DEFENSIS

ROMA, 25 SETTEMBRE 2017

CYBERSECURITY
E PERIZIE INFORMATICHE

DEFENSIS

GRUPPO ITALIANO 1972

INTELLENET
International Intelligence Network

WAD
World Associations of Detectives

CII
Council of International Investigators

GIDP
Associazione Direttori Risorse Umane

COMPLIANCE / CYBER SECURITY

PERIZIE INFORMATICHE

INVESTIGAZIONI/ DUE DILIGENCE

DEFENSIS

DIGITAL RISK

DEFENSIS

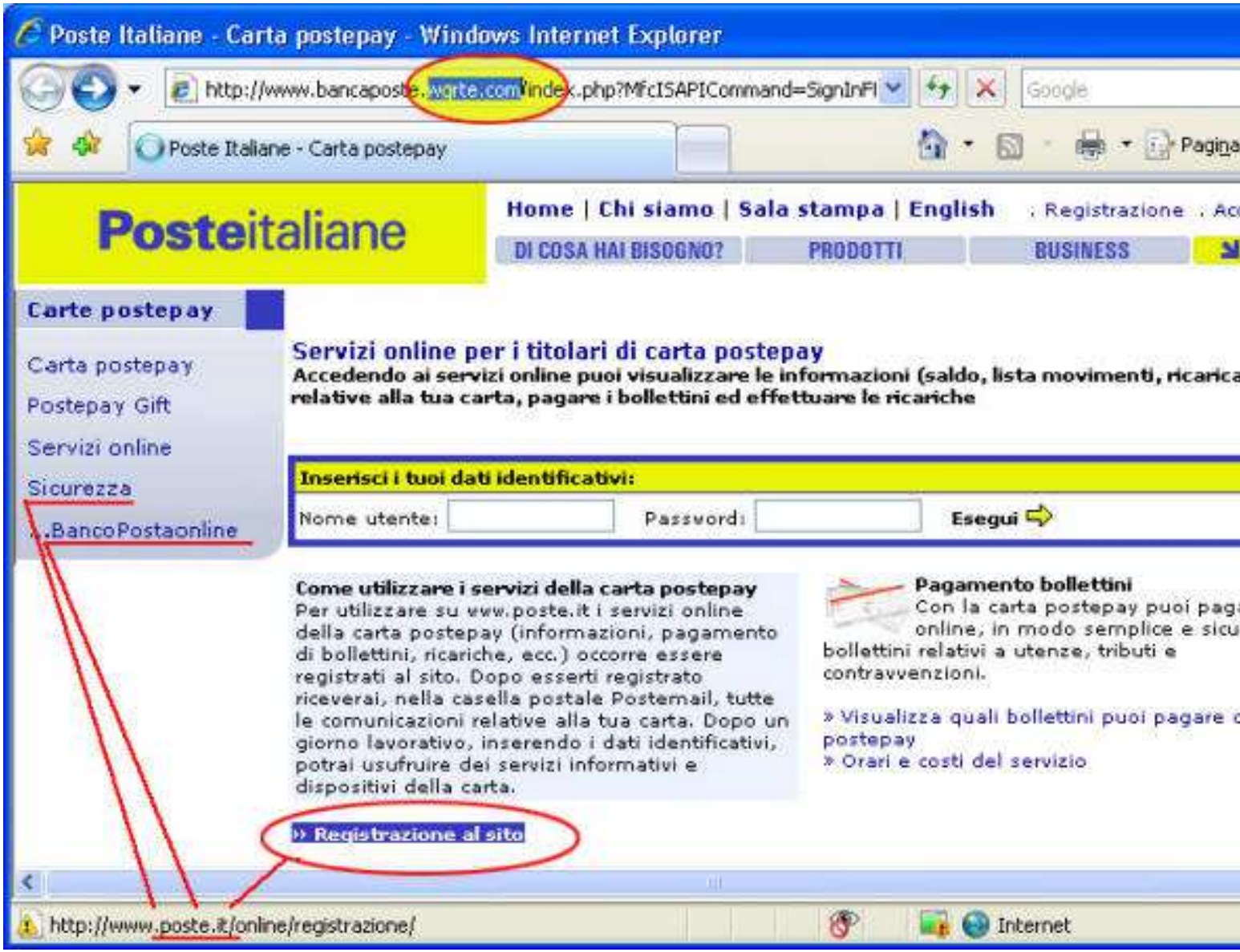
Baiting

USB RUBBER DUCKY DELUXE

$44.99

DEFENSIS

Phishing




oppo
SMARTPHONE
Xiaomi
Smartphone
lenovo
SAMSUNG
ASUS
LG Mobile
nexus

The Washington Post

13/09/2017

In a binding directive, acting homeland security secretary Elaine Duke ordered that federal civilian agencies **identify Kaspersky Lab software** on their networks. After 90 days, unless otherwise directed, they **must remove the software**, on the grounds that the company has **connections to the Russian government** and its software poses a security risk.

30/08/2017

L’APP che consente di scambiare messaggi anonimi, memorizza la rubrica sui propri server

DEFENSIS

393 996 6699

Michele Cogo

GET FULL REPORT

PHONE NUMBER

393 996 6699

Mobile

3 Italia

MICHELE COGO'S SOCIAL NETWORK PROFILES

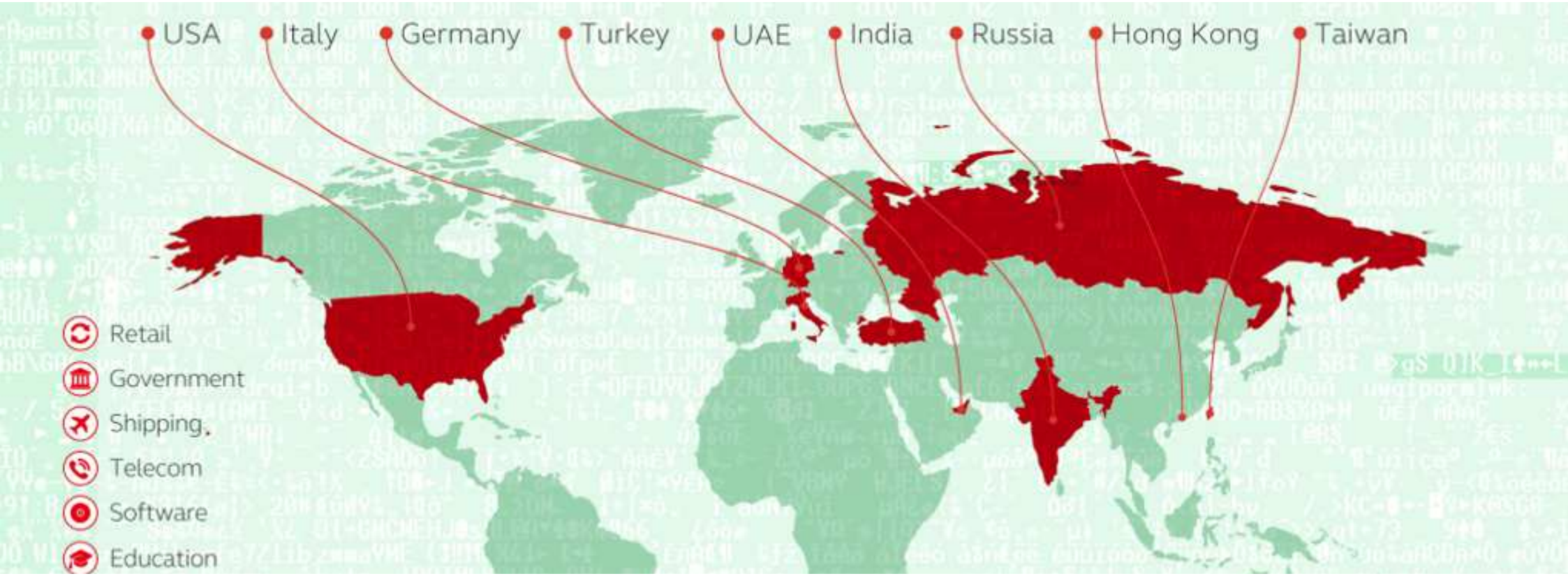
LOCATION

Italy

DEFENSIS

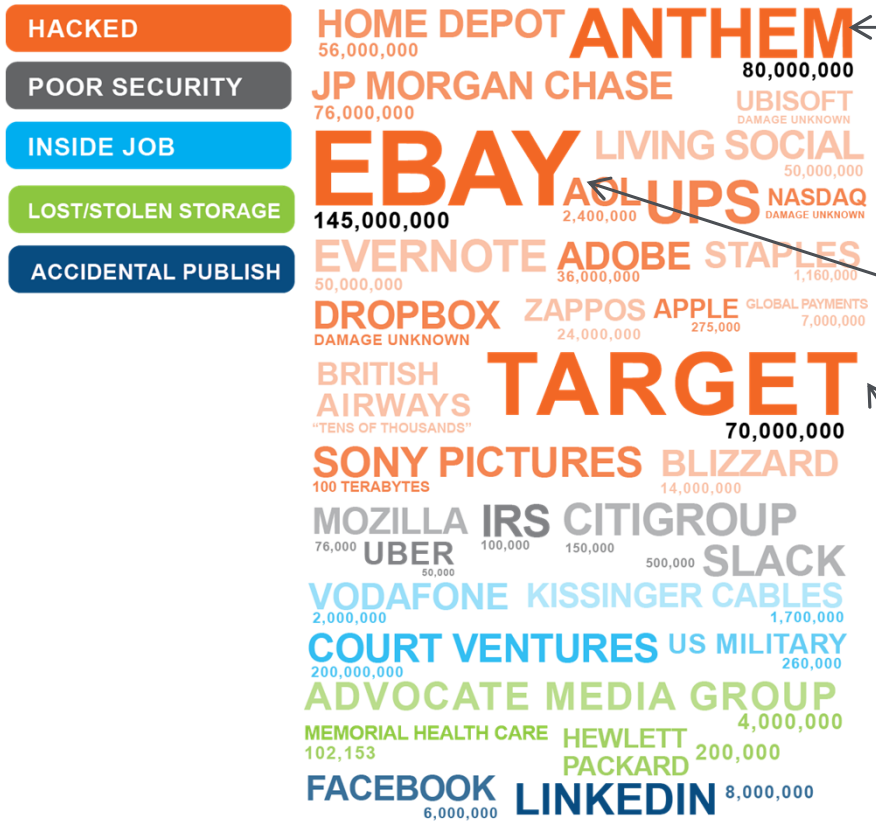
ADWIND: MALWARE-AS-A-SERVICE PLATFORM

68.000 COMPROMISSIONI, 1.800 «CLIENTI»



DEFENSIS

DATA BREACH NOTI



Anthem: Jan 2015

2nd Largest US Health Insurer

Customer PII

Ebay: March 2015

Used employee details to access User Credentials

Target: Summer 2013

$10B drop in market cap (30%)

CEO Terminated

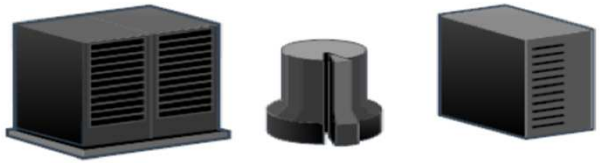
CIO Resigns

DEFENSIS

Perizie Informatiche

L’Informatica Forense è la disciplina che si occupa dell’identificazione, preservazione e «trasformazione» del dato digitale in prova utilizzabile in giudizio.

DEFENSIS



CED Sistemi informativi di grandi e medie aziende

Apparati di comunicazione e di Backup

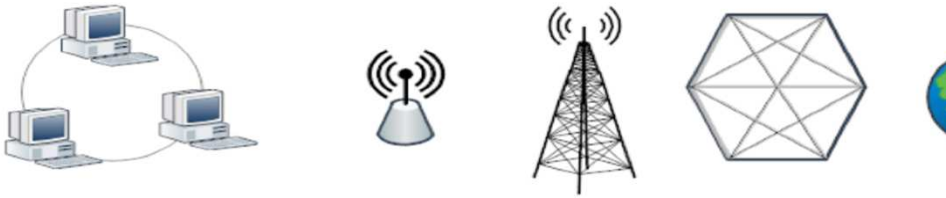
Sistemi di posta elettronica Aziendali e pubblici

Personal Computer e Stazioni di lavoro con diversi S.O.

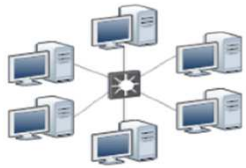
LapTop NetBook, etc

PBX(centralini) VOIP

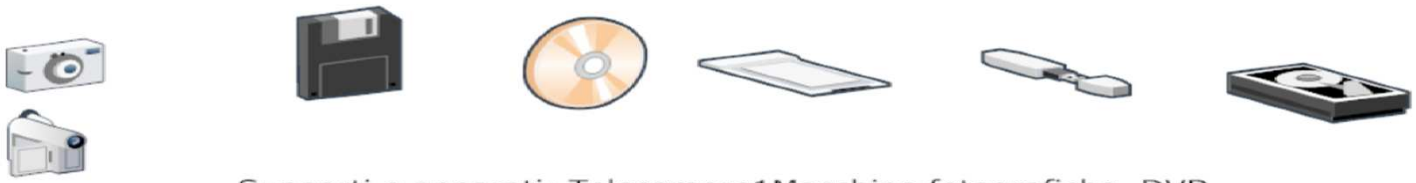
Cellulari, Smartphone, Ipad



Reti locali, Wirelss, Satellitari, Geografiche, Internet



Social Networks e sistemi collaborativi



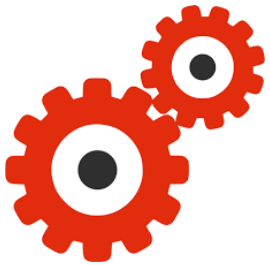
Supporti e apparati: Telecamere1Macchine fotografiche, DVD, supporti magnetici, dischi esterni, PenDrive

DEFENSIS

Intella®

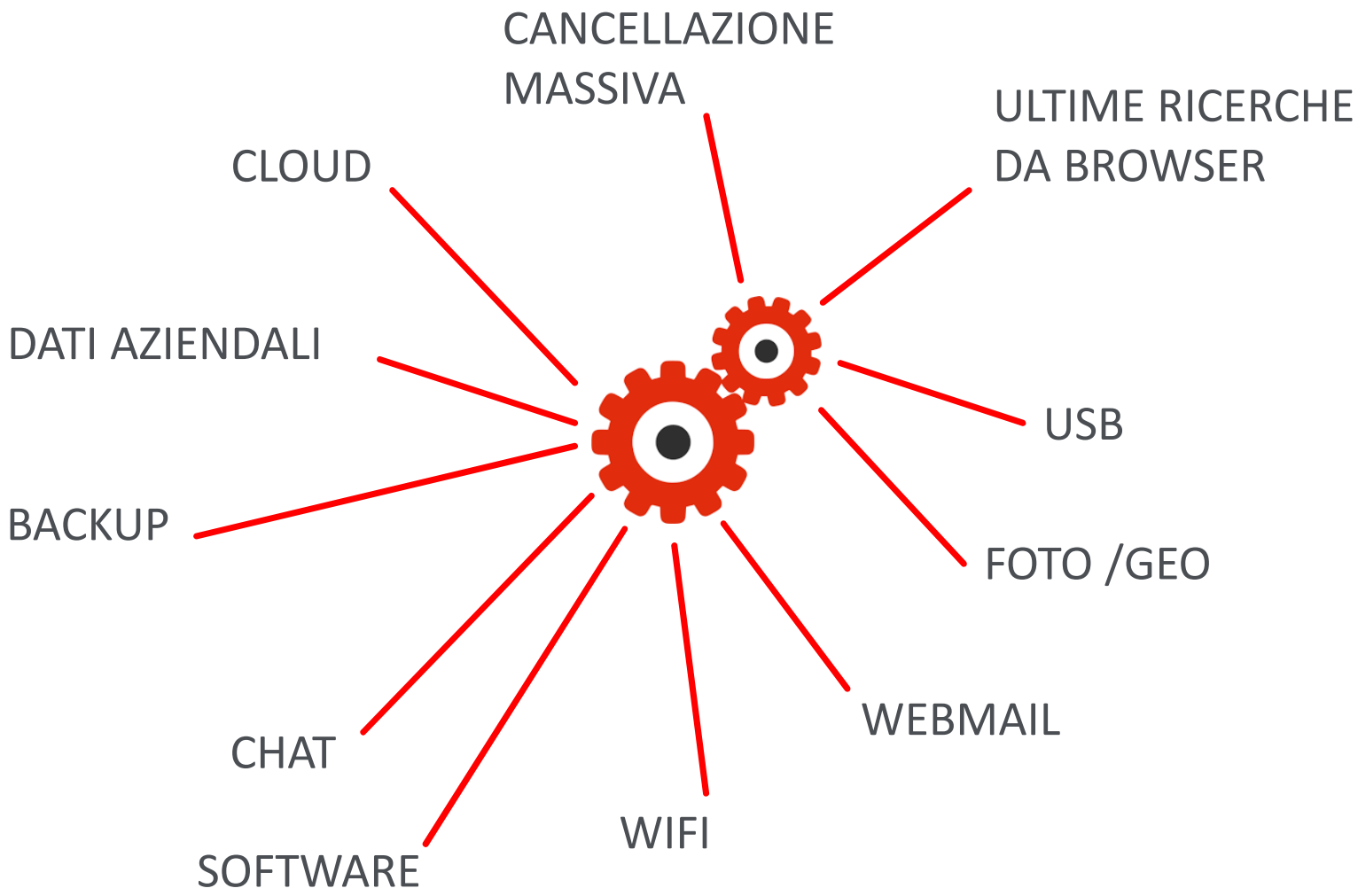
EnCase®

MAGNET FORENSICS®



3-5 ore	3 giorni	15 giorni	5 giorni

DEFENSIS


CANCELLAZIONE MASSIVA
ULTIME RICERCHE DA BROWSER
CLOUD
DATI AZIENDALI
USB
BACKUP
FOTO /GEO
WEBMAIL
CHAT
WIFI
SOFTWARE

DEFENSIS

Cybersecurity

Cerca

Home

Evidence You Can Trust - Targeted computer forensic exa

3°

Francesca Maria Occhionero

Managing Director, Co-founder

Jubilee • Università di Roma La Sapienza

Roma, Italia • 65

Invia messaggio InMail | Collegati

Da circa quindici anni ha ricoperto ruoli direzionali all'interno di diverse soci
amministrazione, occupandosi e maturando quindi esperienza sia nei settori tipicamen

Esperienza

Casa Vacanze

Jubilee

Cerca

Home

Rete

Evidence You Can Trust - Targeted computer forensic exams save yo

3°

Giulio Occhionero

Co-Founder and Managing Director

Westlands Securities • University of Rome, La Sapienza

Altro • 269

Messaggio InMail | Collegati

Investment Banking | Hedge Funds | Quantitative Strategy | Analysis | Development | Research | Mar
committed, focused and professional quant with director experience in stochastic financial modellin

Visualizza altro

Post di Giulio


Polizia di Stato
DELL

DEFENSIS

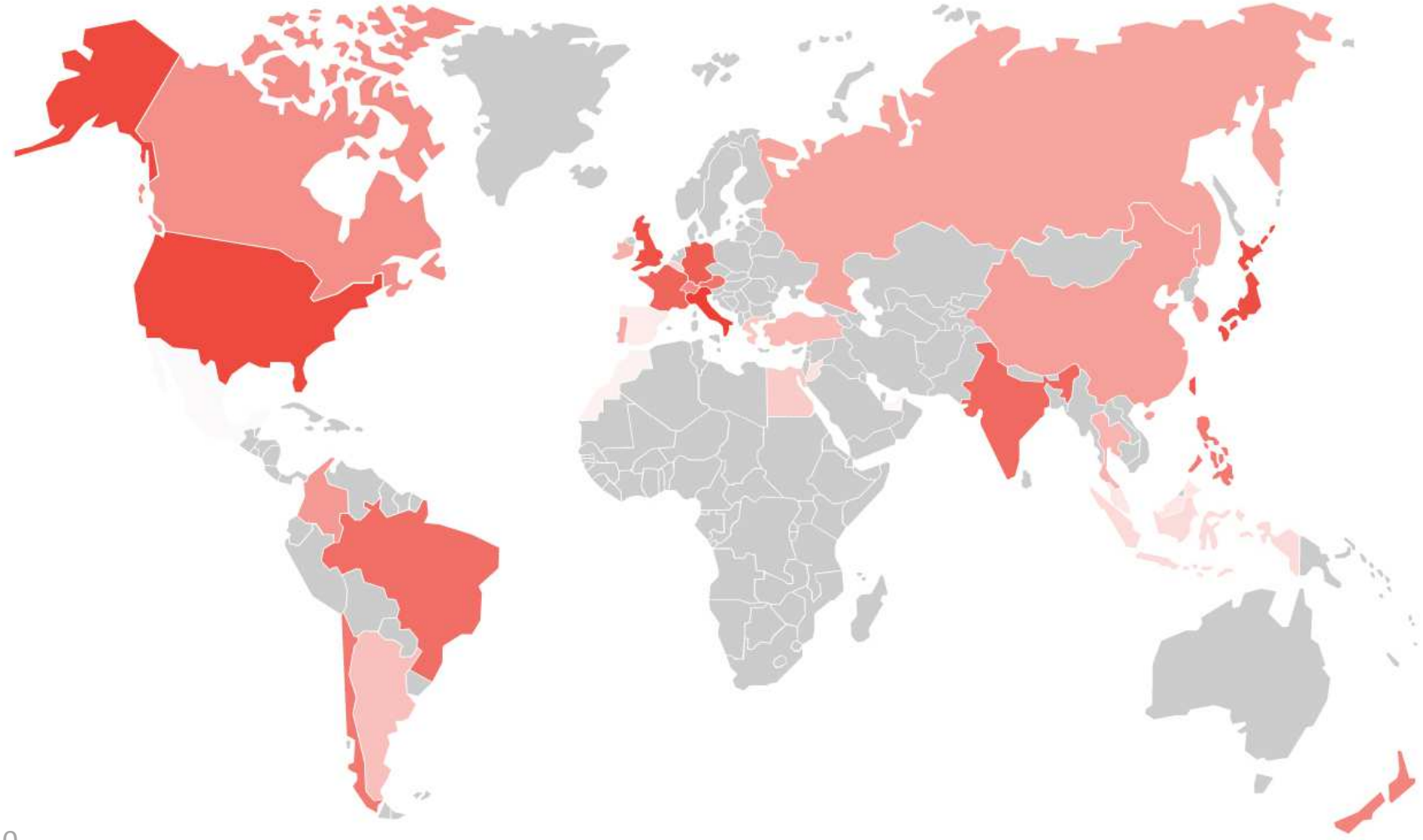
EYE PIRAMID

From: ***Michelangelo Giorgianni***
Subject: R: Re: CONVOCAZIONE]
Time: 2014/01/28 17:28:56]
Attachment: ***Note.zip//sistemi.pdf (…) .exe***

Eye Pyramid	**Altri Malware** (JSRedir-BV, Mal/Dloadr-Y , …)
1,3 – 2 MB	**350k**

DEFENSIS

Diffusione nel mondo



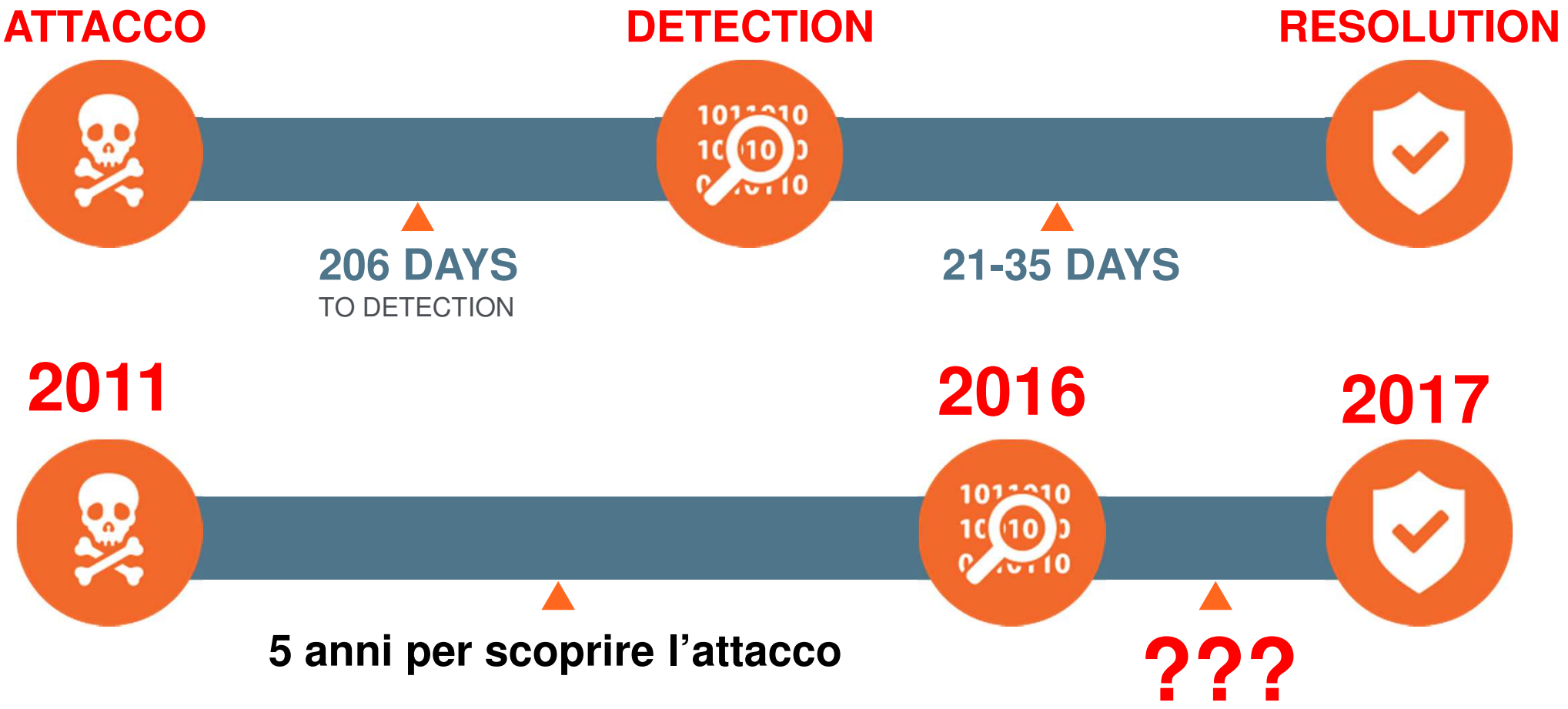
DEFENSIS

18.327 Attaccati
1.793 Compromessi

DEFENSIS


IRS
ESPORTAZIONE USB
Scottrade
MILIONI DI RECORD
Costo Attacchi
$500M
ALL'ANNO
Ponemon Institute 2016
ASHLEY MADISON
ESTORSIONE DI MASSA
FDIC
HACKER CINESI
YAHOO!
MILIONI DI ACCOUNT
12 M
/ anno in prevenzione
PERIMETRO AZIENDALE
CLOUD
RAT
ANTIVIRUS
Bloccano il 99% degli attacchi
Stimato
1%
ENTRA
SECURITY FORENSIC
RANSOMWARE & PHISHING
USB
IOT
VARIANTI MALWARE
DECINE DI MIGLIAIA
Attacchi al giorno

DEFENSIS


ATTACCO
DETECTION
RESOLUTION
206 DAYS
TO DETECTION
21-35 DAYS
2011
2016
2017
5 anni per scoprire l'attacco
???

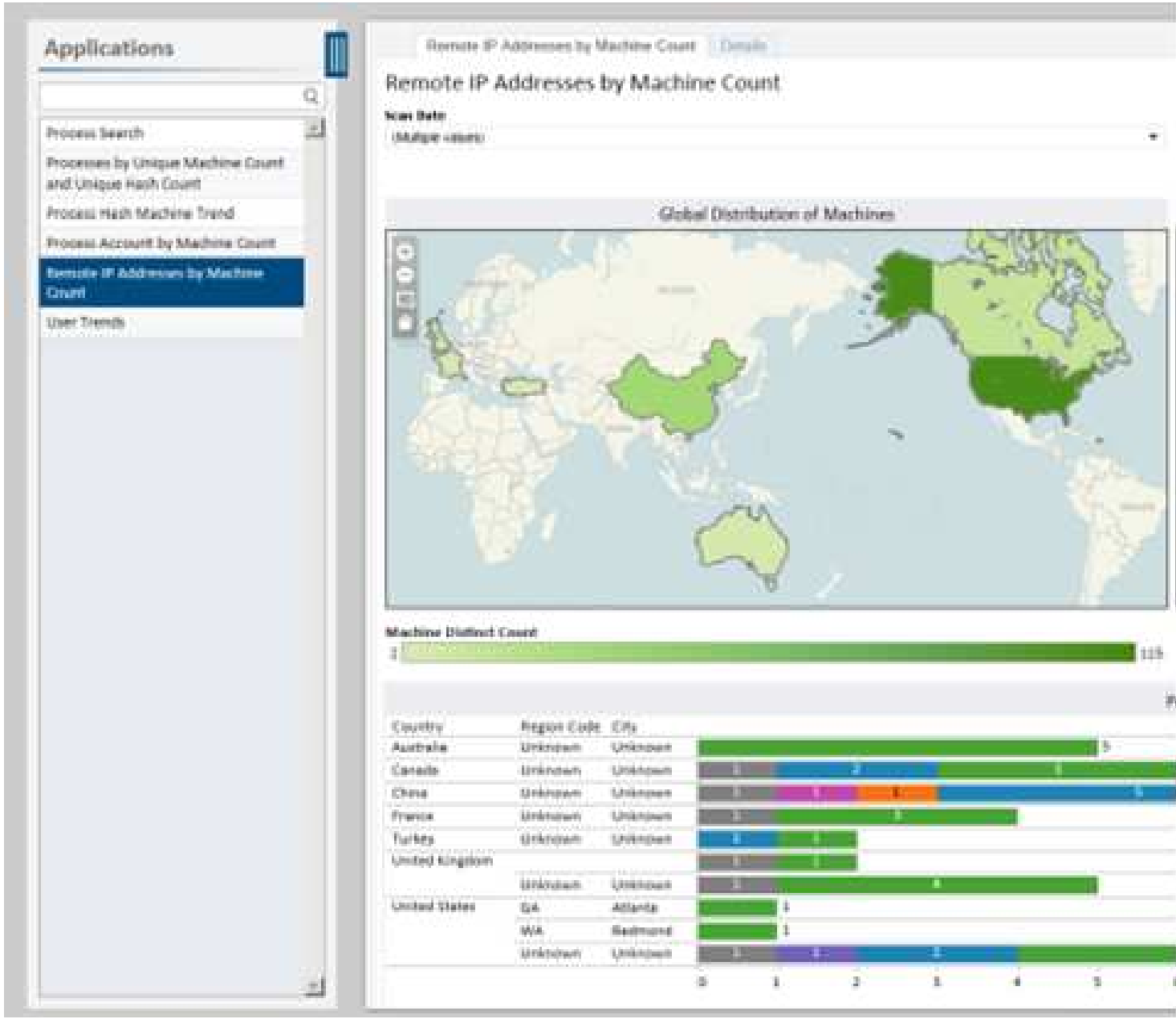
DEFENSIS

THREAT DETECTION

CONNESSIONI ANOMALE

CORRELAZIONE TRA APPLICAZIONI

RICERCA IOC



POS / SCADA / ATM

DEFENSIS

CASE STUDY

FURTO DI INFORMAZIONI RISERVATE

Ente Pubblico scopre furto di dati dalla rete interna

- Lista di 226 keywords dai documenti trafugati
- Ricerca su 1.700 PC/SERVER, 80GB di PST e 10 TB di file nella rete aziendale
- In 4 settimane, 70 PC/SERVER si sono scoperte contenere materiale non autorizzato
- 7% falsi positivi
- Ogni macchina é stata verificata in circa 1 ora

GRAZIE

MICHELE COGO

DEFENSIS
MICHELE.COGO@DEFENSIS.IT