BOLETÍN DE CIBERSEGURIDAD

VISA: un fallo de seguridad permite eludir el PIN

Si el pago por medios electrónicos, Visa, Paypal, monederos electrónicos, etcétera, no había dejado de crecer durante los últimos años, con la situación provocada por el coronavirus su uso se ha disparado hasta niveles que no eran previsibles. En parte por el auge del comercio electrónico, y también en una parte importante por los temores asociados a emplear dinero en efectivo, y que este pueda actuar como vector de difusión del patógeno.

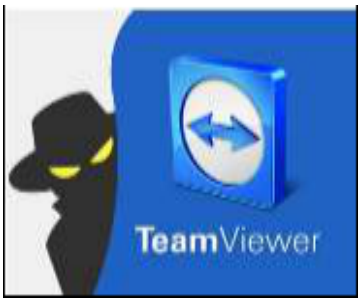
Un equipo de investigación suizo, que ha encontrado un problema de seguridad en el protocolo EMV, empleado por Visa, y que es vulnerable a un ataque de tipo man-in-the-middle que permite realizar transacciones sin que sea necesario validarlas mediante el PIN asociado a las tarjetas.

EMV («Europay, MasterCard, Visa) es el protocolo utilizado por todos los principales bancos e instituciones financieras del mundo. Europay, Mastercard y Visa desarrollaron el estándar y existe desde hace más de 20 años. La razón más importante para la adopción generalizada del protocolo EMV tiene que ver con el «cambio de responsabilidad», un procedimiento que garantiza que, siempre que el cliente apruebe la transacción con un PIN o firma, la institución financiera no es responsable.

De esta manera, un delincuente que lograra hacerse con una tarjeta Visa robada, podría realizar compras con ella sin que fuera necesario emplear el PIN para validar la operación. Y, debido al planteamiento asociado a EMV, la responsabilidad del mismo recaería sobre el titular de la tarjeta robada, y no de la entidad, pese a que el problema de seguridad tenga su origen en ésta. Cabe entender, no obstante, que de darse algún ataque in the wild que aproveche esta vulnerabilidad, las entidades financieras actuarán de forma responsable.

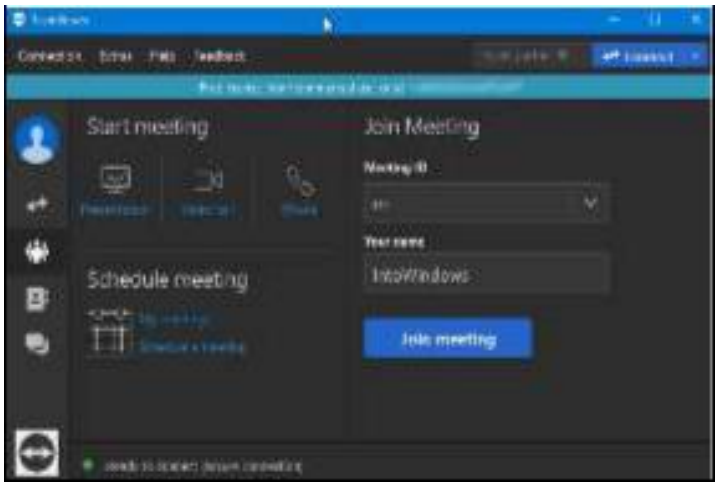
La mala noticia es que todas las tarjetas Visa con chip se ven afectadas por este problema, y la entidad financiera tiene que emitir una actualización del software empleado en datáfonos y TPVs. En su parte positiva, el problema de seguridad no es inherente a EMV, sino a una implementación deficiente de las medidas de seguridad asociadas a la validación de los pagos mediante PIN en operaciones contactless. Eso sí, los investigadores cifran en alrededor de 161 millones los TPVs que hay a lo largo del mundo, por lo que vaticinan que la actualización de todos ellos será un proceso que llevará cierto tiempo.

FALLA EN TEAMVIEWER PARA WINDOWS PERMITE COMPROMETER COMPLETAMENTE EL DISPOSITIVO DE LA VÍCTIMA



Un nuevo riesgo de seguridad para los usuarios de TeamViewer ha sido reportado. Especialistas en seguridad en redes inalámbricas detallan el hallazgo de una vulnerabilidad en la plataforma de acceso remoto que podría permitir a los actores de amenazas descifrar las contraseñas de los usuarios, exponiendo completamente los sistemas afectados.

TeamViewer es una aplicación de software remoto, uso compartido de escritorio, videoconferencias y transferencia de archivos entre computadoras desarrollada por la empresa alemana TeamViewer GmbH.



La vulnerabilidad fue identificada como CVE-2020-13699 y recibió un puntaje de 8.8/10 en la escala del Common Vulnerability Scoring System (CVSS). Este hallazgo se produce en un momento en el que las aplicaciones de comunicación y acceso remoto han experimentado un aumento considerable en su uso, debido al confinamiento y el trabajo en casa.

La falla está presente en cualquier versión de la aplicación de TeamViewer para equipos de escritorio Windows anterior a 8.0.258861, 9.0.258860, 10.0.258873, 11.0.258870, 12.0.258869, 13.2.36220, 14.2.56676, 14.7.48350 y 15.8.3.

Los especialistas en seguridad en redes inalámbricas mencionan que la falla existe debido a una ruta de búsqueda o elemento sin comillas, pues la aplicación no cita correctamente sus controladores URI personalizados. Los hackers maliciosos deben redirigir a la víctima a un sitio web malicioso empleando una versión vulnerable de TeamViewer para explotar la falla.

Posteriormente, el sistema Windows realizaría la autenticación NTLM al abrir el recurso compartido. Esa solicitud permite a los atacantes capturar una autenticación y enviarla a otro servidor, otorgándole la capacidad de realizar operaciones en el servidor remoto aprovechándose de los privilegios del usuario autenticado.

Acorde a los especialistas en seguridad en redes inalámbricas, la explotación exitosa de esta vulnerabilidad permitiría a los hackers remotos iniciar TeamViewer con parámetros arbitrarios. Los cibercriminales podrían forzar el envío de solicitudes de autenticación NTLM al sistema malicioso, permitiendo ataques de fuerza bruta, entre otros ataques derivados del robo de credenciales.

Error de Android que permite robar datos de aplicaciones

Un investigador de seguridad y fundador de la empresa de seguridad de aplicaciones Oversecured, Sergey Toshin, encontró una vulnerabilidad grave que afecta a Android. Compartió los detalles de los hallazgos con TechCrunch que reveló el asunto.

Como se reveló, el investigador encontró un error en el sistema operativo Android que podría facilitar que las aplicaciones maliciosas extraigan los datos del usuario. De hecho, estas aplicaciones podrían aprovechar el error para robar datos confidenciales de otras aplicaciones que se ejecutan en el dispositivo de destino.

Específicamente, el error existía en la biblioteca de Play Core que permite a los desarrolladores de aplicaciones implementar actualizaciones para las aplicaciones.

Por lo tanto, todas las aplicaciones que dependen de este componente para las actualizaciones eran potencialmente vulnerables a la amenaza. Considerando que, una aplicación maliciosa podría explotar este componente para inyectar módulos maliciosos a otras aplicaciones para robar datos.

Como prueba de concepto, el investigador incluso creó una aplicación de prueba que podía robar datos con éxito, incluidas las contraseñas, el historial de navegación y las cookies de inicio de sesión.

La fuga de datos de Telegram expone millones de registros en Darknet

La aplicación de mensajería cifrada Telegram sufrió una fuga masiva de datos que expuso los datos personales de millones de usuarios. Un rival de WhatsApp, Telegram permite a los clientes intercambiar de forma privada textos, llamadas, notas de voz y videos cifrados de extremo a extremo. Pero la vulnerabilidad en su función de importación de contactos comprometió millones de registros, incluidos números de teléfono e ID de usuario, que luego se filtraron a la red oscura.

La publicación rusa de tecnología Kod.ru fue la primera en informar sobre el problema, y dijo que información personal como identidades de usuario y números de teléfono se han publicado en un foro de la red oscura. Según los informes, el servicio de la aplicación de mensajería reconoció la existencia de una violación de datos, que ocurrió después de explotar la función de importación de contactos incorporada durante el registro.

No es la primera fuga

La fuga de datos actual no es el primer rodeo de Telegram. En agosto de 2019, la compañía estaba en el centro de la controversia cuando un error expuso los números de teléfono de los activistas a favor de la democracia en Hong Kong. El problema técnico se encontró en la función de mensajería grupal de la aplicación, lo que permite a las autoridades chinas identificar y localizar a los manifestantes.

Error de Safari que permite robar datos revelados después de que Apple retrasa un parche

Según se informa, el investigador de seguridad Pawel Wylecial descubrió un error grave en Apple Safari. La vulnerabilidad, tras la explotación, puede permitir el robo de datos locales de las víctimas.

Al compartir los detalles en una publicación, el investigador reveló que el error existe dentro de la API Web Share. Permite compartir enlaces o archivos directamente desde el navegador a través de aplicaciones de terceros, como aplicaciones de correo electrónico o mensajería.

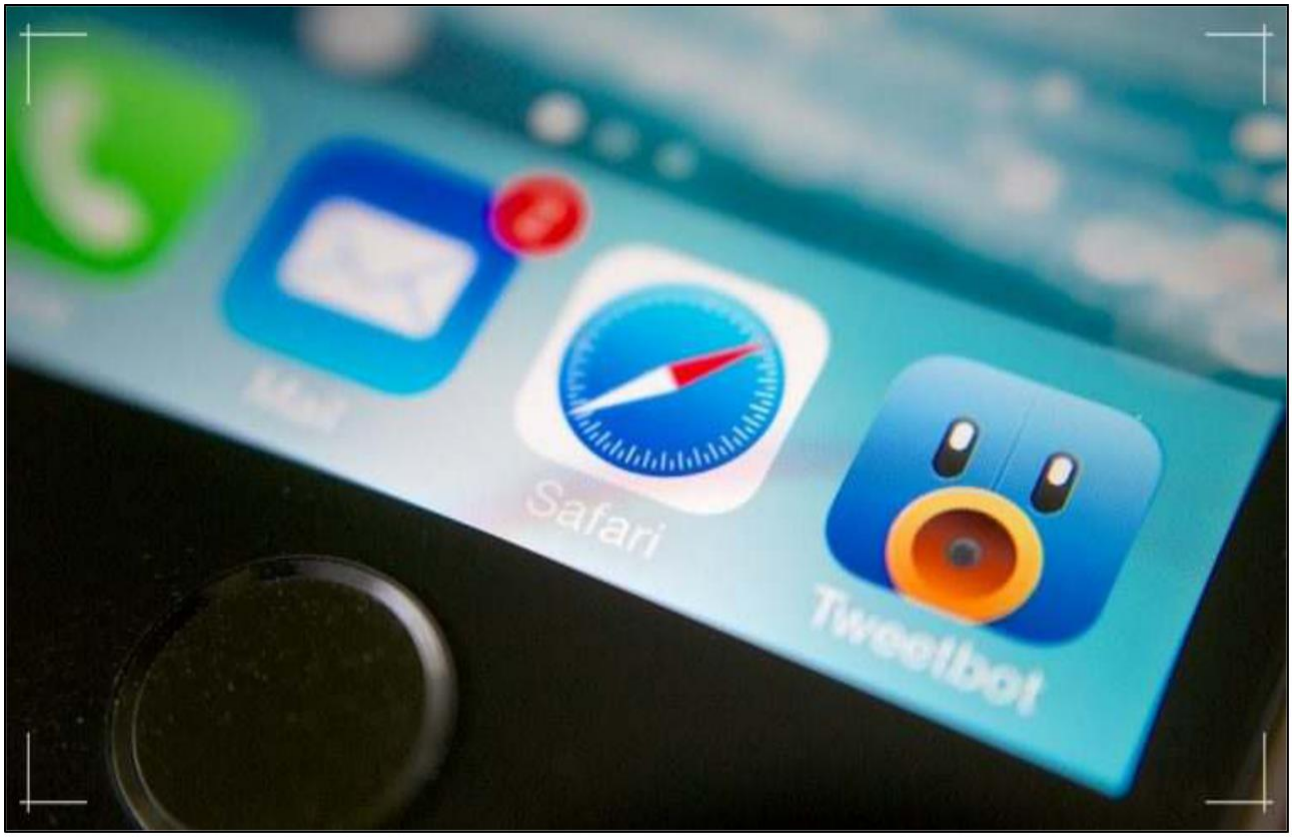
Por lo tanto, un adversario puede engañar a la víctima para que comparta un enlace malicioso o un archivo para robar archivos locales del dispositivo de la víctima.

Apple retrasó la solución durante aproximadamente un año

El investigador descubrió el error en abril de 2020. Inmediatamente después de este descubrimiento, se acercó a Apple para informar del asunto.

Si bien reconocieron el error, no implementaron una solución para él. Y, como reveló el investigador, Apple aplazó la fecha de lanzamiento para una solución a la primavera de 2021, un año después de la divulgación.

Por lo tanto, el investigador descontento dio un paso al frente para revelar el error públicamente.



La vulnerabilidad de Google Drive permite ataques de spearphishing

Existe una grave vulnerabilidad en Google Drive que aún espera una solución. Como se descubrió, la vulnerabilidad permite a un adversario realizar ataques de phishing a través de imágenes creadas con fines malintencionados.

El investigador A. Nikoci, principalmente un administrador de sistemas, ha encontrado una vulnerabilidad grave en Google Drive. La explotación de la vulnerabilidad podría tener un impacto grave en los usuarios correspondientes de Google Drive.

Según los detalles que compartió, la vulnerabilidad afectó la función 'administrar versiones' de Google Drive. Idealmente, esta función permite a los usuarios cargar nuevas versiones en un archivo existente sin tener que cambiar la extensión del archivo. De esta manera, los usuarios pueden administrar diferentes versiones a la vez.

Sin embargo, el problema apareció porque esta funcionalidad incluso permitía a cualquiera cargar archivos con cualquier extensión a cualquiera de los archivos existentes. Esto incluso permitió cargar archivos con ejecutables maliciosos como nuevas versiones.

Google solucionó una vulnerabilidad de Gmail a solo 7 horas de la divulgación pública

Una grave vulnerabilidad de suplantación de identidad afectó al servicio Gmail de Google. Sin embargo, a pesar del descubrimiento y la divulgación responsable, el gigante tecnológico entregó la solución a solo 7 horas de la divulgación pública.

La investigadora de seguridad Allison Hussain descubrió un error grave que afectaba a Gmail.

Al compartir los detalles en una publicación, reveló que encontró una vulnerabilidad de suplantación de correo en Gmail. Sin embargo, esto no era similar a los errores anteriores. Más bien, normalmente afectó a Google, permitiendo que un adversario eludiera los controles de seguridad y enviara correos electrónicos haciéndose pasar por otros usuarios de Gmail o G Suite.

Por lo general, los servidores de correo electrónico emplean dos técnicas para abordar la vulnerabilidad de suplantación de identidad: el marco de políticas del remitente (SPF) y la autenticación, informes y conformidad de mensajes basados en dominios (DMARC).

Sin embargo, el error de Gmail recién descubierto podría eludir fácilmente las reglas SPF y DMARC.

Al principio, el error permitía a un atacante enviar correos electrónicos falsificados a una puerta de enlace entrante en el backend de G Suite. Considerando que, el segundo error podría permitir la configuración de reglas personalizadas para reenviar un correo electrónico falso entrante.

Detecciones de malware que utiliza el nombre de Fortnite son constantes

La industria de los videojuegos y en particular los gamers son desde hace ya un tiempo un blanco atractivo para los cibercriminales dadas ciertas condiciones, como el gran número de jugadores alrededor del mundo, el uso de diversas plataformas susceptibles de ser atacadas y una industria multimillonaria y en constante crecimiento.

De hecho, continuamente se identifican nuevas amenazas relacionadas con los videojuegos, que van desde robo de información, phishing, estafas y engaños, hasta vulnerabilidades en plataformas y malware de distinto tipo como mineros de criptomonedas, botnets o ransomware.

Malware que utiliza el nombre de Fortnite para engañar a sus víctimas

Tras analizar algunos datos obtenidos, observamos que en los últimos años existe una importante y constante actividad maliciosas en la órbita de los videojuegos, especialmente en torno a títulos que gozan de una gran popularidad entre la comunidad gamer, como es el caso de Fortnite.

En WeLiveSecurity hemos publicado varios artículos y noticias sobre campañas maliciosas que giran alrededor de Fortnite, como fue hace dos años la campaña que, mediante la descarga de cheats para el juego, infectaba a los usuarios con malware para distribuir publicidad.

El nombre del juego es utilizado por los cibercriminales para la distribución de diferentes tipos de códigos maliciosos, como el spyware, mineros de criptomonedas o troyanos bancarios, e incluye a diferentes familias de malware, como Win32/Floxif, Win32/Kryptik, Win32/Ramnit, Win32/HoudRat o Android/FakeAV, por mencionar algunas.

La mayoría de estos códigos maliciosos están diseñados para sistemas operativos Windows, pero también aparecen casos de malware para Android, aunque en menor proporción. Además, llama la atención que incluso son utilizados nombres erróneos para intentar engañar a los usuarios, a través de palabras como “Fornite”.

Mekotio: análisis de esta familia de malware bancario que apunta a Latinoamérica

Como parte de nuestra serie sobre troyanos bancarios de América Latina, en esta oportunidad presentamos Mekotio, un troyano bancario que apunta principalmente a Brasil, Chile, México, España, Perú y Portugal cuya característica más notable en las variantes más recientes es el uso de una base de datos SQL como servidor de C&C.

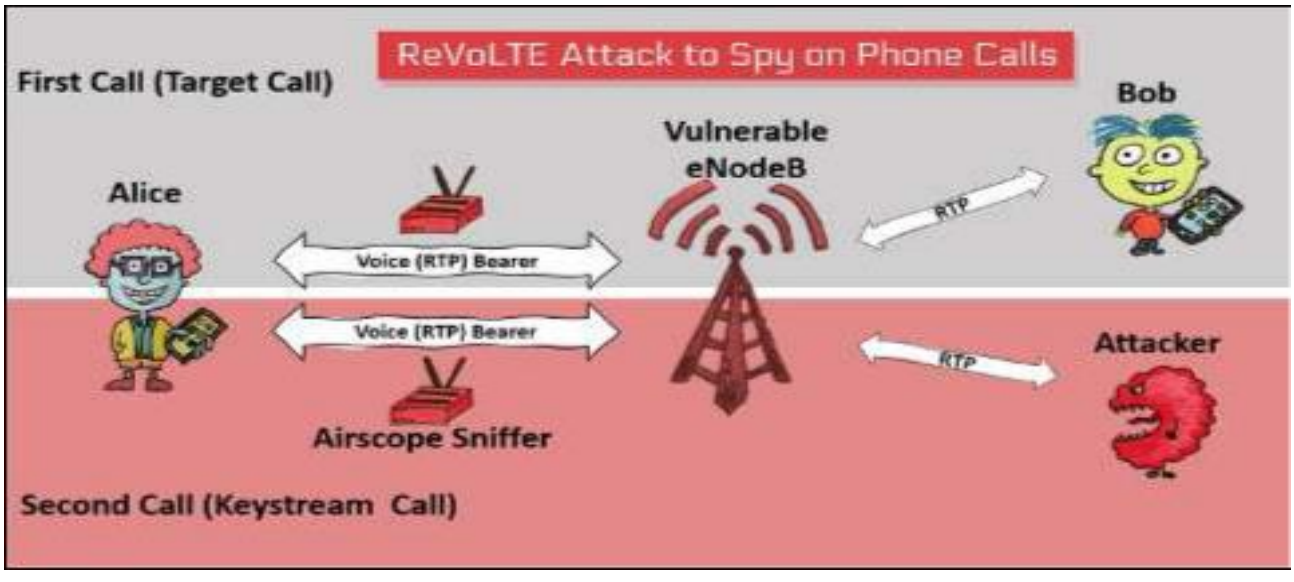
Características de Mekotio

Mekotio es un típico troyano bancario latinoamericano que ha estado activo desde al menos 2015. Como tal, su forma de atacar es desplegando a la víctima ventanas emergentes falsas con el objetivo de convencerla para que divulguen información confidencial. Estas ventanas emergentes están cuidadosamente diseñadas para suplantar la identidad de diferentes entidades bancarias latinoamericanos, así como otras instituciones financieras.

Mekotio recopila la siguiente información sobre sus víctimas:

- Configuración del firewall
- Si la víctima tiene privilegios de administrador
- Versión del sistema operativo Windows instalado
- Si están instalados productos de protección antifraude, más específicamente GAS Tecnología Warsaw e IBM Trusteer.
- Lista de soluciones antimalware instaladas en el equipo

ReVoLTE, ataque para comprometer llamadas telefónicas



El ataque ha sido publicado por un grupo de académicos de la Universidad de Ruhr de Bochum y ha sido bautizado así debido a que **ataca al protocolo de Voz sobre LTE (VoLTE)**, pero no es debido a la existencia de ninguna vulnerabilidad en el protocolo, sino a una débil implementación que mantienen los operadores de telefonía sobre este protocolo.

VoLTE (Voice over Long Term Evolution) es un protocolo de comunicación inalámbrica utilizados por distintos dispositivos terminales de datos, como pueden ser los dispositivos móviles, dispositivos *wearables* (portados corporalmente) y dispositivos de Internet de las cosas (IoT).

El ataque es posible gracias a que cuando una víctima, conectada a una estación base de transmisión de datos, realiza varias llamadas de voz, transcurriendo entre una llamada y otra un periodo corto de tiempo, la estación base utilizará para la segunda llamada las mismas claves de encriptado que para la llamada previa.

Sabiendo esto, un ataque exitoso, constará de 2 fases:

- En la primera fase, será necesario que el atacante esté conectado a la misma estación que la víctima, que coloque un capturador de tráfico y esperar a que la víctima realice la llamada que desea descifrar más tarde.
- Una vez terminada la llamada anterior, en una segunda fase, el atacante deberá realizar una llamada a la víctima dentro de un tiempo mínimo (sobre unos 10 segundos) y volver a capturar estos datos de llamada. Esta llamada debe tener una duración igual o superior a la anterior, para poder descifrar toda la conversación previa, sino no será posible descifrar toda la conversación.

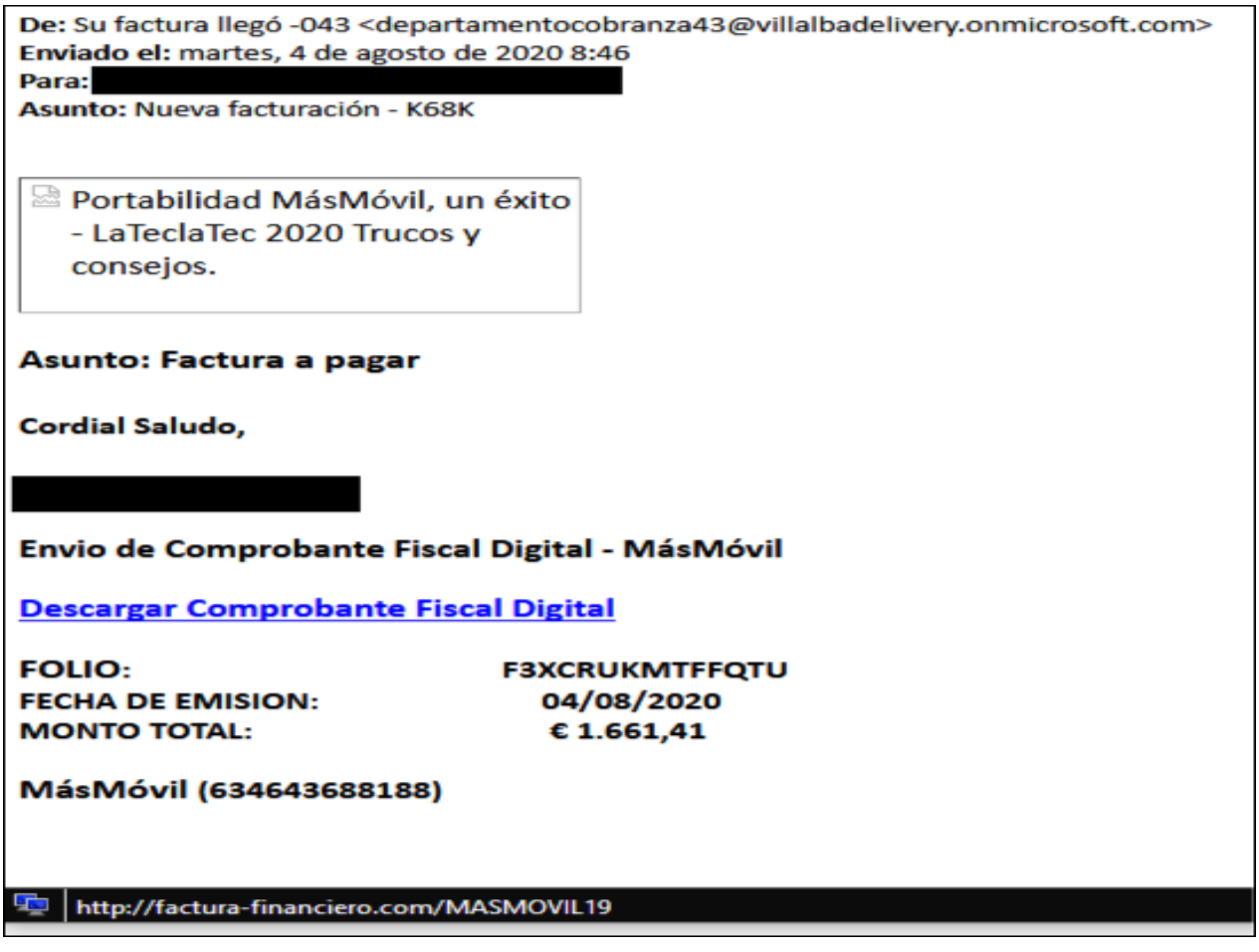
El troyano Grandoreiro ataca a clientes de MásMóvil

Grandoreiro, es un troyano bancario que se ha centrado en países como Brasil, México, Perú y España y que en su última campaña se hace pasar por MásMóvil.

MásMóvil es una compañía de telecomunicaciones que da servicios de telefonía fija, móvil e internet en España que fue fundada en 2006 y que en 2016 llega a su mejor punto empresarial tras la compra de Pepephone y Yoigo.

Aunque el principal objetivo de los atacantes suele ser el robo de credenciales bancarias, se suelen utilizar como cebo empresas energéticas o de telefonía. Esta vez el malware Grandoreiro ha fijado como objetivo la compañía de telefonía MásMóvil.

El patrón de ataque es similar a otros ya vistos anteriormente: el punto de entrada es un correo electrónico fraudulento que utiliza una dirección falsa que se hace pasar por la empresa objetivo y que en este caso en particular se informa a la futura víctima de un impago que tiene la posibilidad de revisar descargando dicha factura no pagada.


De: Su factura llegó -043 <departamentocobranza43@villalbadelivery.onmicrosoft.com>
Enviado el: martes, 4 de agosto de 2020 8:46
Para: [redacted]
Asunto: Nueva facturación - K68K

Portabilidad MásMóvil, un éxito - LaTeclaTec 2020 Trucos y consejos.

Asunto: Factura a pagar

Cordial Saludo,

[redacted]

Envio de Comprobante Fiscal Digital - MásMóvil

Descargar Comprobante Fiscal Digital

FOLIO:	**F3XCRUKMTFFQTU**
FECHA DE EMISION:	**04/08/2020**
MONTO TOTAL:	**€ 1.661,41**

MásMóvil (634643688188)

http://factura-financiero.com/MASMOVIL19

El malware para criptominado y DDoS, llega a Linux

Recientemente se han detectado muestras de una amenaza para Windows desarrollada para realizar criptominado y ataques DDoS, que afectan también a sistemas Linux.

Una botnet híbrida DDoS conocida por convertir dispositivos Windows vulnerables en bots de criptominería de Monero ahora también está buscando e infectando sistemas Linux.

Si bien los autores de la botnet lo llamaron Satan DDoS, los investigadores de seguridad lo llaman Lucifer para diferenciarlo del ransomware Satan.

Además de agregar compatibilidad con la orientación de Linux, los creadores de Lucifer también han ampliado las capacidades de la versión de Windows para robar credenciales y escalar privilegios utilizando la herramienta de post-explotación Mimikatz.

Para la propagación, este malware es capaz de explotar las vulnerabilidades EternalBlue, EternalRomance y DoublePulsar. En caso de no poder propagarse utilizando dichas vulnerabilidades, este utiliza un diccionario con unas 300 contraseñas y 7 nombres de usuario para tratar de acceder a los servidores con técnicas de fuerza bruta.

La versión de Linux incorpora la misma funcionalidad que la versión para Windows, aunque añade funcionalidad para realizar ataques de denegación de servicio a través de peticiones HTTP (HTTP GET-flood y POST-flood).

La posibilidad de infectar sistemas Linux abre la puerta a los atacantes para realizar ataques de denegación de servicio más potentes y efectivos gracias al mayor ancho de banda de los servidores alojados en datacenters, que es mucho más habitual encontrarlos con Linux instalado que con Windows.

Campaña de DDoS y extorsión apunta a empresas financieras y minoristas

Durante las últimas semanas, un grupo de cibercriminales ha estado extorsionando a varias organizaciones en todo el mundo tras amenazarlas con lanzar ataques de denegación de servicio distribuidos (DDoS, por sus siglas en inglés) contra ellos a menos que paguen miles de dólares en Bitcoin.

Los atacantes han estado apuntando a organizaciones que operan en diversas industrias, principalmente en sectores como finanzas, viajes y comercio electrónico. Sin embargo, no parecen apuntar a ninguna región específica, ya que se han enviado notas de rescate a organizaciones en Reino Unido, Estados Unidos y también en la región de Asia y el Pacífico.

Según ZDNet, este grupo es responsable también de ataques contra MoneyGram, YesBank, Braintree, Venmo y, más recientemente, contra la bolsa de valores de Nueva Zelanda, que se ha visto obligada a detener sus operaciones por tres días consecutivos.

Como parte de sus tácticas para generar temor, los ciberdelincuentes se hacen pasar por reconocidos grupos de cibercriminales, como Sednit, también conocido como Fancy Bear, y Armada Collective.

Los extorsionadores se ponen en contacto con sus víctimas mediante un correo electrónico en el cual les advierte de un inminente ataque de DDoS a menos que paguen el monto exigido en Bitcoin dentro de un plazo específico.

Los atacantes intensifican aún más sus tácticas de intimidación al describir las posibles consecuencias: "… sus sitios web y otros servicios conectados no estarán disponibles para todos. Tenga en cuenta también que esto dañará gravemente su reputación entre sus clientes.

Los ataques de DDoS, incluidos los acompañados por una extorsión, existen desde hace años, y el especialista en seguridad de ESET, Jake Moore, señala que las organizaciones no deben subestimar la amenaza.

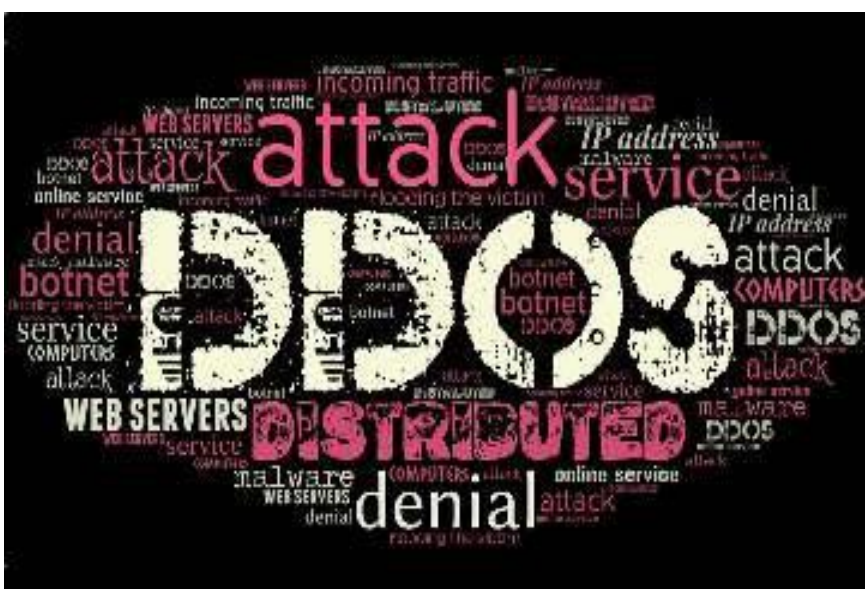
La bolsa de Nueva Zelanda, víctima de un ataque DDoS

El mercado de valores de Nueva Zelanda se ha visto afectado por un ataque distribuido de denegación de servicio (DDoS). Como consecuencia de las acciones de los atacantes, no ha quedado otro remedio que suspender todas las operaciones hasta que finalicen los ataques o sea posible mitigar los problemas de conectividad, que han impedido operar con normalidad.

Según informa NZX, que opera los mercados de capital riesgo y materias primas de Nueva Zelanda, la organización fue capaz de recuperarse de un primer ataque DDoS a primera hora del país, momento en el que volvieron a activar todos los sistemas para recuperar la normalidad. Sin embargo, poco después se produjo una segunda oleada, de mayor intensidad que la primera, y que podría indicar que el atacante aprovisiona un gran volumen de recursos, y que está dispuesto a desplegarlos para mantener la interrupción en el servicio del mercado de valores neozelandés.

En teoría, y después de varias interrupciones ocasionadas por los ataques, los sistemas ya están restaurados y las operaciones deberían funcionar con normalidad a la apertura de los mercados

Si bien este punto no se aclara en la comunicación de NZX, son varios los expertos que conceden una alta probabilidad de que se hayan utilizado los servicios de sitios que ofrecen DDoS as a Service. Esto es una mala noticia, no solo por lo que significa en sí mismo que se oferten este tipo de servicios y que haya quien los contrate, sino porque además dificulta en un grado enorme averiguar a instancia de quien se han llevado los ataques.



Durante los últimos años se han popularizado este tipo de servicios, hasta el punto de que las autoridades han empezado a perseguirlos, logrando éxitos como el del pasado mes de abril de las autoridades holandesas, en las que lograron acabar con 15 redes DDoS en tan solo una semana.

Sin duda, los cibercriminales han encontrado una gran vía de capitalización de sus conocimientos. Desgraciadamente, y como decía antes, hay gente dispuesta a pagar por ellos.

Mapfre, víctima de un ataque de Ransomware

La multinacional aseguradora española Mapfre ha sido víctima de un ataque de ransomware, según ha comunicado la misma compañía a través de su página web. Se trata de una comunicación escueta, en la que informan de la incidencia.

Según dicha comunicación, el ataque sí que ha tenido incidencia en sus operaciones, si bien, y esto me parece un aspecto destacable, partían de contar con un plan de contingencia con procedimientos alternativos, que fueron desplegados por Mapfre al detectar el ataque.

Algo que, según afirma la compañía, ha permitido que puedan mantener su operativa, si bien no en las condiciones de servicio habituales, algo por lo que se disculpan en el comunicado.

Con respecto al ataque, y a falta de más información (Mapfre se ha comprometido a ir proporcionando más información próximamente), lo más probable es que el ataque se iniciara mediante un ataque de phishing o spearphishing y que, desde el sistema comprometido por dicha acción, se produjera la difusión del malware por el resto de la infraestructura. Tampoco sabemos si solo ha incidido en ordenadores o, por el contrario, también se han comprometido las operaciones de servidores y otros recursos de IT.

Tampoco sabemos si se trata de un ataque de secuestro «sin más» o, por el contrario, si también se ha producido alguna exfiltración de datos.

Este es el texto del comunicado oficial de Mapfre:

"Pedimos disculpas a nuestros clientes porque no estamos pudiendo atenderles con la calidad habitual de MAPFRE. Desde hace unas horas estamos actuando sobre nuestros sistemas informáticos para repeler un ataque de ransomware que se ha lanzado contra algunos sistemas de la compañía.

Actualmente continuamos prestando servicio con normalidad, aunque para determinadas operaciones está siendo necesario hacerlo mediante los procedimientos alternativos establecidos en nuestro Plan de Continuidad de Negocio, lo que puede alargar nuestros tiempos de respuesta.

Continuaremos proporcionando actualizaciones periódicas de información a través de nuestros canales habituales".

Canon golpeado por el ataque de ransomware Maze, 10TB de datos supuestamente robados

Se informa que Canon ha sido golpeado por un devastador ataque de rescate. Además de eliminar una larga lista de sitios web de Canon, se dice que el ataque ha resultado en la enorme cantidad de 10 terabytes de datos robados de los servidores de Canon.

BleepingComputer informa que el grupo de rescate llamado Maze ha reclamado la responsabilidad de atacar exitosamente a Canon e impactar una amplia gama de servicios en la compañía, incluyendo el correo electrónico, el software de colaboración de equipo, sus sitios web de EE.UU. y aplicaciones internas.

Canon supuestamente envió una alerta a toda la compañía para informar a los empleados de “problemas de sistema de amplia difusión que afectan a múltiples aplicaciones. Los equipos, el correo electrónico y otros sistemas pueden no estar disponibles en este momento”.

Los siguientes dominios de Canon fueron afectados:

www.canonusa.com
www.canonbroadcast.com
b2cweb.usa.canon.com
canondv.com
canobeam.com
canoneos.com
bjc8200.com
canonhdec.com
bjc8500.com
usa.canon.com
imagerunner.com
multispot.com
canoncamerashop.com
canoncctv.com
canonhelp.com
bjc-8500.com
canonbroadcast.com
imageland.net
consumer.usa.canon.com
bjc-8200.com
bjc3000.com
downloadlibrary.usa.canon.com
www.cusa.canon.com
www.canondv.com

Glosario de Términos de Ciberseguridad

1. **Man in the Middle (MitM):** Permite que el atacante tome el control de un dispositivo sin el conocimiento del Usuario.
2. **Vulnerabilidad:** Fallos o deficiencias de un software o hardware.
3. **Cibercriminal:** Delincuente Informático.
4. **Amenaza:** Cualquier peligro potencial que está asociado a la explotación de una Vulnerabilidad.
5. **Software:** Programa o conjuntos de programas de una computadora.
6. **Hacker:** Persona experto en alguna rama tecnológica que accede a un sistema informático, o red de comunicaciones.
7. **Phishing:** Estafa cometida a través de medios telemáticos mediante la cual el estafador intenta conseguir información confidencial.
8. **Suplantación de Identidad:** Actividad malintencionada que consiste en hacerse pasar por otra persona por diversos motivos (cometer delitos, obtener datos de manera ilegal)
9. **Malware:** Cualquier código que pueda utilizarse para robar datos, evitar controles de acceso, ocasionar daños o comprometer un Sistema.
10. **Criptomoneda (Bitcoin):** Moneda digital o virtual diseñada para funcionar como medio de intercambio a través de internet mediante un sistema criptográfico.
11. **Botnet:** Cualquier grupo de computadoras infectados y controlados por un atacante de forma remota.
12. **Ransomware:** Diseñado para mantener captivo un sistema o los datos que contiene hasta que se realice un pago.
13. **Troyano:** Malware que ejecuta operaciones maliciosas bajo la apariencia de una operación deseada.
14. **DDoS (Ataque Distribuido de Denegación de Servicio):** Ataque a un servidor o servicio desde muchos ordenadores para que deje de funcionar.
15. **Linux:** Sistema Operativo enfocado al Hacking Ético o Pruebas de Penetración.
16. **Windows:** Sistema Operativo para computadoras.