bafing

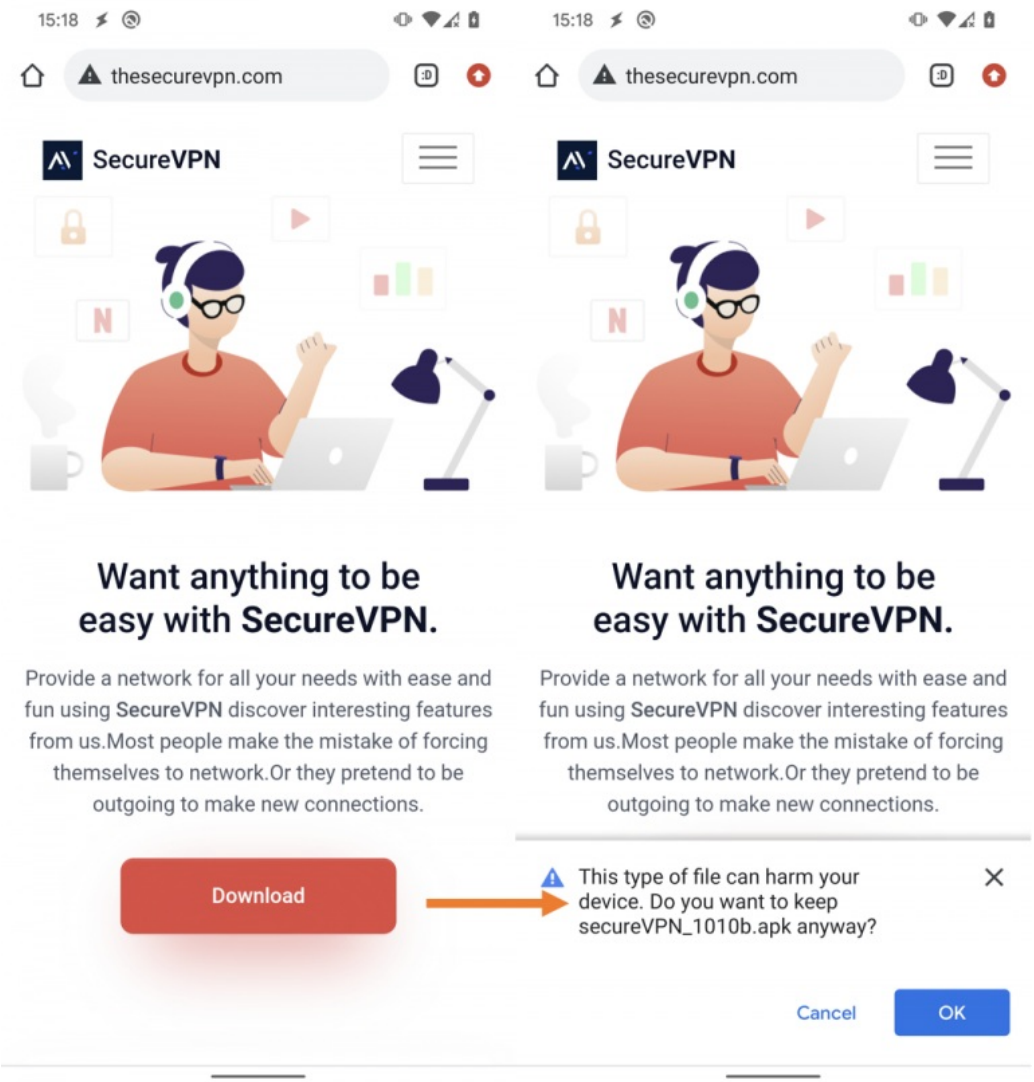
BOLETÍN
De Inteligencia de Ciberseguridad

Grupo cibercriminal Bahamut apunta a usuarios de Android con falsas apps de VPN

Las aplicaciones maliciosas utilizadas en esta campaña en curso roban contactos, mensajes SMS, llamadas telefónicas grabadas e incluso mensajes de chat de aplicaciones como Signal, Viber y Telegram.

El equipo de investigación de ESET identificó una campaña en curso dirigida a los usuarios de Android y que lleva adelante el grupo de APT Bahamut. Esta campaña ha estado activa desde enero de 2022 distribuyendo aplicaciones maliciosas a través de un sitio web falso de SecureVPN que solo ofrece para descargar apps de Android. Vale la pena tener en cuenta que aunque el malware empleado a lo largo de esta campaña utiliza el nombre SecureVPN, no tiene asociación alguna con el servicio y el software multiplataforma legítimo SecureVPN.

> El grupo de APT Bahamut generalmente apunta a entidades e individuos ubicados en Medio Oriente y en el sur de Asia a utilizando como vector de ataque mensajes de phishing y aplicaciones falsas. Bahamut se especializa en ciberespionaje, y creemos que su objetivo es robar información sensible de sus víctimas. Bahamut también se conoce como un grupo de mercenarios que ofrece servicios de piratería a sueldo a una amplia gama de clientes.



La campaña dirigida a dispositivos móviles operada por el grupo de APT Bahamut sigue en curso y utiliza el mismo método para distribuir sus aplicaciones de spyware para Android: a través de sitios web que se hacen pasar por servicios legítimos, como se ha visto en el pasado. Además, el código del spyware y, por lo tanto, su funcionalidad, es la misma que en campañas anteriores, incluida la capacidad de recopilar datos para exfiltrarlos en una base de datos local antes de enviarlos al servidor de los atacantes, una táctica que rara vez se ve en las aplicaciones móviles para ciberespionaje.

Parece que esta campaña ha mantenido un perfil bajo, ya que no vemos instancias en nuestros datos de telemetría. Esto probablemente se logra a través de una distribución altamente dirigida, donde junto con un enlace al spyware Bahamut, la potencial víctima recibe una clave de activación, que es necesaria para habilitar la capacidad de espionaje del malware.

Continúa leyendo aquí

Fuente: WeLiveSecurity by ESET

BumbleBee solía soltar un agente Meterpreter

Una campaña de ataque que comenzó a mediados de 2022 usó el cargador BumbleBee para lanzar un agente Meterpreter y Cobalt Strike Beacons.

Se utilizó un aviso de derechos de autor, que suponía una violación de la Ley de derechos de autor del milenio digital (DMCA), como vector de infección inicial. Después de obtener acceso a la red, el actor aprovechó la vulnerabilidad ZeroLogon (CVE-2020-1472) para obtener acceso al controlador de dominio principal. Trellix Threat Intelligence Group (TIG) recopila y analiza información de múltiples fuentes abiertas y cerradas antes de difundir informes de inteligencia. Esta campaña fue investigada por DFIR y compartida públicamente.

> La tasa de detección es la cantidad de detecciones de artefactos informadas por los sensores globales de McAfee para esta amenaza durante 4 días.

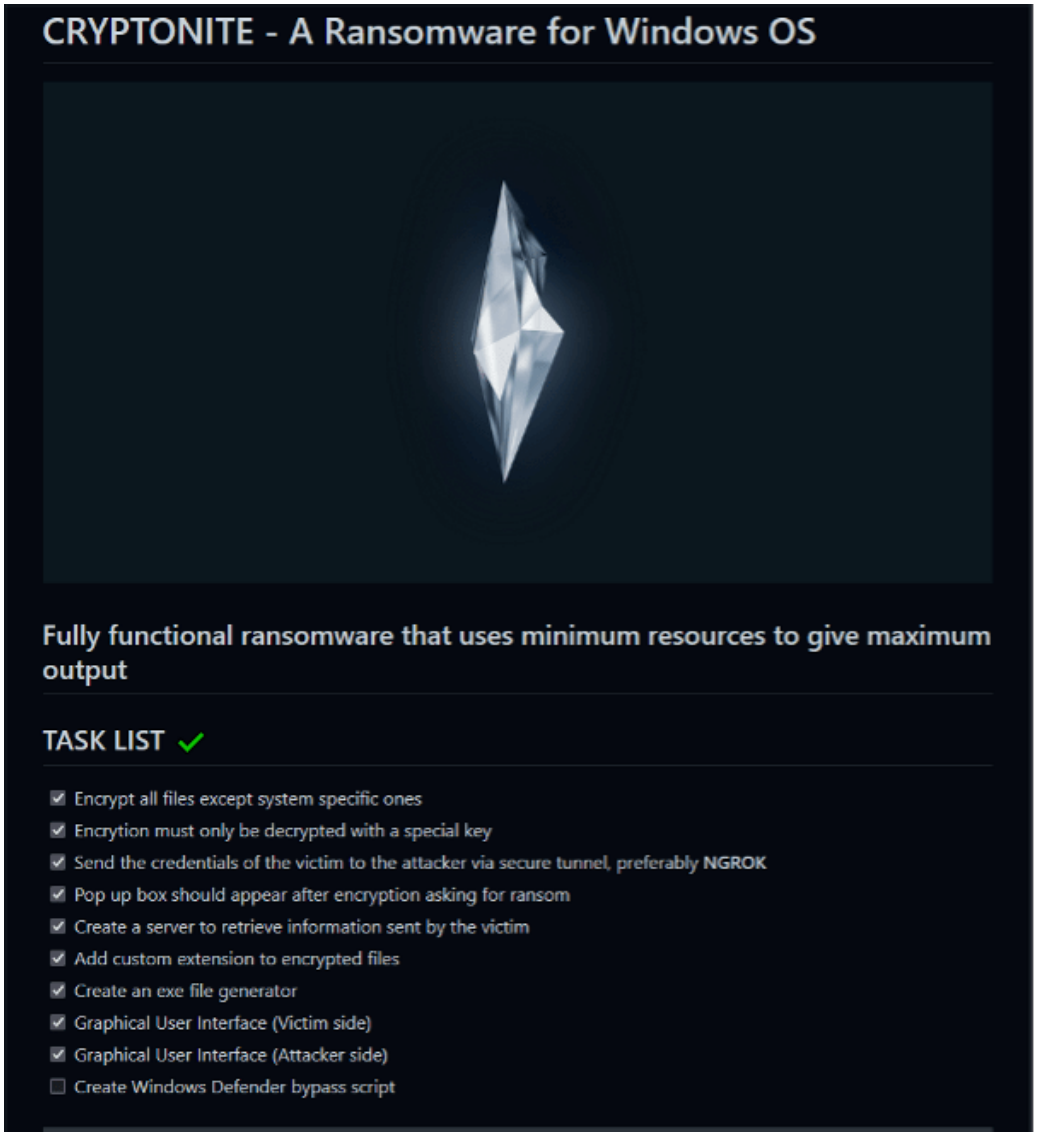
Los adversarios pueden eludir los mecanismos de UAC para elevar los privilegios de proceso en el sistema. El Control de cuentas de usuario (UAC) de Windows permite que un programa eleve sus privilegios (registrados como niveles de integridad que van de menor a mayor) para realizar una tarea con permisos de nivel de administrador, posiblemente solicitando la confirmación del usuario. El impacto para el usuario varía desde denegar la operación bajo un estricto cumplimiento hasta permitirle al usuario realizar la acción si está en el grupo de administradores locales y hacer clic en el aviso o permitirle ingresar una contraseña de administrador para completar la acción.

Continúa leyendo aquí

Fuente: Trellix

Investigación de amenazas: Cryptonite ransomware

El informe Ransomware Roundup tiene como objetivo brindar a los lectores información breve sobre el panorama en evolución del ransomware y las soluciones de Fortinet que protegen contra esas variantes.



Cryptonite (que no debe confundirse con la variante de ransomware Chaos, también llamada Cryptonite) es un kit de ransomware que existe como FOSS (Software libre y de código abierto). Inusualmente, está disponible para descargar por cualquier persona con las habilidades para implementarlo (en lugar de estar disponible para la venta en la clandestinidad criminal).

> Cryptonite está codificado en Python y requiere cierta configuración antes de empaquetarse y prepararse para su implementación. Además, un servidor también debe configurarse y ejecutarse para recibir información del ejecutable que se ejecuta en la máquina de una víctima para que el malware funcione correctamente.

Organizaciones como CISA, NCSC, FBI y HHS advierten a las víctimas de ransomware que no paguen un rescate, en parte porque el pago no garantiza que se recuperarán los archivos. De acuerdo con un aviso de la Oficina de Control de Activos Extranjeros (OFAC) del Departamento del Tesoro de EE. UU. , los pagos de rescate también pueden animar a los adversarios a apuntar a organizaciones adicionales, alentar a otros actores criminales a distribuir ransomware y/o financiar actividades ilícitas que podrían ser potencialmente ilegales. Para organizaciones e individuos afectados por ransomware, el FBI tiene una página de quejas de ransomware donde las víctimas pueden enviar muestras de actividad de ransomware a través de su Centro de quejas de delitos en Internet (IC3).

Continúa leyendo aquí

Fuente: Fortinet

Las falsas entidades de regulación financiera

Los estafadores están mandando mails simulando ser agencias gubernamentales para obtener datos personales y dinero de los usuarios.

El fraude online no conoce límites. Aunque no siempre tienen éxito, los ciberdelincuentes siguen adaptando sus estrategias usuales en cada país. Para obtener los datos personales y bancarios de sus víctimas, mandan mails en los que aparentan ser tiendas online, plataformas de streaming y, por claro, agencias gubernamentales. Hoy analizamos dos estafas aisladas en las que los ciberdelincuentes se hacen pasar por reguladores financieros que investigan el fraude, como seguro imaginaste. Con este pretexto, extraen una gran cantidad de información personal de sus pobres víctimas.

> La primera estafa se enfoca en los residentes alemanes. Comienza con un correo en el que una organización “llamda” Finanzmarktaufsicht (un nombre que sugiere tener algo que ver con la regulación financiera) asegura que la policía

de Osnabrück supuestamente ha arrestado a unos delincuentes y confiscado unos discos duros que contenían datos personales descifrados de los ciudadanos, los cuales incluyen los del destinatario.

FMA RECHTSABTEILUNG <promo@i6ny.com>
Aktenzeichen 520 Js 345/16

Sehr geehrte/r

Wir kontaktieren Sie im Zusammenhang mit einer Straftat. Ihre Persönlichen Daten wurden auf konfiszierten Festplatten von Betrügern entschlüsselt und möglicherweise sind Sie Geschädigter in einem Betrugsfall.

Aufgrund der hohen Anzahl von Geschädigten, gehen wir von einer Bandenkriminalität aus. Mit der Beschlagnahmung von Festplatten und der Verhaftung mehrerer Beteiligter durch die Osnabrücker Bundespolizei, würden wir Sie bitten uns in dem laufenden Verfahren zu unterstützen. Für eine erfolgreiche Verurteilung benötigen wir ihr mithilfe und vertiefende Informationen zu ihrem Fall.

Füllen Sie unser dafür angefertigtes Onlineformular aus oder kontaktieren Sie uns unter der unten stehen Telefonnummer persönlich.

Onlineformular:

Aktenzeichen: **520 Js 345/16** (Bitte stets angeben)

Artikel über die laufende Untersuchung:

FMA · FINANZMARKTAUFSICHT

FINANZMARKTAUFSICHT
Fasanenstraße 85 10623 Berlin,
Germany

Email:
Tel: +49 30 800932202-2

La segunda estafa se centra en Suiza. Esta vez, el mail le “recuerda” al destinatario que entre el 2015 y 2017 supuestamente invirtió en una empresa llamada SolidCFD que desgraciadamente, ha tenido que cerrar por alguna actividad ilegal. El “gestor de recuperación y resolución” de un regulador financiero independiente quiere ayudar a recuperar la inversión. Desgraciadamente, este “empleado no consigue comunicarse con el destinatario por teléfono, por lo que le pide que responda por mail para hablar de su inversión.

Continúa leyendo aquí

Fuente: Kaspersky

Vulnerabilidad destacada: vulnerabilidades de denegación de servicio del filtro CBFS de Callback Technologies

Cisco Talos descubrió recientemente una vulnerabilidad sin doble atributo de clase en Microsoft Office.

Cisco Talos descubrió recientemente tres vulnerabilidades de denegación de servicio en el filtro CBFS de Callback Technologies.

Callback Technologies tiene una solución de almacenamiento de archivos CBFS para

personalizar la persistencia de datos en los dispositivos. Para acompañar esto, su filtro CBFS administra esta solución de almacenamiento de archivos, lo que permite a los usuarios crear reglas de filtro y acceso, modificar y cifrar datos, etc.
Talos ha identificado tres vulnerabilidades de desreferencia de puntero nulo en el filtro CBFS:
TALOS-2022-1647 (CVE-2022-43588)
TALOS-2022-1648 (CVE-2022-43589)
TALOS-2022-1649 (CVE-2022-43590)

Un paquete de solicitud de E/S (IRP) especialmente diseñado puede provocar una denegación de servicio. Un atacante puede emitir un ioctl para desencadenar estas vulnerabilidades.

Cisco Talos trabajó con Callback Technologies para garantizar que estos problemas se resolvieran y que hubiera una actualización disponible para los clientes afectados, todo en cumplimiento de la política de divulgación de vulnerabilidades de Cisco.

> Se recomienda a los usuarios que actualicen este producto afectado lo antes posible: Tecnologías de devolución de llamada CBFS Filter 20.0.8317. Talos probó y confirmó que esta versión del filtro CBFS podría ser aprovechada por estas vulnerabilidades.

Las siguientes reglas de Snort detectarán intentos de explotación contra estas vulnerabilidades: 60811-60812, 60807-60808, 60809-60810. Es posible que se publiquen reglas adicionales en el futuro y las reglas actuales están sujetas a cambios, en espera de información adicional sobre vulnerabilidades. Para obtener la información más actualizada sobre las reglas, consulte su Firepower Management Center o Snort.org.

Continúa leyendo aquí

Fuente: Talos by Cisco

Cuidado con los ciberdelincuentes que se aprovechan de los compradores en línea el Black Friday

Si bien los ciberdelincuentes regularmente presentan nuevas ideas para encontrar más víctimas, un archivo PDF que encontró recientemente FortiGuard Labs demuestra que no siempre es así.

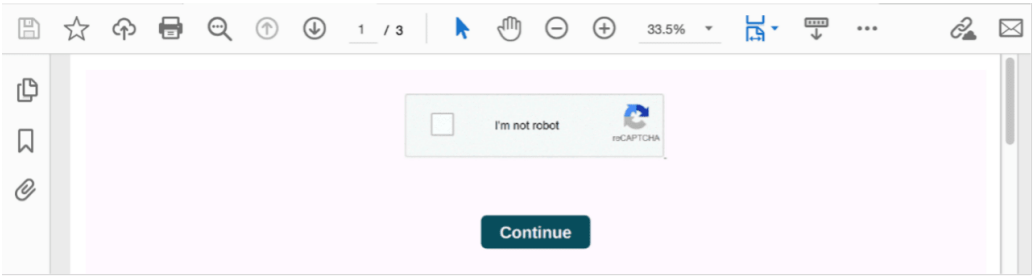
Los minoristas también esperan con ansias esta época del año. Muchos ganarán

alrededor de un tercio de sus ingresos anuales durante las próximas semanas. Y, lamentablemente, lo mismo ocurre con los ciberdelincuentes.

Según el FBI, las estafas cibernéticas cuestan a los consumidores cientos de millones cada temporada de vacaciones. En este blog, veremos dos ciberataques orientados al Black Friday que están cobrando fuerza, uno que utiliza un archivo PDF antiguo y otro que aprovecha la typosquatting.

Como indica el nombre del archivo, "walmart_black_friday_11_14_20.pdf" era probablemente de 2020. Sin embargo, se envió a VirusTotal a principios de noviembre de 2022.

La primera página del PDF solo incluye una autenticación humana CAPTCHA "No soy un robot".

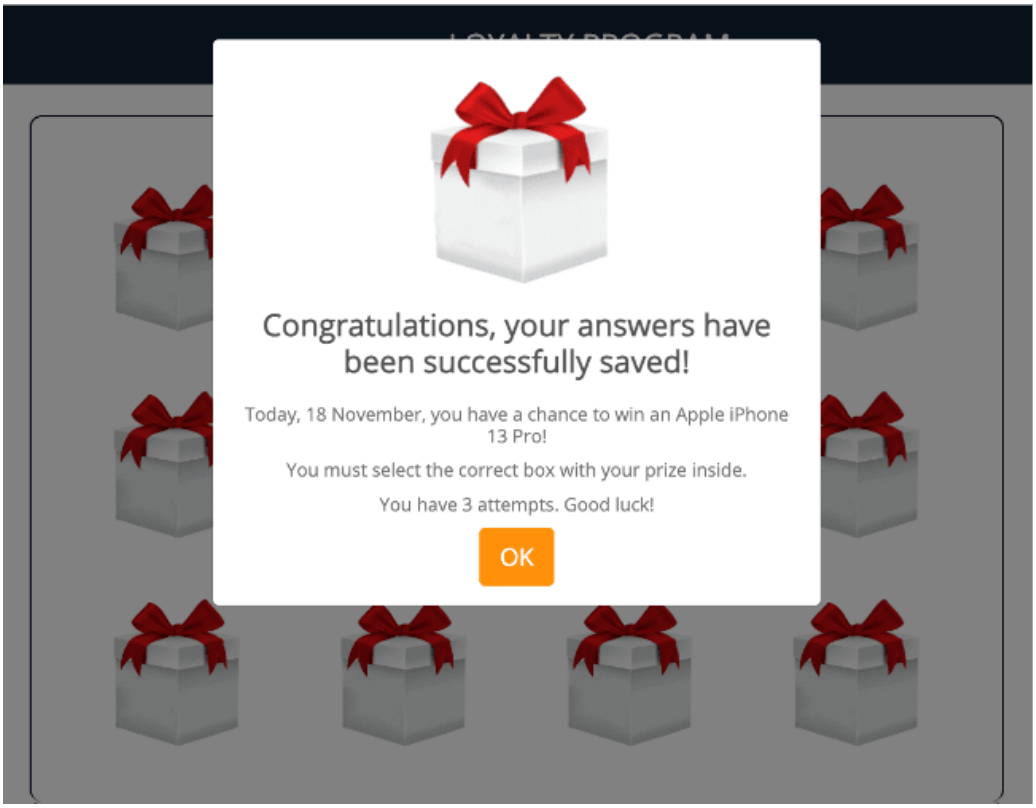


La encuesta en sí es trivial: pregunta por sexo, edad, frecuencia de compra en Amazon y cómo califica el usuario el servicio de Amazon.

Una vez respondidas todas las preguntas, el usuario tendrá tres intentos para sacar un iPhone de 12 cajas de regalo.

Además del ataque que responde a la actividad del usuario, la redirección también parece tener en cuenta la ubicación. El acceso desde Japón, por ejemplo, terminó en un servicio de chat en vivo, "Str**Chat", en lugar de la encuesta falsa de Amazon.

Afortunadamente, estos resultados son relativamente benignos. Este mismo ataque podría arrojar malware, cargar aplicaciones potencialmente no deseadas o lanzar una explotación de vulnerabilidad si el atacante decide hacerlo.



Continúa leyendo aquí

Fuente: Fortinet

Contáctenos

Central: +511 2259900 anexo 110
Equipo de Marketing: igrandez@bafing.com o al +51 969454618
Command Center y SOC: helpdesk@bafing.com o al +51 971500877

www.bafing.com

Facebook **Twitter** **LinkedIn**

Síguenos Síguenos Síguenos

Acerca de Bafing

Somos una empresa con más de 27 años de experiencia en el mercado de Tecnologías que ofrece soluciones muy especializadas en Ciberseguridad, eHealth y Smart Buildings.
El presente documento es una comunicación de carácter general hecha exclusivamente con propósitos informativos. Usted recibe este newsletter tras haberse suscrito al mismo. Si no desea continuar recibiéndolo, por favor escribir a bdigital@bafing.com