



# **Mpayments & security: un modello in via di definizione**

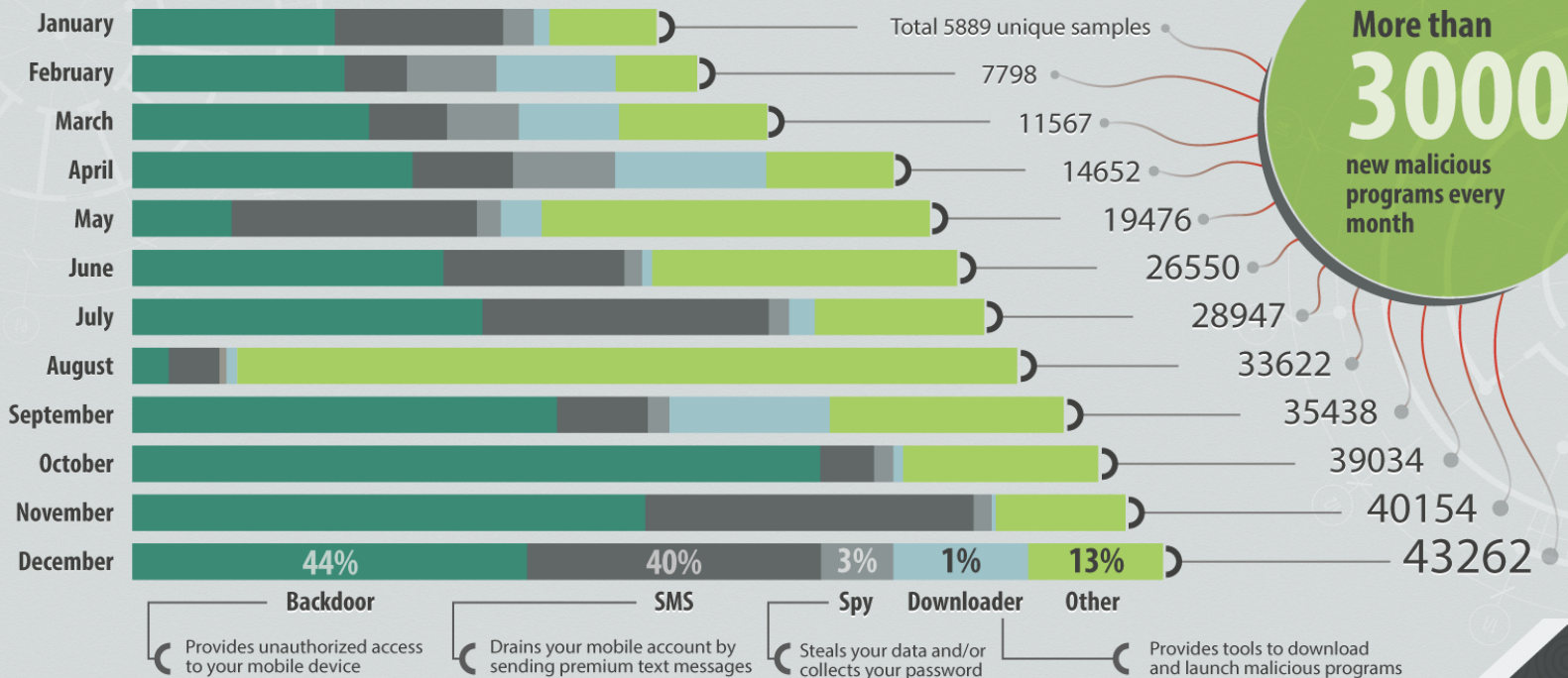


**Alessandro Cian**

Carte 2013 – 5 dicembre 2013

# Trend diffusione Malware

## Android Threats in 2012



### NOTABLE MALWARE BY REGION

USA

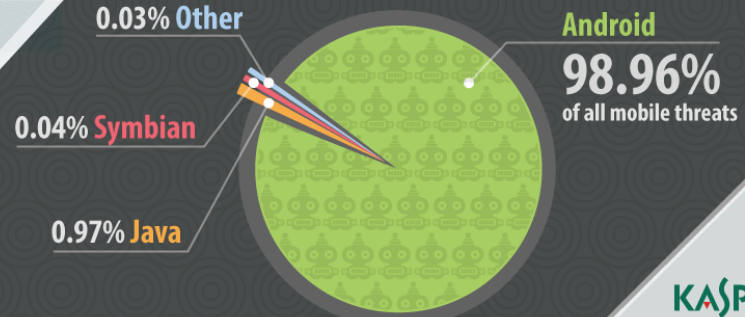
**Trojan**  
**AndroidOS.FakeRun.a**  
 displays annoying ads instead of promised game or useful software

Europe

**Trojan**  
**AndroidOS.Plangton.a**  
 displays ads and modifies browser bookmarks. Exposes victims to online scams as well

Russia

**Trojan**  
**SMS.AndroidOS.Opfake.bo**  
 sends texts to premium-rate numbers, directly stealing victims' money



## Attenzione dei media...

# Juniper study: 80% of smartphones still unprotected from malware, attacks

**Summary:** Smartphones (and tablets) are just open hotspots for trouble waiting to happen if their owners don't take precautions immediately.



By Rachel King for Zero Day | October 9, 2013 -- 19:28 GMT (12:28 PDT)

## Sicurezza mobile: italiani bocciati. Uno smartphone Android su due non è protetto

di G.Rus 19 novembre 2013

Tweet 6 Consiglia 55 g+1 6 My24



Smartphone e tablet: qualsiasi sia il mezzo, è appurato ormai che gli italiani passano parecchio tempo collegati alla Rete per comunicare (e altro) in totale mobilità. Gli internauti del Belpaese, lo dice una ricerca diffusa oggi da Kaspersky Lab, sono però meno attivi in fatto di operazioni bancarie o acquisti online e si confermano in tal senso più reticenti, rispetto agli utenti di altri Paesi, verso l'uso sistematico del Web per azioni considerate sensibili sotto il profilo della sicurezza. La percentuale di chi effettua transazioni finanziarie attraverso il

proprio dispositivo mobile è pari all'88% del totale degli utenti Internet; in Francia si arriva al 97%.

## Tablet e smartphone, il 97,5% di tutti gli attacchi malware colpisce il sistema operativo Android

17 Pubblicato 24 novembre 2013



(Sesto Potere) – Milano – 24 novembre 2013 - Il terzo trimestre del 2013 è stato fondamentale per i produttori di malware specializzati in piattaforme mobile come Tablet e smartphone. In sintesi?

A giugno gli esperti hanno scoperto il nuovo Trojan Sypeng, in grado di accedere al conto bancario della vittima direttamente dal proprio smartphone.

A settembre è stato individuato il primo caso di utilizzo di botnet di terze parti per distribuire Trojan.

Kaspersky Lab ha individuato complessivamente 500.284.715 attacchi nel periodo dell'anno da luglio a settembre.

Nel mirino: dati personali e accesso a conti correnti bancari! [Nel dettaglio](#)

## Smartphone e tablet, occhio alla sicurezza

Installare antivirus, pin o criptare informazioni

25 ottobre, 11:01

g+1 1 Tweet 5 Consiglia 77

Indietro Stampa Invia Scrivi alla redazione Suggestisci ()



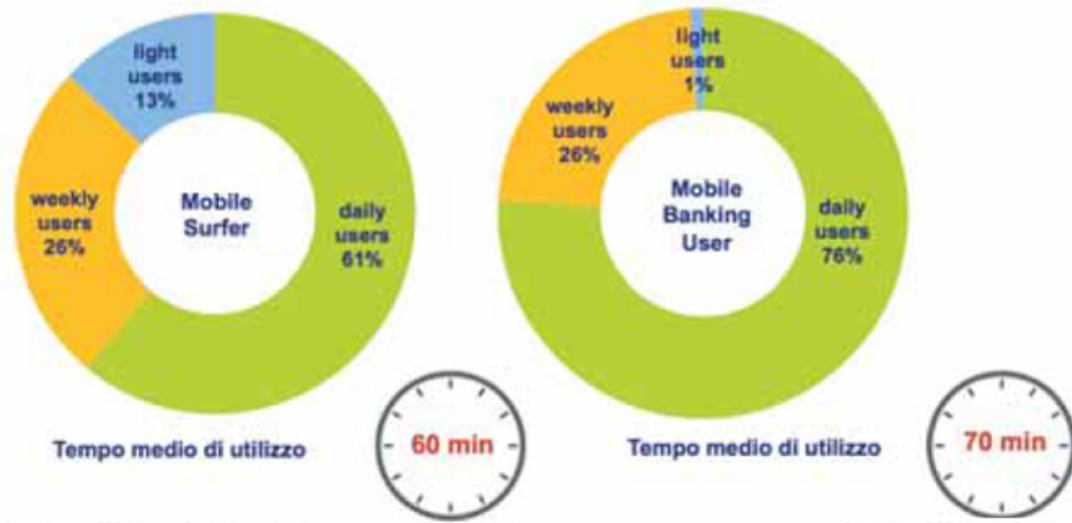
Smartphone e tablet a rischio sicurezza

# Frequenza utilizzo Smartphone

Figura 4.4 – Tempo medio di utilizzo giornaliero  
Fonte: Osservatorio Mobile Marketing & Service,  
dati Doxa (dicembre 2012)



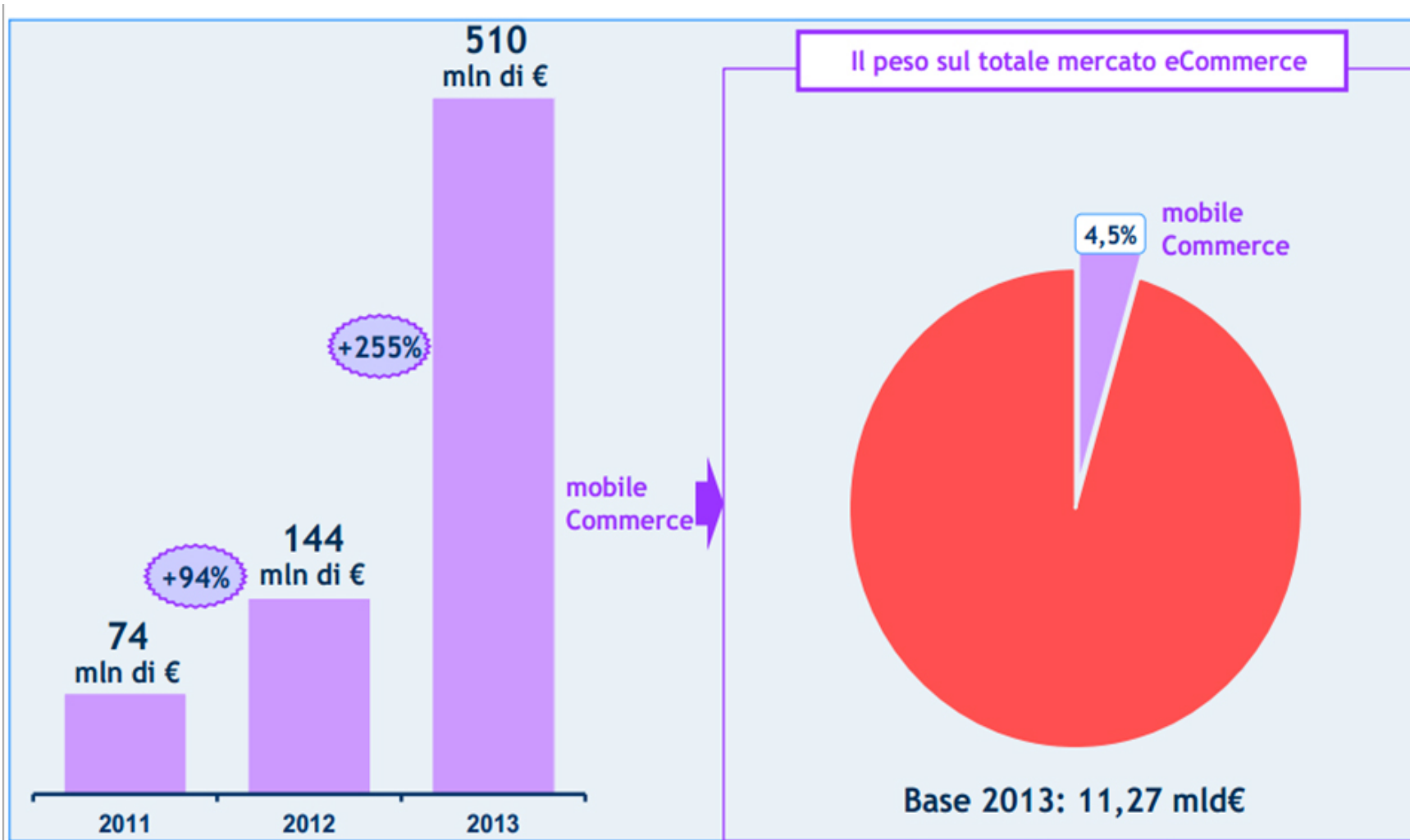
Figura 4.10 – Frequenza di utilizzo dello Smartphone  
per utenti Mobile Banking e per Mobile Surfer



Campione: 1502 Mobile Surfer intervistati  
Fonte: Osservatorio Mobile Marketing & Service, dati Doxa (dicembre 2012)

Campione: 700 Mobile Banking User intervistati  
Fonte: Osservatorio Mobile Banking 2013

# Mobile Payments



Osservatorio eCommerce B2c della School of Management del Politecnico di Milano



**Carte  
C-less**



**Credito  
Debito  
Prepagate**



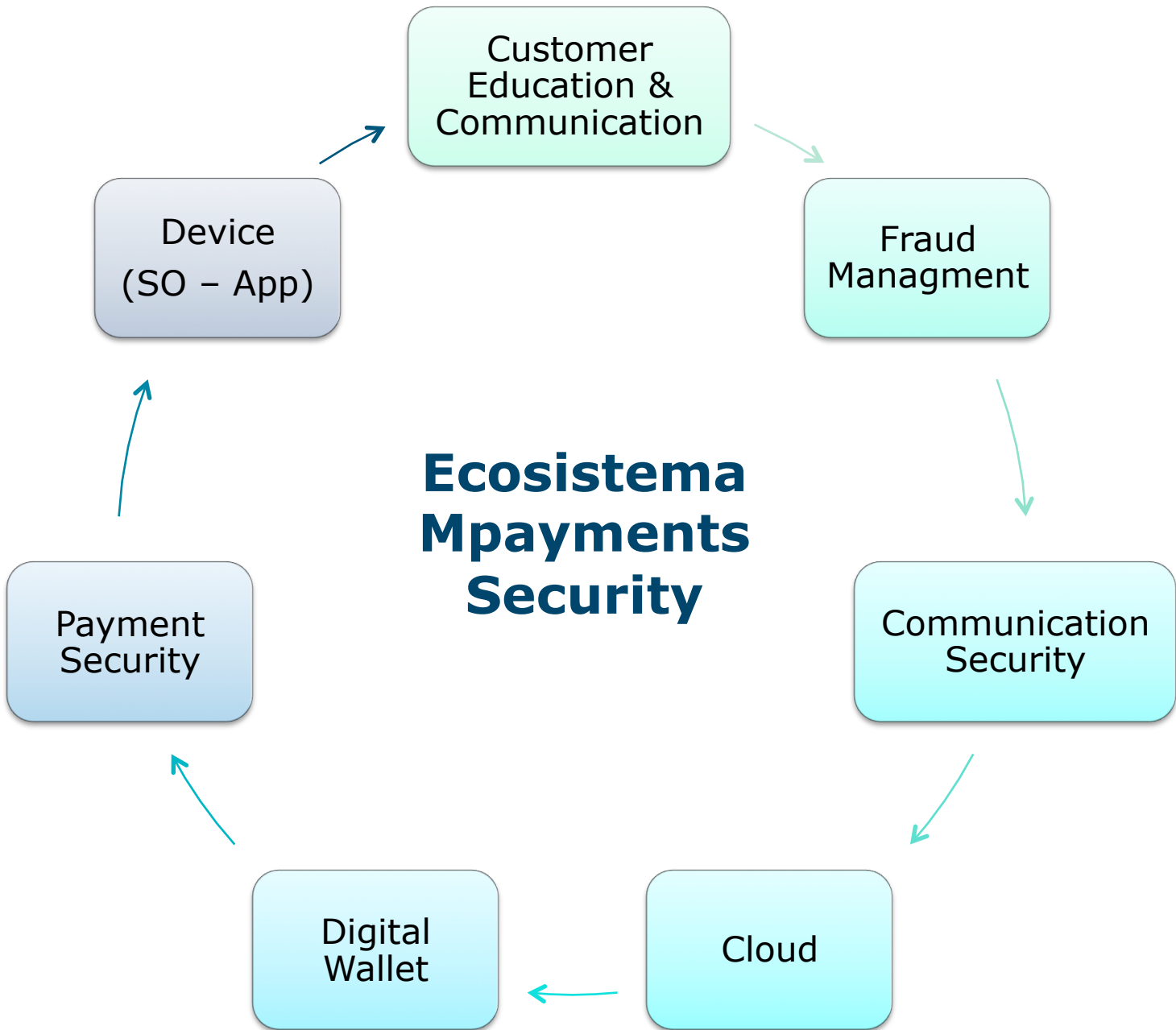
**Danni  
causati  
dalle frodi**

**Costi**

**Danno  
d'immagine**

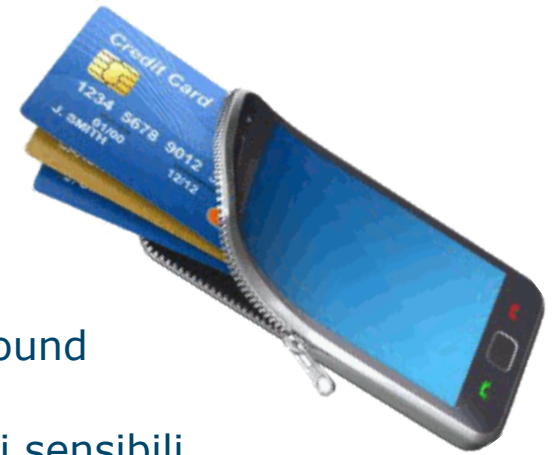






# Digital Wallet

- Strong authentication
- Log out automatico per inattività o se l'App lavora in background
- Distribuzione su canali sicuri dei software di gestione dei dati sensibili
- Disattivazione Wallet: dal device lato utente, da remoto lato Banca
- Monitoraggio delle transazioni (Prevention – Protection)
- Definire il numero massimo di autenticazioni fallite e un processo remoto sicuro per la riattivazione del Wallet
- Protezione dei dati sensibili anche nel caso in cui il device venga smarrito o rubato
- Sistema di Alert per gli utenti (sms – email – contatto telefonico)
- Verifica in tempo reale dello stato di una transazione lato utente



# Customer Education & Communication

## Comportamento d'uso

- Antivirus/Malware
- Download APP
- APPstore
- No APP «Salva Password»
- Attenzione a phishing
- Attivazione bluetooth solo all'uso
- Aggiornamento SO, in particolare patch sicurezza
- Blocco Telefono (protezione identità digitale)
- Chiusura APP Transazionali alla conclusione dell'operazione
- Segnalazione alla banca del furto/smarrimento del device



**Tutto ciò deve essere comunicato all'utente...**



**EUROPEAN CENTRAL BANK**

**EUROSYSTEM**

**RECOMMENDATIONS FOR THE SECURITY OF MOBILE PAYMENTS  
DRAFT DOCUMENT FOR PUBLIC CONSULTATION**

European Forum on the Security of Retail Payments - SecuRe Pay (BCE)

**<http://www.ecb.europa.eu/paym/cons/pdf/131120/recommendationsforthesecurityofmobilepaymentsdraftpc201311en.pdf>**

**La vita è come  
una scatola di cioccolatini:  
non sai mai cosa ti capita!**

**Forrest Gump**