other services available to the market. This article enforces the goal to educate the audience in general regarding the progress of the technology and raising awareness

about the risks that are implied in the use of all these devices that are part of this worldwide network that we know under the name of the Internet.

Keywords: State of the Internet, Cibersecurity, Internet of Things, Ciberattacks.

INTRODUCCIÓN

Formamos parte de una sociedad que desde hace algunos años se caracteriza por estar en línea y en la cual nosotros como ciudadanos del mundo cada día somos más dependientes de esa interconectividad que nos ofrece el Internet.

El avance de la tecnología ha sido vertiginoso y no termina de sorprendernos, pero en ocasiones somos protagonistas ausentes de la inversión que realizan las empresas por ser más competitivas y tener mucha más presencia en el mercado digital, un nicho que ya dejó de ser opcional y el cual ofrece oportunidades inimaginables de éxito comercial, aunque de igual manera podría ser una segura ruta al fracaso si estos emprendimientos no se adaptan a estas tendencias de negocio. El usuario tradicional, llámese usted amigo lector o cualquiera de nosotros, se enfoca en ingresar a un navegador o aplicación web y entonces visita el sitio de su elección, consulta la información, realiza alguna compra o realiza pagos desde su cuenta bancaria, entre un abanico de opciones bastante amplio, quedando en manos de otros la confianza que los usuarios puedan tener por ese servicio.

Es cada vez más común que los usuarios de Internet se vuelvan consumidores activos de redes sociales, blogs, sitios web con diversidad de temas y donde todos se creen dueños de la verdad absoluta.

Pero la realidad es que somos ajenos a la forma en que estos sitios web operan, desconocemos la infraestructura que hay detrás, quienes manipulan la información y las políticas de seguridad que poseen. Al usuario de Internet le falta malicia, basta con recordar el sonado tema de Cambridge Analytica, una empresa que se encargó de comprar información personal de aquellos sectores expuestos entre otros,

a las redes sociales. Es correcto, aunque parezca increíble, esta empresa en su momento hizo un análisis de los gustos, expectativas y aspiraciones de sectores de la población que estaban enfrentando campañas presidenciales en sus países (Estados Unidos para la campaña de Donald Trump para dar un ejemplo), Cambridge Analytica también estuvo presente para el Brexit y está comprobado que fueron capaces de manipular a una gran mayoría de los votantes, influyendo en su decisión de voto y en los resultados finales, lo que hizo estallar un gran escándalo. Al final del día, ninguno de nosotros somos tan siquiera conscientes de situaciones como estas.

A todo esto, debemos sumar servicios en la nube que seducen y toman mayor fuerza día con día, una solución pronta para diversidad de clientes que asumen con compromiso los beneficios o riesgos que estos ecosistemas representan pero que en definitiva se han consolidado y cada vez son más las empresas que hacen uso de estos. Para muestra un botón, los números son escandalosos, el crecimiento en definitiva ha sido exponencial, atreviéndonos a decir que el concepto de la nube tomó un poco más de fuerza en el 2017 y ya para el 2018 el crecimiento fue de un 32%, en cifras algo así como unos $250.000 millones que fueron directo a los bolsillos de los proveedores de estos servicios.

Y si queremos seguir conversando sobre el ímpetu con el que la tecnología evoluciona y crece sin ninguna reserva, podemos hablar horas sobre una moda que ya es parte de nosotros y que conocemos con el nombre del ***Internet of Things (IoT)*** o el ***Internet de las Cosas***. Dispositivos inteligentes que cobran vida con una simple conexión a Internet y que logran complacer muchos de nuestros caprichos, por ejemplo, el ***Google Home Voice Controller, Amazon Echo Plus, August Doorbell Cam, Mr. Coffee Smart Coffeemaker*** y vaya que podría nombrar cientos más. Pero veamos el siguiente gráfico tomado del sitio web **Statista:**

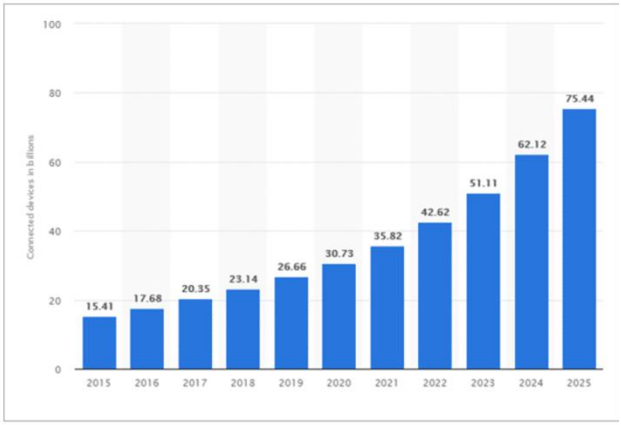


Figura 1. Incremento en la demanda de dispositivos IoT

Fuente: Statista (2019)

Lo interesante del gráfico anterior, es que la población mundial supera los 7 billones de personas, sin embargo, se proyecta que para el 2025, los dispositivos IoT se contarán por ***75 billones***. Es una industria en pleno crecimiento, que nos cautiva, hoy en día nos encanta hablar con un parlante y hacerle preguntas de todo tipo y pedirle inclusive favores, desde la comodidad de nuestra cama apagar las luces de la casa, hablarle a nuestro televisor, desde nuestro dispositivo celular poner el café o que la refrigeradora nos haga órdenes de compra cuando nos quedamos sin leche, ***¿cómo no sentirse deslumbrado con todos estos dispositivos? ¿cómo no rendirse ante la necesidad de adquirir "juguetes" de este tipo?***

Dicho todo lo anterior, la pregunta que queda es ***¿Conoce usted de los riesgos que se corren con el uso de toda esta tecnología? ¿Es usted consciente del riesgo de hacer transacciones bancarias o del uso de sus tarjetas? ¿Se detiene usted a leer los acuerdos de uso y confidencialidad de sus redes sociales?***

Tipos de ataques – Algunos números del 2019

Las empresas hoy en día invierten miles o millones de dólares en soluciones de seguridad, con el único objetivo de garantizar la confidencialidad, integridad y disponibilidad de la información y de sus sistemas y con esto garantizar una experiencia total y absoluta para el usuario final. Aún así, la batalla es diaria, una vez que se identifica alguna vulnerabilidad y se protege, los que atacan encontrarán otra, harán que su ataque mute y entonces el ciclo continúa.

De acuerdo con el ***Open Web Application Security Project (OWASP)*** en su lista más reciente del Top 10 (año 2017), los siguientes son los riesgos en seguridad a nivel de aplicaciones más significativos:

1. Injection (SQL Injection, Command Injection, PHP Injection, etc.)
2. Broken Authentication
3. Sensitive Data Exposure
4. XML External Entities (XEE)
5. Broken Access Control
6. Security Misconfiguration
7. Cross-Site Scripting (XSS)
8. Insecure Deserialization
9. Uso de dispositivos con vulnerabilidades conocidas

Los anteriores tal vez sean algo desconocidos para el lector, pero nos podemos enfocar en ataques como ***SQL Injection***, que consiste a nivel muy general, en el robo de información a bases de datos, además de corromper esta información, en un ataque como ***Broken Authetication***, el atacante ingresa a cuentas de usuarios debido a problemas de seguridad en las aplicaciones, con ***Cross-Site Scripting*** se puede capturar información tan sensible como claves de bancos, credenciales para sitios de compra en línea, información de tarjetas, entre otros. Y el número 9 en la lista, consiste en el ataque o infección de gran cantidad de dispositivos que con acceso a Internet se encuentran sin ninguna protección o totalmente vulnerables, ¡es correcto!, si estás pensando en todos esos aparatos maravillosos que forman parte del ***Internet de las Cosas***, la gran mayoría no cuentan con ninguna protección y entonces están expuestos a todo tipo de ciberataques. Así es como se crean los ***Botnets***, Kaspersky lo define como “el nombre genérico que denomina a cualquier grupo de PC infectados y controlados por un atacante de forma remota”.

Para dar una perspectiva en números, de acuerdo con ***Akamai Technologies***, empresa especializada en soluciones para la web y la cual maneja aproximadamente el 40% del tráfico de Internet, en su sitio web destaca que entre el 30 de agosto y el 6 de septiembre del año en curso, se observaron un total de ***98,721,399*** ataques en verticales de negocios tan variadas como la automotriz, servicios

de consumo, hotelería, gaming y streaming, entre otros, y ¡sí!, en tan solo una semana. Estados Unidos es el país que más ataques en ciberseguridad sufre a diario y en esta misma semana se observaron un total de ***15,538,309***, siendo ***SQL Injection*** el ataque que más se ejecutó con un total de ***90,364,797***.

El siguiente gráfico tomado del sitio web de Akamai Technologies, muestra un panorama más amplio de los tipos de ataques más comunes:

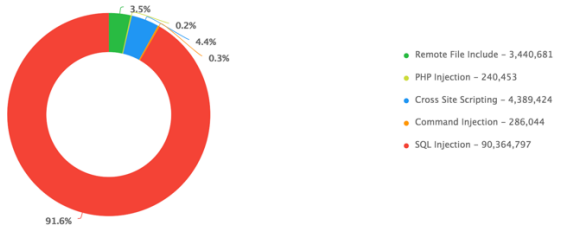


Figura 2. Cantidad de ataques por tipo de ataque entre el 30 de agosto y 6 de septiembre, 2019

Fuente: Akamai Technologies (2019)

Como sociedad estamos expuestos siendo un error creer que los ciberataques impactan únicamente a empresas y que nosotros como consumidores estamos a salvo. Uno de los tipos de ataques más comunes en el 2019, relacionado con usuarios finales de acuerdo con el informe del Estado del Internet de Akamai Technologies, fue el de **Credential Stuffing.** Este tipo de ataque consiste en el robo de información personal por parte de un atacante, el cual inyecta código malicioso en una aplicación o sitio web que presenta alguna vulnerabilidad, por ejemplo, en la sección de comentarios de una página de compras en línea. Una vez que el usuario publicó su comentario, el atacante comenzará a recibir información de todo tipo, ¡así de simple! Estamos hablando de datos tan sensibles como cuentas de usuario, datos de tarjetas de crédito, credenciales, tarjetas de regalo, entre otros. De acuerdo con este informe, se reportaron poco más de **30 millones** de ataques sólo en lo que va del 2019, el tema es amplio y bastante delicado, así como muy interesante el cual invita a continuar investigando al respecto.

El impacto económico

Detrás de un ataque cibernético existen diferentes motivaciones: extorsión, políticas, ideológicas, guerra cibernética, económicas, insatisfacción, broma, venganza, entre otras.

Un ***DDoS (denegación distribuida de servicios)*** el cual es uno de los ataques más comunes, puede provocar que las empresas inviertan sumas millonarias en sus equipos debido al bajo rendimiento que estos puedan mostrar o pérdidas económicas importantes a razón de la caída de sus servicios, lo cual genera además una mala reputación y por consiguiente pérdida de clientes, todos daños irreparables en sus operaciones.

Las empresas reportan pérdidas entre los $500 y $1000 por minuto una vez que hay interrupción de sus servicios y dependiendo de la magnitud las cifran van desde los cientos de miles de dólares hasta algunos millones.

El 28 de febrero del 2018, la empresa ***GitHub*** sufrió el que se considera el ataque de DDoS más grande de la historia, recibiendo un aproximado de ***127 millones de paquetes*** de información por segundo, un total de ***1.35 Tbps (terabits por segundo)***. El ataque fue mitigado en segundos. Lo normal en ataques de este tipo, es que se lleven a cabo por ***Botnets***, que como hemos comentado anteriormente, consisten en miles de dispositivos infectados atacando simultáneamente su objetivo, sin embargo, el ataque de GitHub no sucedió por este medio, se hizo a través de los servidores de Memcached, lo cual demuestra que los ataques evolucionan y se vuelven más complejos. En las referencias bibliográficas encontrarás un video muy interesante sobre este tema. En el 2016 tomó lugar un ataque de magnitud similar, enviando un total de 1.2 Tbps y afectando una cantidad importante de empresas como Spotiy, Twitter, Paypal, entre otras.

El robo de credenciales **(credential stuffig / account takeover)**, otro tipo de ataque que hemos analizado en este artículo, que se ejecuta por medios tales como el ***phishing*** (solicitud de información por correo, mensajes de texto, etc.)***, troyanos*** (archivos que se disfrazan en los equipos de cómputos que contienen código malicioso) *y* ***botnets***, genera pérdidas aproximadas a los ***$93.000 millones de dólares*** a bancos y usuarios en general. Esto por dar algunas cifras, ya que sabemos que el espectro de verticales que pueden ser atacas es muy extenso.

CONCLUSIONES

1. Se considera al usuario final como ***la primera línea de defensa*** en cuanto a ciberseguridad, es por esto por lo que se debe procurar no bajar los brazos, ser más desconfiados y cuidadosos de los sitios web que se visitan, no abrir enlaces que sean sospechosos y mucho menos brindar información de cuentas mediante correo electrónico, llamadas telefónicas, mensajes de texto, entre muchos medios que los estafadores utilizan para usurpar información de las personas.

2. Es muy común también que los usuarios dejen abiertas sus cuentas de correos, redes sociales y demás, aceptando cualquier tipo de cookies (archivos que guardan información sobre el usuario), compartiendo además memorias o discos duros portables y haciendo uso de cualquier señal abierta de Internet que se encuentren, porque es la naturaleza del ser humano - confiar en todo y en todos -, la bandera será siempre ser más malicioso, tener aplicaciones que protejan nuestros dispositivos, preguntar si no se está seguro de algo o simplemente no dar ese clic.

3. Las empresas ya hacen lo necesario de su lado implementando políticas de seguridad cada día más robustas: firewalls que controlan el tráfico que entra y sale de sus redes, así como firewalls para sus aplicaciones (WAF – Web Application Firewall), sistemas de detección e intrusión (IDS/IPS), redes de distribución de contenido (CDNs), administradores para Bots, reputación de clientes, control de solicitudes, listas de acceso, entre muchas otras soluciones, y en lugar de dar la batalla por ganada siguen en constante evolución, porque los atacantes también evolucionan y cada vez son más agresivos. Así que ninguno de nosotros está a salvo y la seguridad depende de cada uno, asusta, pero tampoco es imposible, es una cuestión de administrarse bien, ser más vigilante y estar

atentos a señales que nos indiquen que estamos bajo una posibilidad de amenaza o ataque.

REFERENCIAS

Akamai Technologies (30 de agosto de 2019). Cómo los Ingenieros de Seguridad frustraron el ataque DDoS más grande actualmente registrado. *Youtube.* Recuperado de https://www.youtube.com/watch?v=tUqqR5S7boU

Akamai Technologies (abril de 2019). Estado de Internet / Seguridad Credential Stuffing: Ataques y Mercados. Recuperado de https://www.akamai.com/es/es/multimedia/documents/state-of-the-internet/soti-security-credential-stuffing-attacks-and-economies-report-2019.pdf

Akamai Technologies (7 de septiembre de 2019). Visualización de ataques web. Recuperado de https://www.akamai.com/es/es/resources/our-thinking/state-of-the-internet-report/web-attack-visualization.jsp

IT Trends (10 de enero de 2019). El ecosistema relacionado con la nube continúa su tendencia de crecimiento. Recuperado de https://www.ittrends.es/infraestructura/2019/01/el-ecosistema-relacionado-con-la-nube-continua-su-tendencia-de-crecimiento

Kaspersky (25 abril de 2013). ¿Qué es un botnet?. Recuperado de https://www.kaspersky.es/blog/que-es-un-botnet/755/

Lloyd, A. (2 de julio de 2018). The Effects of DDoS Attacks on Essential Services. *Corero.* Recuperado de https://www.corero.com/blog/887-the-effects-of-ddos-attacks-on-essential-services.html

Molza, C. (14 de enero de 2019). El mercado de la nube: Un ecosistema en crecimiento. *Logitheque*. Recuperado de https://www.logitheque.com/es/articulos/mercado_de_la_nube_2957.htm

Statista Research Department (27 de noviembre de 2016). Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions). *Statista.* Recuperado de https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/