FS/ASSI – CURSO 2019-2020

Giacomo Mossio

– PRÁCTICA 2 –

INFORME SOBRE NOTICIAS EN LA PRENSA DIGITAL Y ESCRITA RELATIVAS A AMENAZAS INFORMÁTICAS

HACKERS CAN TURN YOUR HOME COMPUTER INTO A BOMB

. . . & blow your family to smithereens!

By RANDY JEFFRIES / *Weekly World News*

WASHINGTON — Right now, computer hackers have the ability to turn your home computer into a bomb and blow you to Kingdom Come — and they can do it anonymously from thousands of miles away!

Experts say the recent "break-ins" that paralyzed the Amazon.com, Buy.com and eBAY websites are tame compared to what will happen in the near future.

Computer expert Arnold Yabenson, president of the Washington-based consumer group National CyberCrime Prevention Foundation (NCPF), says that as far as computer crime is concerned, we've only seen the tip of the iceberg.

"The criminals who knocked out those three major online businesses are the least of our worries," Yabenson told *Weekly World News*.

"There are brilliant but unscrupulous hackers out there who have developed technologies that the average person can't even dream of. Even people who are familiar with how computers work have trouble getting their minds around the terrible things that can be done.

"It is already possible for an assassin to send someone an e-mail with an innocent-looking attachment connected to it. When the receiver downloads the attachment, the electrical current and molecular structure of the central processing unit is altered, causing it to blast apart like a large hand grenade.

"As shocking as this is, it shouldn't surprise anyone. It's just the next step in an ever-escalating progression of horrors conceived and instituted by hackers."

Yabenson points out that these dangerous sociopaths have already:

- **Vandalized FBI and U. S. Army websites.**
- **Broken into Chinese military networks.**
- **Come within two digits of cracking an 87-digit Russian security code that would have sent deadly missiles hurtling toward five of America's major cities.**

"As dangerous as this technology is right now, it's going to get much scarier," Yabenson said.

"Soon it will be sold to terrorists cults and fanatical religious-fringe groups.

"Instead of blowing up a single plane, these groups will be able to patch into the central computer of a large airline and blow up hundreds of planes at once.

"And worse, this e-mail bomb program will eventually find its way into the hands of anyone who wants it.

"That means anyone who has a quarrel with you, holds a grudge against you or just plain doesn't like your looks, can kill you and never be found out."

KABOOM! It might not look like it, but an innocent home computer like this one can be turned into a deadly weapon.

Sickos can wreak death and destruction from thousands of miles away!

Arnold Yabenson.

Índice

1.- Noticias relativas a: Phising, estafas a través de la red

1.1.- Noticia 1: **Furto di dati alla Pubblica amministrazione, hacker in manette**

Fecha de la noticia: **22/11/2019**

Título de la noticia: **Furto di dati alla Pubblica amministrazione, hacker in manette**

Enlace a la noticia: https://www.repubblica.it/cronaca/2019/11/22/news/furto_di_dati_alla_pubblica_amministrazione_hacker_finisce_in_manette-241621581/

Medio (prensa digital): **la Repubblica**

Enlace al medio: www.repubblica.it

Nacionalidad del medio: **italiana**

Idioma de la noticia: **italiano**

Breve resumen de la noticia :

Un cracker de 66 años que tenía muchas competencias informáticas, y también muchos antecedentes penales, ha obtenido miles de informaciones sensibles de los ciudadanos italianos. Su estrategia consistía en el infectar computadores de los empleados públicos con la técnica del phishing y, después robar los dato, los almacenaba en server extranjeros creándose su propia base datos. Gracias también a 6 cómplices, el cracker gestionaba también un portal llamado 'PEOPLE1' que usaba para vender el acceso a los datos sensibles a las empresas interesadas. Fueron comprobados decenas de miles de accesos al portal PEOPLE1 sobre pagamento y acceder a un singolo dato costaba 1 euro.

Relación con la amenaza:

La técnica de phishing era usada para obtener el control de los computadores de los empleados públicos

Impacto ocasionado por la amenaza en esta noticia:
El objetivo del cracker era robar los datos sensibles de los ciudadanos inconscientes para venderlos después. Aunque el impacto no es inmediato (no se robaba dinero) la cantidad de ganancia era muy elevada considerando el pago de 1 euro solicitado para acceder a un singolo dato. El impacto ocasionado fue que los datos fueron distribuidos a cualquier empresa sin permiso y cómo estas impresas utilizaban los datos no podemos saberlo, entonces es muy difícil de estimar pero se puede entender la entidad del daño desde cuanto las empresas eran dispuestas a pagar. La violación de la privacidad de los ciudadanos fue el impacto mayor.

1.2.- Noticia 2: **Dutch man loses €1 million to phishing sms**

Fecha de la noticia: **04/12/2019**
Título de la noticia: **DUTCH MAN LOSES €1 MILLION TO PHISHING SMS**
Enlace a la noticia:
https://nltimes.nl/2019/12/04/dutch-man-loses-eu1-million-phishing-sms
Medio (prensa digital): **NL Times**
Enlace al medio: nltimes.nl
Nacionalidad del medio: **holandés**
Idioma de la noticia: **inglés**

Breve resumen de la noticia:
La noticia trata de un hombre que en una noche perdió un millón de euros. El hombre recibió un SMS, creyendo que llegaba de su banco, donde estaba escrito que su carta de débito estaba agotándose, accediendo al enlace del SMS el hombre puso los datos de su carta para renovarla y simplemente se fue a dormir. La mañana después se dio cuenta que había sido robado de más de un millón de euros y inmediatamente denunció todo a la policía. Después las investigaciones se

descubrió que el dinero había sido distribuido por 136 otras cuentas. Todavía no se sabe cuánto dinero se podrá recuperar pero se espera la mayoría dado que las cuentas son rastreables y probablemente el dinero llegado en esas cuentas fue congelado inmediatamente porque inusual.

Relación con la amenaza:
El SMS enviado conducía a un sitio falso donde la víctima puso sus datos, un perfecto ejemplo de phishing

Impacto ocasionado por la amenaza en esta noticia:
El impacto ocasionado fue inmediato y la víctima se vio desaparecer un millón de euros en una noche, dicho esto no podemos afirmar que fue un daño de un millón de euros porque la mayoría del dinero será recuperada aunque el dinero fue distribuido entre muchas cuentas y por cierto no se recuperará todo. Leyendo un millón de euros puede parecer un impacto grande pero al final no es grave porque afectó a una sola persona y las pérdidas se limitan meramente a un aspecto económico. Todavía no se sabe cuanto se pudo recuperar pero ya solamente que se puede cuantificar el daño es algo que disminuye la gravedad del impacto.

1.3.- Comparativa entre noticias

La grande diferencia entre los dos ataques es que el primero fue más organizado y planeado mientras el segundo fue algo de fortuito y con el objetivo de obtener algo en el inmediato. El primero constituye una amenaza mayor porque fueron afectados miles de ciudadanos y, aunque no fue robado dinero, fueron robados datos sensibles que son muy relevantes.
En el primer caso se sabe que el estafador tiene mucha competencias y experiencia en este campo; esto se puede entender desde su organización y su estrategia, el cracker no se limita a robar algo, él crea servicios basados sobre los datos robados. Todo esta planificación requiere mucho trabajo pero al final es mucho más peligrosa de la segunda y es también mucho más difícil de descubrir.

Ambos los ataques pero tienen algo en común, y es la técnica utilizada para estafar; en el primer caso el cracker se fingía una autoridad pública para obtener las informaciones necesarias a obtener el control de las máquinas mientras en el segundo caso el estafador se fingía una otra autoridad, un banco, para obtener los datos de las carta de debito. En ambas las situaciones los estafadores usaron el engaño para hacerse pasar por algo autorevole y simplemente preguntando los datos relevantes.

2.- Noticias relativas a: Malware en redes sociales

2.1.- Noticia 1: **Instagram, violato l'account di Laura Pausini: "Regalo smartphone Apple"**

Fecha de la noticia: **24/11/2019**

Título de la noticia: **Instagram, violato l'account di Laura Pausini: "Regalo smartphone Apple"**

Enlace a la noticia: https://www.repubblica.it/tecnologia/social-network/2019/09/24/news/instagram_violato_l_account_di_laura_pausini_regala_smartphone_apple_-236819072/

Medio (prensa digital): **la Repubblica**

Enlace al medio: www.repubblica.it

Nacionalidad del medio: **italiana**

Idioma de la noticia: **italiano**

Breve resumen de la noticia:

La cuenta de Instagram de una famosa cantante italiana, llamada Laura Pausini, con casi 3 millones de seguidores ha sido hackeado. Los estafadores han aprovechado del control de la cuenta para editar la bio, publicar un post y añadir contenido a las historias. En esos lugares han escrito las clásicas frases engañosas prometiendo iPhone, Macbook, Apple Watch y muchos otros premios de regalo (con un pésimo italiano demostrando la probable nacionalidad extranjera) y poniendo un enlace para

obtener dichos regalos. Claramente no existía ningún iPhone o similar de regalo y las víctimas eran redirigidas en un sitio que pedía de descargar malware para obtener el premio.

Relación con la amenaza:
La visibilidad de Instagram fue explotada para alcanzar más personas posibles con la publicidad engañosa y estafar las víctimas haciéndole instalar malware.

Impacto ocasionado por la amenaza en esta noticia:
La estimación del impacto en este caso es bastante difícil pero se puede empezar pensando que la cuenta tenía 2,8 millones de seguidores. Haciendo estimaciones personales, se puede suponer que 1 millón de personas vio el post o la historia, de estas suponemos que "solamente" 20 mil han abierto el enlace y finalmente 2 mil personas han descargado malware. Considerando estas estimaciones observamos que la percentual de engañados es muy baja frente al número inicial pero, gracias a la visibilidad de las redes sociales, el número final no puede ser ignorado. Hay también de tener en cuenta el daño a la imagen pública de la cantante que por cierto empeoró un poco.

2.2.- Noticia 2: **Get a weird Facebook message? It might be an attempt to scam you**

Fecha de la noticia: **24/09/2019**
Título de la noticia: **Get a weird Facebook message? It might be an attempt to scam you**
Enlace a la noticia:
https://www.news4jax.com/2019/09/24/get-a-weird-facebook-message-it-might-be-an-attempt-to-scam-you/
Medio (prensa digital): **News4Jax**
Enlace al medio: www.news4jax.com
Nacionalidad del medio: **Estadounidense**

Idioma de la noticia: **inglés**

Breve resumen de la noticia:
La estafa que trata la noticia no es nueva, es algo que circula por Facebook hace mucho tiempo. La estafa empieza con el recibo de un mensaje desde un tu amigo de Facebook que capta la atención escribiendo: “No me lo puedo creer! Creo que te grabaron en esto video! Puedes confirmar?” y el enlace para acceder al supuesto video. Cuando se intenta a acceder al video, se llega en una pagina clon de Facebook que pide efectuar el acceso a la red social; una vez insertado los datos, un malintencionado guarda la contraseña de Facebook obtenida y, efectuando el acceso con tu perfil envía el mismo mensaje a todos tus amigos.

Relación con la amenaza: Las cuentas de Facebook son usadas para guardar más contraseñas posibles

Impacto ocasionado por la amenaza en esta noticia:
La noticia descrita puede parecer casi inocua porque aunque alguien puede acceder a cuentas facebook de otras personas, no puede directamente robar dinero pero el objetivo en esta estafa es diferente. Los estafadores aprovechan la debilidad de las contraseñas de la gente, en ese caso particular explotan el hecho de que la gente utilice la misma contraseña para muchas cuentas de diferentes plataformas. Una vez obtenida la contraseña de Facebook de una persona, intentarán la misma contraseña en diferentes plataformas, esperando que la gente sea tan descuidada de usar la misma contraseña en diferentes lugares, por ejemplo en la cuenta de Amazon, donde está conectada una carta lista para comprar artículos.

2.3.- Comparativa entre noticias

En ambas las noticias la probabilidad que alguien cada en la trampa inventada es muy baja porque esta tipología de estafa es una de las más conocidas en la red.

Dicho esto, la difusión de estos timos sigue sobre las redes sociales porque la cantidad de gente al que se puede alcanzar es muy alta aprovechando de la estructura a telaraña sobre la cual las redes sociales se basan y tienen sus fortaleza. En la primera noticia, los malintencionados aprovechan de la visibilidad que tiene una cuenta con millones de seguidores para llegar al mayor número de personas, mientras en la segunda noticia intentan a aprovecharse de la confianza que todos tenemos entre nuestros amigos de las redes sociales.

Los ataques trámite las redes sociales casi siempre no quieren dañar a nadie en particular, podemos decir que son indiscriminadas. Este factor no ayuda los estafadores porque siendo mensajes sin personalización, tienden a ser menos creíbles; hay también pero malware que pueden poner automáticamente el nombre del destinatario, así que parezcan más reales.

En estos casos es siempre muy difícil cuantificar los daños porque es también difícil identificar quien cayó en la trampa, pero no se deben subestimar porque revelar su propia contraseña puede tener amplios efectos no deseados.

3.- Noticias relativas a: Ataques dirigidos contra grandes corporaciones y gobiernos

3.1.- Noticia 1: **Ransomware attack targets Portuguese energy company**

Fecha de la noticia: **17/04/2020**

Título de la noticia: **Ransomware attack targets Portuguese energy company**

Enlace a la noticia:

https://micky.com.au/ransomware-attack-targets-portuguese-energy-company/

Medio (prensa digital): **Micky**

Enlace al medio: https://micky.com.au/

Nacionalidad del medio: **australiana**

Idioma de la noticia: **inglés**

Breve resumen de la noticia:
La noticia trata de un ataque ransomware de un grupo de hackers directo a una multinacional portuguesa llamada Energias de Portugal que opera en 19 países. Los hackers han conseguido robar 10 terabyte de datos privados del grupo industrial portugués y quieren un pago de 1,580 bitcoins (más que 10 millones de euro al 17/04/2020) para no render públicas las informaciones en su poder. Los datos robados incluyen informaciones privadas de los clientes, contratos, transacciones, socios y mucho más. Los estafadores han publicado un mensaje pidiendo el dinero y demostrando efectivamente con imágenes de poseer los datos guardados en sus servers.

Relación con la amenaza: El ataque es directo a una grande corporación

Impacto ocasionado por la amenaza en esta noticia:
Los atacantes han usado un ransomware llamado Ragnar locker [1] para cifrar los datos de la multinacional. El rescate que piden los estafadores es de 10 millones de euro y puede parecer una cifra exagerada pero es una cifra sustancial considerando que los datos robados tienen mucho valor. Conseguir infiltrarse en un sistema tan grande y importante demonstra que los atacantes son un grupo con experiencia y el ataque fue organizado con escrúpulo. Si “Energias de Portugal” cederá al chantaje, los daños se pueden cuantificar en 10 millones de euro, y cifras de este orden se pueden permitirse solamente de grandes corporaciones.

3.2.- Noticia 2: **Hacker attaccano 42 server dell’ONU, sconosciuta l’entità dei danni**

Fecha de la noticia: **30/01/2020**

Título de la noticia: **Hacker attaccano 42 server dell'ONU, sconosciuta l'entità dei danni**

Enlace a la noticia:
https://www.ilfattoquotidiano.it/2020/01/30/hacker-attaccano-42-server-dellonu-sconosciuta-lentita-dei-danni/5690364/

Medio (prensa digital): **il Fatto Quotidiano**

Enlace al medio: https://www.ilfattoquotidiano.it/

Nacionalidad del medio: **italiana**

Idioma de la noticia: **italiano**

Breve resumen de la noticia:

El artículo trata de un ataque informático dirigido a servidores de la Organización de las Naciones Unidas en Viena y Ginebra. El ataque empezó en el julio del 2019 pero los primeros señales de alerta se remontan al 30 de agosto cuando un grupo de informáticos que trabaja en las ONU señaló una posible intrusión a daños de los servidores. Según las reconstrucciones [2], el ONU intentó a esconder el suceso al exterior y también en su interior, por eso las informaciones son un poco confundidas. Las estimaciones hablan de 400 GB de datos robados y la identidad de los malintencionados sigue siendo desconocida pero se sospecha que los hackers pueden tener el apoyo de algún gobierno.

Relación con la amenaza:

El ataque tiene por objeto una organización a nivel mundial, la ONU

Impacto ocasionado por la amenaza en esta noticia:

El impacto en esta situación es muy difícil de estimar porque se intentó a esconder la noticia a la opinión pública pero cuando se habla de organizaciones a nivel mundial siempre es algo de grande importancia. La intrusión afectó a decenas de server en Viena y en Ginebra y fueron comprometidos componentes infrastructural y puede que fueron robados documentos internos, bases de datos, correos, informaciones comerciales y datos personales. En estas situaciones el impacto generado solitamente no es de carácter económico, sino de carácter político; por

eso se sospecha el apoyo de gobiernos. Aunque no se registraron daños económicos, esto no sustrae importancia a la noticia, al contrario hay que tener mucho cuidado a esta tipología de ataques.

3.3.- Comparativa entre noticias

En ambas las noticias los ataques son orientados a grandes corporaciones pero la diferencia es que en la primera el objetivo es una corporación privada mientras en la segunda es pública; por eso el carácter que encontramos es economico nel primer caso y político en el segundo. Cuando los ataques son de esas magnitud casi siempre hay detrás un grupo de hackers y no una singula persona, y cuando tienen carácter político, casi siempre los atacantes son dirigidos por gobiernos de países. Conseguir irrumpir en sistemas informáticos de esto nivel por cierto no es algo de sencillo y esto puede contarnos mucho sobre los atacantes.
En ambas las noticias lo que sabemos al final es filtrado por los periódicos y cuando se trata de numeros grande es siempre muy difícil saber toda la verdad y reconstruir a la perfección las noticias, aún más cuando se hable de gobiernos.
Esta tipología de ataque suele aprovecharse, como la mayoría de otras tipologías, de la debilidad humana, aprovechando de la imprudencia de los empleados para obtener el acceso a las redes de las corporaciones. La única manera de aumentar la seguridad desde esta perspectiva es educar los empleados sobre la materia gracias a cursos de entrenamiento específico.

4.- Noticias relativas a: Botnets y ordenadores zombies

4.1.- Noticia 1: **Microsoft takes down global zombie bot network**

Fecha de la noticia: **11/03/2020**

Título de la noticia: **Microsoft takes down global zombie bot network**

Enlace a la noticia: https://www.bbc.com/news/technology-51828781

Medio (prensa digital): **BBC**

Enlace al medio: https://www.bbc.com/

Nacionalidad del medio: **británica**

Idioma de la noticia: **inglés**

Breve resumen de la noticia:

El artículo en cuestión anuncia la derrota de una red global de ordenadores zombie llamada Necurs [3]. Esta botnet era una de las más grandes en el mundo (infectó a un total de más de 9 millones de ordenadores) y apareció por primera vez en el 2012. Equipos de informáticos de 35 países diferentes, dirigidos por Microsoft, trabajaron 8 años para eliminar definitivamente la botnet [4]. La botnet es famosa por distribuir una cantidad elevadísima de malware principalmente trámite correos y se cree que era bajo el control de hackers rusos. El funcionamiento de Necurs se basaba sobre un algoritmo para generar dominios que eran después convertidos en sitios web y usados para controlar los ordenadores infectados; los equipos de técnicos, conociendo esta preciosa información, pudieron romper el algoritmo y entonces predecir los próximos dominios que generará para 25 meses. Deshabilitando los dominios existentes y no permitiendo la generación de nuevos, la botnet puede considerarse derrotada.

Relación con la amenaza:

Necurs era una entre las botnets más grande del mundo

Impacto ocasionado por la amenaza en esta noticia:

Los impactos de Necurs son muy amplios y a nivel global considerando que se puede afirmar que prácticamente la totalidad de los países del mundo tenían al menos un ordenador infectado. El equipo de Microsoft analizó las actividades de un singolo ordenador infectado y en un periodo de 58 días se observó el envío de 3,8 millones de correos de spam. Las utilidades de una botnet son muchas y esta fue usada por spamming, varias estafas, robar credenciales, robar datos personales y confidenciales; además de eso, parte de la botnet se podía alquilar o comprar tras un pagamento y, aunque no se conocen ataques DDos, la capacidad de esto no se pone en duda.

4.2.- Noticia 2: **La 'botnet' de sextorsión Phorpiex controla 450.000 equipos con capacidad para extorsionar a 27 millones de personas**

Fecha de la noticia: **17/10/2019**

Título de la noticia: **La 'botnet' de sextorsión Phorpiex controla 450.000 equipos con capacidad para extorsionar a 27 millones de personas**

Enlace a la noticia: https://www.lavanguardia.com/vida/20191017/471033546239/la-botnet-de-sextorsion-phorpiex-controla-450000-equipos-con-capacidad-para-extorsionar-a-27-millones-de-personas.html

Medio (prensa digital): **La Vanguardia**

Enlace al medio: https://www.lavanguardia.com/

Nacionalidad del medio: **española**

Idioma de la noticia: **español**

Breve resumen de la noticia:

El artículo es una description de la botnet llamada Phorpiex que se estima controlar 450.000 ordenadores en todo el mundo. Esta botnet es usada principalmente para enviar correos de sextorsion, osea correos en la que el ciberdelincuente chantajea a la víctima y exige un pago bajo amenaza de exponer contenido sexual del receptor y para aumentar el miedo se envian tambien contraseñas del receptor, si en poseso.

La practica de sextorsion es solamente el ultimo utilizo de la botnet, Phorpiex está circulando por la red desde más que una década y antes fue ya utilizada para distribuir malware como GrandCab, Pony o Pushdo, y utilizando a sus víctimas para minar criptomonedas. Su capacidad de difusión estimada es de 30 mil correos por hora llegando en total a 27 millones de usuarios diferente.

Relación con la amenaza:
Phorpiex es una otra famosa botnet

Impacto ocasionado por la amenaza en esta noticia:
Los impactos de una botnet son gigantes porque las tipologías de ataques que se tienen con un ejército de ordenadores infectados son muchísimas. En este caso particular, segundo una análisis de check point research [6] la ganancia de esta botnet es estimada en medio millón de dólares americanos anualmente. Los modos de generar dinero con una botnet son varios, por ejemplo sextorsion, minería de criptomonedas, difusion de otros malware, ransomware varios y muchos más. Para entender las cifras de que estamos hablando podemos decir que el tráfico estimado generado de esta botnet es de 70 TB al mes y la mayoría del tráfico está en Asia.

4.3.- Comparativa entre noticias

Las botnets se crean con el tiempo, trámite la propagación de virus o gusanos que permit a malintencionados de controlar ordenadores sin que el propietario se dé cuenta de lo que está pasando y entonces sin su permiso. El desplazamiento de identidad hace que los criminales puedan cumplir acciones ilegales sin ser descubiertos y puedan ejecutar ataques con una potencia de cálculo enorme dado el grande número de ordenadores controlados.
En esos artículos se ha hablado sobre dos botnets muy grandes que tienen muchos factores en común. Desde las noticias podemos entender que las botnets se pueden usar para cumplir varios crímenes y por eso son muy peligrosas. Las aplicaciones principales son el envío de spam, la minería de criptomonedas y los ataques DDos.

Por eso la aplicaciones de ambas las botnets son similar, solamente puede variar el porcentaje de utilización para las diferentes actividades. Necurs era más grande y tenía una extensión a nivel global mientras Phorpiex era más concentrada en Asia y tenía menos ordenadores infectados. Lo único que pueda limitar esas botnet es el tráfico de datos que genera controlar muchos ordenadores contemporaneamente, ese tráfico difícilmente puede pasar inadvertido a los ojos de los expertos de seguridad y muchas veces dicho tráfico es lo que permite descubrir los servidores privados virtual trámite que se controlan los ordenadores zombie.

5.- Noticias relativas a: Malware en dispositivos móviles

5.1.- Noticia 1: **"Clicca qui e ti dico chi è contagiato": così il malware che sfrutta il coronavirus attacca gli smartphone**

Fecha de la noticia: **25/03/2020**

Título de la noticia: **"Clicca qui e ti dico chi è contagiato": così il malware che sfrutta il coronavirus attacca gli smartphone**

Enlace a la noticia: https://www.repubblica.it/tecnologia/sicurezza/2020/03/25/news/_clicca_qui_e_ti_dico_chi_e_contagiato_cosi_il_malware_che_sfrutta_il_coronavirus_attacca_gli_smartphone-252294097/

Medio (prensa digital): **la Repubblica**

Enlace al medio: https://www.repubblica.it/

Nacionalidad del medio: **italiana**

Idioma de la noticia: **italiano**

Breve resumen de la noticia:

Ginp es un troyano que se ha evolucionado desde su primera versión y tiene como objetivo los móviles Android. En esta noticia se alertan los ciudadanos de la periculosidad del troyano que en la versión actual aprovecha de la pandemia global

del COVID-19 para engañar sus víctimas. Su medio de transmisión principal son los SMS pero, siendo un troyano, se puede descargar escondido mientras se descargan otras aplicaciones. La estafa que los criminales intentan a poner en práctica se basa sobre la falta de información que todos tenemos sobre los infectados del COVID-19; el mensaje recibido tiene escrito algo como: “quieres saber quien está contagiado acerca de ti?”, abriendo el enlace del mensaje se llega en una página llamada “Coronavirus Finder” que pide el pago de 75 céntimos para obtener las informaciones requeridas, una vez insertados los datos de la carta, obviamente no se obtiene nada y ahora los cibercriminales pueden disfrutar sus compras online con los datos de la carta robados.

Relación con la amenaza:
El medio de transmisión del troyano son los móviles Android

Impacto ocasionado por la amenaza en esta noticia:
Aprovechándose de la situación actual los estafadores intentan obtener las cartas de las víctimas, la ingeniería social utilizada está reforzada dal panico general de este periodo y de la falta de información resultante. La elección de los SMS como medio de transmisión puede parecer rara hoy en dìa pero se debe tener en cuenta que muchas cartas de crédito utilizan SMS como sistema de confirmación para las compras y obtener el acceso a los SMS además de los datos de la carta significa pleno control de la carta. Una estimación de los daños generado da Ginp resulta difícil pero teniendo en cuenta lo que pueda pasar a los estafadores si descubiertos, y viendo el continuo desarrollo de software similares se puede entender la ganancia económica de esta tipología de malware.

5.2.- Noticia 2: **New Android Ransomware Threatens FBI Action Unless You Hand Over Credit Card Details**

Fecha de la noticia: **30/04/2020**

Título de la noticia: **New Android Ransomware Threatens FBI Action Unless You Hand Over Credit Card Details**

Enlace a la noticia:
https://www.forbes.com/sites/leemathews/2020/04/30/new-android-ransomware-threatens-fbi-action-unless-you-hand-over-credit-card-details/#6dd72a57180f

Medio (prensa digital): **Forbes**

Enlace al medio: www.forbes.com

Nacionalidad del medio: **estadounidense**

Idioma de la noticia: **inglés**

Breve resumen de la noticia:

La noticia en cuestión habla sobre otro malware que circula por la red, llamado Black Rose Lucy [7] y generado en Rusia. Su existencia fue descubierta en el 2018 pero antes era usado para obtener el control de los móviles (botnet) y añadir cargas útiles, mientras ahora es un auténtico ransomware. Para obtener la autorización a instalar el malware en los móviles, los cibercriminales engañan a las víctimas diciéndole que se necesita la instalación de un reproductor de videos para ver películas en sitios poco recomendables. Una vez autorizado y descargado en el móvil, todos los archivos serán cifrados con la extensión .Lucy comunicando a las víctimas que la encriptación se debe al hecho que las víctimas han visitado sitios pornografico illegales y para evitar problemas judiciales tienen que pagar una multa de 500 dólares.

Relación con la amenaza:

Lucy se aprovecha de la libertad dejada a los usuarios Android

Impacto ocasionado por la amenaza en esta noticia:

El malware que infecta los móviles en este caso es un ransomware con la adición de sextorsion. La ingeniera social usada aquí intenta a intimidar las víctimas haciéndolas creer de la existencia de un foto incriminatoria seguida de una amenaza de problemas judiciales, algo que todos queremos evitar, por eso puede parecer razonable pagar 500$ para salir de la situación incómoda. Caer en trampas de esto

tipo es bastante difícil, aunque descargar algo de no querido, sobre todo en los móviles, es algo de muy común; sin embargo calcular el impacto económico ocasionado resulta casi imposible pero se deben tener en cuenta los daños personal que se suben debidos a la encriptación , y entonces inaccesibilidad, de todos los archivos de un móvil personal.

5.3.- Comparativa entre noticias

Los ataques informáticos dirigidos a los móviles en general están aumentando porque el número de posesores de smartphone está subiendo también y no es tan raro que alguien tenga un móvil y no un ordenador. Los ataques de phishing en móviles pueden también aprovechar de las dimensiones reducida de la pantalla de los móviles, por ejemplo por esconder URLs falsos.

En cuanto a la descarga de los malware, en ambas las circunstancias los cibercriminales recurren al engaño, ocultando los malware de forma que las víctimas ni siquieras se den cuenta de lo que están haciendo.

Después, en ambas las noticias los estafadores utilizan técnicas de ingeniería social para arrancar dinero; en el primer caso aprovechan de la poca claridad de las informaciones y del caos debidos a la pandemia global actual, mientras en el segundo caso se aprovechan del miedo y de la vergüenza que las víctimas pueden sentir.

Ambos los malware tienen puntos de fuerza, el primero porque utiliza el sistema de SMS para garantizarse las confirmaciones de los pagos trámite carta de crédito y el segundo porque la presión que pone y las amenazas son más fuertes, es decir en el primer caso se usa el engaño mientra en el segundo las amenazas.

6.- Noticias relativas a: Inyección de código SQL

6.1.- Noticia 1: **In vendita i dati degli impiegati di Unicredit**

Fecha de la noticia: **22/04/2020**

Título de la noticia: **In vendita i dati degli impiegati di Unicredit**

Enlace a la noticia: https://ilmanifesto.it/in-vendita-i-dati-degli-impiegati-di-unicredit/

Medio (prensa digital): **il manifesto**

Enlace al medio: https://ilmanifesto.it/

Nacionalidad del medio: **italiana**

Idioma de la noticia: **italiano**

Breve resumen de la noticia:

Telsy, una sociedad de ciberseguridad italiana del grupo Tim, dio la alarma [8] después haber encontrado en venta en la web oscura los datos de 3000 empleados de UniCredit (la mayor sociedad bancaria de Italia). Según los expertos se ejecutó un ataque de inyección de código SQL que dio como resultado la visualización de nombres, apellido, numeros de telefono, correos y contraseñas cifradas de 3000 empleados. La sociedad bancaria desmintió todo lo que pasó pero un hacker con el pseudónimo de c0c0linoz ha publicado parte de la base de datos robado como démonstration de su poseso. El hacker afirma que los datos se remontan al termine del 2018 y pide como método de pago la criptomoneda Monero.

Relación con la amenaza:

El obtenimiento de los datos fue alcanzado con la técnica de inyección de código SQL.

Impacto ocasionado por la amenaza en esta noticia:

El impacto ocasionado de esta noticia se divide en dos tipologías; la primera es la violación de la privacidad de los empleados a quien robaron los datos personales y la segunda es el daño a la imagen de la sociedad bancaria. Aunque no es un

impacto muy elevado, no es la primera vez que UniCredit sufre de ataques informáticos y unos clientes podrían ser intimidados a usar los servicios ofrecidos del banco. El cibercriminal pide una suma de 1000 dólares solamente por los nombres y apellidos y una suma de 10.000 dólares por el total de la base de datos (150.000 líneas de datos); desde los precios se puede entender el valor económico de los datos.

6.2.- Noticia 2: **Violate 600mila caselle di posta di Email.it. Account in vendita nel dark web**

Fecha de la noticia: **07/04/2020**

Título de la noticia: **Violate 600mila caselle di posta di Email.it. Account in vendita nel dark web**

Enlace a la noticia: https://www.ilsole24ore.com/art/violate-600mila-caselle-posta-emailit-account-vendita-dark-web-ADVnnrI?refresh_ce=1

Medio (prensa digital): **Il Sole 24 Ore**

Enlace al medio: www.ilsole24ore.com

Nacionalidad del medio: **italiana**

Idioma de la noticia: **italiano**

Breve resumen de la noticia:

Un grupo de hacker italiano, llamado NoName Hacking Group, ha publicado un tweet [9] sobre su página declarando que el centro de datos de la empresa email.it fue comprometido ya hace 2 años y en todo ese período los hackers han conseguido robar más de 5 TeraByte de datos de los usuarios incluyentes 44 bases de datos, datos sensibles de 600.000 usuarios (con contraseñas guardadas sin encriptación), SMS y FAX enviados y todos los mensajes con los allegados enviados y recibidos de los usuarios [10]. La principal técnica empleada fue la inyección de código SQL, que junta a inyección de otro tipo de código y privilege

escalation ha permitido a los cibercriminales de obtener el control total del sistema de almacenamiento de datos a lo largo de 2 años.

Relación con la amenaza:
Los estafadores consiguieron inyectar código SQL para obtener el control de la base de datos.

Impacto ocasionado por la amenaza en esta noticia:
El impacto de esta amenaza es muy grande si consideramos que se robaron los datos de 600.000 usuarios y estos datos incluyen contraseñas en claro y todos los contenidos de los correos. Los hackers sostienen que email.it tenía conocimiento de la infiltración desde meses porque los estafadores pidieron un rescate pero la empresa siguió como si nada había pasado, sin comunicar nada a los usuarios.
Los datos, en venta en un sitio web huésped de la red Tor, tienen diferentes opciones de compra en base a la tipología de datos; solamente los datos usuarios cuestan medio Bitcoin (aproximadamente 3.000€ al tiempo) y la totalidad de los datos (más que 5 TB) a un precio de 3 Bitcoins.

6.3.- Comparativa entre noticias

Las características común de las dos noticias son el empleo de la técnica de inyección de código SQL, la visualización de los datos y el medio de venta utilizado. Dicho esto la diferencia de cantidad y la tipología de datos robados es amplia.
En el primer caso se robaron relativamente pocos datos y las contraseñas quitadas son cifradas pero el valor económico sigue siendo alto porque los datos son de empleados y poder acceder a servicios bancarios con cuentas de empleados sería un gran negocio; en esta situación los daños a la reputación de UniCredit no son muchos y la multinacional ha garantido que sus sistemas son seguros al cien por cien.
En vez, en el segundo incidente se robó una cantidad de datos elevada y las pruebas garantizan que todo pasó como descrito de los cibercriminales con la

adición del escarnio de los estafadores que se broman de las contraseñas guardadas en claro (algo de increíble hoy en día) y también de la pesima organizacion y gestion de la base de datos. NN Hacking Group ha declarado en un entrevista [10] que tienen en su poder otros centros de datos de otras empresas y optaron por la difamación publica de email.it porque es en absoluto la con más brechas de todos. Un ataque personal de esta portada puede tener consecuencias devastadoras por una empresa y, por cierto, le hizo perder un montón de clientes. Con búsquedas personales se puede observar que la página web sigue existiendo [11] y en actividad (cómico que en el blog de la página el último artículo, datado un mes antes de la publicación del grupo hacker, trata sobre el aumento de las fraudes informáticas) pero las páginas de las redes social de la empresa ya no existen más. En la página web oficial hay un aviso donde la empresa admite el sucedido pero menospreciando los daños y simplemente aconseja a los usuarios de cambiar contraseña.

7.- Noticias relativas a: Cross-Site Scripting (XSS)

7.1.- Noticia 1: **A hacker group tried to hijack 900,000 WordPress sites over the last week**

Fecha de la noticia: **05/05/2020**

Título de la noticia: **A hacker group tried to hijack 900,000 WordPress sites over the last week**

Enlace a la noticia: https://www.zdnet.com/article/a-hacker-group-tried-to-hijack-900000-wordpress-sites-over-the-last-week/

Medio (prensa digital): ZDNet

Enlace al medio: https://www.zdnet.com/

Nacionalidad del medio: **estadounidense**

Idioma de la noticia: **inglés**

Breve resumen de la noticia:
Wordpress, un sistema de gestión de contenidos usado para crear blog, ya subió varios ataques informáticos en pasado y está luchando cada día contro los hackers. Todas las fallas descubiertas han sido resueltas con actualizaciones pero todavía hay usuarios que no actualizaron unos plugins y temas que pueden resultar peligrosos, en particular Easy2Map, Blog Designer, WP GDPR Compliance, Total Donations y el tema Newspaper. El grupo de hackers intentaron atacar más de 900.000 sitios con 24.000 direcciones IP diferentes. La mayoría de las vulnerabilidades de que se aprovecharon son de tipo Cross Site Scripting (XSS) sobre todo del plugin Easy2Map (arreglado en agosto del 2019) que resultó el trámite de más de la mitad de la totalidad de los ataques.

Relación con la amenaza:
Los atacantes se aprovecharon de vulnerabilidad XSS

Impacto ocasionado por la amenaza en esta noticia:
El grupo de hacker tiene dos estrategias de ataque diferentes: la primera se efectúa cuando el administrador no ha efectuado el acceso y consiste en el desvío de los visitantes de la página a otra dirección malévola elegida por los hackers, mientras la segunda se aprovecha del acceso a las funcionalidades de administrator y intenta inyectar una backdoor en el archivo PHP.
En esta estrategia los blogs de Wordpress son un medio para hacer que las víctimas visiten sitios malévolos y estimar el daño final resulta muy difícil pero por cierto ataques de esta portada pueden tener resultados importantes además de dañar a la imagen pública del portal.

7.2.- Noticia 2: **Un fallo en TikTok permitió acceder a los datos personales de los usuarios**

Fecha de la noticia: 08/01/2020

Título de la noticia: **Un fallo en TikTok permitió acceder a los datos personales de los usuarios**

Enlace a la noticia:

https://www.elmundo.es/tecnologia/2020/01/08/5e15be62fc6c8336088b456e.html

Medio (prensa digital): El Mundo

Enlace al medio: https://www.elmundo.es/

Nacionalidad del medio: española

Idioma de la noticia: español

Breve resumen de la noticia:

Los investigadores de Check Point Research, una famosa sociedad de ciberseguridad, encontraron una importante falla en la aplicación Tik Tok que podían poner en peligro los datos personales de los usuarios [12]. Apenas descubierta la falla, Check Point avisó a ByteDance (la empresa propietaria de Tik Tok) que rápidamente procedió a resolver los problemas emitiendo una actualización con las correcciones necesarias. La función de búsqueda del centro de apoyo para la publicidad resultó responsable de potencial ataques de tipo XSS donde los atacantes podían insertar script incluyente código malévolo que venía erróneamente ejecutado por el servidor web.

Los fallos permitían a los hackers de acceder a las cuentas de los usuarios para manipular el contenido, eliminar y publicar vídeos y cambiar la privacidad de los vídeos.

Relación con la amenaza:

Tik Tok sufría de ataques de Cross Site Scripting

Impacto ocasionado por la amenaza en esta noticia:

Los hackers podían controlar las cuentas privadas y estoy comprendía: subir y eliminar videos, obtener los datos personales como nombres, apellidos, direcciones de correo y fechas de nacimiento; además de esto, los malintencionados podían redirigir la víctimas hacia sitio web clones de tiktok.com y podían tambien hacerse pasar por Tik Tok mismo enviando SMS modificados a sus antojo.

También aquí estimar los daños resulta muy complicado; los impactos generados incluyen daños a la imagen pública de la sociedad y además daños personales a los usuarios porque pueden verse eliminados o publicados videos sin autorización y el direccionamiento hacia páginas web maliciosas.

7.3.- Comparativa entre noticias

Los artículos resultan muy parecidos porque en ambos la sucesión de los eventos sigue el mismo esquema: primero los atacantes descubren una falla por donde pueden inyectar código malévolo y lo hacen, después los investigadores descubren el hecho y contactan la sociedad responsable explicando lo que está pasando y finalmente la empresa emite una actualización que provee a la resolución de los problemas. Fallas de esta tipología siguen siendo concedidas a los cibercriminales porque las páginas web modernas tienen muchos campos donde los usuarios pueden insertar informaciones y, olvidarse de controlar que lo que inserta un usuario no sea código malicioso es bastante común por los desarrolladores. Los ataques de Cross Site Scripting son muy peligrosos y utilizados porque, si efectuados, pueden robar los datos de los cookies y ejecutar código sin que nadie se da cuenta en un servidor web y por eso pueden tener efectos devastadores por las víctimas.

Una diferencia entre las noticias se puede encontrar en el hecho que el primer ataque fue de tamaño mayores y más evidente mientras el segundo fue de tamaño menor y más cuco.

Ataques que se aprovechan de vulnerabilidad XSS pueden resultar nocivos por la reputación de las empresas que los sufren, por eso estas últimas solitamente intentan callar los periódicos que pero esperar solamente noticias de esta tipología para escribir artículos atrayentes por los lectores.

8.- Conclusiones del informe

En este informe analizé unas noticias relacionadas con las amenazas informáticas que se pueden encontrar hoy en día. Aunque escribí sobre siete de las principales tipologías de amenazas, hay más que no afronté y, en general, el mundo de los ataques informáticos es muy amplio.

Las medidas de seguridad siguen avanzando con nuevas tecnologías y técnicas para hacer frente a los ataques de los criminales que son también siempre más sofisticados.

Consideraciones personales sobre cada una de las amenazas:

1.- Phishing: Es la tipología más frecuente de ataque porque comprende muchas variantes y el límite de las técnicas es la fantasía de los estafadores. Es una amenaza ínfima porque se basa en el engañar a las víctimas y utiliza técnicas de ingeniería social. Su principal ventaja es que se aprovecha de la ingenuidad humana que al final resulta ser siempre el eslabón más débil de la cadena de la seguridad.

2.- Malware en redes sociales: Esta tipología se basa en la multiconectividad de las redes sociales para alcanzar la amplia difusión de malware; personalmente me parece que, en general, la seguridad de las redes sociales ha aumentado en los últimos años porque la atención de los usuarios se movió en esa dirección y la reputación de las redes depende de su seguridad. Dicho esto, impedir cualquier forma de estafa en las redes sociales es imposible porque la libertad de expresión es un fundamento de ellas.

3.- Ataques dirigidos contra grandes corporaciones y gobiernos: Esta tipología se diferencia bastante de las otras porque aquí se intenta a dañar una entidad y no las personas individuales. Esta amenaza suele tener fines políticos y, como se sabe cuando se habla de política, se habla de poder y el poder influencia todo, noticias incluidas. Es decir, cuando hay noticias de esta portada difícilmente se descubrirá toda la verdad.

4.- Botnets, ordenadores zombies: Es una tipología de ataque que raramente se encuentra por encima del campo de la informática porque su fortaleza está en el alto nivel de interconexión, y entonces de infectividad, que las redes modernas tienen.

Las botnets son solamente un medio gracias a la cual se pueden obtener muchos beneficios y sus potencia es limitada por la dificultad de coordinar todos los dispositivos infectados sin despertar sospechas.
5.- Malware en dispositivos móviles: El mercado mundial de los móviles es ahora más grande que lo de los ordenadores, debido sobre todo a la influencia del continente asiático por el coste reducido de los smartphones frente a los ordenadores. Sin embargo los móviles se basan en aplicaciones descargadas desde servicios de distribución seguras como el Play Store o el Apple Store, por eso es más difícil infectar los móviles con malware. Personalmente creo que hay relativamente pocos ataques en los móviles y estos dispositivos tendrán más enfoque por los hackers en futuro.
6.- Inyección de código SQL: Es una práctica muy difusa que se aprovecha de las fallas introducidas por los desarrolladores de las bases de datos. El objetivo de los ataques son los datos almacenados y como se suele decir los datos son el nuevo petróleo. Hoy en día las empresas más grandes del mundo gestionan datos y la protección de ellos es fundamental; me parece que en términos generales se valoran poco los datos personales y se tiende a subestimar la importancia que tienen.
7.- Cross-Site Scripting (XSS): Esta tipología se aprovecha de fallas muy común en los sitios web y sigue siendo un aspecto fundamental de la ciberseguridad por el número elevado de los ataques dirigidos a páginas web (más del 70% del total). Con el hecho de que siempre más páginas son creadas por individuos que no tienen competencias en ciberseguridad, muchas de ellas sufren de esta debilidad.

Los cibercriminales existen desde los primeros años de la historia informática y existirán hasta que existirán los ordenadores por qué esta es la natura humana que, por algunos, incluye el aprovecharse de las personas más débiles.
Creo que se debería hacer más formación en general y la gente tendría que saber cual son las amenazas o simplemente saber lo que no es seguro porque las personas son los responsables de la casi totalidad de los errores.

Analizando muchos artículos sobre el argumento me di cuenta que el factor más importante para las prensas (sobre todo aquellas no específicas) es sorprender el lector, muchas veces alterando la verdad para atraer unos clics más.
Noté también que muchos blogs y sitios suelen copiar y pegar exactamente los contenidos de otros y no es raro encontrar los mismos textos en diferentes medios.
Otro aspecto interesante es que buscando en diferente idiomas y países los estilos y los contenidos de las noticias son muy similares creo siempre porque las imitaciones son muy difundidas.
Otra consideración personal que puedo hacer es que me parece que la gente a menuda valora los daños económicos ocasionados por los ataques informáticos pero no considera aquellos personales, sociales y políticos.

9.- Bibliografía

[1] "Ragnar Locker", Malware Wiki Fandom, 2020. [En línea]. Disponible en: https://malware.wikia.org/wiki/Ragnar_Locker. [Accedido: 29-abr2020]

[2] "EXCLUSIVE: The cyber attack the UN tried to keep under wraps", The New Humanitarian, 2020. [En línea]. Disponible en: https://www.thenewhumanitarian.org/investigation/2020/01/29/united-nations-cyber-attack. [Accedido: 03-may2020]

[3] "Necurs botnet", Wikipedia, 2019. [En línea]. Disponible en: https://en.wikipedia.org/wiki/Necurs_botnet. [Accedido: 01-may2020]

[4] "New action to disrupt world's largest online criminal network", Microsoft On the Issues, 2020. [En línea]. Disponible en: https://blogs.microsoft.com/on-the-issues/2020/03/10/necurs-botnet-cyber-crime-disrupt/. [Accedido: 03-may2020]

[5] "Worm:W32/Phorpiex", F-Secure, 2019. [En línea]. Disponible en: https://www.f-secure.com/v-descs/worm_w32_phorpiex.shtml. [Accedido:

05-may2020]

[6] “Phorpiex Breakdown”, Check Point Research, 2019. [En línea]. Disponible en: https://research.checkpoint.com/2019/phorpiex-breakdown/. [Accedido: 05-may2020]

[7] “Meet Black Rose Lucy, the Latest Russian MaaS Botnet”, Check Point Research, 2018. [En línea]. Disponible en: https://research.checkpoint.com/2018/meet-black-rose-lucy-the-latest-russian-maas-botnet/. [Accedido:07-may2020]

[8] “UNICREDIT EMPLOYEES DATABASE FOR SALE ON CYBER-CRIME FORUMS”, Telsy, 2020. [En línea]. Disponible en: https://blog.telsy.com/unicredit-employees-database-for-sale-on-cyber-crime-forums/ [Accedido: 10-may2020]

[9] Tweet de NN Hacking Group, Twitter, 2020. [En línea]. Disponible en: https://twitter.com/NNHackingGroup/status/1246836762980290560 [Accedido: 10-may2020]

[10] “Email.it è stato violato, i dati di 600.000 utenti disponibili nel dark web. Gli aggiornamenti”, Cybersecurity - Startupitalia, 2020. [En línea]. Disponible en: https://cybersecurity.startupitalia.eu/63307-20200407-email-it-data-breach [Accedido: 10-may2020]

[11] Email.it, 2020. [En línea]. Disponible en: https://www.email.it/ [Accedido: 10-may2020]

[12] “Tik or Tok? Is TikTok secure enough?”, Check Point Research, 2019. [En línea]. Disponible en: https://research.checkpoint.com/2020/tik-or-tok-is-tiktok-secure-enough/ [Accedido: 12-may2020]