NEWSLETTER | totalsec

Expertos en Ciberseguridad

No. 288 | Sep 06 - Sep 10

CIBERSEGURIDAD: CÓMO ES EL "ATAQUE DE MANO FANTASMA" DIRIGIDO A SMARTPHONES

SEPTIEMBRE 02, 2021/FUENTE: INFOBAE[1]

Los celulares representan hoy uno de los principales objetivos de los ciberdelincuentes. En materia de ciberseguridad, en la actualidad el "ataque de mano fantasma" se refiere a apps maliciosas tipo RAT (herramientas de acceso remoto), por medio de las cuales los atacantes realizan una intrusión a dispositivos móviles, abriendo aplicaciones financieras y haciendo transacciones de forma sigilosa. Los ataques cibernéticos en América Latina crecieron un 24% durante 2021 respecto de los primeros 8 meses de 2020.

Así lo indica la firma de ciberseguridad Kaspersky en su informe anual Panorama de Amenazas en América Latina 2021 que dio a conocer esta semana en una cumbre de analistas de seguridad. El estudio toma en cuenta los 20 programas maliciosos más populares, los cuales representan más de 728 millones de intentos de infección en la región, un promedio de 35 ataques por segundo.

Asimismo, los intentos de infección por países fueron: Argentina 10 millones, Brasil 481 millones, Chile 8 millones, Colombia 30 millones, México 103 millones, Perú 33 millones, Ecuador 30 millones, Panamá 5 millones, Guatemala 5 millones, Venezuela 4 millones, Republica Dominicana 2 millones y Costa Rica 2 millones.

El software malicioso tiene su foco en las apps de finanzas. Los ataques cibernéticos en América Latina crecieron un 24% durante 2021

Algo curioso que reveló el informe es que los ataques de phishing (mensajes fraudulentos) han disminuido.

Sin embargo, varios países de la región se encuentran entre los más atacados del mundo. Al considerar la proporción de usuarios atacados durante los primeros ocho meses del año, Brasil figura en el primer lugar con 15,37% de usuarios que registraron algún intento de ataque.

Le sigue Ecuador (13,36%), Panamá (12,60%), Chile (11,90% y Colombia (11,09%). Cabe destacar que Venezuela (7,19%) y la República Dominicana (5,62%) figuran entre los países con la menor cantidad de ataques de ingeniería social a nivel mundial.

Crece la banca móvil, crecen los ataques

La pandemia ha provocado el aumento de la cantidad de personas que utilizan la banca móvil en América Latina. Es decir, acceden al homebanking a través del smartphone, realizando sus gestiones desde el móvil.

Esta situación ha hecho que los cibercriminales se enfoquen en los celulares. Uno de los principales problemas es que en los ataques de "mano fantasma", las huellas digitales, la autenticación de reconocimiento facial y otras medidas de seguridad no alcanzan para proteger a la persona.

[1]Fuente: https://www.infobae.com/america/tecno/2021/09/02/ciberseguridad-como-es-el-ataque-de-mano-fantasma-dirigido-a-smartphones/

Las amenazas de “ataque de mano fantasma” nacieron en Brasil. Los delincuentes usan códigos maliciosos para infectar los dispositivos y tomar control de ellos. Así, pueden obtener la información de las app bancarias o de pago, inclusive aunque estén protegidas con medidas de seguridad, como por ejemplo, registro con huellas dactilares.

Los 3 códigos maliciosos (malware) que más se están utilizando son Ghimob, BRata y TwMobo. En el primer caso, generalmente infecta el dispositivo móvil, a través de un correo electrónico que engaña a la persona e invita a descargar una app.

Al instalar Ghimob, es muy difícil removerlo. Este malware tiene una función para grabar la contraseña de la víctima y enviársela al criminal. Entonces, si la víctima quiere desbloquear la pantalla con su huella o reconocimiento facial, abrirá apps, aprobará operaciones y le abrirá más accesos al atacante.

En el caso de BRata, está activo desde 2019, y desde Kaspersky han detectado una campaña de este malware en Google Play, la tienda de apps, en donde se han detectado 40.000 instalaciones. Su distribución se da a través de notificaciones en el navegador ya que se disfraza de actualización de Chrome, actualización de WhatsApp, lector de PDF y Gmail.

Permite el acceso remoto y control, del teléfono incluso redireccionando a páginas de phishing (suplantación de datos), es decir, envía a sitios falsos, que se hacen pasar por páginas oficiales de una compañía o que parecen serias, por ejemplo. El malware BRata está listo para robar datos de apps financieras (sobre todo de Brasil).

En último lugar, se detecta el RAT TwMobo, uno de los más nuevos. No solo está interesado en robar datos financieros, sino también en data de las redes sociales (WhatsApp, Instagram, TikTok, Snapchat y Facebook). Bautizado como “Duro de Matar”, esta herramienta de acceso remoto, tan pronto como se instala, otorga derechos de administrador en el dispositivo, e inicia su módulo de protección. Este troyano impide que el usuario desinstale el malware y lo elimine de la configuración de administración del dispositivo.

Debido al crecimiento de la banca móvil, este tipo de ataques será cada vez más común. El gran desafío de las instituciones financieras es identificar este tipo de operaciones fraudulentas. Las mejores formas de protección son la concientización, la prevención y además, contar con una protección antimalware.

[1]Fuente: https://www.infobae.com/america/tecno/2021/09/02/ciberseguridad-como-es-el-ataque-de-mano-fantasma-dirigido-a-smartphones/

SE FILTRA EL PROYECTO COMPLETO Y EL CÓDIGO FUENTE DEL PELIGROSO RANSOMWARE BABUK

SEPTIEMBRE 04, 2021/FUENTE: HIPERTEXTUAL[2]

Babuk Locker fue una de las operaciones de ransomware más temidas de principios de 2021. Los atacantes se hicieron conocidos por apuntar a empresas y organizaciones gubernamentales, robar sus datos y exigir un pago por rescate. Ahora, el código fuente del software malicioso utilizado por este grupo de ciberdelincuentes se ha filtrado en la red.

Según indica Bleeping Computer, un presunto miembro del grupo publicó el código fuente completo del ransomware Babuk en un foro de piratería ruso. El autor de la publicación afirmó estar sufriendo una enfermedad terminal. Debido a eso decidió publicar los archivos sin ningún tipo de restricción para su descarga.

Las carpetas contienen varios proyectos de ransomware en Visual Studio para VMware ESXi, NAS y Windows. Además, como se menciona al principio, los archivos contienen el código fuente completo del cifrador y descifrador para sistemas operativos de Microsoft y, lo que parece ser un "keygen" de claves públicas y privadas.

Investigadores de la compañía de ciberseguridad Emsisoft y McAfee Enterprise han indicado que la filtración del ransomware Babuk parece legítima. Si bien los archivos pueden servir para descifrar los ordenadores de víctimas pasadas, también son un riesgo, ya que contienen todos los elementos necesarios para ejecutar ataques dirigidos.

En el pasado, precisamente, se filtró un generador de ransomware de Babuk en un sitio de descargas. Desafortunadamente este fue tomado por otro grupo de ciberdelincuentes que montó su propia operación de ataques. Estos cosecharon víctimas en distintas partes del mundo y las extorsionaron para no publicar sus archivos.

Babuk y el ataque de ransomware de la discordia

A principios de este año, el grupo de ciberdelincuentes Babuk parecía imparable. Habían dirigido ataques de ransomware a varias compañías, entre ellas la tienda de telefonía Phone House. Sin embargo, un ataque al Departamento Metropolitano de Policía de Washington D.C. reveló diferencias entre los miembros.

El administrador del equipo, según explica Bleeping Computer , quería filtrar los datos robados a la fuerza policial de Washington mientras que el resto del equipo estaba en contra. No obstante, datos fueron filtrados y los miembros se dividieron en grupos diferentes.

El ransomware de Babuk atacó a principios de año la tienda de telefonía Phone House y el Departamento de Policía de Washington.

Por un lado quedó el administrador original del grupo de ciberdelincuentes Babuk, que lanzó un foro de ciberdelitos conocido como Ramp. El resto del equipo lanzó Babuk V2 y continuaron con distintos ataques de ransomware.

[2]Fuente: https://hipertextual.com/2021/09/se-filtra-el-proyecto-completo-y-el-codigo-fuente-del-peligroso-ransomware-babuk

WHATSAPP: DE QUÉ TRATA EL FALLO EN EL SISTEMA CON EL QUE HACKERS PUEDEN ROBAR INFORMACIÓN DE LOS USUARIOS

SEPTIEMBRE 05, 2021/FUENTE: INFOBAE[3]

Las redes sociales son actualmente unas de las herramientas digitales más usadas por las personas en el mundo, teniendo en cuenta su importancia para comunicar y acercar a los usuarios con sus familiares o amigos. Ya sea por medio de una fotografía o una publicación en texto, las redes han ayudado a crear comunidades digitales como ninguna otra plataforma antes de estas.

Sin embargo, al estar alojadas en internet, y necesitar de una conexión estable, siempre existen riesgos en la seguridad de las personas que las usan, ya sea por medio de ciberdelincuentes que hackean una cuenta o de un error en el protocolo de privacidad de las apps.

Ejemplo de esto fue lo que descubrió Check Point Research (CPR), empresa especializada en la detección y análisis de amenazas cibernéticas, en medio de WhatsApp. La app de mensajería más importante del mundo, con más de 2 mil millones de usuarios registrados en su plataforma, habría tenido una "vulnerabilidad de lectura y escritura de límites" en su software.

Un problema con los filtros en las imágenes sería el culpable de este fallo que coloca en riesgo la privacidad de los internautas

"La vulnerabilidad estaba relacionada con la funcionalidad del filtro de imágenes de WhatsApp y se desencadenó cuando un usuario abrió un archivo adjunto que contenía un archivo de imagen creado con fines malintencionados, luego intentó aplicar un filtro y posteriormente la envió con el filtro aplicado de nuevo al atacante", explicó CPR, en un documento en el que detalla su investigación.

Así, de acuerdo con el análisis realizado por la compañía, la falla se deriva específicamente al momento en el que un usuario intenta aplicar varias capas de filtros a las imágenes, desde el editor nativo de WhatsApp, en formato GIF, lo que ocasiona que el software de la app se bloquee por un instante. Dicho espacio de tiempo es aprovechado por un hacker, que puede perfectamente enviar un código con malware a un usuario, solo empleando una fotografía editada con filtros.

"Un filtro de imagen es un proceso mediante el cual se modifican los píxeles de la imagen original para lograr algunos efectos visuales (por ejemplo, desenfocar, enfocar, etc.). Esto hace que los filtros sean un candidato muy prometedor para causar un bloqueo, ya que se producen muchos cálculos en el archivo de imagen durante la aplicación del filtro, lo que implica leer el contenido de la imagen, manipular los valores de píxeles y escribir datos en una nueva imagen de destino", añade CPR.

Asimismo, indicó que al conocer el problema, este fue notificado de forma inmediata a WhatsApp, empresa que decidió tomar cartas en el asunto para intentar arreglar lo que ellos mismos denominaron como un error de "lectura y escritura fuera de límites", al que llamaro CVE-2020-1910.

[3]Fuente: https://www.infobae.com/tecno/2021/09/05/whatsapp-de-que-trata-el-fallo-en-el-sistema-con-la-que-hackers-pueden-robar-informacion-de-los-usuarios/

"Trabajamos regularmente con investigadores de seguridad para mejorar las numerosas formas en que WhatsApp protege los mensajes de las personas, y apreciamos el trabajo que realiza Check Point para investigar cada rincón de nuestra aplicación. Las personas no deberían tener ninguna duda de que el cifrado de un extremo a otro sigue funcionando según lo previsto y los mensajes de las personas permanecen seguros y protegidos", señaló WhatsApp por medio de un comunicado oficial.

Por su parte, CPR agradeció la atención prestada por WhatsApp y que se haya utilizado su información para tener una experiencia de usuario más segura en dicha plataforma.

"Una vez que descubrimos la vulnerabilidad de seguridad, informamos rápidamente de nuestros hallazgos a WhatsApp, que se mostró colaborador a la hora de emitir una solución. El resultado de nuestros esfuerzos colectivos es un WhatsApp más seguro para los usuarios de todo el mundo", dijo Oded Vanunu, jefe de Investigación de Vulnerabilidades de Productos en Check Point.

Cabe recordar que, según los expertos, WhatsApp es una plataforma que recibe unos 55 mil millones de texto diariamente, además de unas 4,5 mil millones de fotos y cerca de mil millones de videos. Por supuesto, esto hace que cualquier fallo en el sistema pueda poner en riesgo a millones de personas en el planeta; aunque afortunadamente este no fue el caso.

"WhatsApp confirmó que no vieron evidencia de abuso relacionado con esta vulnerabilidad", finalizó CPR, para tranquilidad de los ciento de millones de usuarios que usan esta red social.

[3]Fuente: https://www.infobae.com/tecno/2021/09/05/whatsapp-de-que-trata-el-fallo-en-el-sistema-con-la-que-hackers-pueden-robar-informacion-de-los-usuarios/

NEWSLETTER

totalsec
Expertos en Ciberseguridad