Check Point Software desvela el funcionamiento interno de las ciberestafas más sofisticadas detectadas en España

Comunicados | 25/09/2025 | 00:00

Desde macrocentros criminales con millones de cuentas falsas hasta fraudes con códigos QR en estaciones de carga, los ataques combinan elementos físicos, digitales e inteligencia artificial para engañar al usuario con una eficacia sin precedentes. Durante el segundo trimestre de 2025 las empresas españolas registraron una media de 1.950 ciberataques semanales

Desde macrocentros criminales con millones de cuentas falsas hasta fraudes con códigos QR en estaciones de carga, los ataques combinan elementos físicos, digitales e inteligencia artificial para engañar al usuario con una eficacia sin precedentes. Durante el segundo trimestre de 2025 las empresas españolas registraron una media de 1.950 ciberataques semanales

Las ciberestafas ya no son obra de individuos aislados. Detrás de cada campaña fraudulenta hay organizaciones criminales con estructuras empresariales, divisiones especializadas y tecnología avanzada. Check Point® Software Technologies Ltd. (NASDAQ: CHKP), pionero y líder global en soluciones de ciberseguridad, revela qué hay realmente detrás de tres de las estafas más impactantes detectadas recientemente en España.

Este crecimiento en volumen y sofisticación está estrechamente ligado al auge de tecnologías como la inteligencia artificial generativa, que permite automatizar y escalar campañas delictivas. Datos de Check Point Research revelan que durante el segundo trimestre de 2025 las empresas españolas registraron una media de 1.950 ciberataques semanales, lo que supone un incremento del 36% respecto al mismo periodo de 2024, según su plataforma ThreatCloud AI.

Los ataques de phishing potenciados por IA en España se han incrementado un 466 % en lo que va de año, representando ya uno de cada tres fraudes detectados. Este fenómeno responde a un patrón: los estafadores actúan como auténticas corporaciones del delito, con recursos, personal y metodologías que imitan a empresas legítimas.

¿Qué hay detrás de estas ciberestafas? Tres ejemplos recientes lo evidencian:

1. Macrocentros del fraude: fábricas del crimen digital

En muchos casos, las estafas masivas que reciben los usuarios, ya sea por SMS, WhatsApp o correo electrónico, se generan en macrocentros de fraude ubicados principalmente en Asia o Europa del Este. Estas instalaciones, similares a call centers, emplean a cientos de personas que trabajan por turnos, siguiendo scripts diseñados para manipular psicológicamente a las víctimas.

Pero detrás hay mucho más: departamentos especializados para ingeniería social, redacción, diseño web, manejo de redes sociales falsas e incluso "atención al cliente". Muchas veces, los propios operadores han sido captados mediante ofertas laborales falsas, y terminan ejecutando estafas bajo amenaza.

Estos macrocentros funcionan como una empresa: tienen KPIs, supervisores y protocolos de escalado. La diferencia es que el producto que venden es el engaño. La profesionalización es tal que estas organizaciones utilizan CRMs, campañas segmentadas por región o idioma, y aprovechan datos filtrados de otras brechas para personalizar sus mensajes.

2. La estafa de la DGT: ingeniería social multicanal

Una reciente campaña en España llevó la suplantación de identidad a un nuevo nivel: los usuarios recibían en su domicilio una carta física simulando ser una multa de la DGT, impresa con todo el formato oficial. La trampa estaba en un código QR incluido en la carta, que redirigía a una web clonada de la Dirección General de Tráfico, donde se solicitaba el pago de la supuesta infracción.

Este caso muestra cómo los ciberdelincuentes están cruzando la frontera entre el mundo físico y el digital. No solo dominan el diseño de sitios falsos, sino también la capacidad logística para imprimir y distribuir cartas por correo postal. La estafa está pensada para generar confianza al máximo nivel: si llega a casa y parece oficial, pocos lo cuestionan. Además, esta campaña requería acceso a bases de datos con nombres y direcciones reales, lo que sugiere colaboración con terceros o compras en la dark web.

3. Estaciones de carga: el nuevo campo de ataque físico-digital

Los puntos de recarga para vehículos eléctricos se han convertido en una nueva superficie de ataque. El fraude se ejecuta de forma simple, pero efectiva: pegatinas con códigos QR falsos son colocadas sobre los terminales reales. Al escanear el código, el usuario es redirigido a una web falsa idéntica a la oficial, donde se le solicita iniciar sesión o introducir sus datos bancarios. En

algunos casos, si el intento de recarga falla inicialmente, el usuario puede repetir el proceso desde la web legítima, sin darse cuenta de que ya ha sido víctima de una estafa en el primer intento.

La combinación de inteligencia artificial, operaciones organizadas y nuevos vectores híbridos está marcando un cambio de paradigma. Ya no basta con proteger el correo electrónico o instalar un antivirus: los ataques se adaptan, combinan canales y juegan con la percepción del usuario. "Para combatir esta amenaza creciente, las compañías deben combinar tecnología de protección avanzada, especialmente en navegación y correo electrónico, con educación continua para sus empleados y usuarios finales", explica Rafael López, ingeniero de seguridad en Check Point Software.

Autor: Redacció

https://gironanoticies.com/comunicado/279390-check-point-software-desvela-el-funcionamiento-interno-de-las-ciberestafas-mas-sofisticadas-detectadas-en-espana.htm