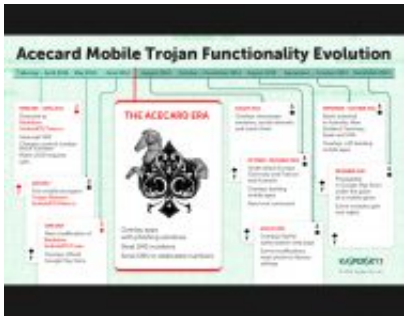
Acecard: il Malware per Android che sfrutta l’ingenuità degli utenti

Date : 16 novembre 2016



Tra i maleware più pericolosi ed efficienti ci sono sicuramente quelli che mascherano le proprie sembianze tramite interfacce meticolosamente studiate per imitare un sito lecito.

A questa famiglia si è recentemente aggiunto Acecard, un maleware studiato per Android che punta all'esportazione di coordinate bancarie, dati di accesso e credenziali di convalida.

Sfruttando le proprie sembianze innocue Acecard porta le vittime a completare i passaggi richiesti riuscendo ad acquisire informazioni sufficienti per prelevare velocemente e senza possibilità di recupero il denaro contenuto nei conti bancari dell’utente ingenuo.

Una tattica di una semplicità disarmante eppure ancora ad oggi una delle più proficue, per questo è bene rimanere informati e attenti in ogni momento.

Secondo le analisi Acecard sarebbe l’evoluzione del malware made in Russia Torec, una vecchia conoscenza nell’ambiente informatico.

In realtà sembrerebbe che l’albero genealogico di Acecard abbia radici molto più profonde: è stato identificato per la prima volta nel febbraio del 2014 ed è rimasto inerte fino al terzo trimestre del 2015, quando è stata riscontrata un’impennata nelle infezioni che ha coinvolto più di seimila utenti - principalmente in Europa.

Fino ad ora sono state rilevate più di 10 varianti di questo malware, ognuna con una lista di funzioni malevole sempre più ampia rispetto alla precedente.

Acecard è in grado di intercettare i messaggi, sia di testo che vocali, e di sovrapporsi alle finestre delle app ufficiali delle banche.

Non solo, la lista delle app che Acecard è in grado di simulare è tanto ricca da risultare preoccupante, il malware è infatti in grado di sostituirsi, tramite finestre di phishing, alle seguenti applicazioni:

- App Social, tra cui Facebook e Twitter ;
- App di messaggistica: WhatsApp, Viber, Instagram, Skype ;
- Gmail ;
- PayPal ;
- Google Play e Google music.

La strategia di infiltrazione non è differente da quella utilizzata da moltissimi malware: Acecard arriva negli smartphone sotto forma di plug-in per file multimediali - come ad esempio filmati a luci rosse - o nascosto in app scaricabili.

Una volta infiltratosi nel dispositivo target Acecard tenta innanzitutto di farsi assegnare volontariamente i permessi di amministratore del dispositivo; se la vittima cede in questa fase dell'attacco fornendo al trojan le informazioni che - sembrando innocuo - richiede, la sua disinstallazione sarà resa praticamente impossibile.

Questo è solo il primo passaggio, in un secondo momento il trojan inizierà a far comparire pop-up malevoli all'apertura di app legate alle compere online, il tutto in maniera molto insistente e sospetta - richiederà dati personali che mal si conciliano persino con le legittime richieste di un'app legata al mobile banking.

Pensate sia tutto qui? Ebbene no, come tocco finale infatti Acecard chiederà all'utente di scattare una fotografia della propria carta di credito e del proprio documento d'identità per "motivi di verifica".

Insomma, Acecard le prova tutte, noi possiamo però essere molto più furbi di lui.

Per evitare di cadere vittime di questo tipo di malware basterà prestare particolare cautela quando si scaricano app di dubbia utilità o reputazione dal Play Store di Google e soprattutto evitare assolutamente di scaricare app dagli *store* non ufficiali.