BANCHE E SICUREZZA 2013

Antonio Apruzzese
Direttore del Servizio Polizia Postale e delle Comunicazioni

"Cybercrime i rischi per i servizi bancari on line"

Roma, 5 giugno 2013

La nostra organizzazione

I principali centri operativi

Dislocazione Territoriale

polizia delle comunicazioni

20 Compartimenti regionali

80 Sezioni provinciali

SEZIONE DISTACCATA PRESSO L'AUTORITA' PER LE GARANZIE NELLE COMUNICAZIONI

Competenze istituzionali

- Cyber Crime
  - Hacking (Violazione di sistemi informatici e sottrazione di dati)
  - Reati interessanti i servizi di : -Home banking
    -Monetica
    -E-Commerce
  - Cyber terrorismo
  - Protezione delle Infrastrutture Critiche
- Pedofilia on line
- Reati contro la persona via web
  - Stalking on line, Cyber bullismo
  - Minacce, molestie e diffamazione online
- Tutela delle Comunicazioni
  - Reati in ambito postale
  - Controlli in materia di telecomunicazioni in generale
- Tutela del diritto d'autore - Pirateria satellitare

LA CRIMINALITA' INFORMATICA

scenario

Utilizzatori della rete Internet* :

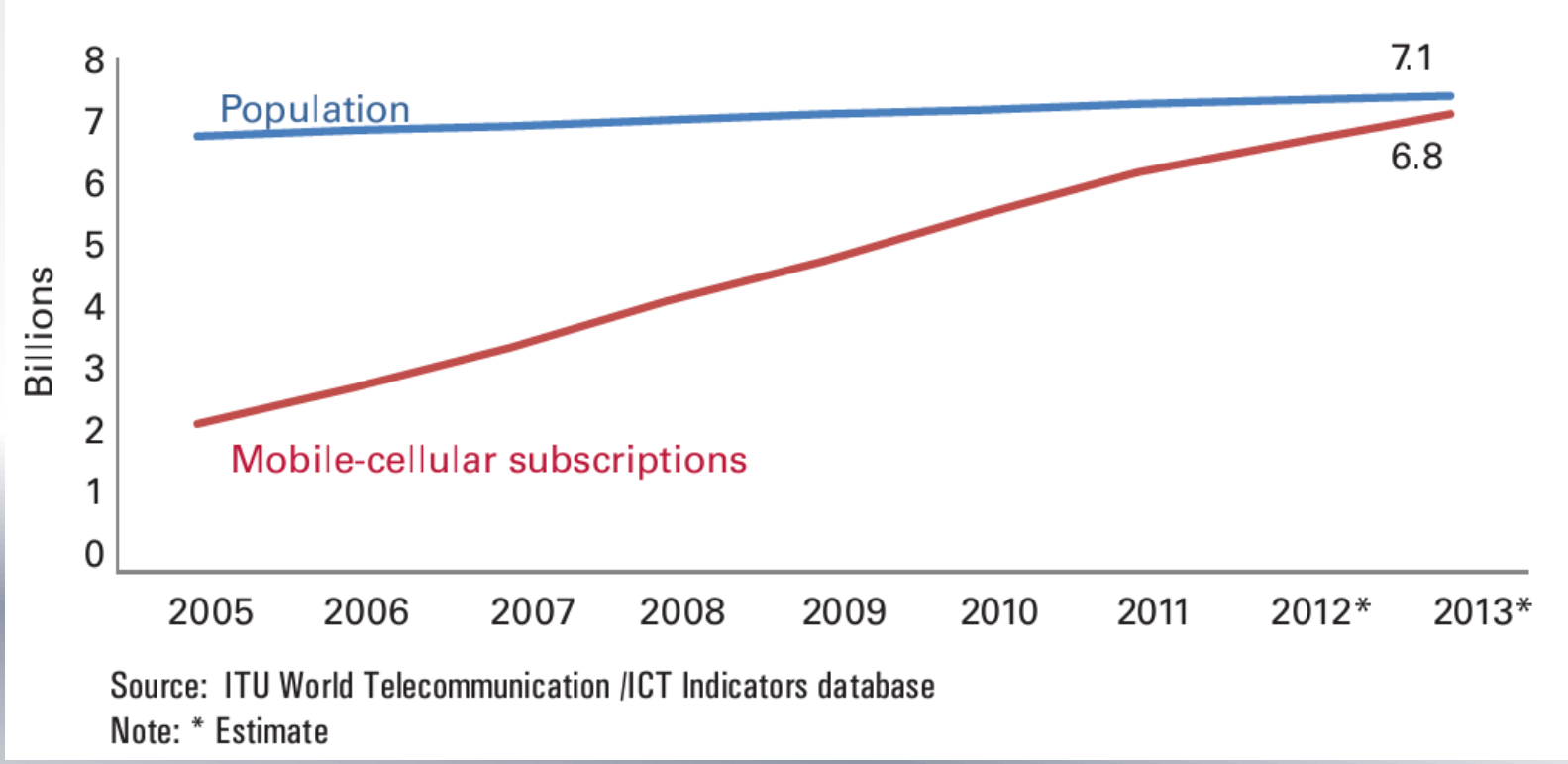
Nel 2000 360,985,492

Oggi 2,7 miliardi

*FONTI: http://www.internetworldstats.com/stats.htm e
http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013.pdf

LA CRIMINALITA' INFORMATICA
scenario

Mobile-Cellular Subscription: 6,8 billions



LA “ NUOVA ” CRIMINALITA’ INFORMATICA

I PERCHE’ DI “ NUOVE ” ANALISI

- LE VASTISSIME DIMENSIONI DEL FENOMENO
- I RISCHI CONNESSI
- L’INDIVIDUAZIONE DI ADEGUATE INIZIATIVE DI CONTRASTO
- I NUOVI PROFILI CRIMINOLOGICI DI AUTORI E VITTIME

LE NUOVE IMPRESE CRIMINALI

- NON PIU' IN FORMA INDIVIDUALE
- NUOVE STRUTTURE ORGANIZZATIVE
- NUOVI SISTEMI DI ARRUOLAMENTO
- NUOVI SCHEMI DI RICICLAGGIO
- TRANSNAZIONALITA'

Furti di IDENTITA' DIGITALE Principali Tipologie

Attacchi rivolti agli utenti

Tecniche di Phishing «tradizionale»

Sottrazione di Poche decine di credenziali

Attacchi ai sistemi informatici degli utenti

Botnet - Phishing di "nuova generazione"

Sottrazione di migliaia di credenziali

Attacchi ai grandi sistemi informatici

Data Breach

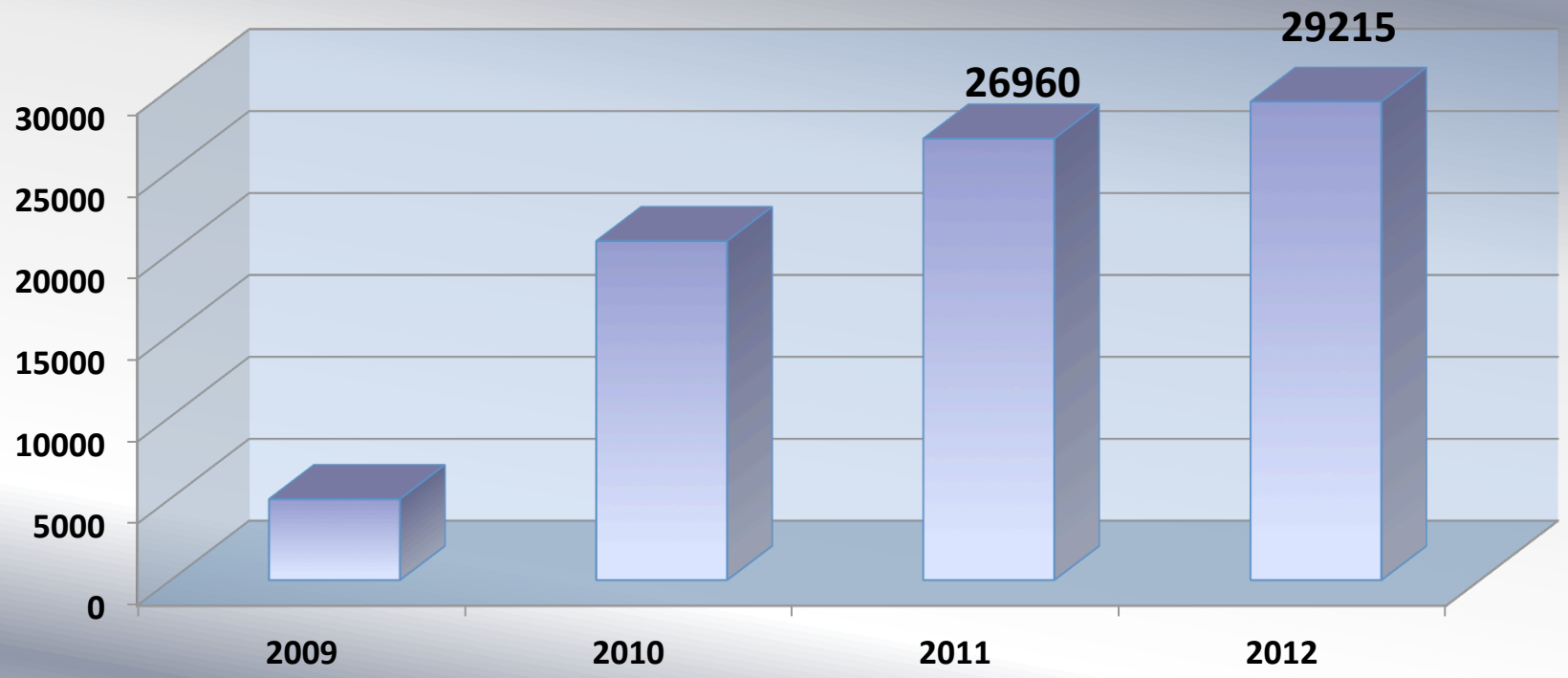
Sottrazione di centinaia di migliaia di credenziali

MINISTERO DELL' INTERNO
REPUBBLICA ITALIANA
@polizia delle comunicazioni
FURTI D'IDENTITA'
... phishing
... attacchi logici
... attacchi fisici
... contraffazione
... social engeneering
ATM
MasterCard

CRIMINI INFORMATICI
in materia di *home banking* e *monetica*

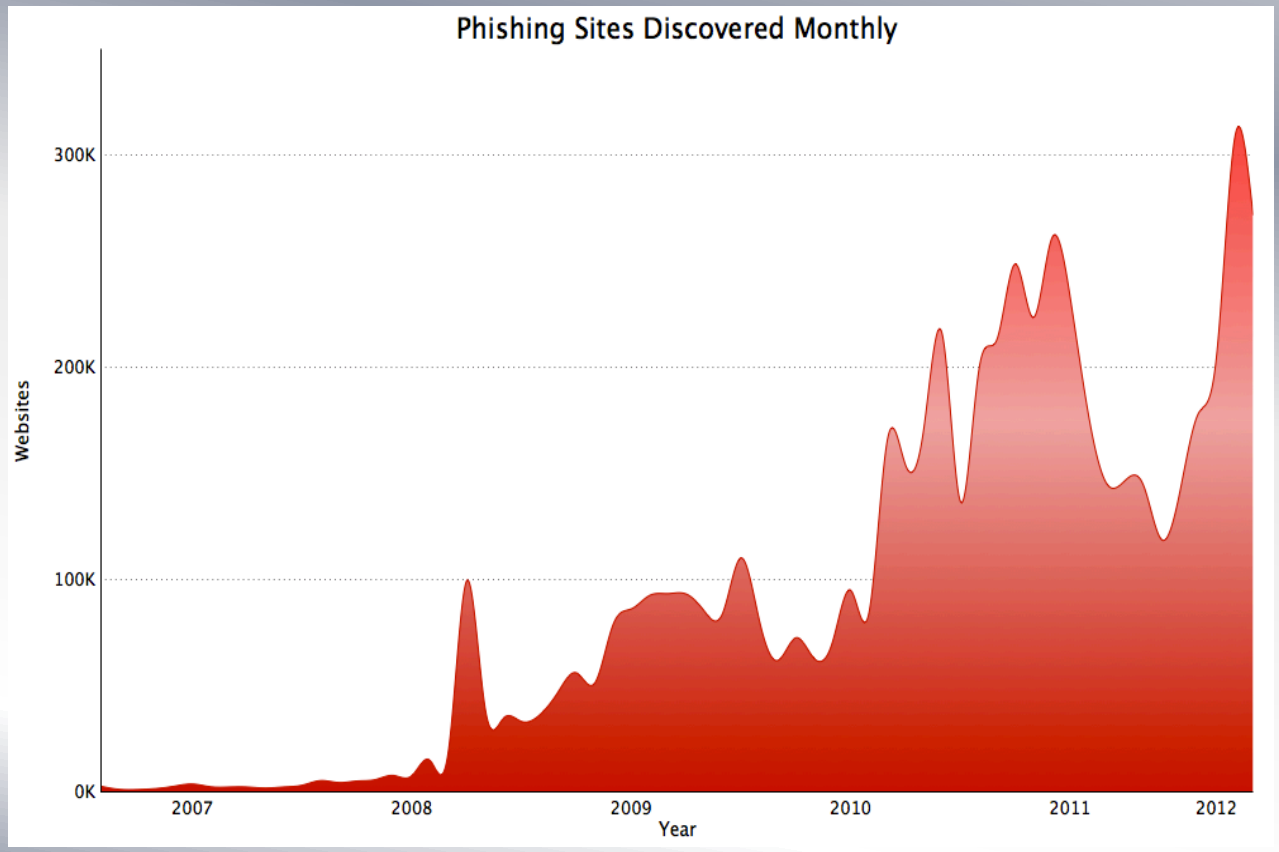
- rappresentano un fenomeno in costante evoluzione
- sfruttano tecniche e tecnologie sempre più sofisticate
- sono posti in essere da vere e proprie organizzazioni criminali transfrontaliere
- hanno effetti transnazionali ed intersettoriali

Furto D'identità
Internet Banking + Monetica
Denunce



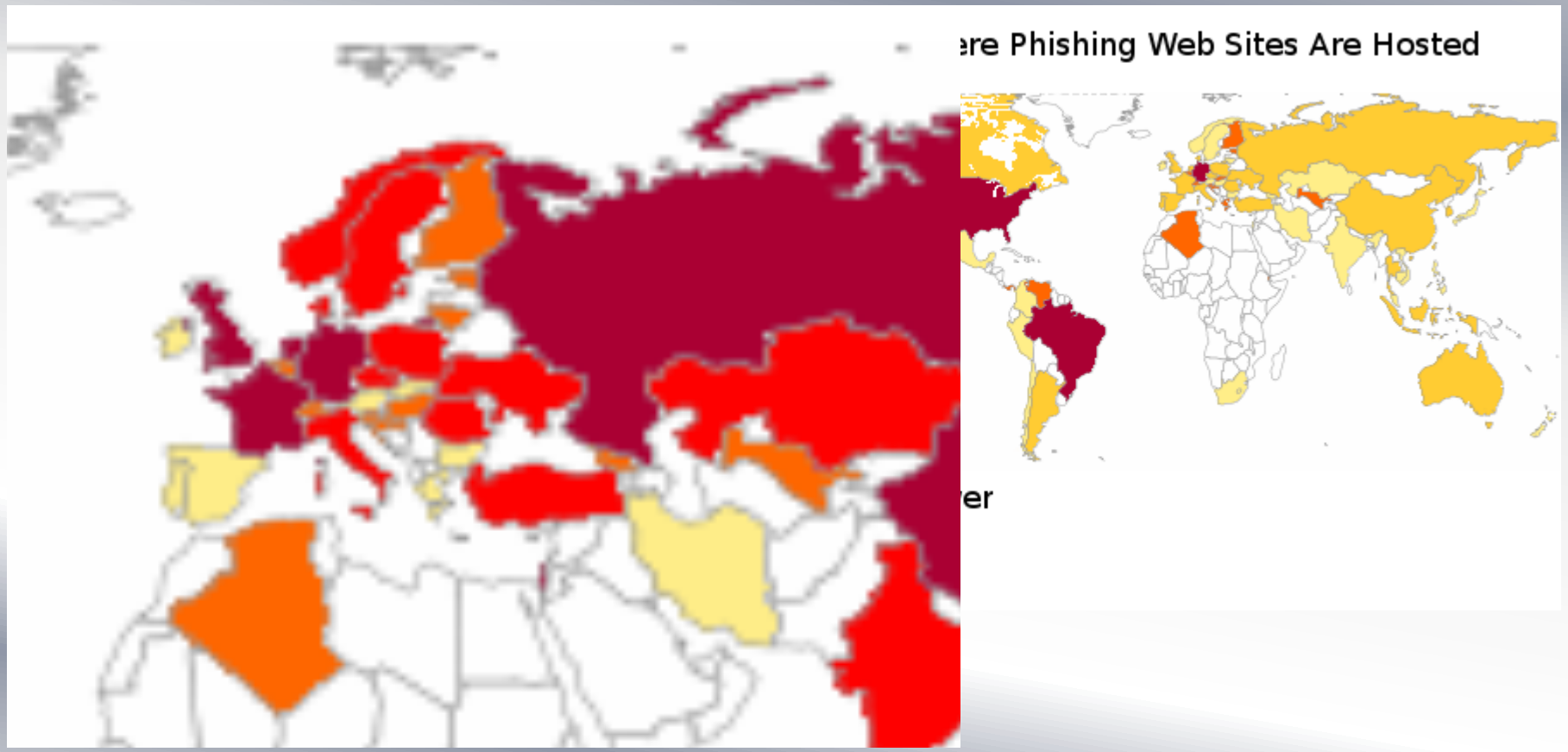
Denunce Numero casi rilevati dalle denunce anni 2009 –2012
Fonte:Polizia Postale e delle Comunicazioni

IL PHISHING “tradizionale”



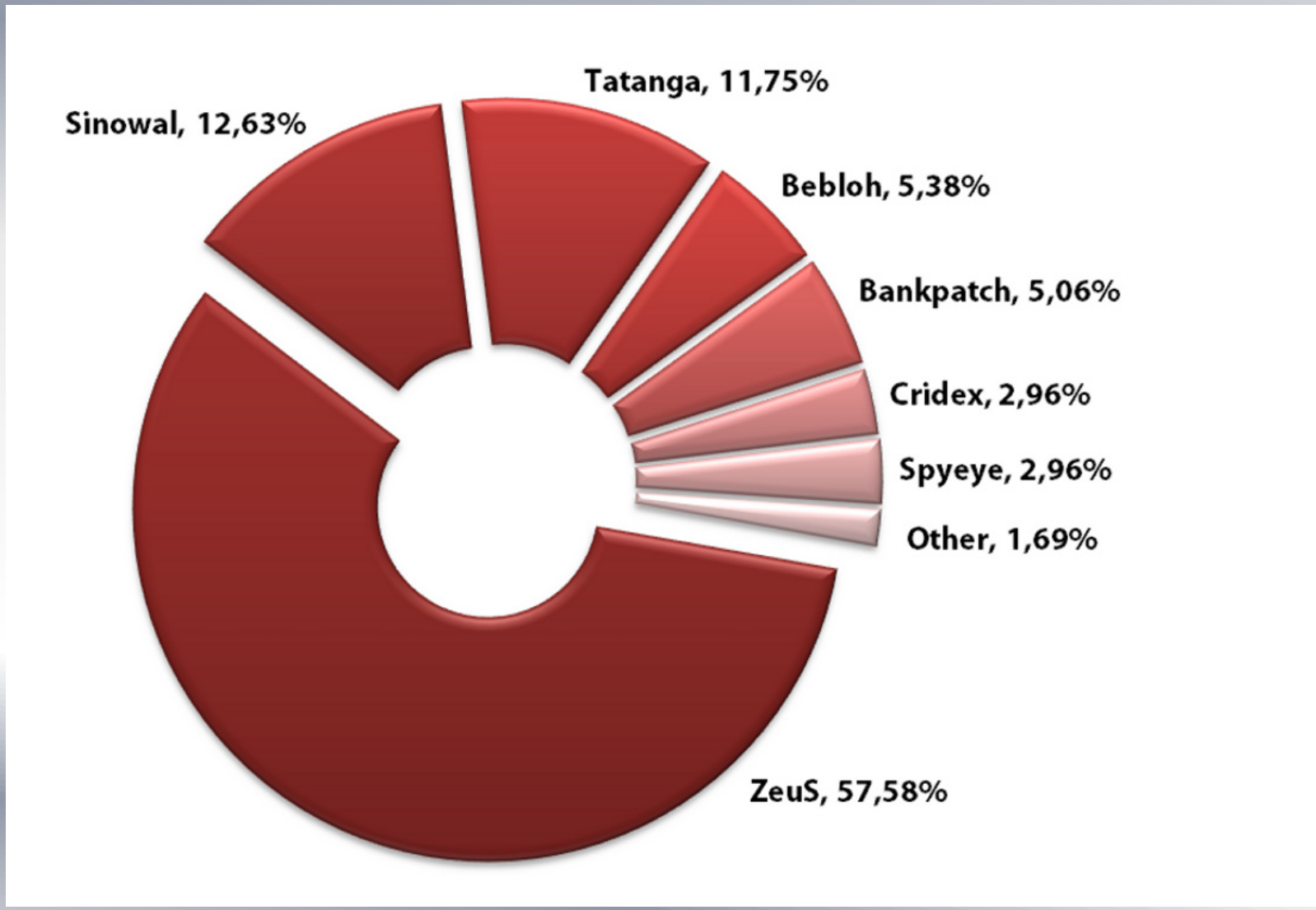
Fonte: Google

IL PHISHING “tradizionale”



Fonte: Google

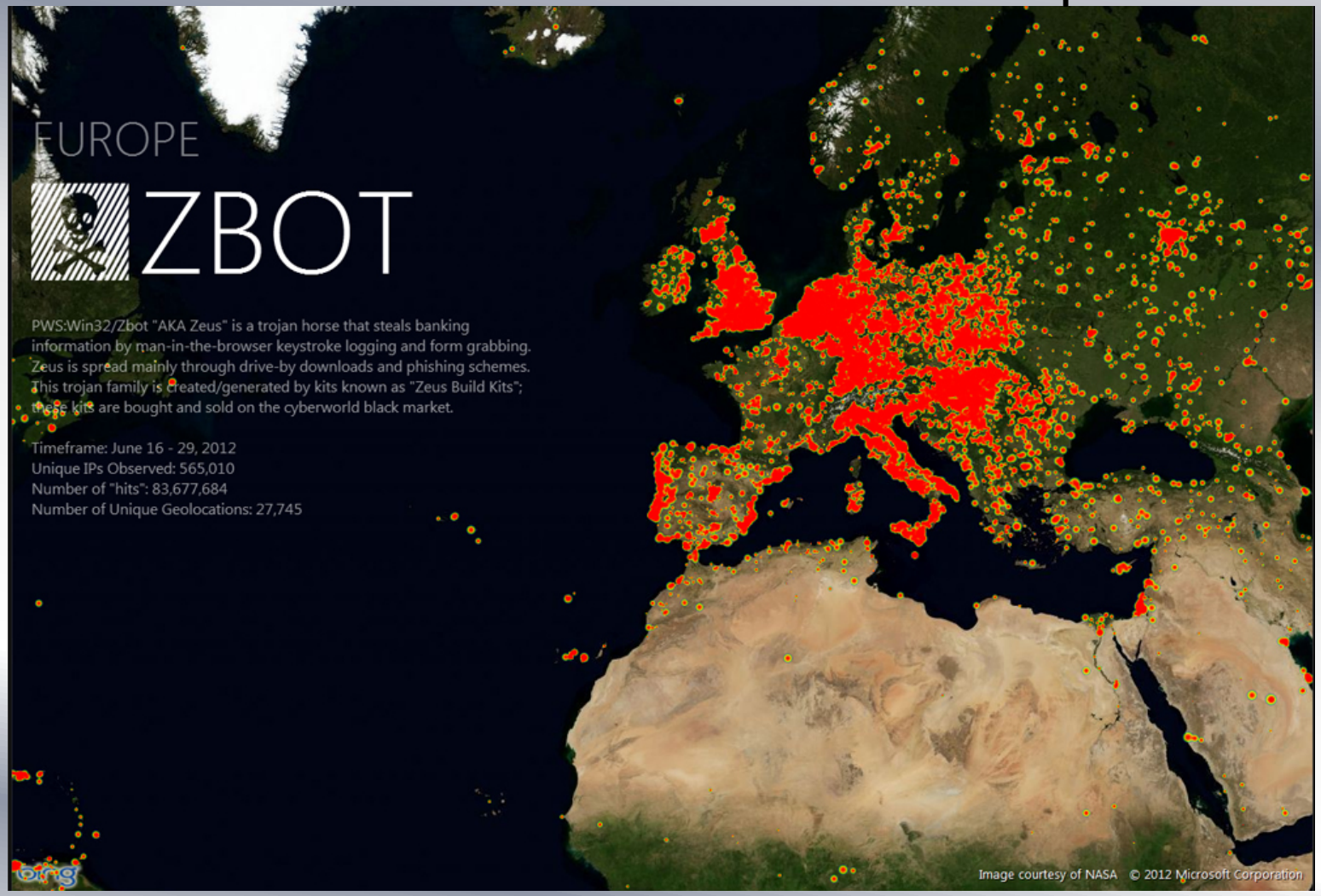
Trojan Banking



FONTE: http://www.gdata-software.com/about-g-data/press-center/news/news-details/article/3204-zeus-trojan-responsible-for-mo.html

BOTNET ZEUS

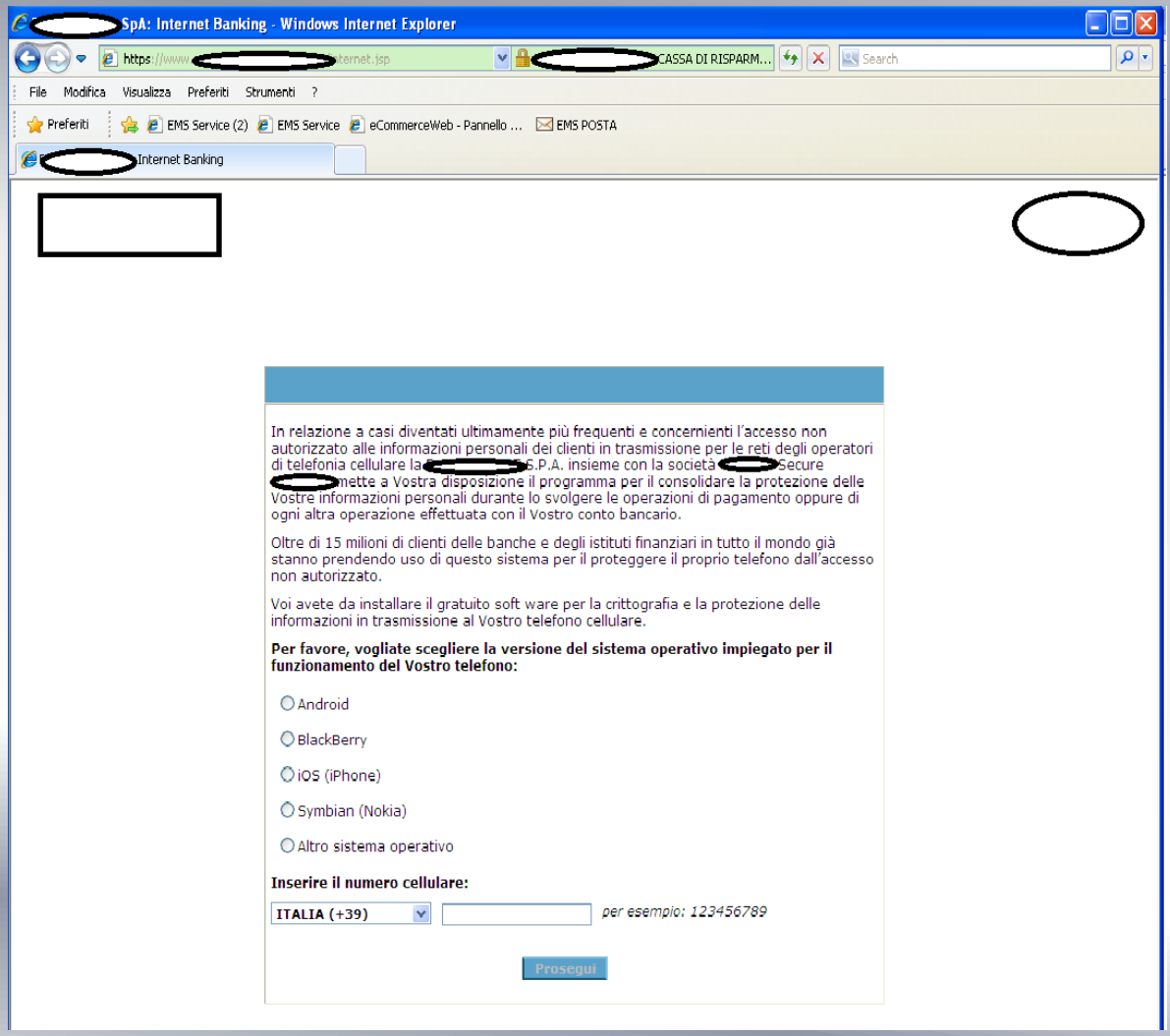
Diffusione dell'infezione in Europa



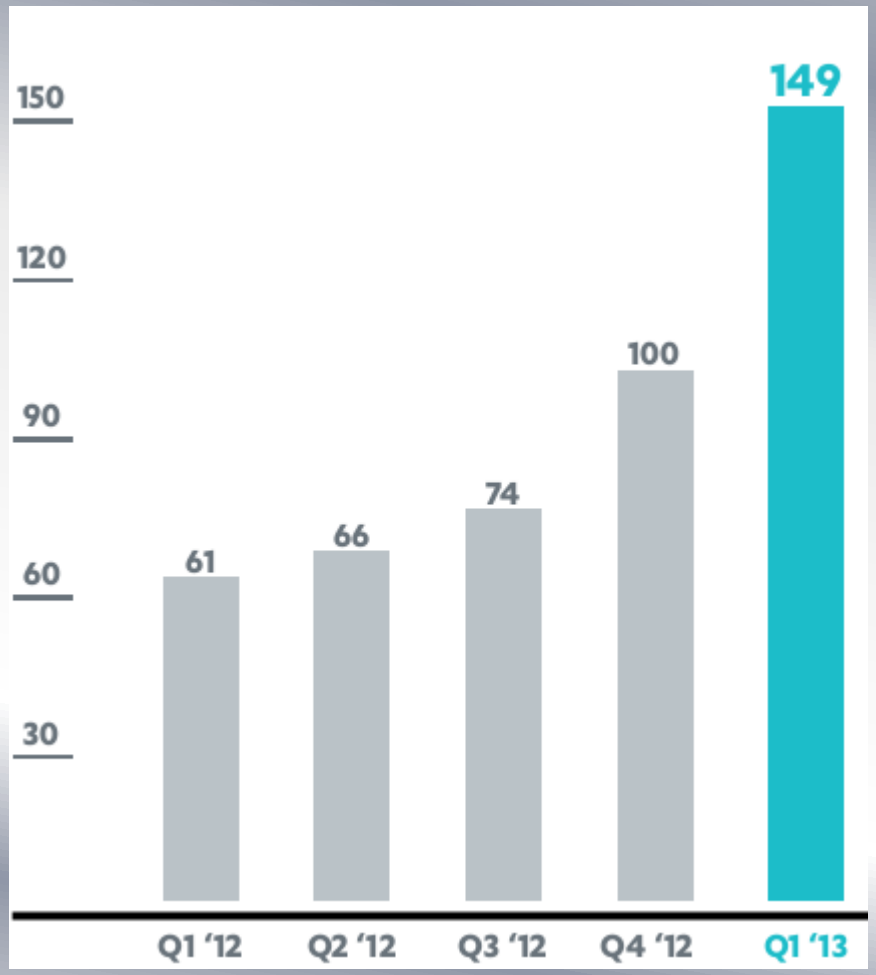
Fonte:
http://www.microsoft.com/global/en-us/news/publishingimages/ImageGallery/Images/theme_zbot_eu_Web.jpg

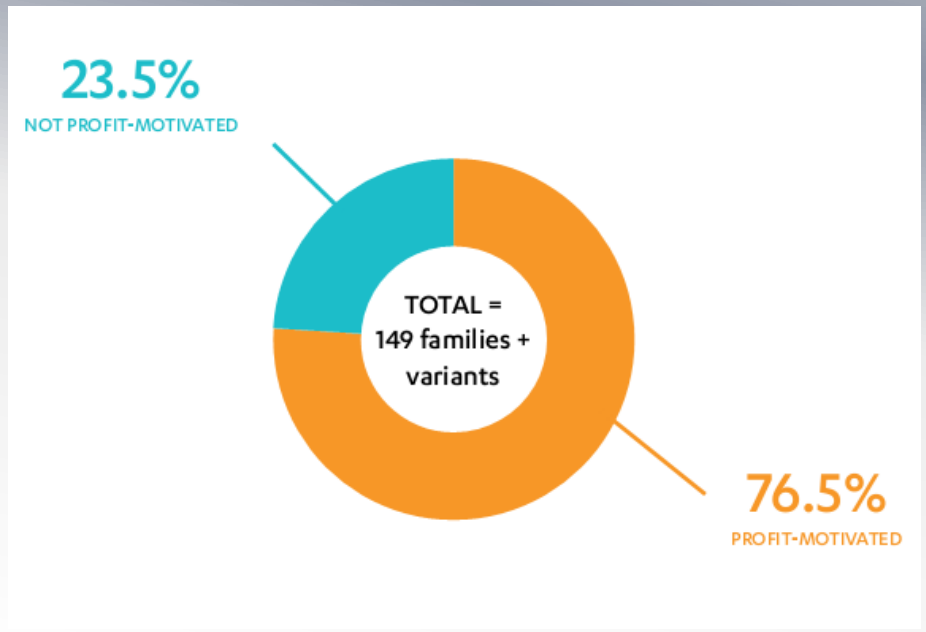
BOTNET ZEUS

Attacco ai sistemi mobile



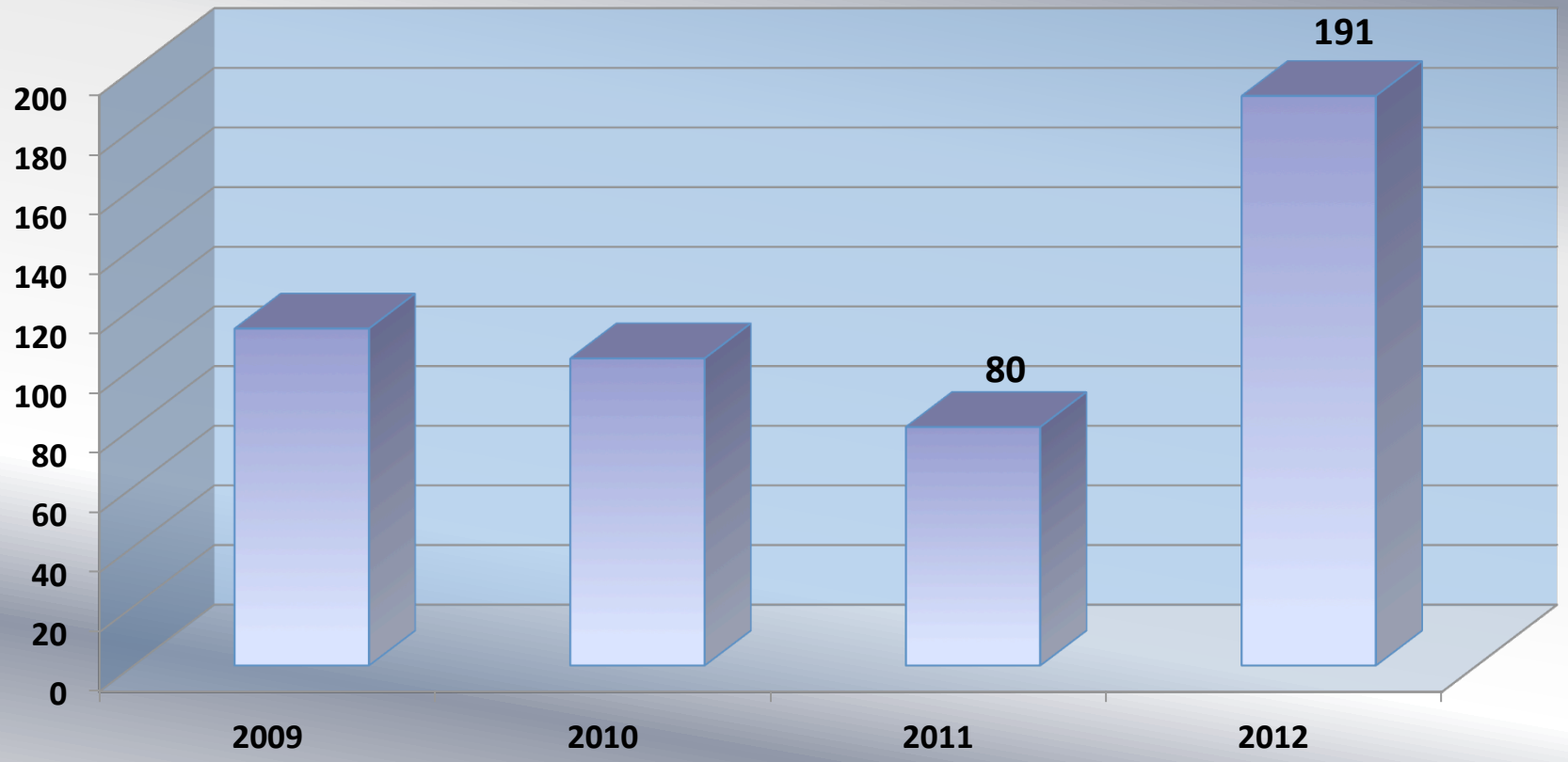
MALWARE
Su dispositivi mobili





Fonte:
http://www.f-secure.com/static/doc/labs_global/Research/Mobile_Threat_Report_Q1_2013.pdf
new Mobile threat families and Variants, Q1 2013

Internet Banking e Monetica arrestati



PREVENZIONE E CONTRASTO

- approccio sinergico = partnership pubblico-privato = sicurezza partecipata

- condivisione e circolarità di dati e informazioni sul fenomeno

- coinvolgimento di organismi investigativi specializzati

In particolare

- realizzazione di *task force pubblico-private*

- condivisione e circolarità dei dati e delle informazioni utili ai fini di prevenzione e repressione dei reati e per la modulazione delle policy di sicurezza

- affinamento delle potenzialità operative e della risposta investigativa

- Cooperazione internazionale

CASO 1 – Esito Positivo

10 aprile - mercoledì ore 12 – bonifico di oltre 100.000 euro verso il Regno Unito

«comunicazione avvenuta entro 48 ore dalla disposizione del bonifico fraudolento»

12 aprile – venerdì ore 10 – Comunicazione al Servizio Polizia Postale

Immediata attivazione dei canali di collaborazione di Polizia

L'intero importo è stato bloccato e restituito al truffato

CASO 2 – Esito Negativo

15 aprile - lunedì ore 12 – bonifico di oltre 110.000 euro verso il Regno Unito

«comunicazione avvenuta oltre le 48 ore dalla disposizione del bonifico fraudolento»

19 aprile – venerdì ore 10 – Comunicazione al Servizio Polizia Postale

Immediata attivazione dei canali di collaborazione di Polizia

L'intero importo è prelevato dai criminali

CASO 3 – Esito Positivo

3 aprile - mercoledì ore 12 – bonifico di circa 500.000 euro verso la Slovacchia

«comunicazione avvenuta entro 48 ore dalla disposizione del bonifico fraudolento»

5 aprile – venerdì ore 10 – Comunicazione al Servizio Polizia Postale

Immediata attivazione dei canali di collaborazione di Polizia

L'intero importo è stato quasi interamente bloccato e restituito alla vittima

polizia delle comunicazioni

Grazie per la vostra attenzione