

Detectados nuevos ataques malware gracias a la tecnología de emulación de Check Point

Los ataques comenzaron con emails fraudulentos dirigidos a empleados de grandes organizaciones de todo el mundo y que simulaban provenir de las entidades Citibank y Bank of America

Madrid, 24 de mayo de 2013.- Check Point® Software Technologies Ltd.(NASDAQ: CHKP), líder en soluciones de seguridad para Internet, ha anunciado la detección por parte de su innovadora solución Check Point Threat Emulation Software Blade de dos nuevos ataques en curso de phishing y bot. Ambas acciones infecciosas utilizaban variantes de la vulnerabilidad (CVE-2012-0158) y estaban dirigidas a empleados de grandes organizaciones de todo el mundo. La última tecnología de emulación de ataques de Check Point ha permitido detectar ambas amenazas antes de que estuvieran reconocidas y disponibles como firmas de antivirus.

Los ataques se iniciaron con correos señuelo que imitaban mensajes de Citibank y Bank of America y que tenían asuntos como "Extracto Bancario" o "Estado de Cuentas". Dichos emails invitaban a los receptores a abrir un documento adjunto de Microsoft Word infectado, como si fuera un documento legal. Este adjunto contenía malware que, si se abría, se ejecutaba automáticamente e infectaba los ordenadores que quedaban bajo el control de una gran red de bots.

El malware también podía abrir puertos de red, robar credenciales de usuario, así como contraseñas, y actuaba como un sistema bot de auto-propagación de spam, listo para ejecutar nuevas instrucciones de ataque y extender los correos maliciosos a otros objetivos, -como una característica única de este tipo de ataques-.

"Los cibercriminales están lanzando constantemente nuevos ataques y distribuyen miles de nuevas variantes de malware todos los días", asegura Dorit Dor, vicepresidenta de productos en Check Point Software Technologies. "Las soluciones antivirus tradicionales no son suficientes cuando se trata de amenazas desconocidas", añade.

"Las organizaciones necesitan una solución de seguridad multinivel que incluya tecnología de Emulación de Amenazas, capaz de detectar y prevenir nuevos ataques y otras variantes de ataques ya existentes. Nuestra tecnología sandboxing (o zona segura, haciendo referencia al lugar de apertura de los archivos sospechosos para supervisar su comportamiento) cierra la brecha que existe desde el momento de lanzamiento de nuevos ataques y la posterior disponibilidad de nuevas actualizaciones de antivirus, logrando la mayor eficacia conocida hasta el momento en lo que se refiere a prevención", concluye Dor.

Check Point ofrece protección global contra todo tipo de amenazas. Su solución Threat Emulation Software Blade previene las infecciones por vulnerabilidades desconocidas, así como los exploits o ataques de día cero y los ataques dirigidos. Esta innovadora solución inspecciona rápidamente los

archivos sospechosos, emula su funcionamiento y permite descubrir un comportamiento malicioso para evitar completamente la entrada de malware a la red. Además, informa inmediatamente de las nuevas amenazas detectadas mediante el servicio ThreatCloud™ de Check Point, que reporta automáticamente estas nuevas amenazas identificadas a todos los clientes.

Datos de contacto:

Ana Garza

Nota de prensa publicada en: [28046](#)

Categorías: [Ciberseguridad](#) [Innovación Tecnológica](#)

NotasdePrensa

<https://www.notasdeprensa.es>