Verne
TECHNOLOGY GROUP

Boletín de alertas

Newsletter Seguridad Verne

Vol. 30/24

ÍNDICE

ACTUALIZACIÓN DEFECTUOSA DE CROWDSTRIKE PROVOCA FALLOS EN SISTEMAS WINDOWS A NIVEL MUNDIAL

CATEGORÍA	NOMBRE VULNERABILIDAD	BRECHA	Criticidad
Ciberseguridad	Actualización de seguridad	Windows	Alta

El 19 de julio de 2024, una actualización defectuosa del software de seguridad Falcon de CrowdStrike provocó interrupciones significativas en sistemas Windows a nivel mundial, afectando a empresas de diversos sectores. Este error generó numerosos "pantallas azules de la muerte" (BSoD), dejando inoperativos numerosos equipos.

CrowdStrike, una empresa reconocida por sus soluciones de ciberseguridad, lanzó una actualización para su producto Falcon Sensor. Sin embargo, esta actualización contenía un fallo crítico que desencadenó bloqueos masivos en sistemas operativos Windows. Los usuarios reportaron inmediatamente problemas de rendimiento y reinicios inesperados, llevando a una cascada de fallos en empresas de sectores clave como aerolíneas, instituciones financieras y hospitales.

El impacto fue notablemente severo en infraestructuras críticas. Los sistemas afectados incluían servidores virtuales en plataformas de nube como Google Cloud, Microsoft Azure y Amazon Web Services (AWS). La magnitud del problema causó que muchas operaciones comerciales se detuvieran, afectando la productividad y la capacidad operativa de numerosas organizaciones.

El sector financiero fue uno de los más golpeados, con interrupciones en transacciones y servicios bancarios en línea. Las aerolíneas reportaron retrasos y cancelaciones de vuelos debido a fallos en los sistemas de gestión de reservas y operaciones. Los hospitales también enfrentaron dificultades con sus sistemas de registro y gestión de pacientes, poniendo en riesgo la atención médica.

CrowdStrike actuó rápidamente para abordar la situación. Emitieron instrucciones para que los usuarios afectados iniciaran sus sistemas en modo seguro y eliminaran el archivo problemático identificado como "C-00000291*.sys". Esta medida ayudó a mitigar los efectos inmediatos del fallo, pero el daño ya estaba hecho.

La compañía también lanzó un parche de emergencia para corregir la actualización defectuosa y prometió realizar una revisión exhaustiva de sus procesos de control de calidad para prevenir futuros incidentes similares.

Las acciones de CrowdStrike cayeron un 15% como resultado directo del incidente, reflejando la pérdida de confianza de los inversores. Este suceso ha puesto de manifiesto la vulnerabilidad de las infraestructuras TI centralizadas y la necesidad urgente de diversificar y fortalecer las medidas de seguridad.

Expertos en ciberseguridad han subrayado la importancia de implementar salvaguardas adicionales y diversificar la infraestructura tecnológica para mejorar la resiliencia y seguridad de las operaciones comerciales. La Agencia de Ciberseguridad e Infraestructura (CISA) de EE.UU. emitió una advertencia sobre posibles ataques de phishing que podrían aprovechar la confusión generada por este fallo.

Este incidente se produce poco después de un fallo significativo en los servicios de Microsoft 365, que también provocó interrupciones generalizadas. Estos eventos destacan la fragilidad de las cadenas de suministro tecnológicas monolíticas y la necesidad de enfoques más robustos para la gestión de actualizaciones y la seguridad.

CrowdStrike ha asegurado a sus clientes que están comprometidos a aprender de este incidente y a implementar medidas correctivas para garantizar que no se repita en el futuro. La comunidad de TI y las empresas afectadas observan de cerca las acciones de la compañía mientras buscan recuperar la estabilidad y la confianza en sus sistemas.

DOS NACIONALES RUSOS SE DECLARAN CULPABLES DE ATAQUES CON RANSOMWARE LOCKBIT

CATEGORÍA	NOMBRE VULNERABILIDAD	BRECHA	Criticidad
Ciberseguridad	Ransomware	Empresas e Instituciones	Alta

El 19 de julio de 2024, dos nacionales rusos, Ruslan Magomedovich Astamirov y Mikhail Vasiliev, se declararon culpables en un tribunal de EE.UU. por su participación en el esquema de ransomware LockBit. Astamirov, de 21 años, y Vasiliev, de 34 años, admitieron haber ayudado en ataques de ransomware a nivel mundial.

Astamirov fue arrestado en Arizona en mayo de 2023, mientras que Vasiliev, también buscado en Canadá por cargos similares, fue extraditado a EE.UU. el mes pasado. LockBit ha atacado más de 2,500 entidades desde 2019, recaudando aproximadamente $500 millones en pagos de rescate. Los dos individuos desplegaron el ransomware en sistemas vulnerables y exigieron rescates para desencriptar los datos de las víctimas.

LockBit ha sido una de las amenazas más persistentes en el ámbito de la ciberseguridad. Este grupo de ciberdelincuentes ha logrado infiltrarse en sistemas de todo el mundo, afectando tanto a empresas como a instituciones gubernamentales. La magnitud de sus operaciones se evidenció en la cantidad de entidades afectadas y el monto total de los rescates pagados.

Astamirov, conocido como BETTERPAY, offtitan y Eastfarmer, admitió haber lanzado ataques contra al menos 12 víctimas entre 2020 y 2023, obteniendo $1.9 millones en pagos de rescate de víctimas en EE.UU., Japón, Francia, Escocia y Kenia. Enfrenta cargos por conspiración para cometer fraude informático y abuso, así como conspiración para cometer fraude electrónico, con una pena máxima de 25 años de prisión.

Vasiliev, operando bajo los alias Ghostrider, Free, Digitalocean90, Digitalocean99, Digitalwaters99 y Newwave110, llevó a cabo ataques contra 12 empresas en los estados de Nueva Jersey y Michigan, así como en el Reino Unido y Suiza. Enfrenta cargos que conllevan hasta 45 años de prisión por conspiración para cometer fraude informático y abuso, daños intencionados a un ordenador protegido, transmisión de una amenaza relacionada con daños a un ordenador protegido y conspiración para cometer fraude electrónico.

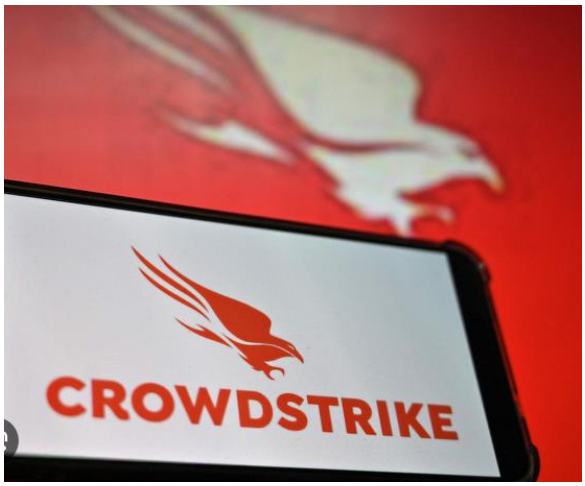
James E. Dennehy, agente especial del FBI en la oficina de Newark, destacó que la captura y condena de estos ciberdelincuentes demuestra que las autoridades pueden detener y llevar a la justicia a los actores maliciosos, desmintiendo la percepción de que los hackers pueden operar impunemente.

Ambos acusados serán sentenciados el 8 de enero de 2025. Este caso se suma a una serie de acciones coordinadas por la ley, como la operación Cronos, que derribó la infraestructura en línea de LockBit, aunque el grupo sigue activo.

El desenlace de este caso podría marcar un precedente significativo en la lucha contra el ransomware y otros cibercrímenes. La cooperación internacional y las acciones decisivas de las fuerzas del orden son cruciales para desmantelar redes criminales y proteger a las víctimas de futuros ataques.

CIBERCRIMINALES APROVECHAN EL ERROR DE ACTUALIZACIÓN DE CROWDSTRIKE PARA DISTRIBUIR MALWARE REMCOS RAT

CATEGORÍA	NOMBRE VULNERABILIDAD	BRECHA	Criticidad
Ciberseguridad	Malware	Usuarios	Alta



El reciente fallo en la actualización del software de seguridad Falcon de CrowdStrike, ocurrido el 19 de julio de 2024, ha sido aprovechado por cibercriminales para lanzar una campaña maliciosa. Este error en la actualización, que causó fallos masivos en sistemas Windows, se convirtió en una oportunidad para los atacantes, quienes rápidamente comenzaron a distribuir archivos ZIP maliciosos haciéndose pasar por una solución oficial de CrowdStrike.

Los archivos ZIP maliciosos, denominados "crowdstrike-hotfix.zip", contienen un loader de malware conocido como Hijack Loader, que instala el Remcos RAT (Remote Access Trojan) en los sistemas afectados. Este malware permite a los atacantes tomar control remoto del equipo infectado, espiar a los usuarios y robar información sensible. Los ciberdelincuentes están apuntando principalmente a los clientes de CrowdStrike en América Latina, proporcionando instrucciones en español para ejecutar el archivo "setup.exe" incluido en el ZIP.

El Remcos RAT es una herramienta potente y versátil que se utiliza para múltiples fines maliciosos, incluyendo el espionaje, el robo de datos y la ejecución de comandos de forma remota en el sistema infectado. La campaña actual de los atacantes aprovecha la confusión y el pánico generado por el fallo en la actualización de CrowdStrike para engañar a los usuarios y hacer que descarguen y ejecuten el archivo malicioso.

CrowdStrike ha emitido advertencias a sus clientes, instándolos a no descargar archivos de fuentes no verificadas y a comunicarse únicamente a través de canales oficiales para obtener soporte técnico. La empresa también ha trabajado estrechamente con Microsoft para proporcionar herramientas de recuperación que ayuden a los administradores de TI a reparar los dispositivos afectados por la actualización defectuosa.

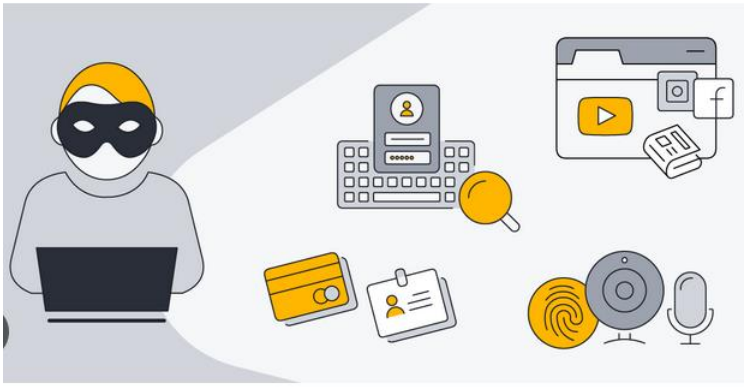
Los usuarios deben estar especialmente atentos a correos electrónicos y mensajes que pretendan ofrecer soluciones rápidas al problema del software de CrowdStrike. Es crucial verificar la autenticidad de cualquier comunicación y seguir las directrices oficiales proporcionadas por el equipo de soporte de CrowdStrike.

Este incidente destaca la vulnerabilidad de las infraestructuras tecnológicas centralizadas y la importancia de tener planes robustos de recuperación ante desastres y procedimientos de seguridad rigurosos. Las empresas deben asegurarse de que sus equipos de TI estén preparados para enfrentar y mitigar los efectos de tales fallos y ataques maliciosos.

CrowdStrike y Microsoft están colaborando para mitigar los daños y proteger a los usuarios contra futuras amenazas derivadas de este incidente. La cooperación entre empresas de seguridad y proveedores de servicios en la nube es crucial para abordar y neutralizar rápidamente las amenazas emergentes.

CÓMO ELIMINAR UN SOFTWARE ESPÍA DE MI TELÉFONO MÓVIL ANDROID

CATEGORÍA	NOMBRE VULNERABILIDAD	BRECHA	Criticidad
Ciberseguridad	Spyware	Usuarios	Media



Eliminar software espía de un teléfono Android es crucial para proteger tu privacidad y mantener la seguridad de tus datos personales. Aquí te presentamos varios métodos para detectar y eliminar este tipo de software malicioso.

Es importante saber reconocer las señales de que tu teléfono podría estar infectado con spyware:

- Rendimiento lento y bloqueos inesperados: Si tu dispositivo se vuelve lento o las aplicaciones se bloquean con frecuencia, podría ser una señal de spyware ejecutándose en segundo plano.
- Consumo excesivo de batería y datos: El spyware consume recursos en segundo plano, lo que puede llevar a un mayor uso de batería y datos.
- Aplicaciones desconocidas o configuraciones alteradas: Si encuentras aplicaciones que no recuerdas haber instalado o cambios en la configuración sin tu conocimiento, esto puede indicar la presencia de spyware.

- Sobrecalentamiento constante: Un dispositivo que se sobrecalienta sin razón aparente puede estar siendo afectado por spyware.
- Comportamiento inusual: Si tu teléfono se despierta de repente, se reinicia sin motivo o muestra dificultades para apagarse, podría estar comprometido.

Aquí te presentamos varios métodos efectivos para eliminar spyware de tu dispositivo Android:

Método 1: Usar una Herramienta de Eliminación de Spyware

Descargar e instalar una aplicación antispyware confiable: Aplicaciones como Avast Mobile Security o AVG AntiVirus son recomendadas para detectar y eliminar spyware automáticamente.

Realizar un análisis completo: Una vez instalada la aplicación, ejecuta un análisis completo para identificar y eliminar cualquier software espía presente en tu dispositivo.

Método 2: Modo Seguro

Reiniciar en Modo Seguro: Mantén presionado el botón de encendido y selecciona "Reiniciar en modo seguro" cuando aparezca la opción. Esto desactivará todas las aplicaciones de terceros, lo que te permitirá identificar si el problema proviene de alguna de estas aplicaciones.

Revisar y eliminar aplicaciones sospechosas: En modo seguro, ve a Configuración > Aplicaciones y desinstala cualquier aplicación desconocida o sospechosa.

Método 3: Revisar Permisos y Actualizar el Sistema

Revisar los permisos de las aplicaciones: Ve a Configuración > Aplicaciones y notificaciones, y verifica los permisos otorgados a cada aplicación. Revoca los permisos de aplicaciones sospechosas.

Actualizar el sistema operativo y las aplicaciones: Asegúrate de que tanto tu sistema operativo Android como todas las aplicaciones estén actualizadas a sus versiones más recientes para evitar vulnerabilidades.

Método 4: Restablecimiento de Fábrica

Hacer una copia de seguridad de tus datos: Antes de proceder, asegúrate de hacer una copia de seguridad de todos tus datos importantes.

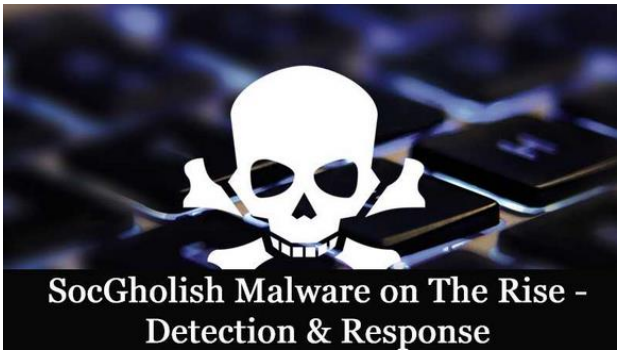
Restablecer el teléfono a su configuración de fábrica: Ve a Configuración > Sistema > Opciones de restablecimiento > Borrar todos los datos (restablecimiento de fábrica). Este método eliminará todos los datos y aplicaciones del dispositivo, incluyendo el spyware.

Para evitar futuras infecciones de spyware, sigue estas recomendaciones:

- Descarga aplicaciones solo de fuentes confiables: Utiliza Google Play Store y revisa las calificaciones y comentarios antes de instalar una aplicación.
- Mantén tu sistema y aplicaciones actualizadas: Las actualizaciones suelen incluir parches de seguridad importantes.
- Utiliza una solución de seguridad móvil: Mantén una aplicación antivirus instalada y actualizada en tu dispositivo (AVG.com).
- Siguiendo estos pasos, podrás detectar y eliminar spyware de tu teléfono Android, protegiendo así tu privacidad y manteniendo la seguridad de tus datos personales.

MALWARE SOCGHOLISH EXPLOTA PROYECTO BOINC PARA CIBERATAQUES

CATEGORÍA	NOMBRE VULNERABILIDAD	BRECHA	Criticidad
Ciberseguridad	Malware	BOINC	Alta



El 21 de julio de 2024, se reveló que el malware SocGholish, también conocido como FakeUpdates, está utilizando el proyecto de computación distribuida BOINC (Berkeley Open Infrastructure Network Computing) para llevar a cabo ataques cibernéticos encubiertos. BOINC es una plataforma utilizada para la computación voluntaria, donde los usuarios donan el tiempo de inactividad de sus computadoras para apoyar proyectos científicos. Sin embargo, en esta ocasión, los atacantes han aprovechado esta infraestructura para sus propósitos maliciosos.

SocGholish ha estado infectando sistemas mediante la descarga y ejecución del troyano de acceso remoto AsyncRAT, además de instalar BOINC en los sistemas comprometidos. Una vez instalado, el malware conecta los dispositivos infectados a servidores de comando y control (C2) controlados por los atacantes, utilizando dominios falsificados como "rosettahome[.]cn" y "rosettahome[.]top". Estos dominios están diseñados para parecerse a los utilizados por el legítimo proyecto Rosetta@home, un conocido proyecto de BOINC.

Los atacantes usan estos servidores C2 para recopilar datos de los sistemas infectados y ejecutar comandos maliciosos. Aunque hasta ahora no se ha observado una actividad maliciosa significativa más allá de la recopilación de datos, los expertos advierten que los atacantes podrían vender las conexiones de los hosts infectados a otros actores maliciosos, incluyendo grupos de ransomware.

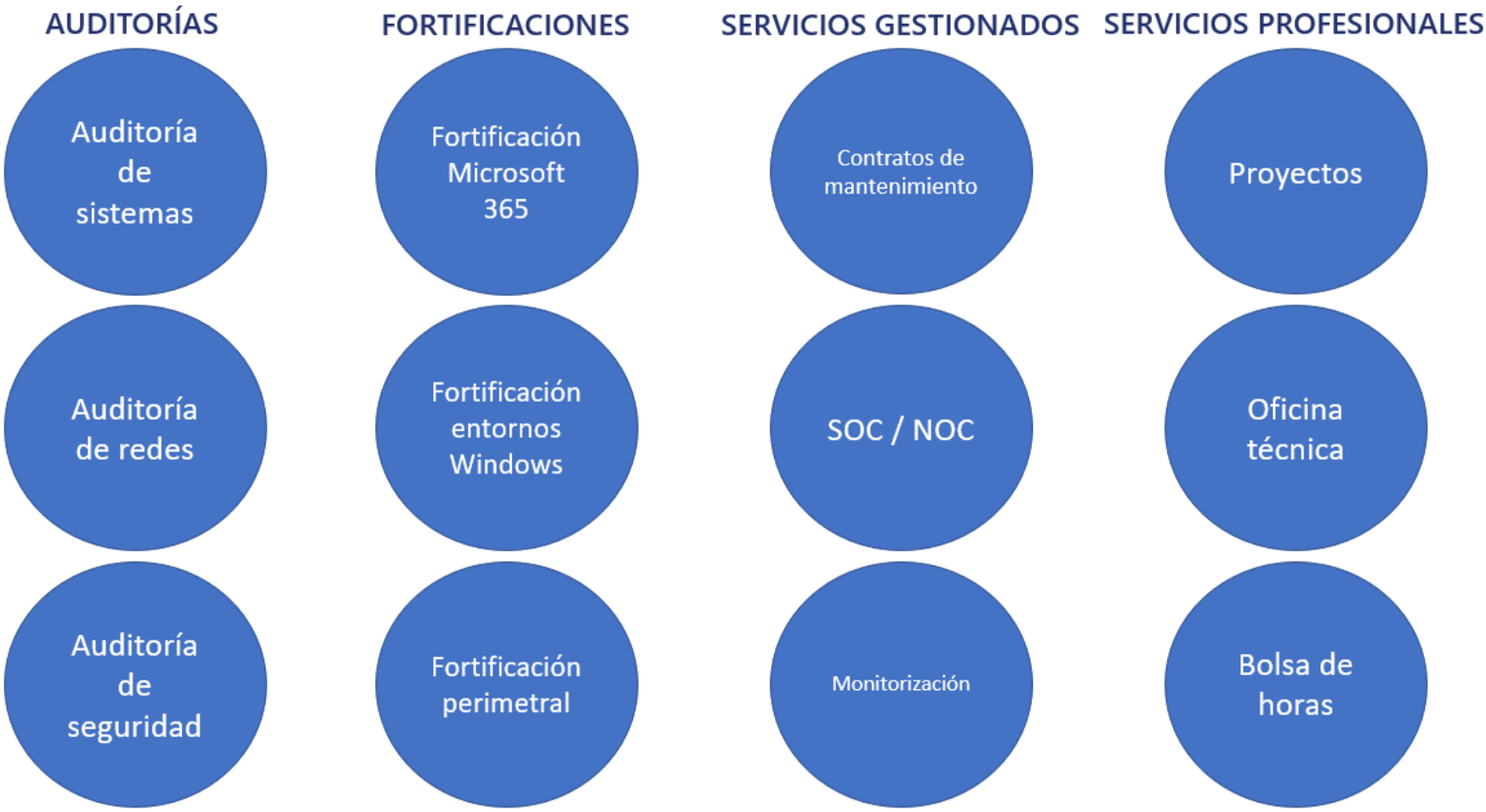
El uso de BOINC para distribuir malware representa un giro preocupante en las tácticas de los cibercriminales, ya que aprovechan una plataforma legítima y respetada para ocultar sus actividades maliciosas. Esto no solo pone en riesgo la reputación de proyectos como Rosetta@home, sino que también expone a los usuarios que participan en estos proyectos a posibles ataques y compromisos de seguridad.

Los expertos en ciberseguridad recomiendan a los usuarios que revisen y monitoreen cualquier software adicional instalado en sus sistemas que pueda estar utilizando BOINC. Además, es crucial mantenerse alerta ante cualquier comportamiento inusual del sistema y asegurarse de que todos los programas de seguridad estén actualizados. Las empresas y organizaciones que participan en proyectos de computación distribuida deben implementar medidas adicionales de seguridad para proteger sus infraestructuras y datos.

Este incidente subraya la necesidad de una vigilancia constante y de la implementación de medidas de seguridad robustas para proteger tanto a los usuarios individuales como a las infraestructuras colectivas contra el creciente ingenio de los cibercriminales.

.

> SERVICIOS VERNE PARA PYMES



¿TE GUSTARÍA AMPLIAR INFORMACIÓN O RECIBIR ASESORAMIENTO DE UN ESPECIALISTA?

www.vernegroup.com

CONTACTA