Publicado en Ciudad de México el 24/02/2022

# [Trickbot infecta más de 140.000 equipos de clientes de Amazon, Microsoft, Google](http://www.notasdeprensa.es)

## Check Point Research señala las 60 compañías cuyos clientes sufrido una infección por Trickbot. Las regiones más afectadas, por orden son: APAC, América Latina, Europa, África, América del Norte

 Check Point Research (CPR), la división de Inteligencia de Amenazas de Check Point® Software Technologies Ltd. (NASDAQ: CHKP), un proveedor líder de soluciones de ciberseguridad a nivel mundial, ha descubierto nuevos detalles de la ejecución de Trickbot. Este conocido troyano bancario, roba y compromete los datos de víctimas de alto perfil. Check Point Research ha contabilizado más de 140.000 equipos infectados por Trickbot desde noviembre de 2020, muchos de los cuales son clientes de conocidas compañías, como Amazon, Microsoft, Google y PayPal. En total, se han documentado 60 corporaciones cuyos compradores han sido víctimas de este troyano a lo largo de los últimos 14 meses. Los ciberdelincuentes están atacando selectivamente objetivos de alto perfil para robar y comprometer sus datos confidenciales. Además, la infraestructura de este ciberataque puede ser utilizada por varias familias de malware para causar más daño en los equipos infectados. Check Point Research recomienda a los ciudadanos que solo abran documentos de fuentes de confianza, ya que los autores de Trickbot están aprovechando las técnicas de anti-análisis (que impiden o dificultan que el malware sea analizado) y anti-desfusión (dificultar la lectura de un código) para permanecer dentro de las unidades. El porcentaje de organizaciones afectadas por este troyano en cada región son: Región Organizaciones afectadas Porcentaje Mundial 1 de cada 45 2,2% APAC 1 de cada 30 3,3% América Latina 1 de cada 47 2,1% Europa 1 de cada 54 1,9% África 1 de cada 57 1% Norte América 1 de cada 69 1,4% Puntos clave de la ejecución de Trickbot El troyano es muy selectivo a la hora de elegir sus objetivos. Los diversos métodos implementados en los módulos -incluyendo anti-análisis y la anti-desfusión demuestran la gran experiencia técnica de los ciberdelincuentes. La infraestructura de Trickbot puede ser utilizada por otras familias de malware para causar más daño en los equipos infectados. Este ataque es sofisticado y versátil con más de 20 módulos que pueden descargarse y ejecutarse bajo demanda. Cómo funciona Trickbot Los ciberdelincuentes reciben una base de datos de correos electrónicos robados y envían documentos maliciosos a las direcciones elegidas. El usuario descarga y abre dicho documento, permitiendo su ejecución en el proceso. Se ejecuta la primera etapa del malware y se descarga la carga útil principal. La carga útil principal del troyano se ejecuta y establece su persistencia en el equipo infectado. Los módulos auxiliares de Trickbot pueden ser cargados en el ordenador infectado a petición de los ciberdelincuentes; la funcionalidad de dichos módulos puede variar: puede ser la propagación a través de una red corporativa comprometida, el robo de credenciales corporativas, la obtención de datos de acceso a webs bancarios, etc. "Las estadísticas de Trickbot han sido sorprendentes. Se documentaron más de 140.000 ataques dirigidos a los clientes de algunas de las mayores y más reputadas empresas del mundo. Asimismo, ,se observó que los ciberdelincuentes tienen la habilidad de abordar el desarrollo de malware desde un nivel muy bajo y prestar atención a los pequeños detalles. Trickbot ataca a víctimas de alto perfil para robar las credenciales y proporcionar a sus operadores acceso a los portales con datos sensibles donde pueden causar aún más daño. Al mismo tiempo, es bien sabido que los ciberdelincuentes que están detrás de la infraestructura también tienen mucha experiencia en el desarrollo de malware a alto nivel. La combinación de estos dos factores es lo que permite que Trickbot siga siendo una amenaza peligrosa desde hace más de 5 años. La recomendación a los usuarios que sólo abran documentos de fuentes fiables y que utilicen diferentes contraseñas en distintos sitios web", destaca Eusebio Nieva, director técnico de Check Point Software para España y Portugal. Consejos de seguridad Abrir sólo los documentos que se reciben de fuentes de confianza. No se debe habilitar la ejecución en macro dentro de los documentos. Hay que asegurarse de tener las últimas actualizaciones del sistema operativo y del antivirus. En los distintos sitios web, utilizar contraseñas diferentes. Apéndice - Listado de empresas afectadas Empresa Sector Amazon E-commerce AmericanExpress Credit Card Service AmeriTrade Financial Services AOL Online service provider Associated Banc-Corp Bank Holding BancorpSouth Bank Bank of Montreal Investment Banking Barclays Bank Delaware Bank Blockchain.com Cryptocurrency Financial Services Canadian Imperial Bank of Commerce Financial Services Capital One Bank Holding Card Center Direct Digital Banking Centennial Bank Bank Holding Chase Consumer Banking Citi Financial Services Citibank Digital Banking Citizens Financial Group Bank Coamerica Financial Services Columbia Bank Bank Desjardins Group Financial Services E-Trade Financial Services Fidelity Financial Services Fifth Third Bank FundsXpress IT Service Management Google Technology GoToMyCard Financial Services HawaiiUSA Federal Credit Union Credit Union Huntington Bancshares Bank Holding Huntington Bank Bank Holding Interactive Brokers Financial Services JPMorgan Chase Investment Banking KeyBank Bank LexisNexis Data mining M and T Bank Bank Microsoft Technology Navy Federal Credit Union Paypal Financial Technology PNC Bank Bank RBC Bank Bank Robinhood Stock Trading Royal Bank of Canada Financial Services Schwab Financial Services Scotiabank Canada Bank SunTrust Bank Bank Holding Synchrony Financial Services Synovus Financial Services T. Rowe Price Investment Management TD Bank Bank TD Commercial Banking Financial Services TIAA Insurance Truist Financial Bank Holding U.S. Bancorp Bank Holding UnionBank Commercial Banking USAA Financial Services Vanguard Investment Management Wells Fargo Financial Services Yahoo Technology ZoomInfo Software as a service Check Point Software ofrece protección Zero-Day a través de su red, la nube, los usuarios y las soluciones de seguridad de acceso. Tanto si está en la nube, en el centro de datos o en ambos, las soluciones de seguridad de red de Check Point Software simplifican su seguridad sin afectar al rendimiento de la red, proporcionan un enfoque unificado para agilizar las operaciones y le permiten escalar para un crecimiento empresarial continuo. Quantum proporciona la mejor protección zero-day a la vez que reduce la sobrecarga de seguridad. Seguir a Check Point Research vía: Blog: https://research.checkpoint.com/Twitter: https://twitter.com/\_cpresearch\_ Acerca de Check Point ResearchCheck Point Research proporciona inteligencia sobre ciberamenazas a los clientes de Check Point Software y a la comunidad de inteligencia. El equipo de investigación recopila y analiza datos de ciberataques globales almacenados en ThreatCloud para mantener los ciberdelincuentes a raya, al tiempo que se asegura de que todos los productos de Check Point estén actualizados con las últimas protecciones. El equipo de investigación está formado por más de 100 analistas e investigadores que cooperan con otros proveedores de seguridad, las fuerzas de seguridad y varios CERTs. Seguir a Check Point Software a través de: Blog: https://blog.checkpoint.com/Twitter España: @CheckPointSpainFacebook: https://www.facebook.com/checkpointsoftwareLinkedIn España: https://www.linkedin.com/showcase/check-point-software-espana/YouTube: https://www.youtube.com/user/CPGlobal Acerca de Check Point Software Technologies Ltd. Check Point Software Technologies Ltd. es un proveedor líder de soluciones de ciberseguridad para empresas corporativas y gobiernos a nivel mundial. La cartera de soluciones de Check Point Infinity protege a las empresas y organizaciones públicas de los ciberataques de quinta generación con una tasa de captura líder en la industria de malware, ransomware y otras amenazas. Check Point Infinity se compone de tres pilares fundamentales que ofrecen una seguridad sin compromisos y una prevención de amenazas de quinta generación en todos los entornos empresariales: Check Point Harmony, para usuarios remotos; Check Point CloudGuard, para proteger automáticamente la nube; y Check Point Quantum, para proteger los perímetros de la red y los centros de datos, todo ello controlado por la gestión de seguridad unificada más completa e intuitiva del sector. Check Point Software protege a más de 100.000 empresas de todos los tamaños. ©2022 Check Point Software Technologies Ltd. Todos los derechos reservados.

**Datos de contacto:**

Moises Hernandez

Market21

5544884729

Nota de prensa publicada en: [https://www.mexicopress.com.mx/trickbot-infecta-mas-de-140-000-equipos-de](http://www.notasdeprensa.es/educalivecom-disfruta-de-cursos-presenciales-y-clases-particulares-a-traves-de-internet)

Categorías: Software Ciberseguridad



[**http://www.mexicopress.com.mx**](http://www.notasdeprensa.es)