NEWSLETTER

Boletín 282 | Jul 26 - Jul 30

totalsec
Expertos en Ciberseguridad

UBEL ES EL NUEVO OSCORP

JULIO 28, 2020/FUENTE: THE HACKERS NEWS[1]

Un malware de Android que se observó abusando de los servicios de accesibilidad en el dispositivo para secuestrar las credenciales de usuario de las aplicaciones bancarias europeas se ha transformado en una botnet completamente nueva como parte de una campaña renovada que comenzó en mayo de 2021.

El CERT-AGID de Italia, a fines de enero, reveló detalles sobre Oscorp , un malware móvil desarrollado para atacar múltiples objetivos financieros con el objetivo de robar fondos de víctimas desprevenidas. Sus características incluyen la capacidad de interceptar mensajes SMS y realizar llamadas telefónicas, y realizar ataques de superposición para más de 150 aplicaciones móviles mediante el uso de pantallas de inicio de sesión similares para desviar datos valiosos.

El malware se distribuyó a través de mensajes SMS maliciosos, y los ataques a menudo se realizaban en tiempo real haciéndose pasar por operadores bancarios para engañar a los objetivos por teléfono y obtener acceso subrepticiamente al dispositivo infectado a través del protocolo WebRTC y, en última instancia, realizar transferencias bancarias no autorizadas. Si bien no se informaron nuevas actividades desde entonces, parece que Oscorp pudo haber realizado un regreso después de una pausa temporal en la forma de una botnet de Android conocida como UBEL.

"Al analizar algunas muestras relacionadas, encontramos varios indicadores que vinculan a Oscorp y UBEL con la misma base de código malicioso, lo que sugiere una bifurcación del mismo proyecto original o simplemente un cambio de marca por parte de otros afiliados, ya que su código fuente parece ser compartido entre múltiples actores", dijo el martes la empresa italiana de ciberseguridad Cleafy , al trazar la evolución del malware.

Anunciado en foros clandestinos por $ 980, UBEL, como su predecesor, solicita permisos intrusivos que le permiten leer y enviar mensajes SMS, grabar audio, instalar y eliminar aplicaciones, iniciarse automáticamente después del inicio del sistema y abusar de los servicios de accesibilidad en Android para acumular información confidencial del dispositivo, como credenciales de inicio de sesión y códigos de autenticación de dos factores.

Una vez descargado en el dispositivo, el malware intenta instalarse como un servicio y ocultar su presencia al objetivo, logrando así la persistencia durante largos períodos de tiempo.

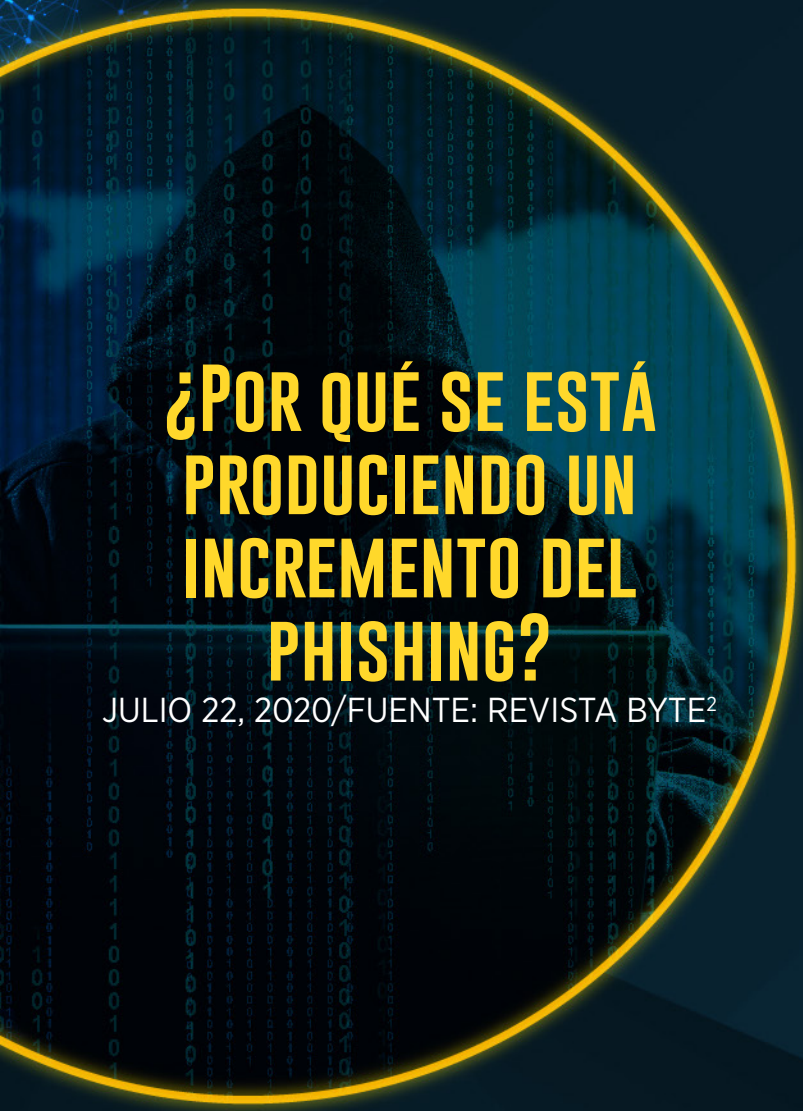
El malware se distribuyó a través de mensajes SMS maliciosos

Curiosamente, el uso de WebRTC para interactuar con el teléfono Android comprometido en tiempo real evita la necesidad de inscribir un nuevo dispositivo y hacerse cargo de una cuenta para realizar actividades fraudulentas.

"El objetivo principal de este al utilizar esta función es evitar una 'inscripción de un nuevo dispositivo', lo que reduce drásticamente la posibilidad de ser marcado como 'sospechoso', ya que los indicadores de huellas dactilares del dispositivo son bien conocidos desde la perspectiva del banco, ", dijeron los investigadores.

La distribución geográfica de los bancos y otras aplicaciones a las que apunta Oscorp se compone de España, Polonia, Alemania, Turquía, Estados Unidos, Italia, Japón, Australia, Francia e India, entre otros, según el informe.

[1]Fuente: https://thehackernews.com/2021/07/ubel-is-new-oscorp-android-credential.html



¿POR QUÉ SE ESTÁ PRODUCIENDO UN INCREMENTO DEL PHISHING?

JULIO 22, 2020/FUENTE: REVISTA BYTE[2]

Ivanti acaba de publicar los resultados de un estudio que demuestra que el teletrabajo ha incrementado el número, la sofisticación y el impacto de los ataques de phishing en las empresas. Casi tres cuartas partes (74 %) de los encuestados, afirman que sus empresas han sido víctimas de un ataque de phishing durante el último año, y el 40 % reconoce haber sufrido un ataque en el último mes.

> *El 80 % de los encuestados declara haber experimentado un aumento en el número de intentos de phishing*

El 80% de los encuestados declara haber experimentado un aumento en el número de intentos de phishing, y el 85% considera que éstos son cada vez más sofisticados. De hecho, el 73% reconoce que su departamento informático fue objeto de intentos de phishing, un 47% de los cuales se llevó a cabo con éxito.

Las estafas de smishing (ataque a través de mensajes de texto) y vishing (ataque a través de llamadas de voz) son las últimas variantes de phishing dirigidas a los usuarios de dispositivos móviles que han ganado más adeptos en el último año. Según un reciente estudio realizado por Aberdeen Strategy & Research, los ataques tienen una mayor tasa de éxito en los móviles que en los servidores, una tendencia que se consolida cada vez más. En cifras, las pérdidas económicas provocadas por los ataques de phishing se estiman en unos 1,7 millones de dólares anuales, cantidad que se prevé aumente hasta los 90 millones.

Los hackers están explotando las brechas de seguridad consecuencia del teletrabajo, pues los trabajadores remotos utilizan más que nunca los dispositivos móviles para acceder a los datos de la empresa. El 37% de los encuestados atribuye gran parte del éxito de los ataques de phishing a una tecnología insuficiente y al desconocimiento de los empleados, con un 34% que lo vincula exclusivamente a este último factor. Aunque el 96 % de los responsables de TI encuestados asegura que su organización forma a su plantilla sobre cómo afrontar ataques comunes como el phishing y el ransomware, un 30 % reconoce que tan solo el 80-90% de los empleados había completado la formación.

La encuesta de Ivanti revela también que los efectos de los ataques de phishing se han visto agravados por la falta de talento en el área de tecnología. Así, más de la mitad (52%) de los encuestados reconoce que su organización ha sufrido escasez de personal en el último año, y de ellos, el 64% atribuye la falta de recursos a la prolongación en el tiempo de resolución de incidencias. Por otra parte, el 46% de los encuestados opina que el aumento de los ataques de phishing es la consecuencia directa de la escasez de personal; y al reducir el personal, la capacidad de ofrecer una respuesta rápida a los problemas de seguridad disminuye considerablemente.

"Reducir el riesgo de ataques de phishing es una carrera contra el tiempo, a diferentes niveles. Los profesionales de TI deben ir por delante no solo de los hackers, que están continuamente ideando nuevos ataques, sino también de los propios empleados de sus empresas, que son sorprendentemente rápidos a la hora de hacer clic en enlaces maliciosos", afirmó Derek E. Brink, vicepresidente e investigador de Aberdeen Strategy & Research. "Además de invertir en formación y concienciación sobre ciberseguridad, las empresas deberían tener entre sus prioridades la aplicación de tecnologías avanzadas de automatización, inteligencia artificial y aprendizaje automático, con el fin de identificar, verificar y remediar más rápida y consistentemente las amenazas de phishing."

"Cualquier persona, independientemente de su experiencia o conocimientos de ciberseguridad, es susceptible de sufrir un ataque de phishing. En este sentido, la encuesta revela que casi la mitad de los profesionales de TI fueron engañados", declaró Chris Goettl, director senior de Gestión de Productos en Ivanti.

[2]Fuente: https://revistabyte.es/ciberseguridad/incremento-del-phishing/

Cómo Kaseya recuperó la información tras el ciberataque de REvil

JUNIO 26, 2020/FUENTE: EXPANSIÓN[3]

El proveedor de servicios Kaseya recibió un descifrador universal para solucionar el secuestro de información que sufrió el pasado 4 de julio. De esta manera, las víctimas del ataque ransomware, perpetrado por el grupo de ciberdelincuentes REvil, tendrán la facultad de recuperar sus archivos de forma gratuita.

La situación ha generado interés, debido a que hace unos días el grupo desapareció de la dark web, donde también cerraron sus sitios de pago e infraestructura. Esto habría dejado a Kaseya sin la posibilidad de pagar el rescate; sin embargo, la empresa declaró haber recibido la herramienta por parte de un "tercero de confianza".

Dana Liedholm, vicepresidenta ejecutiva de marketing corporativo de Kaseya, comentó para Bleeping Computer que obtuvieron "un descifrador de un tercero de confianza, pero no podemos compartir más detalles sobre la fuente". A pesar de ello, sí detallaron que se trata de la clave de descifrado universal, por lo que todos sus clientes pueden acceder a sus archivos.

Ante el cuestionamiento de si Kaseya tuvo que pagar un rescate para obtener el descifrador, Liedholm dijo que "no podían confirmar, ni negar eso". Por otra parte, la empresa de ciberseguridad Emsisoft también confirmó que ellos trabajaron de la mano con Kaseya, con el objetivo de validar la clave para recuperar la información.

La empresa no ha detallado si pagó un rescate, y el misterio en torno al caso se acrecienta tras la desaparición del grupo de hackers que protagonizó un ataque masivo a esta firma de software.

"Estamos trabajando con Kaseya para respaldar sus esfuerzos de participación del cliente. Hemos confirmado que la clave es efectiva para desbloquear víctimas y continuaremos brindando soporte a Kaseya y sus clientes", declaró Fabian Wosar, CTO de Emsisoft.

Si bien este representa un paso hacia la recuperación de las miles de empresas que fueron afectadas durante el ataque a Kaseya, todavía no está claro cómo se obtuvo la clave después de que REvil desapareciera.

Hasta el momento se han explorado diversas hipótesis en torno a esta situación. Una de ellas apunta a que el gobierno ruso lo haya obtenido directamente de los ciberdelincuentes y posteriormente haya sido entregado a las autoridades de Estados Unidos.

Sin embargo, el FBI no ha ampliado la información en torno al caso, pues dijo estar investigando. "El Departamento de Justicia y el FBI tienen una investigación en curso sobre la empresa criminal detrás de la variante de ransomware REvil y los actores del ataque a Kaseya específicamente. Según la política del Departamento de Justicia, no podemos comentar más sobre esta investigación en curso", señaló el organismo.

Aunque la desaparición de REvil ha generado interés, esto no significa el final de sus días. En junio de 2019 el grupo GandCrab cerró, pero posteriormente volvió aparecer bajo el nombre de REvil ransomware.

El ataque masivo a Kaseya se dio después de que los cibercriminales explotaran una vulnerabilidad de día cero en la aplicación de administración remota de la empresa, a partir de la cual se cifró a cerca de 60 proveedores de servicios, así como a cerca de 1,500 empresas. Además, exigieron 70 millones de dólares como recompensa.

Derivado de esta situación, la tensión política entre Estados Unidos y Rusia se elevó hasta el punto que los presidentes de ambos países se reunieron en una llamada para tratar el asunto.

[3]Fuente: https://expansion.mx/tecnologia/2021/07/26/cronica-como-kaseya-recupero-la-informacion-tras-el-ciberataque-de-revil

NEWSLETTER

totalsec
Expertos en Ciberseguridad