PUBLICACIÓN No. 3 | JUNIO 22 DE 2020 | BOGOTÁ - COLOMBIA

CÁPSULAS SOBRE Ciberseguridad

AL DÍA CON FELABAN

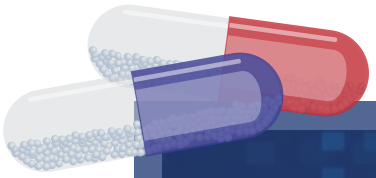
2020: Viviendo una Pandemia de Salud Pública y Cibernética

FIC
FRAUD INFORMATION CONTROL
by FELABAN

FELABAN
FEDERACION LATINOAMERICANA DE BANCOS

55 AÑOS
1965 - 2020

2020: Viviendo una Pandemia de Salud Pública y Cibernética



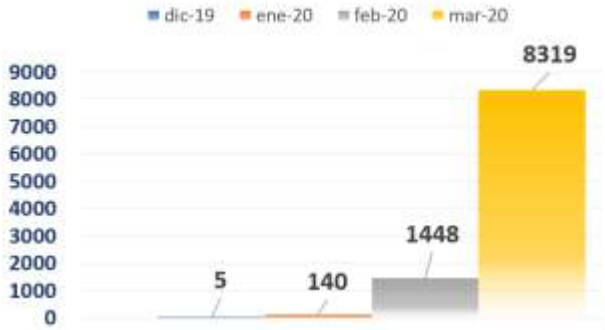
Si bien las actividades fraudulentas cibernéticas hoy en día son parte de las preocupaciones de las operaciones diarias, tanto de empresas como de los ciudadanos, la pandemia que se vive actualmente ha desplazado las actividades diarias a un campo cada vez más digital, generando como consecuencia que los actos delictivos tengan crecimientos desbordados, poniendo en riesgo un mayor número de empresas e individuos. El mundo abraza la revolución digital en momentos de emergencia, sin embargo, hay que decir que la misma no viene libre de riesgos ni mucho menos.

Los fraudes a través de phishing[1], smishing[2] y vishing[3] con campañas fraudulentas junto con la ingeniería social[4], son modalidades que se usan para realizar fraudes, los cuales tienen un componente de miedo y urgencia que ínsita a todos los individuos a no ignorar dicha información y por tanto convertirse en víctimas. La pandemia ha entonces generando grandes oportunidades para los delincuentes para generar nuevos anzuelos, enviando información de productos de protección ante el COVID, vacunas, aplicaciones de seguimiento del COVID y páginas web falsas como canales para realizar sus ataques.

Google reportó que ha seguido a diario más de 240 millones de mensajes de spam relacionados al COVID-19, según publicó el diario colombiano "El Tiempo". En el mismo sentido, según el diario "The Hill "a mediados de abril, el FBI reportó estar recibiendo alrededor de 3.000 y 4.000 denuncias de ciberseguridad por día en el primer trimestre de 2020, cuando antes de la pandemia estaba recibiendo alrededor de 1.000 denuncias diarias. Todos estos ataques, tiene un factor en común, ninguno discrimina el sector objetivo, abriendo campo a que todas las industrias están en latente riesgo de caer en alguno de estos ataques. Dicha exposición a ataques genera-lizada crea señales de alerta, indicando que es vital, tanto para individuos como para empresas, estar en constante revisión de la información de tendencias y como otros sectores están siendo afectados, ya que es muy probable que esto indique lo que está por venir en términos de ciberdelitos. ¡Si le pasa a un sector, le puede pasar a todos!

1. Phishing: Actividad de engañar a una persona para obtener su identidad, datos de cuenta, entre otros, a través de e-mail, para luego ser utilizada en robo de su dinero. (Oxford Advanced Learner's Dictionary)
2. Smishing: Actividad de engañar a una persona para obtener su identidad, datos de cuenta, entre otros, a través de mensaje de texto, para luego ser utilizada en robo de su dinero. (Norton)
3. Vishing: Actividad de engañar a una persona para obtener su identidad, datos de cuenta, entre otros, a través de llamadas telefónicas verbales o con VoIP, para luego ser utilizada en robo de su dinero.(Kasperky)
4. Ingeniería social: un conjunto de técnicas que usan los cibercriminales para engañar a los usuarios incautos para que les envíen datos confidenciales, infecten sus computadoras con malware o abran enlaces a sitios infectados. .(Kasperky)

Reportes Maliciosos Relacionados a Coronavirus - Datos a Nivel Mundial



Fuente: Bitdefender, Antimalware research, elaboración propia.

A manera de contextualizar de la importancia de la integración intersectorial y el trabajo armonizado en un gran ecosistema empresarial, desde FELABAN se pretende resaltar a través de esta cápsula, la necesidad de la interconectividad y cooperación para combatir este flagelo.

EL SECTOR SALUD: HOY PRENDE TODAS LAS ALARMAS:

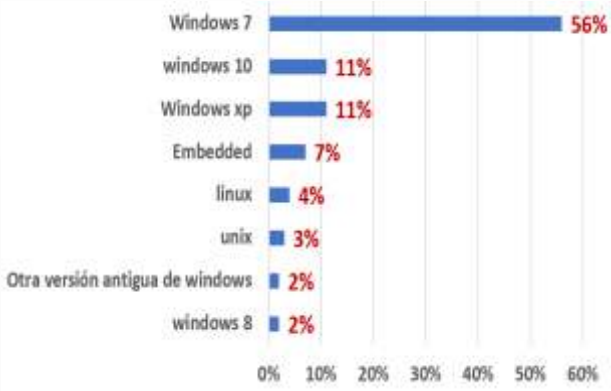
La industria de la salud, por citar un ejemplo, está mostrando incrementos importantes en temas de ciberataques y fugas de información, que evidencian la exposición en el ciber espacio de datos personales sensibles de millones de pacientes a nivel mundial, tema que debe prender las señales de alarma en otras industrias, como la Financiera, ya que dichos datos sensibles, están siendo comercializados en la Dark web[5]

El diario "La vanguardia", informó que, durante el primer semestre de 2020, la OMS (Organización Mundial de la Salud), ha sido blanco de múltiples suplantaciones de su página web, desde las cuales se han disparado miles de campañas de phishing. Durante dicho periodo, esta organización recibió un ataque de ransomware, si bien este este ataque no fue exitoso, otra afectación por medio de fuga de información terminó exponiendo a la OMS como víctima, reportando que a mediados de abril una sola semana 450 cuentas de correo activas con las respectivas contraseñas, fueron publicadas en la web, y miles relacionadas a personal que se encuentra trabajando en la respuesta del coronavirus, se encontraban también publicadas, de acuerdo con una publicación de Caracol Noticias.

La OMS no ha sido la única entidad relacionada al sector salud que se ha visto afectada; en un artículo publicado por la BBC de Londres, se menciona que el NIC, Instituto nacional de salud de los EE. UU., (por sus siglas en inglés) tuvo una fuga de información de 9.938 e-mails y contraseñas, la fundación Gates 269 y el Instituto de Virología de Wuhan 21, según lo publicado por la cadena de noticias "nbc news"

Por otro lado, un estudio de Atlas VPN, publicado en marzo de 2020, indicó que solo en Estados Unidos, el 83% de los sistemas y programas de los centros de salud operan con sistemas operativos de versiones muy anteriores, lo que imposibilita obtener actualizaciones esenciales de seguridad dejando múltiples vulnerabilidades que los ciber-delincuentes pueden usar para los ciberataques.

Sistemas Operativos Usados por la Industria de la Salud -US -2020



Fuente: Atlas VPN, sistemas de salud con programas desactualizados, elaboración propia

5. Dark Web: Se refiere a un conjunto de páginas web que no son identificables por los motores de búsqueda, donde se realizan operaciones ilegales, como venda de bienes y servicios, así como archivos o bases de datos que no se encuentran abiertos al público que usualmente pertenecen a información privada y sensible que administran empresas con respecto a sus clientes o aliados. (Kaspersky).

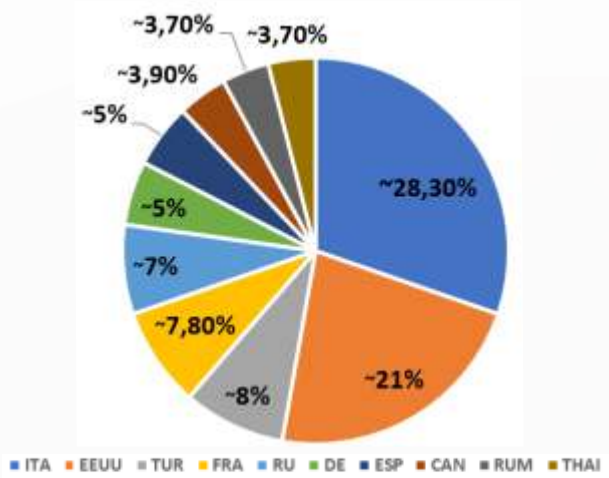
Adicionalmente, este estudio revelo que el 26% de los dispositivos de monitoreo de pacientes con coronavirus, están en riesgo de sufrir un hackeo y cerca del 16% de los sistemas de imágenes diagnosticas están en el 51% de riesgo de sufrir un ataque de hacking.

En el mismo sentido y de acuerdo con el artículo "Ensuring Cybersecurity for critical civilian infrastructure" publicado por los autores Marietje Shaake y Stéphane Duguin, no solo es necesario apoyar el personal de la salud sino también reconocer la importancia de la tecnología en esta industria y asegurar que está protegida contra las amenazas externas. Del mismo modo, mencionan que además de los retos que los profesionales de la salud enfrentan atendiendo a los pacientes de COVID y horas extras, también tiene que afrontar los ciberataques dirigidos a los centros de salud con campañas de ransomware y demás que usen los ciberdelincuentes.

La industria de la salud ha logrado avances importantes en temas de digitalización y menos consumo de papel, así como también manteniendo los perfiles de los pacientes en sistemas informáticos que permiten consultar a cualquier profesional la historia clínica de un paciente desde cualquier lugar. Sin embargo, entre más avanzados estos sistemas y más abierta la puerta a mantener datos en la nube, los ciberdelincuentes han aumentado los ciberataques, con la intención de generar brechas de información. Lo alarman te de estos desarrollos es que el nivel de inversión en sistemas de seguridad y de sistemas de protección de datos, es relativamente bajo comparado con otras industrias como la financiera, tal y como lo arrojó una encuesta a profesionales de seguridad de las entidades de la salud conducida por Black Book Market Research, en la que se indica que el presupuesto para 2020 destinado a Ciberseguridad fue de una asignación de menos del 1% del total del presupuesto en tecnología; mientras que el sector bancario destina alrededor del 10,4%, y el sector gobierno del 11.9%, según arrojan resultados de "IDC" en su documento" Worldwide Semiannual Security Spending Guide.

De acuerdo con un reporte de Bitdefender, la industria de la salud ha sido el quinto sector más atacado en el mundo; esta situación en Estados Unidos revela que fue el segundo país más atacado después de Italia. Los riesgos Asociados a la exposición de datos personales, tras fuga de información de las entidades de salud, mediante ataques dirigidos a dichas entidades, tiene un agravante implícito.

Los 10 países más afectados por ciber ataques en el 2020 en sector salud



Fuente: Antimalware Research, Bitdefender.20-3-2020

La filtración de los registros de datos de las personas afiliadas a entidades de salud o quienes hayan recibido tratamientos médicos en clínicas y hospitales, poniendo exponiendo dichos documentos en la Dark Web, no solo se vulnera el derecho a la confidencialidad de su estado de salud, sino que con esta información pueden generarse diferentes crímenes: robo de identidad para fraudes financieros, ya que es más fácil tener dichas bases de datos de las entidades de salud que de las entidades financieras, fraudes de seguro, ya que con dicha información pueden generarse suplantaciones de clientes para hacer efectivas las coberturas de tratamientos médicos, extorsiones a los pacientes por la no publicaciones de historiales clínicos, extorsiones de rescate de sitios web a hospitales con amenazas de borrar, modificar o inclusive bloquear los equipos para imposibilitar la correcta operatividad de dichos establecimientos, sin mencionar el grave impacto a la salud de los pacientes y su integridad humana.

De acuerdo con un reporte de CBC Canadá, a principios de abril, los historiales médicos podrían costar en la Dark Web alrededor de 200 Dólares y de acuerdo con un experto citado en dichos reportes, la industria de la salud de Canadá se encuentra 20 años atrás de los Bancos con respecto a las prácticas de Ciber higiene. Del mismo modo Bitdefender, reportó que los ciberataques a hospitales solo para el mes de marzo de 2020 se incrementaron en el 60% comparado con el mes de febrero del mismo año.

Evolución Global de CIBER-ATAQUES Dirigidos a Hospitales

Fuente: Bitfedender, Ciberataque de ransomware al sector salud, aumenta durante pandemia, 13-5-2020

Otros reportes de Bitdefender, mencionan que los incidentes de seguridad del sistema de salud también han mostrado que listas más completas de datos pueden llegar a ser vendidos en Dark Web hasta por 250 dólares por un solo registro médico siendo este costo 50 veces más que el que incurren los ciberdelincuentes en un solo registro de tarjeta de crédito.

De acuerdo con el Departamento de Salud y Servicios Humanos (HHS) por sus siglas en inglés, de los Estados Unidos, se espera que estas fugas de información cuesten alrededor 4 mil millones dólares en 2020 y los datos potenciales que pueden parar a manos de los cibercriminales comprenden: Nombre, dirección, número de teléfono, dirección e-mail, número de identificación, beneficiarios, información financiera, datos biométricos, ADN, exámenes de diagnóstico y características de identificación física, todos estos datos facilitan los procesos de ingeniería social y de suplantación de personas.

Estos datos, llaman urgentemente a la preparación, indicando que blindarse aisladamente no es la solución. Si bien es vital que todas y cada una de las entidades estén a la vanguardia de soluciones tecnológicas, preparadas con personal especializados y con una destinación de recursos contundente, si las empresas no se encuentran articuladas en un entorno colaborativo y unidas desde un solo frente desde su misma industria y entre industrias, sus esfuerzos aislados pueden ser en vano. Las organizaciones delincuenciales han demostrado su nivel de escalabilidad delictiva y alta acción de creatividad para el perfeccionamiento de dichas actividades y creación de nuevas líneas de negocio que afectan a la economía transversalmente en todas sus industrias.

A través de esta breve nota, FELABAN considera que la solución cooperativa es primordial actualmente. Un incidente en una industria como la de la salud, puede tener impactos desastrosos en industrias como la financiera y la integridad de datos sensibles de los ciudadanos. Por esto, el llamado a tener una visión integral no solo desde la banca, sino desde la perspectiva de cooperación las autoridades y todos los sectores económicos sin excepción es fundamental.

Bibliografía recomendada sobre el tema

Diccionario para estudiantes de Oxford, Definición Phishing, en:
https://www.oxfordlearnersdictionaries.com/us/definition/american_english/phishing

-Norton. ¿Qué es el mishing? co.norton.com, en:
https://co.norton.com/internetsecurity-emerging-threats-what-is-smishing.html

-Kaspersky, What is Vishing?, Kaspersky.com, en:
https://www.kaspersky.com/resource-center/definitions/vishing

-Kaspersky, What is Social Engineering?, Kaspersky.com, en:
https://latam.kaspersky.com/resource-center/definitions/what-is-social-engineering

-Kaspersky, Cyber Threats and Dangers on the Deep (Dark) Web, en:
https://www.kaspersky.com/resource-center/threats/deep-web

-The Hill, (2020, April 16), FBI sees spike in cyber crime reports during coronavirus pandemic, thehill.com, en:
https://thehill.com/policy/cybersecurity/493198-fbi-sees-spike-in-cyber-crime-reports-during-coronavirus-pandemic

-Bitdefender. (2020, May 13). Global Ransomware and Cyberattacks on Healthcare Spike during,Pandemic. Bitdefender.com., en:
https://labs.bitdefender.com/2020/05/global-ransomware-and-cyberattacks-on-healthcare-spike-during-pandemic/

-Bitdefender. (2020, March 17). US is fighting COVID-19 with 83% of healthcare systems running on outdated software. atalsvpn.com, en:
https://atlasvpn.com/blog/us-is-fighting-covid-19-with-83-percent-of-healthcare-systems-running-on-outdated-software

-CBC Canada. (2020, June 2). US is fighting COVID-19 with 83% of healthcare systems running on outdated software. atalsvpn.com, en: https://www.cbc.ca/news/canada/nova-scotia/hospitals-health-care-cybersecurity-federal-government-funding-1.5493422

-MARIETJE SCHAAKE , STÉPHANE DUGUIN. (9-6-2020). Ensuring Cybersecurity for Critical Civilian Infrastructure. Recuperado de Ensuring Cybersecurity for Critical Civilian Infrastructure, en: https://www.project-syndicate.org/commentary/cybersecurity-against-attacks-on-hospitals-by-marietje-schaake-and-stephane-duguin-2020-06

-El tiempo. (2020, April 17). Gmail bloquea correos maliciosos relacionados con covid-19. eltiempo.com, en:
https://www.eltiempo.com/tecnosfera/novedades-tecnologia/gmail-bloquea-correos-maliciosos-relacionados-con-coronavirus-485606

-Caracol. (2020, April 24). OMS denuncia filtración de 450 correos y contraseñas de funcionarios. caracol.com.co, en:
https://caracol.com.co/radio/2020/04/24/tecnologia/1587729056_815504.html

-La Vanguardia. (2020, April 20). ¿Por qué los ciberdelincuentes están suplantando a la OMS y a Netflix en las redes? lavanguardia.com, en: https://www.lavanguardia.com/seguros/empresa/20200420/48627317821/ciberdelincuencia-oms-netflix-fraude-seguros.html

-NBC News. (2020, April 22). Logins of WHO, Gates Foundation employees circulate on fringes of the internet. nbcnews.com en:
https://www.nbcnews.com/tech/security/logins-who-gates-foundation-employees-circulate-fringes-internet-n1189636

-Bitdefender. (20-3-2020). 5 Times More Coronavirus-themed Malware Reports during March, Antimalware Research, en:
https://labs.bitdefender.com/2020/03/5-times-more-coronavirus-themed-malware-reports-during-march

-Atlas vpn. (17-3-2020). US is fighting COVID-19 with 83% of healthcare systems running on outdated software, en:
https://atlasvpn.com/blog/us-is-fighting-covid-19-with-83-percent-of-healthcare-systems-running-on-outdated-softwarr

-Bitdefender. (13-5-2020). Global Ransomware and Cyberattacks on Healthcare Spike during Pandemic., en:
https://labs.bitdefender.com/2020/05/global-ransomware-and-cyberattacks-on-healthcare-spike-during-pandemic/

SECRETARÍA GENERAL DE FELABAN

GIORGIO TRETTENERO CASTRO
Secretario General
gtrettenero@felaban.com

JORGE ARTURO SAZA G.
Director Económico
jsaza@felaban.com

DANIEL JUVINAO
Director Concentrador de Fraudes Regional
y Proyectos especiales
djuvinao@felaban.com

LAURA M. GORDILLO V.
Directora Adjunta Concentrador de Fraudes
Regional
lgordillo@felaban.com

ADRIANA RODRÍGUEZ
Diseñadora Gráfica
arodriguez@felaban.com

FIC FRAUD INFORMATION CONTROL by FELABAN

FELABAN FEDERACION LATINOAMERICANA DE BANCOS
55 AÑOS 1965 - 2020

siganos en: