Frodi e Mobile Banking:
siamo pronti alla prossima sfida?

ABI Lab
Banche e sicurezza - 05 giugno 2015

Teo Santaguida
Resp. Centro Competenza Antifrode IKS

Malware e frodi su Mobile: un falso problema?

- **Su un campione di 150mil di dispositivi monitorati solo lo *0,0064%* di device si è connesso a domini malevoli (C&C).**
- **"There is a bigger chance of being struck by lightning (*0.01%* chance in a lifetime) than having a mobile device infected with malware"**

DAMBALLA

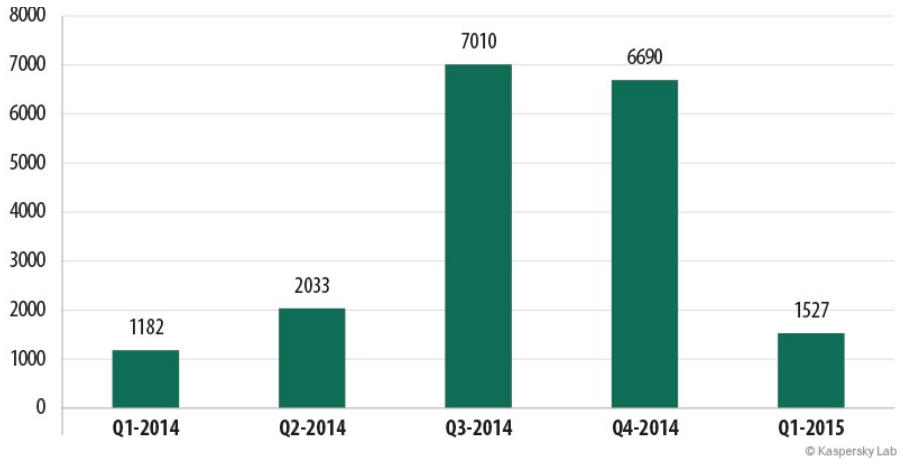
Fonte: Damballa @ RSA Conference 2015 – Characterizing Malicious Traffic on Cellular Networks: A Retrospective

- **Su un campione di 10mil/sett di dispositivi connessi, solo lo *0,003%* di device ha rilevato segni di compromissione da parte di malware realmente pericolo.**
- **"Mobile devices are not a preferred vector in data breaches"**

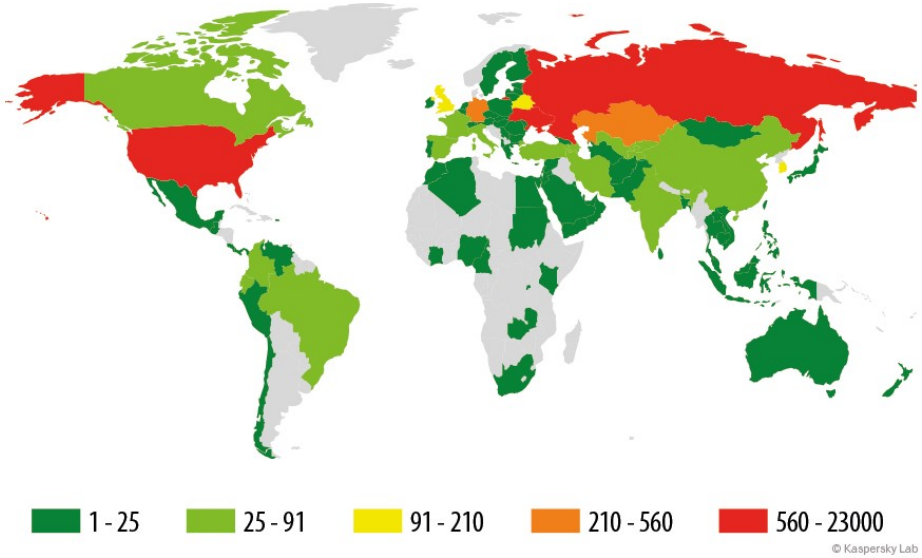
verizon

Fonte: Verizon – 2015 Data Breach Investigation Report

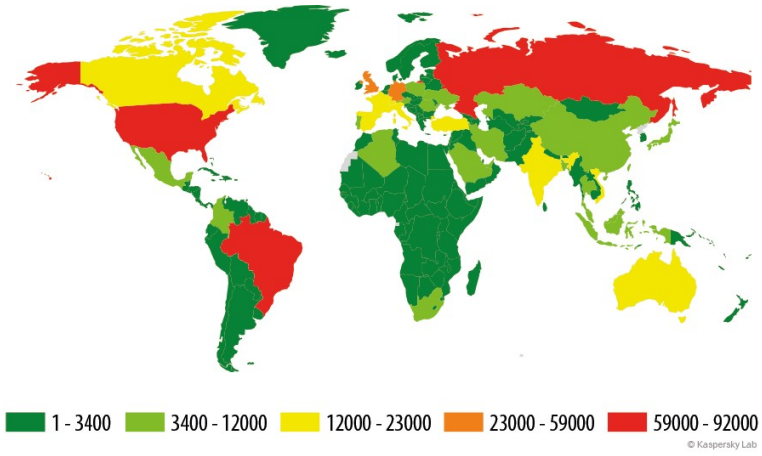
Malware e frodi su Mobile: un falso problema?



Number of mobile banker Trojans detected



Geography of mobile banking threats in Q1 2015
(number of users attacked)



Geography of banking malware attack

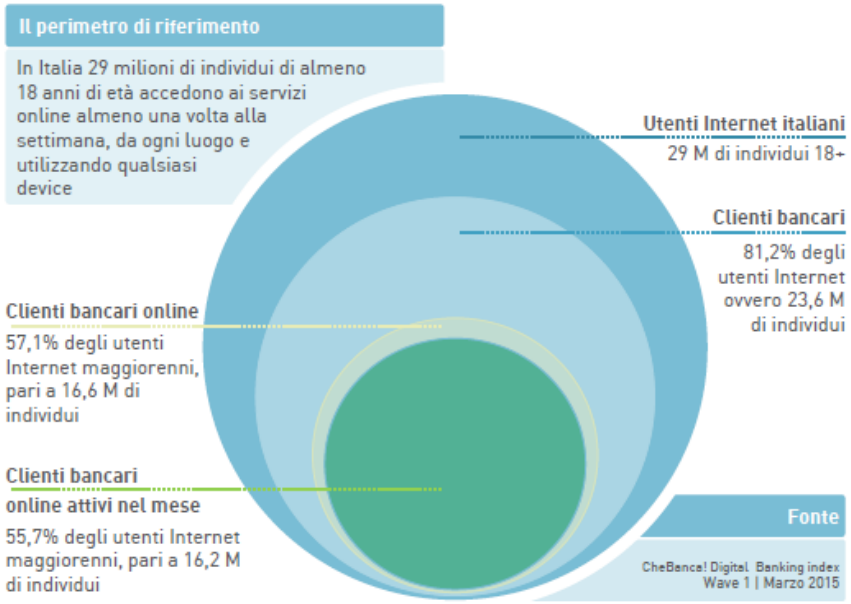
Infezioni da malware finanziario per dispositivi tradizionali (PC, laptop) cresciuto del 65% rispetto a 4Q-2014

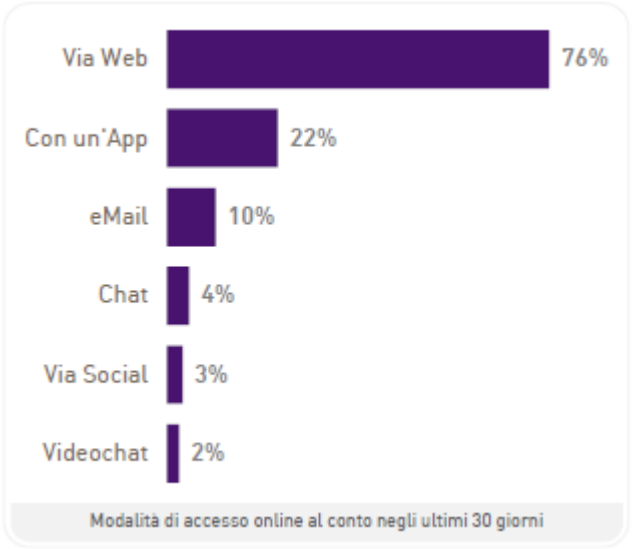
Fonte: Kaspersky – IT threat evolution in Q1 2015

Malware e frodi su Mobile: ma perchè preoccuparsi allora?

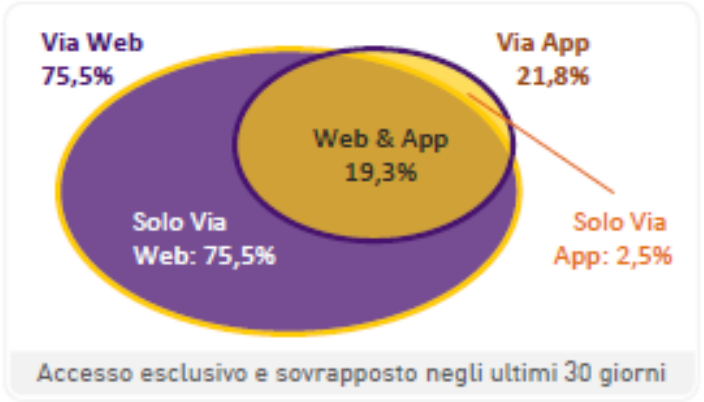
- *Diffusione di utilizzo del canale mobile*
- *Bassa percezione dei rischi di sicurezza*
- *Nuove armi in fase di industrializzazione*
- *Livelli di difesa app mobile banking non ottimali*

Diffusione di utilizzo del canale mobile banking



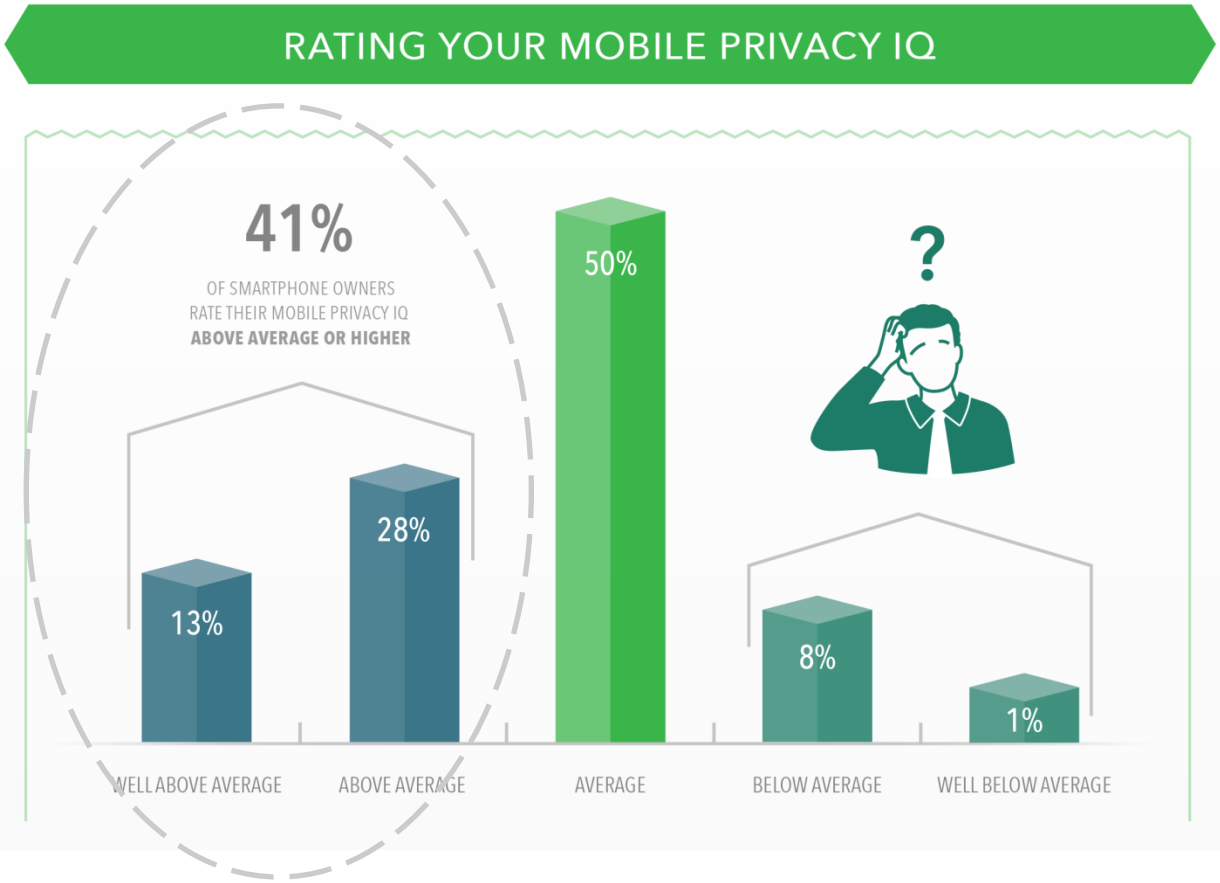


- **Se l'internet banking in *15 anni* circa si è diffuso al 76% nelle abitudini dei correntisti…**
- **… oggi Il 22% degli utenti accedono tramite app (circa 3Mil di utenti)…**
- **… in meno di *4 anni***



Fonte: CheBanca! – Digital Banking Index – Wave 1 (Marzo 2015)

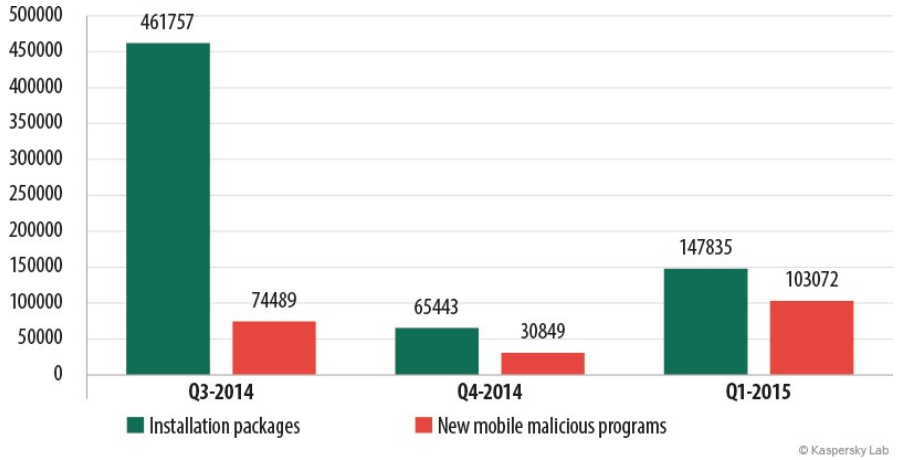
Bassa percezione dei rischi di sicurezza

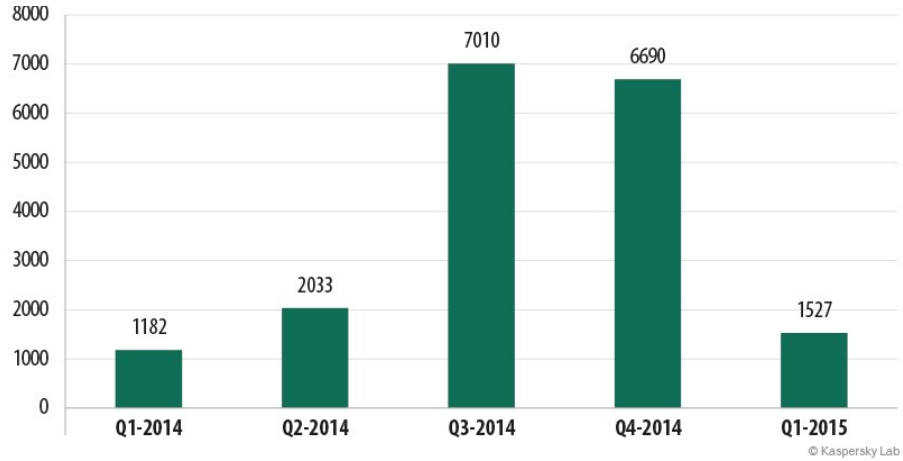


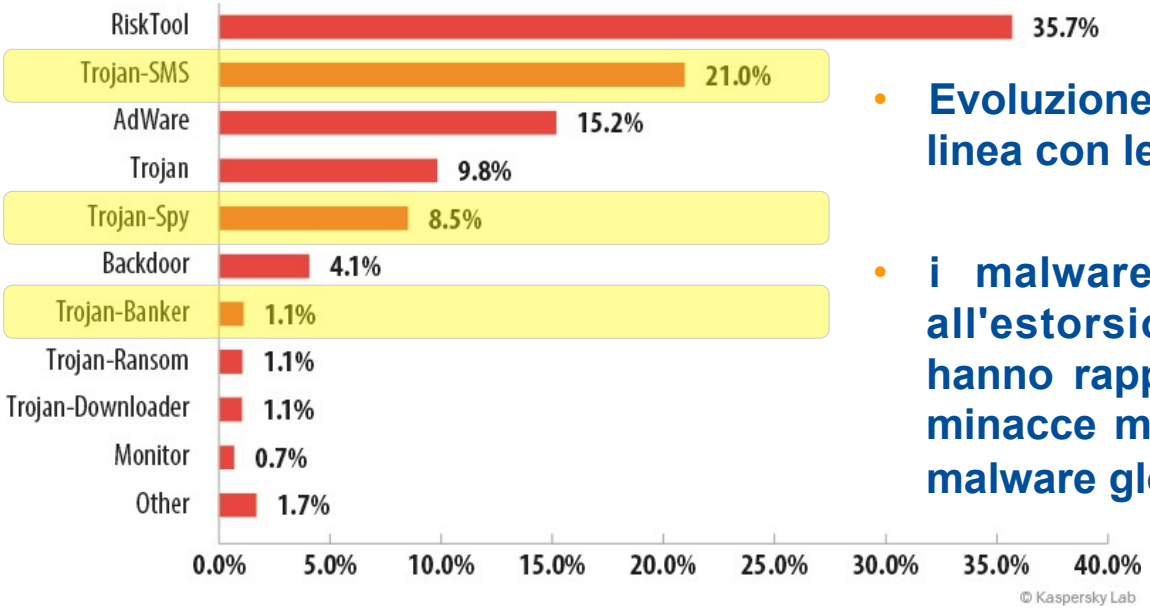
- Il ***35%*** scarica app da Marketplace non ufficiali
- Il ***52%*** non legge le policy di permission richieste in fase di installazione delle app
- Il ***35%*** usa reti wi-fi pubbliche e/o aperte senza preoccuparsene
- Il **34%** non imposta un PIN di sicurezza
- Il **61%** naviga su siti sconosciuti

Fonte: Lockout - Mobile Privacy IQ 2015

Nuove armi in fase di industrializzazione







- **Evoluzione dei malware sempre più in linea con le esigenze di monetizzare.**
- **i malware mobile preposti al furto e all'estorsione del denaro degli utenti hanno rappresentato il 23,2% delle nuove minacce mobile comparse sulla scena del malware globale.**

Fonte: Kaspersky – IT threat evolution in Q1 2015

Nuove armi in fase di industrializzazione
Esempio 1: svpEng

- **svpEng è un malware finanziario scoperto in Russia a metà del 2013.**
- **Le prime versioni si attivavano in fase di accesso da parte degli utenti a 3 grandi banche russe e tramite injection dirottavano gli utenti verso sito di phishing, al fine di sottrarre credenziali**

2013

Scoperta del malware
Target:
solo banche russe

2014

Nuove varianti estendono funzionalità (ransonware) e ambito geografico di azione.

Nuovi Target:

- USAA Mobile
- Citi Mobile
- Amex Mobile
- Wells Fargo Mobile
- Bank of America Mobile Banking
- TD App
- Chase Mobile
- BB&T Mobile Banking
- Regions Mobile

2015

- ***91% degli attacchi diretti in USA e UK (target app in lingua inglese)***
- ***7 % verso altre «lingue» (Germania, Svizzera e India)***

Nuove armi in fase di industrializzazione
Esempio 2: opFake

- **Un numero sempre crescente di Trojan-SMS risulta ora provvisto della specifica funzionalità nociva che consente di poter attaccare gli account bancari degli utenti-vittima.**

- **Il malware OpFake.cc si è evoluto ed è ora in grado di condurre attacchi nei confronti di almeno 29 applicazioni collegate alla sfera bancaria e finanziaria.**

	Name	% of attacks *
1	DangerousObject.Multi.Generic	10.90%
2	AdWare.AndroidOS.Viser.a	9.20%
3	Trojan-SMS.AndroidOS.Podec.a	7.92%
4	RiskTool.AndroidOS.MimobSMS.a	7.82%
5	Trojan-SMS.AndroidOS.OpFake.a	6.44%
6	Trojan.AndroidOS.Mobtes.b	6.09%
7	Adware.AndroidOS.MobiDash.a	5.96%
8	Exploit.AndroidOS.Lotoor.be	4.84%
9	RiskTool.AndroidOS.SMSreg.gc	4.42%

Percentage of users attacked by the malware in question, relative to all users attacked

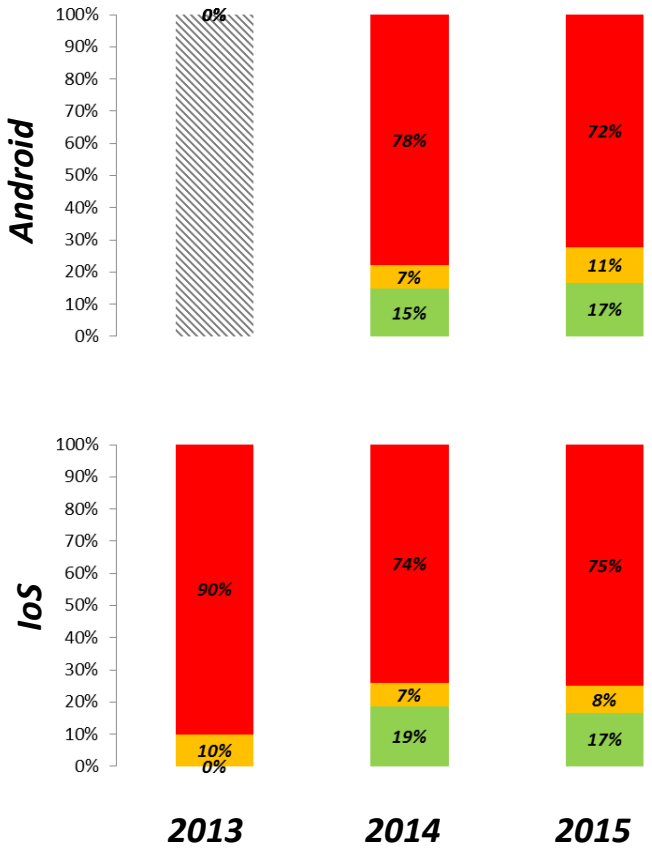
Fonte: Kaspersky – IT threat evolution in Q1 2015

Livelli di difesa Mobile app Banking: IKS Mobile Security Report

- **Realizzato dal Competence Center Mobile di IKS, il report si pone l'obiettivo di fotografare lo stato dell'arte rispetto alla sicurezza delle app mobile in ambito finance.**
- **Considera un campione significativo di app mobile banking rilasciate da realtà bancarie italiane e (in quantità minore) internazionali**
- **A settembre verrà rilasciata la terza edizione del report, della quale si forniscono a seguire elementi di preview**

Livelli di difesa Mobile app Banking: IKS Mobile Security Report

Ambito di analisi	Descrizione
Sicurezza run-time	Resistenza ad attacco dall'interno del sistema operativo
Network Communication Security	Robustezza delle comunicazioni verso il back-end.
Intellegibilità della logica implementativa	Elementi architetturali che possano generare vulnerabilità specifiche
Persistenza File-System	Presenza di cache e file sensibili su disco dopo l'esecuzione dell'app



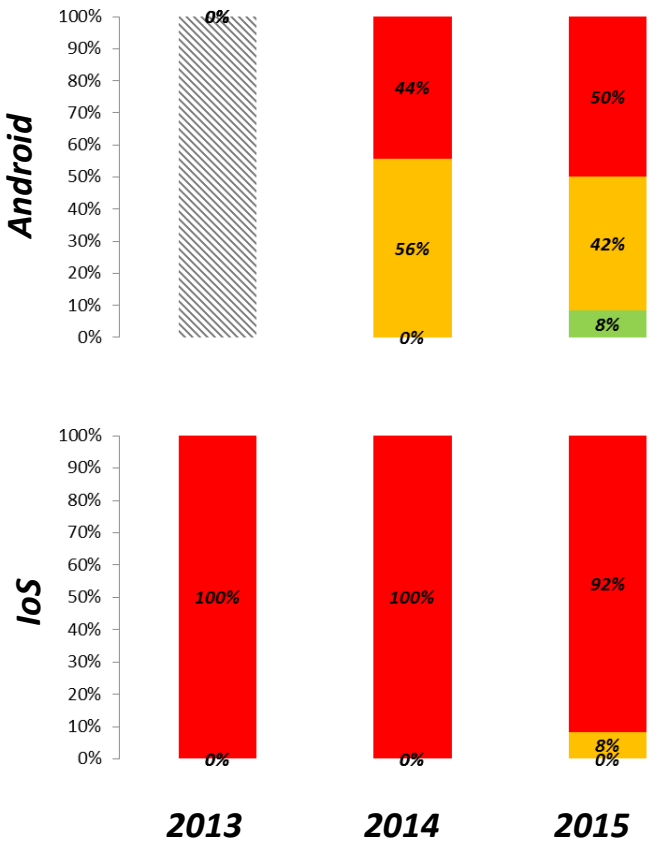
Il livello di attenzione alla sicurezza runtime è mediamente basso. Rispetto al 2013 si evidenzia un miglioramento, tuttavia le verifiche fatte per determinare la presenza di jailbreak o rooting e le contromisure adottate sono spesso rudimentali e facilmente aggirabili.

Rischi

E' possibile modificare il funzionamento di un'applicazione mobile mentre è in esecuzione attraverso diverse tecniche:

- ***Jailbreak e/o rooting***: processo di rimozione delle limitazioni di sicurezza imposte dai s.o., che apre le porte all'utilizzo di una serie di strumenti di abuso runtime
  Javascript injection: modifica di script utilizzati dalle app mobile (specie in framework di sviluppo multi-piattaforma). Non richiede compromissione (Jailbreak o rooting).

Livelli di difesa Mobile app Banking : IKS Mobile Security Report Intelligibilità del codice



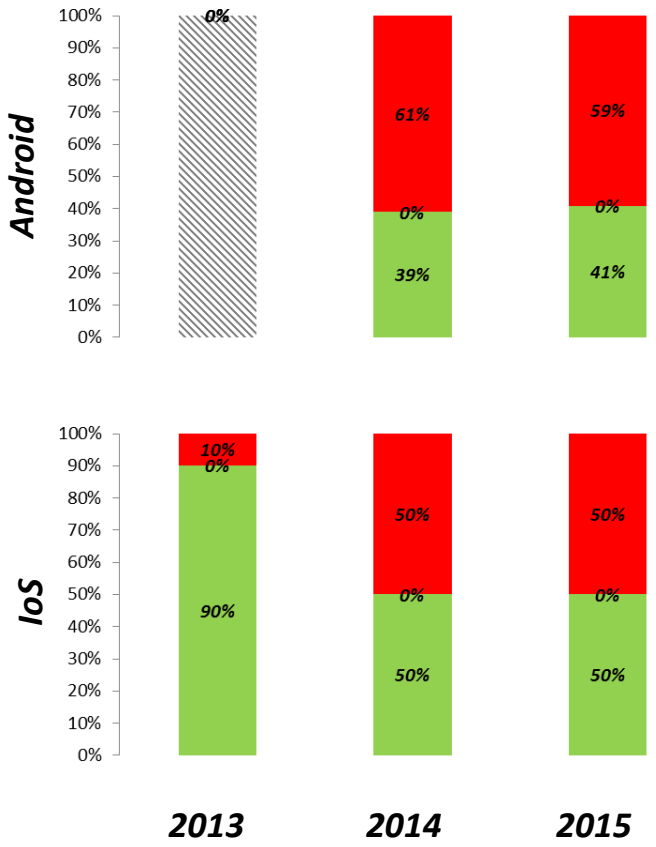
Lo scenario è molto diverso tra iOS e Android: se in iOS quasi il 100% delle applicazioni analizzate non ha evidenziato contromisure per complicare il reverse engineering, in Android sembra esserci più consapevolezza dei rischi (complice anche la disponibilità di tool di offuscamento)

Rischi

All'interno dell'eseguibile di una app, è spesso possibile trovare informazioni molto utili ad un attaccante, quali per esempio:

- Password o salt hardcoded.
- Stringhe costanti utili a individuare le implementazioni critiche del codice
- Informazioni sui servizi di backend
- Informazioni sui controlli anti-compromissione

Livelli di difesa Mobile app Banking: IKS Mobile Security Report Sicurezza Connessione con Back-end



A dimostrazione della maggiore attenzione e consapevolezza delle problematiche di sicurezza legate alle comunicazioni di rete, nelle APP oggetto del test si rileva il corretto utilizzo dallo SDK di Apple e Google per l'utilizzo e la validazione delle connessioni HTTPS.

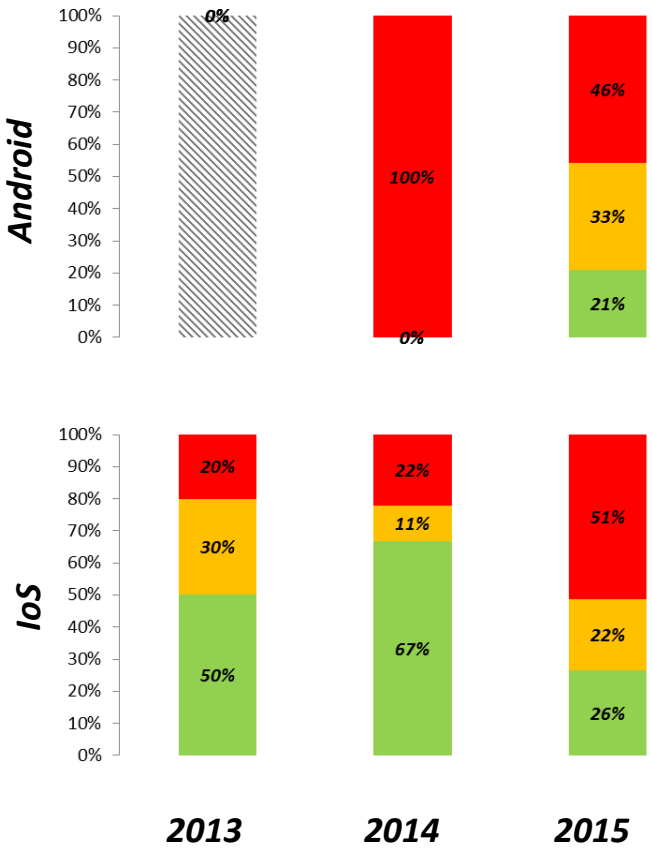
Molto raramente viene verificato che il certificato sia effettivamente quello emesso dal distibutore dell'app.

Rischi

Come tutte le misure di sicurezza, HTTPS deve essere utilizzato in maniera corretta. Frequenti utilizzi erronei riscontrati che possono ricondurre ad attacchi di MITM

- Controllo dei certificati utilizzati non effettuato
- Controllo dell'issuer del certificato non effettuato

Livelli di difesa Mobile app Banking : IKS Mobile Security Report
Gestione della cache



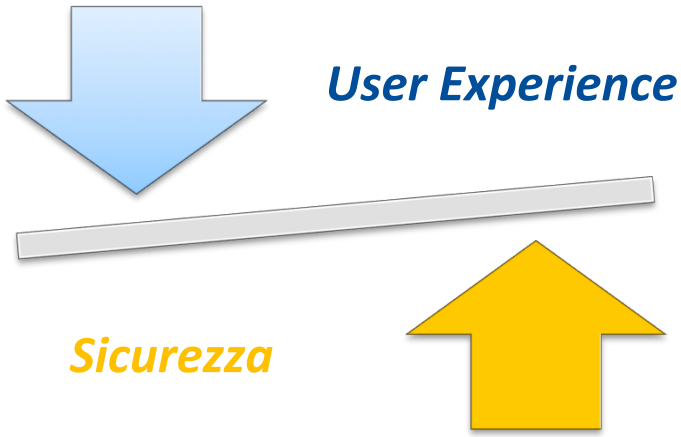
Soprattutto per Android, su questo tema si riscontra un aumento di sensibilità negli anni da parte degli sviluppatori. Tuttavia anche quest'anno registriamo evidenze di una non corretta gestione della cache

Rischi

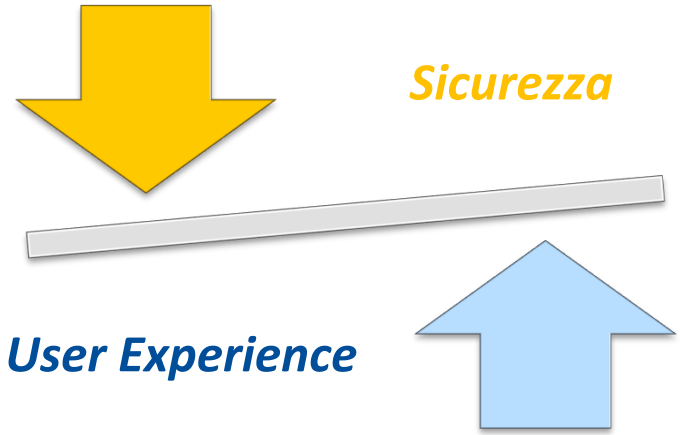
Il file system è una potenziale fonte di informazioni sensibili, soprattutto in caso di smarrimento del dispositivo. Una non corretta gestione della cache può permettere ad un attaccante di rilevare:

- Informazioni sensibili per la privacy
- Informazioni critiche riguardo l'operatività utente
- Dati biometrici
- Informazioni utili a condurre attacchi anche tramite altri canali (es. Online banking).

Una scelta necessaria



- Priorità alla ***Sicurezza***; tutte le transazioni provenienti da device insicuri vengono bloccate
- Il numero di device compromessi è molto alto, e non sempre il servizio mobile banking ne subisce gli effetti
- Risultato? La ***User experience*** è gravemente danneggiata con inevitabili problemi di marketing



- Priorità alla ***User Experience***; si evitano controlli o non si tiene conto dei risultati
- Risultato? ***Sicurezza*** potenzialmente compromessa

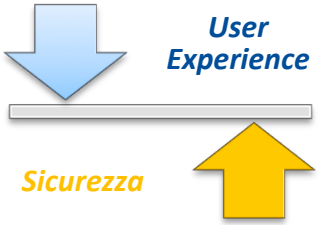
L'approccio IKS: SMASH Mobile

Collection | Analysis | Fraud Management

Canale Mobile

Canale Internet

- SMASH Mobile sfrutta delle librerie come sonde utili a estrapolare campioni rappresentativi dello stato della device:
  - Compromissione
  - Device fingerprint
  - Time Fingerprint:
  - User behaviour:



- L'esito dei controlli viene analizzato dall'engine SMASH attraverso controlli puntuali e di analisi comportamentali, e memorizzato nel database al fine di alimentare la storia del device e dei suoi eventuali cambiamenti nel tempo.

- SMASH Mobile permette la correlazione del livello di sicurezza del dispositivo con un livello di rischio calcolato sulla base del normale utilizzo del servizio da parte del cliente, attraverso l'analisi delle informazioni legate alle transazioni

Strumenti antifrode

Device fingerprint

tx details

Device Check

User Behaviour

Block

Permit

OTP Challenge

Investigation

Grazie per l'attenzione