Detectan 10 de los troyanos bancarios más prolíficos dirigidos a cientos de aplicaciones financieras con más de mil millones de usuarios

10 de los troyanos bancarios móviles más prolíficos pusieron sus ojos en 639 aplicaciones financieras que están disponibles en Google Play Store y se han descargado acumulativamente más de 1010 millones de veces.

Algunas de las aplicaciones más específicas incluyen PhonePe respaldado por Walmart, Binance, Cash App, Garanti BBVA Mobile, La Banque Postale, Ma Banque, Caf-Mon Compte, Postepay y BBVA México. Solo estas aplicaciones representan más de 260 millones de descargas del mercado oficial de aplicaciones.

De las 639 aplicaciones rastreadas, 121 tienen su sede en Estados unidos, seguidas por el Reino Unido (55), Italia (43), Turquía (34), Australia (33), Francia (31), España (29) y Portugal (27).

> *«TeaBot apunta a 410 de las 639 aplicaciones rastreadas. Octo apunta a 324 de las 639 aplicaciones rastreadas y es la única que apunta a aplicaciones populares con solicitudes financieras por robo de credenciales»,* dijo la compañía de seguridad móvil Zimperium.

Además de TeaBot (Anatsa) y Octo (Exobot), otros troyanos bancarios destacados incluyen BianLian, Coper, EventBot, FluBot (Cabassous), Medusa, SharkBot y Xenomorph.

También se considera que FluBot es una variante agresiva de Cabassous, por no hablar de enganchar su vagón de distribución para servir a Medusa, otro troyano bancario móvil que puede obtener un control casi completo sobre el dispositivo de un usuario. La semana pasada, Europol anunció el desmantelamiento de la infraestructura detrás de FluBot.

Estas herramientas maliciosas de acceso remoto, aunque se esconden detrás de la capa de aplicaciones de aspecto benigno, están diseñadas para atacar aplicaciones financieras móviles en un intento de llevar a cabo fraudes en el dispositivo y desviar fondos directamente de las cuentas de la víctima.

Además, las aplicaciones no autorizadas están equipadas con la capacidad de evadir la detección ocultando por lo general sus iconos de la pantalla de inicio y se sabe que registran pulsaciones de teclas, capturan datos del portapapeles y abusan de los permisos de los servicios de accesibilidad para perseguir sus objetivos, como el robo de credenciales.

Esto implica el uso de ataques superpuestos, que dirigen a la víctima a una página de inicio de sesión bancaria falsa que se muestra sobre aplicaciones financieras legítimas y puede usarse para robar las credenciales ingresadas.

Las consecuencias de tales ataques pueden variar desde el robo de datos y el fraude financiero hasta las multas reglamentarias y la pérdida de la confianza del cliente.

> *«en la última década, la industria financiera se pasó por completo a los dispositivos móviles para sus servicios bancarios y de pagos y para el comercio de acciones. Si bien esta transacción brinda mayor comodidad y nuevas opciones a los consumidores, también presenta nuevos riesgos de fraude»,* dijeron los investigadores.