BOLETÍN ESPECIAL DE SEGURIDAD INFORMÁTICA N.- 2020-ESFORSE-TICS-004, SOBRE EL MALWARE DE ANDROID, ROBA CONTRASEÑAS BANCARIAS, DATOS PRIVADOS Y PULSACIONES DE TECLAS

Se ha descubierto un nuevo tipo de malware de banca móvil que abusa de las funciones de accesibilidad de Android para filtrar datos confidenciales de aplicaciones financieras, leer mensajes SMS de usuarios y secuestrar códigos de autenticación de dos factores basados en SMS.

Llamado **"EventBot"** por los investigadores de Cybereason, el malware es capaz de apuntar a más de 200 aplicaciones financieras diferentes, incluyendo servicios bancarios, servicios de transferencia de dinero y billeteras de criptomonedas como **Paypal Business, Revolut, Barclays, CapitalOne, HSBC, Santander, TransferWise y Coinbase.**

"EventBot es particularmente interesante porque está en etapas tan tempranas", los investigadores dijeron. "Este nuevo malware tiene un potencial real para convertirse en el próximo gran malware móvil, ya que está bajo constantes mejoras iterativas, abusa de una característica crítica del sistema operativo y apunta a aplicaciones financieras".

La campaña, identificada por primera vez en marzo de 2020, enmascara su intención maliciosa haciéndose pasar por aplicaciones legítimas ***(por ejemplo, Adobe Flash, Microsoft Word)*** en tiendas APK falsas y otros sitios web sospechosos que, cuando están instalados, solicitan amplios permisos en el dispositivo.

Los permisos incluyen el acceso a la configuración de accesibilidad, la capacidad de leer desde el almacenamiento externo, enviar y recibir mensajes SMS, ejecutarse en segundo plano y ejecutarse después del inicio del sistema.

Si un usuario otorga acceso, EventBot funciona como un keylogger y puede ***"recuperar notificaciones sobre otras aplicaciones instaladas y contenido de ventanas*** **abiertas",** además de explotar los servicios de accesibilidad de Android para obtener el PIN de la pantalla de bloqueo y transmitir todos los datos recopilados en un formato cifrado a un servidor controlado por el atacante.

La capacidad de analizar los mensajes SMS también hace que el troyano bancario sea una herramienta útil para evitar la autenticación de dos factores basada en SMS, lo que les da a los adversarios un acceso fácil a las billeteras de criptomonedas de la víctima y roba fondos de las cuentas bancarias.

"Dar acceso al atacante a un dispositivo móvil puede tener graves consecuencias comerciales, especialmente si el usuario final está utilizando su dispositivo móvil para discutir temas comerciales delicados o acceder a información financiera empresarial", concluyeron los investigadores de Cybereason***. "Esto puede provocar la degradación de la marca, la pérdida de la reputación individual o la pérdida de la confianza del consumidor".***

La familia de aplicaciones maliciosas de EventBot puede no estar activa en Google Play Store, pero es otro recordatorio de por qué los usuarios deberían atenerse a las tiendas de aplicaciones oficiales y evitar la descarga de aplicaciones de fuentes no confiables. **Mantener el software actualizado y activar Google Play Protect también puede contribuir en gran medida a proteger los dispositivos del malware.**

Figura 1: Iconos usador por el malware EVENTBOT