Investigadores en ciberseguridad han identificado lo que consideran el primer malware para Android que aprovecha Gemini, el chatbot de inteligencia artificial generativa de Google, como parte de su flujo de ejecución y que además consigue mantenerse de forma persistente en el dispositivo.

La amenaza ha sido denominada PromptSpy por ESET. Este programa malicioso está preparado para capturar datos de la pantalla de bloqueo, obstaculizar intentos de desinstalación, recopilar información del dispositivo, realizar capturas de pantalla y grabar la actividad en pantalla en video.

"Gemini se utiliza para analizar la pantalla actual y proporcionar a PromptSpy instrucciones paso a paso sobre cómo garantizar que la aplicación maliciosa permanezca fijada en la lista de aplicaciones recientes, evitando así que pueda cerrarse fácilmente deslizándola o que el sistema la finalice", señaló el investigador de ESET Lukáš Štefanko en un informe publicado hoy.

"Dado que el malware para Android suele basarse en la navegación por la interfaz de usuario, el uso de inteligencia artificial generativa permite a los actores de la amenaza adaptarse a prácticamente cualquier dispositivo, diseño o versión del sistema operativo, lo que amplía considerablemente el número potencial de víctimas."

En términos concretos, el malware integra de forma codificada tanto el modelo de IA como un prompt, asignando al agente el papel de un "asistente de automatización de Android". Luego envía a Gemini una instrucción en lenguaje natural junto con un volcado XML de la pantalla activa, que contiene información detallada de cada elemento de la interfaz, incluyendo su texto, tipo y ubicación exacta en la pantalla.

Después, Gemini procesa esos datos y responde con instrucciones en formato JSON que indican al malware qué acción ejecutar (por ejemplo, un toque) y en qué punto realizarla. Esta interacción de múltiples pasos continúa hasta que la aplicación queda bloqueada en la lista de apps recientes y no puede cerrarse.

El objetivo principal de PromptSpy es desplegar un módulo VNC integrado que otorga a los atacantes acceso remoto al dispositivo de la víctima. El malware también está diseñado para aprovechar los servicios de accesibilidad de Android y así impedir su eliminación mediante superposiciones invisibles. Además, se comunica con un servidor de comando y control (C2) integrado en el código («54.67.2[.]84») a través del protocolo VNC.

Es importante destacar que las acciones sugeridas por Gemini se ejecutan mediante los servicios de accesibilidad, lo que permite al malware interactuar con el dispositivo sin intervención del usuario. Todo esto se lleva a cabo comunicándose con el servidor C2 para obtener la clave de la API de Gemini, realizar capturas de pantalla bajo demanda, interceptar el PIN o la contraseña de la pantalla de bloqueo, grabar la pantalla y capturar en video el patrón de desbloqueo.

```
public static void startAutomationLoop(AccessibilityService accessibilityService, String str, String str2) {
    String str3;
    String str4;
    JSONArray jSONArray;
    String str5;
    int i;
    int i2;
    boolean z;
    AccessibilityService accessibilityService2 = accessibilityService;
    String str6 = str;
    if (accessibilityService2 == null) {
        return;
    }
    int i3 = 4;
    String str7 = TAG;
    if (str2 == null || str2.isEmpty()) {
        ServiceInteractionUtil.ToLog(TAG, "未设置 Gemini API Key，无法执行自动化任务", 4);
        return;
    }
    ServiceInteractionUtil.ToLog(TAG, "开始执行任务: " + str6);
    JSONArray jSONArray2 = new JSONArray();
    String string = accessibilityService2.getString(R.string.atuo_load_msg);
    int i4 = 1;
    boolean z2 = true;
    int i5 = 0;
    while (z2 && i5 < 30) {
        int i6 = i5 + 1;
        ServiceInteractionUtil.ToLog(str7, ">>> 步骤 " + i6);
        AccessibilityNodeInfo accessibilityNodeInfoGetActiveWindowNodeInfo = InputService.GetActiveWindowNodeInfo();
        String aIXml = AccessibilityNodeUtil.toAIXml(accessibilityNodeInfoGetActiveWindowNodeInfo);
        if (accessibilityNodeInfoGetActiveWindowNodeInfo != null) {
            accessibilityNodeInfoGetActiveWindowNodeInfo.recycle();
        }
        if (i6 == i4) {
            str3 = "You are an Android automation assistant. The user will give you the UI XML data of the current screen.
        } else {
            str3 = "The previous action has been executed. This is the new UI XML, please determine if the task is complet
        }
        addToHistory(jSONArray2, "user", str3);
        String strCallGeminiApi = callGeminiApi(str2, jSONArray2);
        if (strCallGeminiApi == null) {
            ServiceInteractionUtil.ToLog(str7, "API 请求失败，终止任务", i3);
            AutoClicker.bringHomeToForeground();
            return;
```

Un análisis de los indicios de localización lingüística y de los vectores de distribución empleados sugiere que la campaña tendría una motivación económica y estaría dirigida a usuarios en Argentina. De forma llamativa, las pruebas apuntan a que PromptSpy fue desarrollado en un entorno de habla china, como lo demuestra la presencia de cadenas de depuración escritas en chino simplificado.

“PromptSpy se distribuye a través de un sitio web dedicado y nunca ha estado disponible en Google Play”, afirmó Štefanko.

PromptSpy es considerado una versión más avanzada de otro malware para Android previamente desconocido llamado VNCSpy, cuyas muestras fueron cargadas por primera vez el mes pasado en la plataforma VirusTotal desde Hong Kong.

El sitio web «mgardownload[.]com» se utiliza para distribuir un dropper que, tras instalarse y ejecutarse, abre una página alojada en «m-mgarg[.]com». Esta página se hace pasar por JPMorgan Chase bajo el nombre "MorganArg", en referencia a Morgan Argentina. El dropper también indica a las víctimas que concedan permisos para instalar aplicaciones desde fuentes desconocidas con el fin de desplegar PromptSpy.

"En segundo plano, el troyano contacta con su servidor para solicitar un archivo de configuración, que incluye un enlace para descargar otro APK, presentado a la víctima, en español, como una actualización", indicó ESET. "Durante nuestra investigación, el servidor de configuración ya no estaba accesible, por lo que la URL exacta de descarga sigue siendo desconocida."

Los hallazgos ponen de relieve cómo los actores maliciosos están incorporando herramientas de inteligencia artificial en sus operaciones, haciendo que el malware sea más dinámico y permitiéndoles automatizar acciones que, con enfoques tradicionales, resultarían más difíciles.

Dado que PromptSpy impide su propia desinstalación superponiendo elementos invisibles en la pantalla, la única manera de eliminarlo es reiniciar el dispositivo en Modo Seguro, donde las aplicaciones de terceros se deshabilitan y pueden desinstalarse.

"PromptSpy demuestra que el malware para Android está comenzando a evolucionar de una manera inquietante", señaló ESET. "Al apoyarse en inteligencia artificial generativa para interpretar los elementos en pantalla y decidir cómo interactuar con ellos, el malware puede adaptarse prácticamente a cualquier dispositivo, tamaño de pantalla o diseño de interfaz que encuentre."

"En lugar de depender de toques codificados de forma fija, simplemente entrega a la IA una

captura de la pantalla y recibe a cambio instrucciones de interacción precisas y paso a paso, lo que le ayuda a aplicar una técnica de persistencia resistente a los cambios en la interfaz.”