Códigos QR, la ciberamenaza fantasma que resurge tras la pandemia

Los ciberdelincuentes están aprovechando el renacer de esta tecnología con la pandemia para convertir estos códigos en un vector de ataque “invisible”

La crisis del coronavirus ha producido un cambio radical en el mundo. Las empresas de todos los sectores se han visto en la necesidad de tener que reinventarse y adoptar herramientas tecnológicas para dar solución a algunos de los problemas que planteó la pandemia. Una de las tecnologías que ha resurgido es la de los Códigos QR, muy utilizados en los establecimientos de restauración para sustituir a las tradicionales cartas. Su uso ha crecido de manera exponencial en los últimos meses, puesto que según un estudio llevado a cabo por MobileIron, un 86% de usuarios móviles ha escaneado un código QR en el último año. Sin embargo, el mismo estudio refleja que un 34% de los encuestados no se preocupa por su seguridad al utilizar estos códigos. Por este motivo, Check Point® Software Technologies Ltd. (NASDAQ: CHKP), un proveedor líder especializado en ciberseguridad a nivel mundial, advierte de los ciberriesgos asociados a los códigos QR.

“Los códigos QR son códigos bidimensionales de Quick Response (respuesta rápida) que incorporan una URL incrustada en una imagen que, al escanearla, permite acceder a un sitio web. En definitiva, su funcionamiento es similar al de cualquier programa para acortar URLs”, señala Mario García, director general de Check Point para España y Portugal. “En los últimos meses hemos visto como ha experimentado un nuevo impulso en su uso, lo que, unido a la sensación de fiabilidad y falta de peligro que generan en los usuarios, así como su uso a través del smartphone, hacen que se estén convirtiendo en un nuevo vector de”, añade Mario García.

La amenaza fantasma de los códigos QR

Un caso práctico llevado a cabo por la Universidad Carnegie Mellon (Pensilvania, Estados Unidos), pone de manifiesto la falta de preocupación en materia de protección de datos personales al utilizar este sistema. Los expertos de la universidad colocaron cientos de posters con códigos QR en distintas localizaciones, y tras un mes, 225 personas

habían escaneado los carteles, de los cuáles un 85% visitó la página web asociada. “Los usuarios deben ser conscientes de que, en el fondo, están haciendo clic en un enlace que en muchos casos ni siquiera llegan a ver, por lo que podrían ser phishing y redirigir a una web maliciosa. Es importante tener en cuenta que donde hay internet puede haber un delincuente conectado, por lo que siempre hay que extremar las precauciones”, advierte Mario García.

Además, es importante destacar que los códigos QR se utilizan de forma mayoritaria a través del smartphone, por lo que pueden servir de puerta de acceso a la información que almacena el dispositivo. De hecho, con un código QR, o una aplicación para su lectura en las manos erróneas podría llegar a dar acceso a datos de ubicación, iniciar la descarga de software malicioso en el equipo (troyanos bancarios, malware, etc.) e incluso realizar pagos. De hecho, esta última aplicación se está comenzando a implementar en mayor medida para evitar el uso de dinero físico y como alternativa a las soluciones NFC (Near Field Communications).

En este sentido, desde Check Point señalan que el teléfono móvil es uno de los objetivos prioritarios de los cibercriminales, ya que según el informe Threat Intelligence Report de la compañía, durante la primera mitad del 2020 casi un 8% de los ciberataques en España iban dirigidos contra los smartphone, situándose un 1,5% por encima de la media a nivel mundial.

Asimismo, desde la compañía advierten de la necesidad de aumentar los niveles de seguridad y concienciación ante tecnologías como la de los códigos QR que aparentemente no parecen tener ningún riesgo, pero que pueden comprometer la confidencialidad de nuestros datos. Por ello, es fundamental instalar herramientas de seguridad que protejan los dispositivos. Check Point, por su parte, cuenta con SandBlast Mobile, una solución de defensa contra amenazas móviles que protege los dispositivos corporativos frente a ataques móviles avanzados. Asimismo, SandBlast Mobile protege los dispositivos de los empleados de aplicaciones infectadas, ataques de Man-in-the-Middle a través de Wi-Fi, exploits del sistema operativo, y enlaces maliciosos en mensajes de SMS. Es decir, proporciona seguridad móvil al prevenir, detectar y evitar los ciberataques más sofisticados.

Sigue Check Point Research vía:

Blog: https://research.checkpoint.com/
Twitter: https://twitter.com/_cpresearch_

Acerca de Check Point Research

Check 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.

Sigue a Check Point Software a través de:

Blog: https://blog.checkpoint.com/
Twitter España: @CheckPointSpain
Facebook: https://www.facebook.com/checkpointsoftware
LinkedIn 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.