

Android, scoperto malware che ascolta le conversazioni. Le vittime tutte in Italia

È in grado di ascoltare le conversazioni sugli smartphone **Android** e di origliare tutto ciò che accade nell'ambiente circostante. In più ha nel mirino anche gli utenti **Windows**.

Il *malware* è stato scoperto dai ricercatori di **Kaspersky Lab** ed è stato chiamato **Skygofree** perché deve il proprio nome a una parola usata in uno dei domini: non ha legami con **Sky**, Sky Go o qualsiasi altra società controllata da Sky e non coinvolge il servizio o l'app Sky Go.

Skygofree è uno spyware sofisticato e multilivello che concede ai cyber criminali il pieno controllo remoto del dispositivo infettato.

Skygofree come fa a spiare?

Dopo la creazione della prima versione alla fine del 2014, ha subito costanti aggiornamenti e ora include la possibilità di "origliare" le conversazioni e i rumori dell'ambiente circostante quando il dispositivo entra in un luogo specifico – una funzionalità che non era mai stata trovata in *the wild*. Altre innovative funzionalità avanzate includono la possibilità di usare le impostazioni di accessibilità per rubare i messaggi **WhatsApp** e la capacità di collegare il dispositivo infettato alle reti wi-fi controllate dai cyber criminali.

Il malware include diversi *exploit* per ottenere i permessi di *root* ed è in grado di catturare immagini e registrare video, ottenere l'elenco delle chiamate, SMS, informazioni sulla geolocalizzazione, eventi nel calendario e dati aziendali archiviati nella memoria del dispositivo. Una funzionalità

speciale consente di aggirare una funzionalità per il risparmio della batteria implementata da uno dei maggiori vendor: il malware si inserisce nell'elenco delle "app protette" per non venire disattivato automaticamente quando lo schermo è spento.

Malware progettato da un'azienda italiana e le vittime colpite tutte nel nostro Paese

I cyber criminali sembrano interessati anche agli utenti **Windows** e i ricercatori hanno scoperto diversi moduli sviluppati recentemente che prendono di mira questa piattaforma.

La maggior parte delle *landing page* nocive usate per diffondere il malware sono state registrate nel 2015, quando, secondo la telemetria di *Kaspersky Lab*, la campagna di distribuzione è stata più attiva. La campagna nociva è ancora in atto e il dominio più recente è stato registrato a ottobre 2017. I dati indicano che attualmente sono state colpite diverse vittime, tutte in Italia.

"I malware mobile di alto profilo sono estremamente difficili da identificare e bloccare e gli sviluppatori di Skygofree hanno sfruttato questo fattore a proprio vantaggio, creando e sviluppando uno spyware in grado di spiare gli obiettivi senza destare sospetti. In base agli artefatti scoperti nel codice del malware e alla nostra analisi dell'infrastruttura, siamo piuttosto sicuri che il malware Skygofree sia stato sviluppato da un'azienda IT italiana che offre soluzioni di sorveglianza, come HackingTeam", ha commentato **Alexey Firsh**, Malware Analyst, Targeted Attacks Research, di Kaspersky Lab.

I ricercatori hanno scoperto 48 comandi differenti che possono essere implementati dai criminali, offrendo la massima flessibilità d'uso.

Come proteggersi

Per proteggersi dalle minacce mobile più avanzate, Kaspersky Lab consiglia fortemente di implementare una soluzione di sicurezza affidabile in grado di identificare e bloccare queste minacce sugli *endpoint*. Gli utenti dovrebbero inoltre fare attenzione alle email ricevute da persone o aziende sconosciute o con richieste o allegati inattesi – e verificare sempre l'integrità e l'origine dei siti web prima di cliccare sui link. In caso di dubbio, è sempre meglio chiamare il service provider per una verifica. Gli amministratori di sistema, a loro volta, dovrebbero attivare la funzionalità di *Application Control* della propria soluzione di sicurezza mobile per controllare i programmi potenzialmente dannosi vulnerabili a questi attacchi.

Le soluzioni Kaspersky Lab rilevano le versioni di Skygofree per Android come HEUR:Trojan.AndroidOS.Skygofree.a e HEUR:Trojan.AndroidOS.Skygofree.b e i sample per Windows come UDS:DangerousObject.Multi.Generic.

<https://www.key4biz.it/android-scoperto-malware-ascolta-le-conversazioni/210112/>