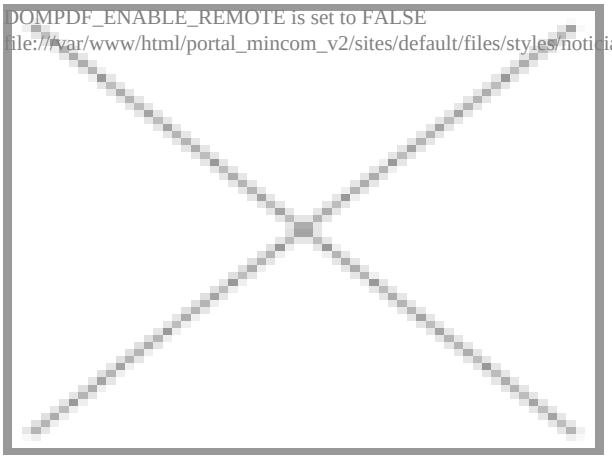

Source:
Tomado del perfil institucional de Facebook de Segurmática.

El pasado jueves 7 de Enero apareció una muestra de malware bancario para dispositivos Android de lo que parece ser una nueva familia no identificada anteriormente.
Se subió a VirusTotal y Koodous una aplicación maliciosa destinada a robar credenciales bancarias de aquellos usuarios que decidan instalarla en sus dispositivos. No se tiene constancia de que exista una familia de malware bancario a la que pueda pertenecer esta nueva muestra, por lo que todo parece apuntar a que se trata de una familia nueva que se une a las ya populares y habituales familias de ‘bankers’ para Android, como Cerberus o Anubis Bankbot.

Poco después de que esta muestra fuese subida a VirusTotal, la cuenta de Twitter ‘MalwareHunterTeam‘ se hizo eco del nuevo descubrimiento en un tweet en el que se indica el hash de la muestra y las imágenes de las detecciones de las diferentes soluciones de seguridad para Android.

Como se observa en estas mismas imágenes, e incluso si accedemos directamente a VirusTotal, hay antivirus para Android que detectan esta nueva muestra, aunque lo hacen con firmas genéricas de malware bancario o con firmas que detectan otras familias, como Cerberus o Anubis Bankbot. Sin embargo, tras nuestro análisis de la muestra no se trataría de ninguna de estas dos familias, sino de una nueva familias que no habíamos visto antes.

Las detecciones con firmas de otras familias se producen por que esta nueva familia sigue la estrategia habitual para el robo de credenciales que utilizan prácticamente todos los ‘bankers’ para Android hoy en día, el uso de inyecciones web que se muestran tan pronto como se detecta la apertura de la aplicación bancaria afectada.

Para lograr detectar el momento en el que el usuario abre la aplicación legítima, el malware bancario para Android aprovecha los permisos de accesibilidad, que solicita tan pronto como el usuario ejecuta el malware tras su instalación. Esto permite al malware instalar un servicio de accesibilidad en el dispositivo al que se notifican todos los eventos de accesibilidad que se producen (pulsaciones de botones, cambios en campos de texto, etc).

De esta forma, tan pronto como se produce un evento en la interfaz de usuario, el malware recibe la información asociada, permitiendole determinar si se ha abierto una aplicación bancaria de entre las afectadas, en cuyo caso se procede a mostrar una vista web con un formulario de phishing similar a la ventana de inicio de sesión legítima de la entidad.

Además de las inyecciones de phishing, el malware bancario de Android está aprovechando últimamente estos servicios de accesibilidad para robar las credenciales bancarias, aprovechando los eventos que se

generan cuando se modifica un campo de texto, lo que permite al ‘banker’ obtener dichos cambios y registrarlos para enviarlos al servidor de control. Esta estrategia de robo de credenciales recuerda a los ‘keyloggers‘ de sistemas de escritorio, y, de hecho, este nuevo malware lo llama así.

En la anterior imagen podemos ver que se realizan dos peticiones diferentes al servidor de control para obtener la lista de entidades afectada en función del tipo de estrategia de robo de credenciales. En el caso de las entidades afectadas por el keylogger, la petición devuelve la lista completa de entidades afectadas, sin embargo, para obtener la lista de entidades afectadas por la estrategia basada en inyecciones, se debe proporcionar la lista de aplicaciones instaladas y el servidor de control devolverá el subconjunto de aplicaciones afectadas, junto al código HTML de la inyección a mostrar. Esto impide obtener de forma sencilla la lista completa de entidades bancarias afectadas, y es algo que cada vez se hace más por parte del malware.

Al parecer, los desarrolladores de este nuevo troyano parecen estar interesados en entidades españolas, ya que la mayor parte de entidades afectadas son entidades de nuestro país. Aunque también hemos encontrado afectación para algunas entidades alemanas.
