I pirati attaccano i programmi fedeltà

Ott 16, 2019 Giancarlo Calzetta Kaspersky Partner Space 0

Le aziende si impegnano in modo costante per avere sempre più successo rispetto ai competitor e spesso possono trovarsi in difficoltà quando si tratta di acquisire nuovi clienti e di salvaguardare quelli abituali.

I programmi di fidelizzazione, o loyalty program, spesso vengono considerati come una possibile soluzione a queste difficoltà, tanto da essere una delle modalità più popolari per migliorare l’engagement e la fidelizzazione da parte dei clienti. In sostanza, questi programmi offrono un bonus di benvenuto o una ricompensa per acquisti regolari presso lo stesso rivenditore.

Questo tipo di campagne vengono accolte in modo positivo dai consumatori e, secondo un sondaggio condotto da Kaspersky[1], il 53% delle persone interpellate ha dichiarato di aver acquistato qualcosa proprio attraverso dei punti ricevuti come bonus nei programmi fedeltà.

I programmi di fidelizzazione sono nati alla fine del XIX secolo: all’epoca gettoni di rame o speciali francobolli potevano essere scambiati con punti bonus. Negli anni ’90, poi, le carte fedeltà sono diventate qualcosa di familiare per i consumatori: speciali carte dotate di codici a barre o bande magnetiche utili per caricare rapidamente i punti e per averli a disposizione attraverso un unico mezzo fisico.

Oggi questo tipo di carta viene considerata superflua visto che le persone sembrano preferire lo shopping online. La percentuale di consumatori che sceglie di acquistare via Internet, infatti, sembra aver raggiunto il 70%.

Oggi molti commercianti stanno passando ai programmi di fidelizzazione digitali. Questi programmi sono in grado di dare vita ad una customer experience praticamente ininterrotta, permettendo ai consumatori di accedere al proprio account da qualsiasi dispositivo, di controllare quanti punti fedeltà hanno accumulato, e persino trasferirli agli amici, o di utilizzarli per il loro prossimo acquisto online. C'è però un piccolo difetto in questi sistemi. I loyalty program digitali possono anche permettere ai malintenzionati di condurre attività illecite. Nella pratica i possibili scenari di sfruttamento di un loyalty program da parte dei cybecriminali sono sostanzialmente due.

Sottrazione di punti bonus

Ci sono diversi modi attraverso i quali dei malintenzionati possono accedere agli account di chi ha sottoscritto un programma fedeltà. Come prima cosa, possono tentare di ottenere la password legata ad uno specifico indirizzo email, attraverso un attacco "forza bruta".

Questa operazione può rivelarsi addirittura semplice, nel caso in cui l'attaccante cerchi di utilizzare credenziali precedentemente messe in pericolo attraverso una violazione o una fuga di dati.

Questa possibilità moltiplica le chance di successo di un attacco: le persone, infatti, tendono a utilizzare sempre le stesse password anche per account diversi.

Esistono poi dei programmi malevoli che raccolgono segretamente password e nomi utente (denominati "password stealer") che possono aiutare un malintenzionato a ottenere credenziali valide.

Una volta che il truffatore ha avuto accesso ad un account personale, può sfruttare diverse opportunità per far sì che le sue azioni diventino redditizie.

Prima di tutto, nel caso in cui il programma fedeltà permetta di trasferire dei punti bonus da un account ad un altro, il truffatore può decidere di spostare tutti i punti raccolti, dall'account violato al suo.

Altrimenti, può decidere di fornire il suo indirizzo di consegna facendo un acquisto per sé direttamente dall'account compromesso. Se il malintenzionato non desidera ricevere nessuno dei prodotti messi a disposizione dal rivenditore, allora può decidere di vendere i dati dell'account violato nel Dark Web. Un esempio è quello del business fiorente legato alla vendita di miglia aeree dei frequent flyer.

Questo tipo di cyber crimine sembra essere molto diffuso: secondo l'indagine che abbiamo condotto, circa il 70% dei consumatori coinvolti ha ammesso di aver scoperto personalmente che i propri punti fedeltà sono spariti o di conoscere persone che hanno già affrontato questo problema[2].

Non bisogna poi dimenticare che gli attaccanti possono riuscire ad avere accesso non solo ai punti fedeltà, ma anche a varie informazioni di carattere personale, come indirizzi, contatti telefonici o preferenze di acquisto.

Welcome gift per i truffatori

Gli account di utenti già esistenti non rappresentano l'unico obiettivo dei criminali informatici. Per i truffatori è ancora più facile compromettere o sfruttare gli eventuali punti assegnati come benvenuto ai nuovi clienti, tramite la creazione di diversi account fake e l'accumulo di punti. Il team di Kaspersky che si occupa di analizzare le frodi digitali ha scoperto un caso particolare: i cybecriminali

avevano creato quasi 3.000 account registrati con un solo indirizzo email. La procedura è stata possibile perché Gmail e la piattaforma di e-commerce coinvolta avevano un diverso metodo di approccio per l'identificazione degli indirizzi email. Gmail non è in grado di distinguere eventuali "punti" all'interno degli indirizzi email, quindi rileva come identici, ad esempio, l'indirizzo johnsmith@gmail.com e l'indirizzo j.o.h.n.s.m.i.t.h@gmail.com: in questo modo il proprietario dell'indirizzo email potrà ricevere i messaggi anche se il mittente ha digitato un punto per errore.

Di solito, i cybercriminali utilizzano un insieme limitato di dispositivi per creare e controllare una serie di account fasulli. La figura 2 qui sotto mostra come questo tipo di schema malevolo differisca da quello relativo ad un uso legittimo (quello visibile nella figura 1), che mostra l'accesso di un utente al proprio account anche attraverso dispositivi diversi. Il team di Kaspersky che si occupa di analizzare le frodi digitali, ad esempio, ha rilevato l'esistenza di più di 9.000 account fake controllati attraverso dispositivi diversi da un gruppo ristretto di persone che stavano cercando di ottenere punti bonus da una delle principali piattaforme di e-commerce. È necessario sapere anche che i cybercriminali a volte non si preoccupano nemmeno di utilizzare diversi dispositivi per questo tipo di operazioni: sulla stessa piattaforma, infatti, abbiamo anche trovato circa 230 account registrati a partire da un solo dispositivo.

Figura 1 – Gli schemi mostrano come gli utenti e i dispositivi siano interconnessi tra di loro in modo legittimo

Figura 2. Lo schema mostra un sistema fraudolento con numerosi account falsi creati a partire da un unico dispositivo.

Per concludere, cosa fanno i cybercriminali con i welcome bonus generati in modo illegale? Potrebbero trovare un utente legittimo, offrirgli un prodotto con uno sconto maggiore rispetto a quello che applicherebbe un normale commerciante agli utenti appena registrati e tenere il denaro come guadagno. Più persone sono in grado di attrarre, maggiore sarà lo sconto che avranno come clienti abituali. Grazie a metodi come questo, non c'è alcun bisogno di navigare nel Dark Web, questa attività può essere facilmente riscontrata su popolari piattaforme di e-commerce di tipo peer-to-peer o sui social media.

Se un’azienda non presta attenzione alla possibile creazione di account fake, inoltre, può essere indotta a pensare che il suo programma di fidelizzazione stia stimolando le vendite in modo efficace, quando, in realtà, sta solo aiutando dei truffatori digitali ad ottenere un guadagno.

Dal punto di vista delle aziende

Un loyalty program può rivelarsi uno strumento di marketing molto efficace, ma le frodi digitali possono trasformarlo da vantaggio a ostacolo. Nel caso in cui il programma di fidelizzazione di una realtà professionale venisse sfruttato in modo malevolo, l’azienda non solo perderebbe potenziali clienti e profitti, ma potrebbe trovarsi ad affrontare anche le reazioni negative degli utenti che sta cercando di attirare, se un giorno i loro punti fedeltà iniziassero improvvisamente a scomparire.

Normalmente, i clienti non si preoccupano della sicurezza dei loro punti fedeltà. Il sondaggio di Kaspersky ha rivelato, ad esempio, che solo il 26% dei consumatori è in grado di ricordare esattamente quanti sono. Il motivo principale è che i consumatori non li considerano come una vera e propria moneta di scambio – a meno che questi punti non scompaiano del tutto dai loro account, provocando delusione nei confronti del venditore. Bisogna però considerare il fatto che, per le aziende che investono economicamente nei programmi di fidelizzazione e che si aspettano un ritorno da questo investimento, questi bonus hanno un concreto valore economico.

Per proteggere i loyalty program dalle frodi digitali, Kaspersky consiglia ai commercianti di implementare delle soluzioni di sicurezza per la prevenzione che siano in grado di:

- Identificare i dispositivi unici e capire se ogni dispositivo in uso è effettivamente unico per il programma fedeltà stesso.

- Scoprire l’eventuale creazione account fake, applicando principi biometrici e firme digitali per la rilevazione dei bot.
- Scoprire possibili anomalie nell’apertura delle finestre del browser grazie all’implementazione di modelli di Machine Learning.
- Garantire un equilibrio tra funzionalità e sicurezza della soluzione e utilizzare diversi livelli di autenticazione solo per i casi sospetti, ad esempio, grazie alla **risk-based authentication** per i vari account di un loyalty program. Questo aiuterà a prevenire eventuali compromissioni degli account.

Condividi l’articolo

Il worm Graboid fa strage di Docker vulnerabili Uno strano bug di Linux consente l’invio di comandi root

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/10/16/i-pirati-attaccano-i-programmi-fedelta/