# Campaña De Espionaje Con APPS De Malware Se Enfoca A Dispositivos iOS


Se ha encontrado una **campaña de malware enfocada a dispositivos iOS** y entidades importantes, incluidas las organizaciones europeas de defensa, gobiernos y los sectores de medios de comunicación, usando un software espía, capaz de violar los dispositivos sin jailbreak.

La campaña spyware, llamada «**Operation Pawn Storm**» por expertos en seguridad, se detectó por primera vez en los ordenadores con Windows a finales del año pasado, pero ahora ha hecho su camino a los dispositivos iOS, un informe de los investigadores de seguridad de TrendLabs han informado.

# APP Spyware XAgent

Uno de los dos spywares utilizados en la campaña es en realidad una aplicación, la empresa ha nombrado la aplicación como XAgent, la cual intenta instalarse y ejecutarse en los **dispositivos iOS**.

> *«La aplicación **XAgent es un malware** completamente funcional. Los métodos exactos de la instalación de este malware es desconocida, sin embargo, sí sabemos que **el dispositivo iOS no tiene que tener hecho el jailbreak** … Hemos visto un caso*

*en el que un señuelo que implica XAgent simplemente dice» Toque aquí para instalar la aplicación '».*

El sitio web falso distribuye el spyware mediante la función de aprovisionamiento **ad-hoc de Apple**, destinado a empresas y desarrolladores que deseen distribuir sus aplicaciones a un pequeño grupo de personas y permite a los usuarios pasar por alto la App Store.

# XAgent Obtiene Casi Todo

Una vez instalado, **XAgent** recogerá los mensajes de texto, listas de contactos, imágenes, datos de geolocalización, información de una lista de aplicaciones instaladas en un dispositivo iOS, y el estado de Wi-Fi del dispositivo. La información se envía a un servidor controlado por los piratas informáticos. XAgent también es capaz de activar el micrófono del teléfono y grabar todo lo que oye.

La aplicación de malware XAgent funciona tanto en iOS 7 y 8, ya sea que hayan sido liberados con jailbreak o no. La aplicación maliciosa es más peligrosa en iOS 7, ya que esconde el icono para evadir la detección, pero es incapaz de ocultarse o automáticamente reiniciará en dispositivos iOS 8.

# Malware En Juego MadCap

Este malware se enfoca en la grabación de audio y sólo funciona en dispositivos con jailbreak. MadCap trabaja al igual que XAgent, pero difiere en que sólo se puede **instalar en dispositivos con jailbreak**.

Los investigadores de seguridad dijeron que las aplicaciones

de malware parecen estar cuidadosamente mantenidas y constantemente actualizadas por los piratas informáticos. Aún se desconocen los propietarios de este software, aunque el servidor usado y de control utilizado en los ataques estaba en funcionamiento en el momento de la investigación.