DOSSIER G DATA - QUANDO UN GIOCO SOTTOSCRIVE ABBONAMENTI A PAGAMENTO A TUA INSAPUTA

Una App del Google Play Store ti iscrive automaticamente a servizi a pagamento di provider olandesi.
I servizi di SMS "premium" erano noti circa sei anni fa come la prima vera minaccia per gli utenti di Android. Malware dotati di tali funzioni rappresentavano ai tempi il pericolo numero 1. Da allora il panorama del malware per dispositivi mobili ha subito notevoli trasformazioni, proprio per questo è curioso che un nuovo tipo di trappola spillasoldi con iscrizione nascosta a servizi „premium" possa mantenersi per numerose settimane nel Google Play Store, cagionando concreti danni economici agli utenti. Eccone un esempio in tutti i dettagli.

BREVE PANORAMICA DEL CASO

- Interessante modalità di diffusione: gli utenti vengono indotti da una App legittima ad installare una App fraudolenta chiamata *Blend Color Puzzle*.
- Nuove vie per l'iscrizione nascosta a servizi premium: la App malevola, presente dall'inizio di novembre 2015 sul Google Play Store* abbona l'utente alla prima apertura e senza alcuna esplicita autorizzazione a due servizi erogati da aziende olandesi. A ale scopo la App taglia la connessione mobile al wifi e utilizza connettività a pagamento via WAP-Billing.
- Prima si incappava in eventuali trappole spillasoldi cliccando su un banner presente in una app (cfr. banner fasulli in WhatsApp). In questo caso particolare tuttavia, la trappola scatta senza alcuna interazione da parte dell'utente.
- La fatturazione dell'abbonamento ha luogo tramite un intermediario, cosa che rende ancor più difficile risalire ai responsabili e richiedere un risarcimento danni. Riteniamo che dietro a questa particolare azione si celi una rete internazionale di aziende di dimensioni ancora maggiori.
- Valutazioni negative così come commenti privi di contesto o architettati ad hoc sottolineano il dubbio carattere della app. Nello store non sono reperibili altre app dello stesso sviluppatore o dell'azienda.

I DETTAGLI

Un utente vittima del raggiro si è rivolto a G DATA per ulteriori analisi di quello che pare essere una novità nel panorama delle minacce per utenti Android. Nello specifico l'utente si avvale di una app di incontri tramite smartphone. Alcune funzioni premium offerte dalla app possono essere acquistate regolarmente oppure è possibile portare a termine dei "compiti" per «guadagnarsi» l'accesso a tali servizi. Le proposte di attività non hanno un carattere immorale, in realtà basta selezionare una o più app da un elenco predisposto, scaricarle, installarle ed eventualmente fare un'azione in più, come avviare la app almeno una volta o similari. Anche invitare gli amici o partecipare a sondaggi viene "ricompensato".

Screenshot 1: Un esempio di compito da svolgere (acquisto di un cospicuo buono Amazon), la cui ricompensa è un elevato numero di ore di fruizione gratuita dei servizi premium della app.

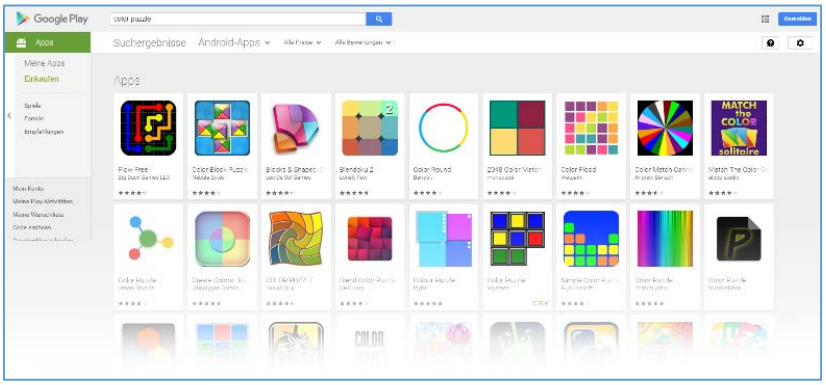
Non trattandosi di ostacoli troppo gravosi, gli utenti si avvalgono spesso di tali proposte senza pensarci due volte. Il produttore della dating app guadagna ovviamente soldi (provvigioni, introiti pubblicitari e similari) con questo metodo. Ogni azione condotta dagli utenti desiderosi di flirtare gli porta profitti. Solo in pochi si chiedono „cosa può mai succedere?“ scambiando „lavoro“ con tempo utile per la fruizione dei servizi premium. Qualche giorno fa però una delle app dell'utente si è dimostrata fraudolenta.

LA APP

Il gioco selezionabile tramite dating app si chiama *Blend Color Puzzle*. Consiste nel riconoscere e quindi selezionare sfumature di colori. Dato che dalla descrizione la app sembrava simpatica, l'utente ha deciso di scaricarla. La app di appuntamenti prometteva come ricompensa per il completamento di "installazione e avvio" un'ora di funzioni premium gratis, una ricompensa decisamente minore rispetto all'esempio di amazon, ma adeguata al livello di risorse "investite" dall'utente.

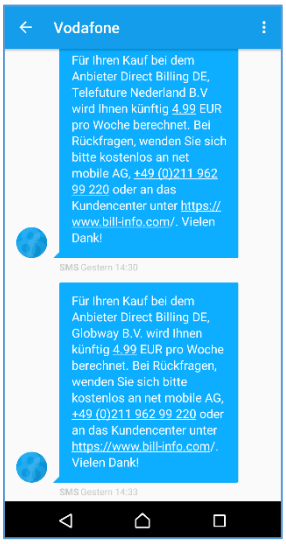
Screenshot 2: la panoramica relativa al completamento del "task" inclusa la ricompensa "guadagnata" una volta scaricata la app.

Blend Color Puzzle è stata presente dal 03 novembre 2015 al 25 gennaio nel Google Play Store ufficiale* e presentava verso la fine circa 100.000 downloads. Un numero stupefacente per il probabile primo lavoro dello sviluppatore (fartye.polisertg@gmail.com) o dell'azienda (GHR Corp) –nominati nella pagina informativa della app. Altre app di entrambi gli autori non sono reperibili. La somiglianza visiva con il noto gioco *Blendoku* potrebbe essere uno dei motivi per cui tanti utenti hanno voluto provare il gioco gratuito. Le immmagini stesse della app mostrate nello Store recavano



Screenshot 3: Se si cerca in modo attivo un gioco simile ad un puzzle di colori, la App dubbiosa si presenta tra le prime della lista.

nella parte sinistra della schermata di gioco il nome Blendoku. Ciò nonostante, l'utente non avrebbe mai scaricato la app se non le fosse stato proposta tramite la app di appuntamenti.



Screenshot 4: SMS, che notificano l'abbonamento

Dopo l'avvio del gioco l'utente ha ricevuto due SMS che notificavano la sottoscrizione dei due abbonamenti, azione mai condotta dall'utente. L'utente peraltro indica che in quel momento la connessione al wifi domestico, sempre utilizzato quando è in casa, era stata tagliata. La app trappola ha dato luogo ad un acquisto, passato del tutto inosservato presso l'utente. Ecco una nuova forma di attacco, che vale la pena analizzare in modo dettagliato.

AUTORIZZAZIONI RICHIESTE DALLA APP

L'elenco dei diritti di accesso richiesti dalla app é particolarmente cospicuo per un semplice gioco. Tra le autorizzazioni si rinviene anche la funzione di chiusura della connessione wifi. Tuttavia la app può solo ricevere SMS, non ne può inviare. Gli analisti dei G DATA Security Lab partono dal presupposto che la app sottoscriva gli abbonamenti in modalità WAP-Billing.

- Storico dispositivi e app
  - Verificare le app attive
- SMS
  - Ricevere SMS
- Foto/Media/Dati
  - Modificare o cancellare i contenuti di memorie USB
  - Leggere i contenuti di memorie USB
- Informazioni connessione WIFI
  - Verificare la connessione wifi
- Informazioni dispositivo e chiamate
  - Accesso allo stato del telefono e ai dati personali
- Altro
  - Disattivare lo stand-by
  - Accesso a tutte le reti
  - Visualizzare le connessioni di rete
  - Stabilire o interrompere connesssioni wifi
  - Modificare la connettività di rete
  - Lanciare all'avvio
  - Disattivare il blocco schermo
  - Mostrare su altre app

IL CODICE DELLA APP

Con l'intento di celare il codice effettivo della app, lo sviluppatore lo ha offuscato in più livelli. Secondo quanto oggi noto da una decriptazione parziale, la app salva i seguenti dati e variabili caricandoli su un server:

- Informazione sul provider della SIM
- Informazione sul provider di rete
- Stato del wifi
- Carica della batteria
- Impostazione linguistica del dispositivo
- Produttore del dispositivo
- Modello
- Risoluzione del display
- ID di Android
- IMSI
- IMEI
- Numero di telefono

Sebbene hostato in germania, il dominio che viene contattato è stato registrato dalle Bahamas il 2.11.2015, un giorno prima che il Color Blend Puzzle apparisse nel Google Play Store.

In tutto la app mostra un congruo numero di variabili e azioni dipendenti l'una dall'altra. Ad esempio, 60 secondi dopo che la app ha switchato dal wifi alla rete mobile, viene lanciata una cosiddettà Webview, quindi una pagina web, che però non viene mostrata all'utente. A conclusione delle analisi risulta che questa sia la connessione al server utilizzata per la trasmissione dei dati per la fatturazione dell'abbonamento in modalità WAP-Billing. Tale attività è stata identificata dalle soluzioni di sicurezza G DATA e resa innocua.

"Sono molti gli utenti che si rivolgono a centri per la tutela dei consumatori a posteriori di spiacevoli situazioni sperimentate in rete. Abbonamenti sottoscritti perché l'utente non ha letto cautamente termini e condizioni accettandole frettolosamente, sono all'ordine del giorno, ma questo trucco per spillare soldi senza interazione dell'utente è un nuovo fenomeno" spiega Ralf Benzmüller, Direttore dei G DATA Security Labs. „Quello che stiamo osservando é un espediente tecnico realizzato con forti investimenti, per colpire un'ampia massa di utenti. La app viene introdotta tramite applicazioni legittime, raccoglie dati personali, interviene sui canali di trasmissione mobile e viene pubblicizzata con commenti positivi postati ad hoc. A parte il nostro interesse deontologico, la sottoscrizione di un abbonamento senza esplicita approvazione dell'utente presenta numerose ombre anche dal punto di vista legale. Gli utenti colpiti dovrebbero assolutamente richiedere assistenza e procedere contro tale abuso."

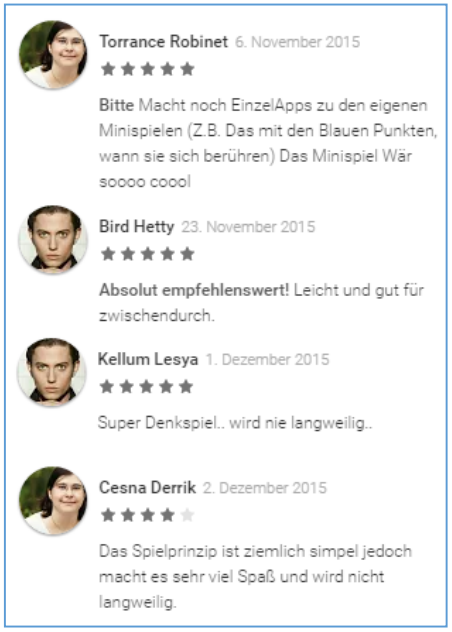
LE VALUTAZIONI

Un certo sospetto nasce dal fatto che su oltre 1000 valutazioni il 25% sia negativo e che, nella maggior parte dei casi, la app abbia ricevuto meno di 3 stelle. Il primo commento negativo é stato registrato il 6 novembre 2015, solo tre giorni dopo la pubblicazione della app nello Store. Dopo questo avviso, é tutto un susseguirsi di valutazioni negative.

Anche i commenti positivi dovrebbero essere analizzati dettagliatamente. Leggendo con maggior accuratezza si nota che molte valutazioni non hanno senso. Alcuni utenti ad esempio indicano tutt'altra azienda come sviluppatore della app, o fanno riferimento al numero di livelli del gioco. Peccato che il gioco non abbia livelli. Si gioca a tempo e si ricomincia sempre da zero. Anche la nota di una utente in merito ad un minigioco che parte nel momento in cui i punti blu si toccano è errata: non esistono punti blu, né pallette, né compiti particolarmente complessi da risolvere, invece vengono annoverati in altre valutazioni.

Screenshot 5: Il primo commento negativo sulla app, avvisa contro abbonamenti illeciti.

A parte il fatto che molti nomi delle persone che rilasciano commenti positivi suonano esotici o particolarmente artefatti, esistono tra loro persone che hanno la stessa identica foto. Secondo il rispettivo profilo di Google+ Torrance Robinet e Cesna Derrick sono entrambi uomini. Dalle foto non si direbbe. Le foto dei due esempi indicati qui di seguito sono chiaramente di altre persone: in particolare l'uomo è Jackson Rathbone, attore statunitense, e la donna è a quanto pare una professoressa di storia all'università di Rio de Janeiro. Le sue immagini vengono usate qui a scopo fraudolento e probabilmente senza che lei lo sappia. Infine non é inusuale che un utente utilizzi come immagine del proprio profilo quella del proprio idolo, ma in questo caso l'insieme dei particolari insensati non dà adito a dubbi in merito al fatto che l'organizzazione abbia architattato il tutto ad arte.



Screenshot 6: Selezione di „gemelli" tra i commenti, in ordine cronologico

Alcune delle valutazioni che non collimano con il gioco fanno riferimento anche ad altre app in cui la trappola spillasoldi era integrata. Otre alla dating app segnalataci dall'utente, vengono menzionati almeno due altri programmi, tramite i quali gli utenti sono stati indirizzati verso il gioco. Una volta risaliti a ciò, non ci si chiede più perché la app ha ottenuto un numero di download tanto elevato in così poco tempo.

LE AZIENDE DIETRO AGLI ABBONAMENTI

Le SMS ricevute mostrano, nel nostro caso specifico, il coinvolgimento di tre aziende: la tedesca net mobile AG, la Telefuture Nederland B.V e anche Globway B.V., entrambe olandesi.

I due prodotti letteralmente "rifilati" all'utente sono rispettivamente„ABO MOBIMANIACS DOWNLOADS" e „ABO DE.APPTIPS.ME". Il prezzo cadauno è di € 4,99 la settimana. La rete dietro a questi due prodotti e i siti

specifici come eventuali terze parti coinvolte (ad esempio il produttore della app) non sono oggetto di ulteriore analisi in questa sede.

La net mobile AG si occupa delle transazioni tra gli operatori mobili e entrambe le aziende olandesi in Germania, è quindi solo un intermediario (in Italia, l'intermediario di Globway è la MobilePay). Tramite l'intermediario di Düsseldorf l'utente è riuscito comunque a disdire gli abbonamenti con decorrenza immediata. La richiesta di rimborso però andava indirizzata alle aziende olandesi, questa l'informazione fornita dal servizio clienti della net mobile AG.

Globway B.V. fa parte del Gruppo Telefuture, non ci meraviglia quindi che le sedi legali di entrambe le aziende si trovino a pochi metri di distanza, pochi chilometri a nord di Rotterdam. Note in molti forum e presso i centri di raccolta di reclami dell'utenza, come anche sui media, le due aziende spiccano per il numero di rimostranze relative ad abbonamenti a servizi premium stipulati senza autorizzazione.

Sul proprio sito l'azienda Globway B.V. presenta anche informazioni dettagliate sul potenziale ricavato di tali attività per i propri clienti, annoverando tutti gli importi che si possono guadagnare nei singoli Paesi e con i più diversi metodi di pagamento. Un esempio del servizio di «Mobile Billing» per l'Italia: se un utente acquista un servizio da € 4,99 tramite rete Vodafone, al netto di IVA e commissioni il cliente della Globway guadagna € 2,25. Nella rete Wind invece addirittura € 2,37. Sulle reti mobili tedesche l'importo è ancora superiore. Ovviamente il committente dovrà affrontare anche altre spese, ma questi numeri sono già indicativi dell'enorme profitto ricavabile da un tale business.

CONCLUSIONI

Se da un lato le trappole spillasoldi tramite abbonamento sono una nota minaccia per gli utenti delle reti mobili, dall'altro in questo caso la trappola è stata architettata in modo particolarmente perfido.
La novità di questo caso consiste nel fatto che gli abbonamenti sono stati sottoscritti senza approvazione esplicita o azione specifica dell'utente, bensì esclusivamente tramite espedienti tecnici.

L'esempio conferma nuovamente un dato di fatto: il "gratuito" non é sempre la scelta più economica: l'utente avrebbe potuto avvalersi dei servizi premium della flirt app con acquisto in-app. Al prezzo di € 9,99€ avrebbe disposto di 250 monete virtuali, che - secondo le informazioni su internet - corrispondono ad un mese di fruizione dei servizi premium, un controvalore ben più elevato della singola ora guadagnata scaricando la app, senza considerarne il costo (€ 4,99 / settimana x 2) e il tempo che l'utente ha investito e dovrà investire nel recesso e per la richiesta di risarcimento.

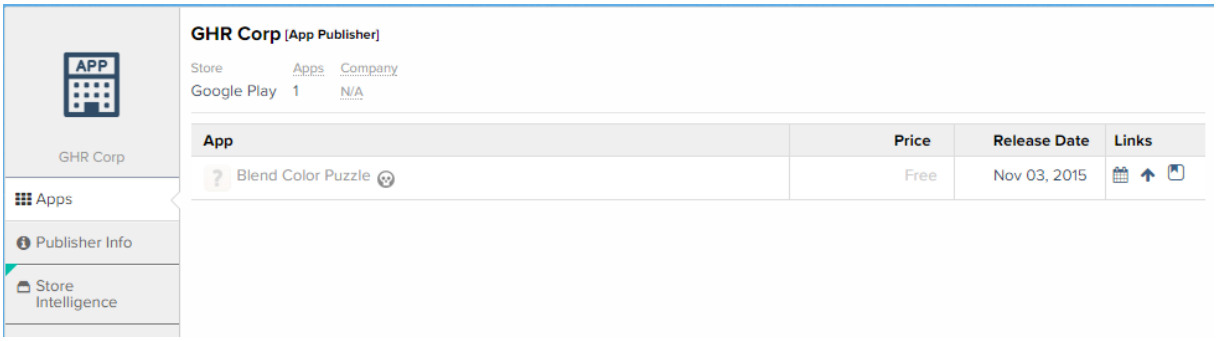
* LA APP E' SCOMPARSA

La app truffa è stata rimossa dal Play Store tre giorni dopo aver inviato a Google un avviso dettagliato, corredato di tutte le prove del caso. Non ci è dato sapere se effettivamente il nostro contributo ha determinato la rimozione della app dallo Store, ma alla luce del fatto che la App fosse online da quasi tre

mesi e che la sua rimozione ha avuto luogo poco dopo il nostro intervento, ci piace pensare di aver avuto un ruolo attivo nel processo di tutela degli utenti.

Ad oggi comunque, dato che Internet non dimentica mai, cercando GHR corp, troviamo risultati dovuti all'indicizzazione della app:

Mentre sullo Store la app è semplicemente scomparsa, su taluni siti è presente l'indicazione sulla sua rimozione.



(Screenshot 7: il teschio indica che la app è stata rimossa)

COSA FARE PER PROTEGGERTI

- Contatta il tuo operatore mobile e fai bloccare i servizi a pagamento di altri operatori sulla tua linea. In questo modo si escludono pagamenti inconsapevoli a terzi. Ciò implica però anche che non sarà possibie avvalersi di servizi sensati, come la prenotazione di biglietti o funzioni simili.
- Installa sullo smartphone una soluzione di sicurezza completa. Il pacchetto G DATA INTERNET SECURITY per Android offre una protezione efficace per il tuo device "smart".
- Controlla le valutazioni e i commenti fatti alle app, specialmente quelli negativi.

E SE TI CAPITA LO STESSO:

- Contatta il tuo operatore mobile e contesta gli addebiti impropri: rivolgiti sia al call center del tuo gestore telefonico sia alle associazioni dei consumatori per ottenere ragguagli sul miglior sistema per richiedere il risarcimento.
- Fatti dare dal tuo operatore mobile tutte le informazioni su intermediari e aziende coinvolte nell'addebito improprio.
- Contatta un avvocato e chiedi informazioni su se nel tuo caso sia sensato procedere anche legalmente.
- Anche la AGCom e la Corecom possono essere un buon punto di riferimento per eventuali controversie sulle fatture, oltre ad aiutarti a mettere in sicurezza le prove della frode subita.