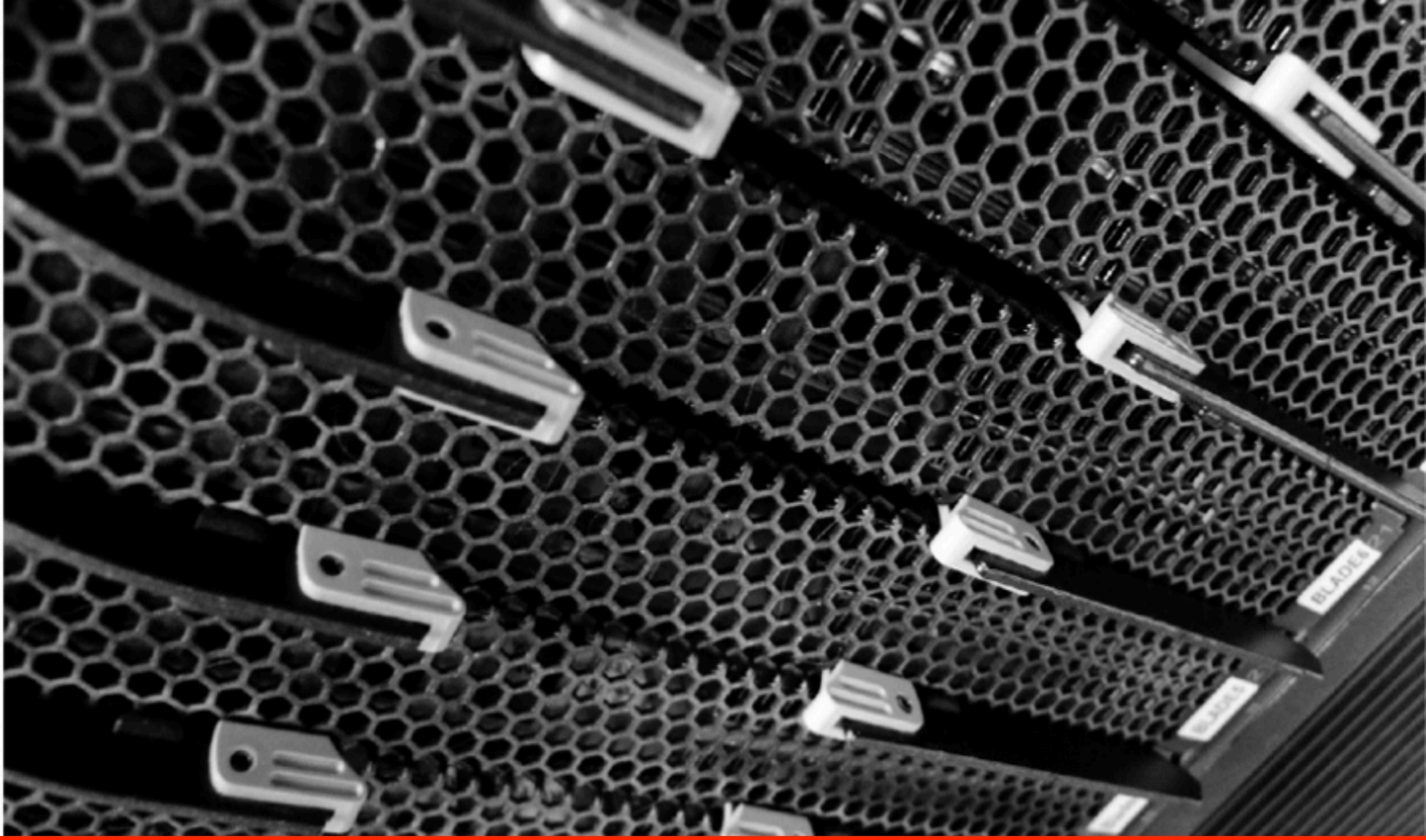
techub
SHARING YOUR VISION

Oltre Eurograbber: nuovi scenari di attacco multidimensionale

Roma, 5 Giugno 2013

Giacomo Paoni - Techub S.p.A.

v1.03



Introduzione

Agenda

- Introduzione
- Cos’è Eurograbber
- Worse-case scenario: oltre Eurograbber
- Conculsioni e Soluzioni

Eurograbber: come si realizza una frode da 36M€

Tutto nasce da un banking Trojan

"Originato in Italia [...] con un trasferimento automatico di importo variabile tra €500 e i €250,000 a transazione, si stima abbia portato al furto €36+ milioni da più di 30,000 account, sia privati che aziendali [..] con funzionalità specifiche per aggirare l'autenticazione a due fattori"

Checkpoint - Eurograbber Report

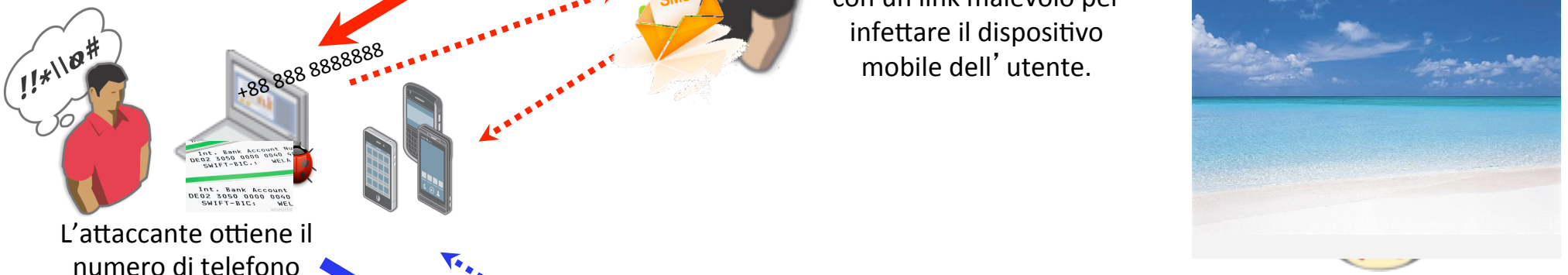
techub
SHARING YOUR VISION

Analisi dello scenario

L'utente riceve dallo attaccante una mail contenente un TROJAN.

Il TROJAN infetta il client e intercetta le comunicazioni con la banca.

L'attaccante invia un SMS con un link malevolo per infettare il dispositivo mobile dell'utente.



L'attaccante ottiene il numero di telefono dell'utente tramite TROJAN

Quando l'utente esegue una dispositiva, la banca invia i codici di controllo al cellulare dell'utente e questi vengono inoltrati all'attaccante

L'attaccante utilizza I codici per trasferire i fondi automaticamente …
… laddove non possano essere rintracciati / recuperati

techub
SHARING YOUR VISION

Aggiungere un ulteriore fattore
di autenticazione
(Defense in Depth)
non sempre aiuta

Apparati di sicurezza e ulteriori controlli
sono insufficienti da soli a garantire una protezione efficace

techub
SHARING YOUR VISION

Questo tipo di TROJAN sono progettati per adattarsi ai controlli di sicurezza specifici presenti nel sito della vostra Banca

La sicurezza è un divenire la cui efficacia è basata sul continuous improvement

techub
SHARING YOUR VISION

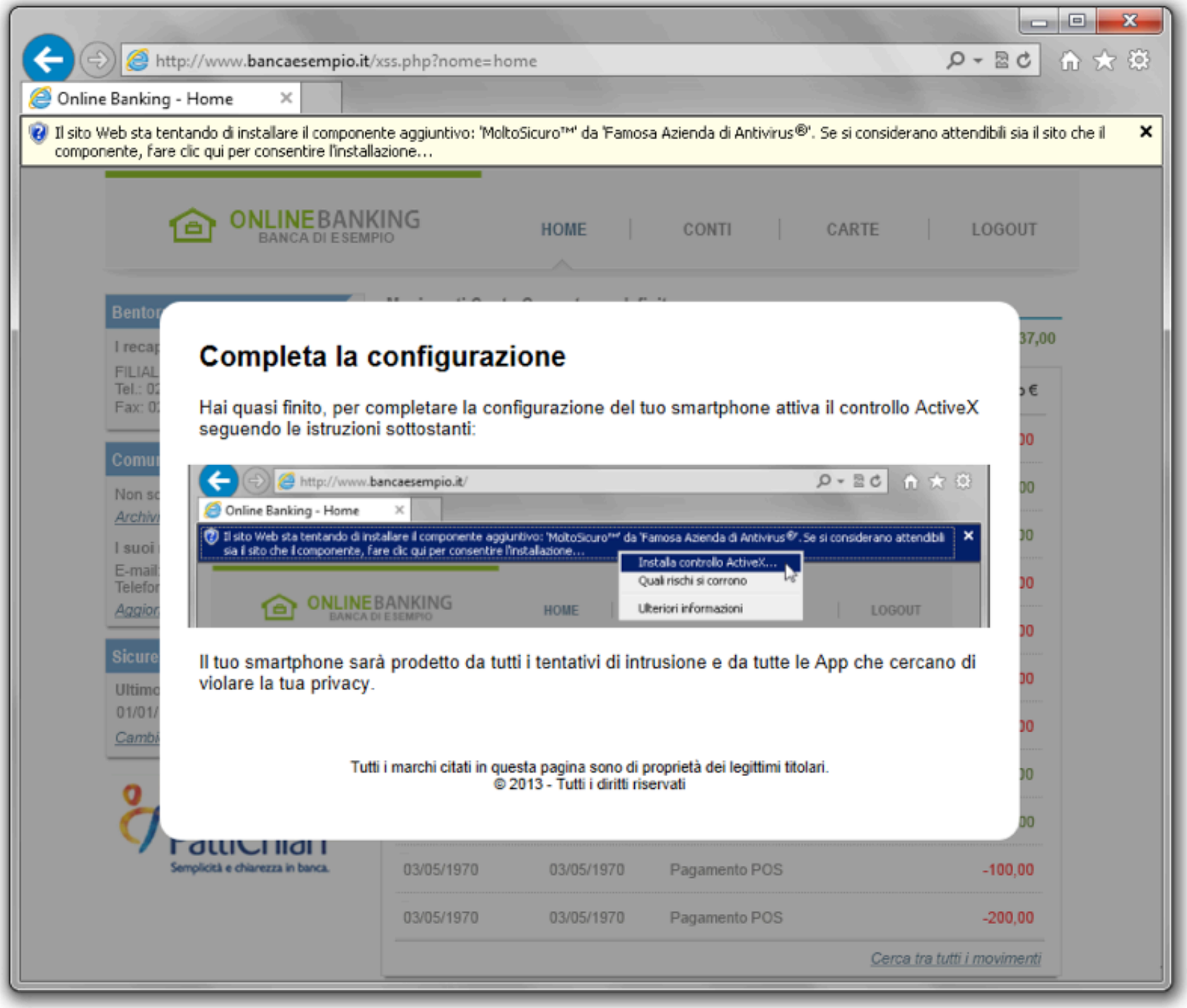
La sicurezza efficace combina
controlli differenti
a livelli differenti
(Defense in Width)

Worse-Case scenario

Lo stesso scenario, partendo pero' da vulnerabilità sul sistema della nostra Banca

techub
SHARING YOUR VISION

techub
SHARING YOUR VISION



techub
SHARING YOUR VISION

Conclusioni, Soluzioni e Proposte

Verifiche periodiche di Server e Applicazioni web, rimozione delle vulnerabilità esistenti per prevenire la compromissione degli utenti.

techub
SHARING YOUR VISION

Verifichiamo le nostre Mobile Apps (altrimenti attaccabili da malware sul dispositivo mobile)

Difesa del perimetro esterno con strumenti adeguati che segnalino anche I tentativi di acquisire informazioni sulle vulnerabilità esistenti

Behavioural Analysis
su abitudini e movimenti per prevenire
attacchi alle logiche di business

techub
SHARING YOUR VISION

Security Intelligence per essere aggiornati sui nuovi scenari di rischio

techub
SHARING YOUR VISION

“Ego te intus et in cute novi.”

(io ti conosco dentro e sotto la pelle.)

Persio – poeta latino III sec.

Grazie per l'attenzione

Giacomo Paoni
giacomo.paoni@techub.it

techub
SHARING YOUR VISION