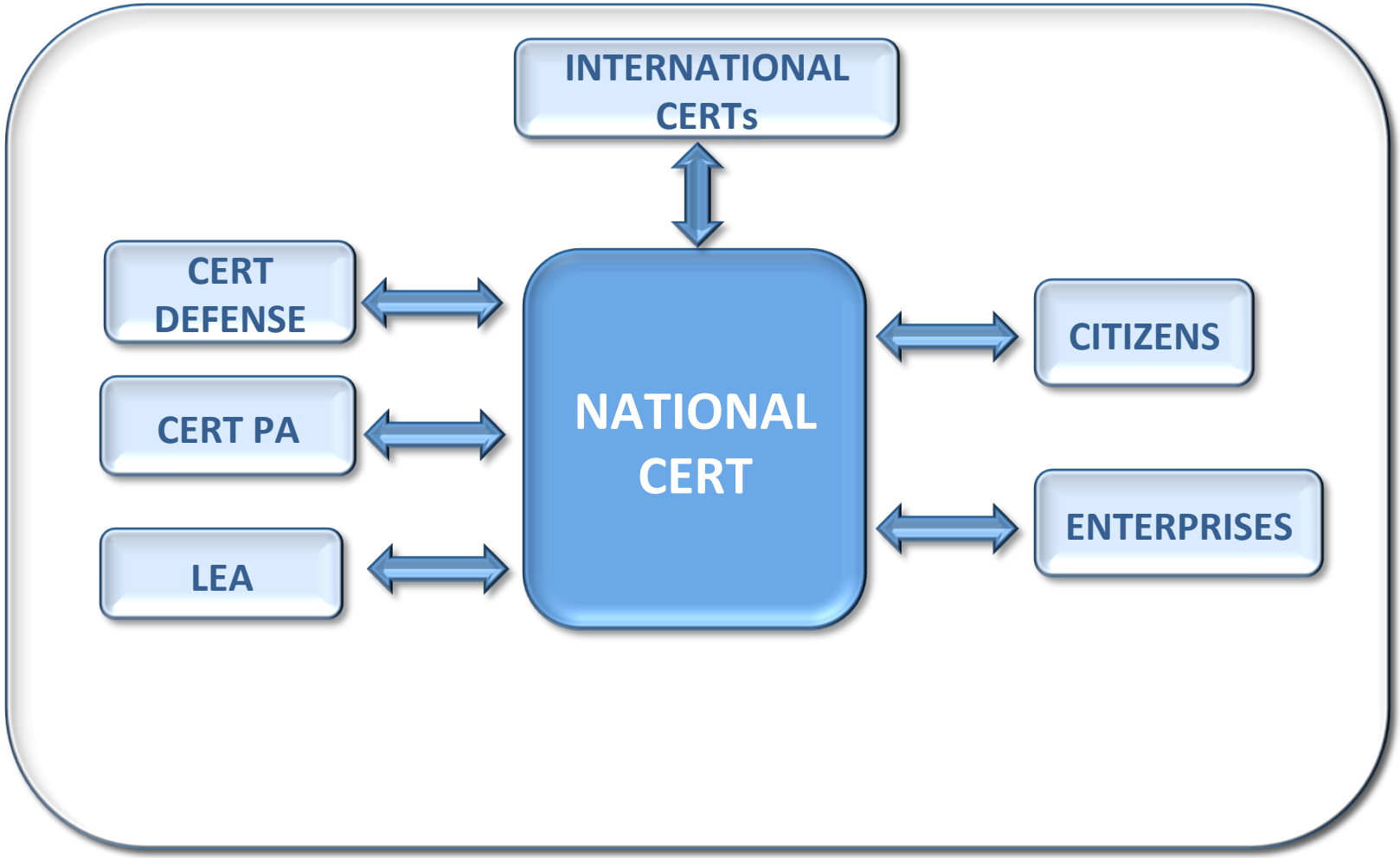
The Italian National CERT: Case Studies in the Operational Activities

BANCHE E SICUREZZA 2015
ROMA, 4 giugno 2015

SOMMARIO

- Attività Generali
- Casi di Studio
- Conclusioni

CERT's RELATIONSHIPS



Activities of the National CERT

Reaction Activities

response to cyber incidents	Coordination of all actors involved and support in response to cyber incidents having national and transnational impact

Prevention Activities

Situational Awareness	Early notification of threats and vulnerabilities, possible mitigation measures, warnings for probable and / or imminent cyber attacks, information and studies about, guidelines and best practices, attack scenarios, preventive actions and mitigation
Guidelines	Definition and dissemination of guidelines and standards for the proper management and prevention of cyber incidents
Education / Awareness	Specialized training in safety, training and awareness-raising campaigns aimed at citizens in order to raise awareness on the issues of computer security.
International Cooperation	Participation in international working groups in the field of prevention and response to cyber incidents

Web site
https://www.certnazionale.it

CERT nazionale Italia

COMPUTER EMERGENCY RESPONSE TEAM

MINISTERO DELLO SVILUPPO ECONOMICO

Link Utili FAQ Glossario

Home Chi siamo News Bollettini Document Contatti Ricerca:

General interest news

CTB-Locker si evolve e si lega ad attività di phishing

Alcuni ricercatori di Trend Micro hanno riportato in un post evidenze di una nuova ondata della diffusione del noto ransomware CTB-Locker che utilizza come esche Email che sembrano provenire da Google Chrome o Facebook. In particolare, l'Email relativa a [leggi tutto]

CTB-Locker phishing ransomware venerdì, 13 febbraio 2015

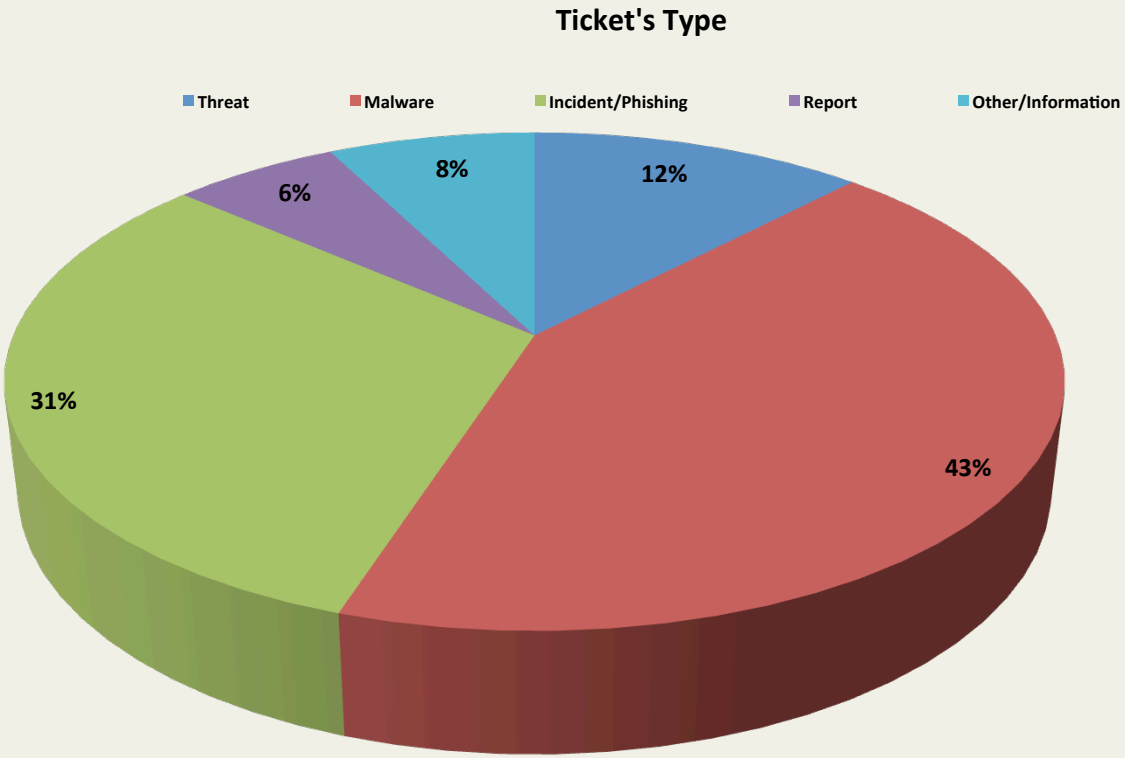
Documents (guidelines etc.)

Contacts (PGP key, RFC-2350 etc)

Techincal bulletins

Descrizione	Gravità (CVSSv2)	Data prima emissione
BOLLETTINO CERT - N 141016.01 VULNERABILITÀ DI SSL 3.0 "POODLE"	4.3	14 ottobre 2014
BOLLETTINO CERT - N 141010.01 VULNERABILITÀ GNU BASH (SHELLSHOCK)	10	10 ottobre 2014
BOLLETTINO CERT - N 140610.01 VULNERABILITÀ OPENSSL	6.8	10 giugno 2014

Tipi di Ticket



Segnalazioni

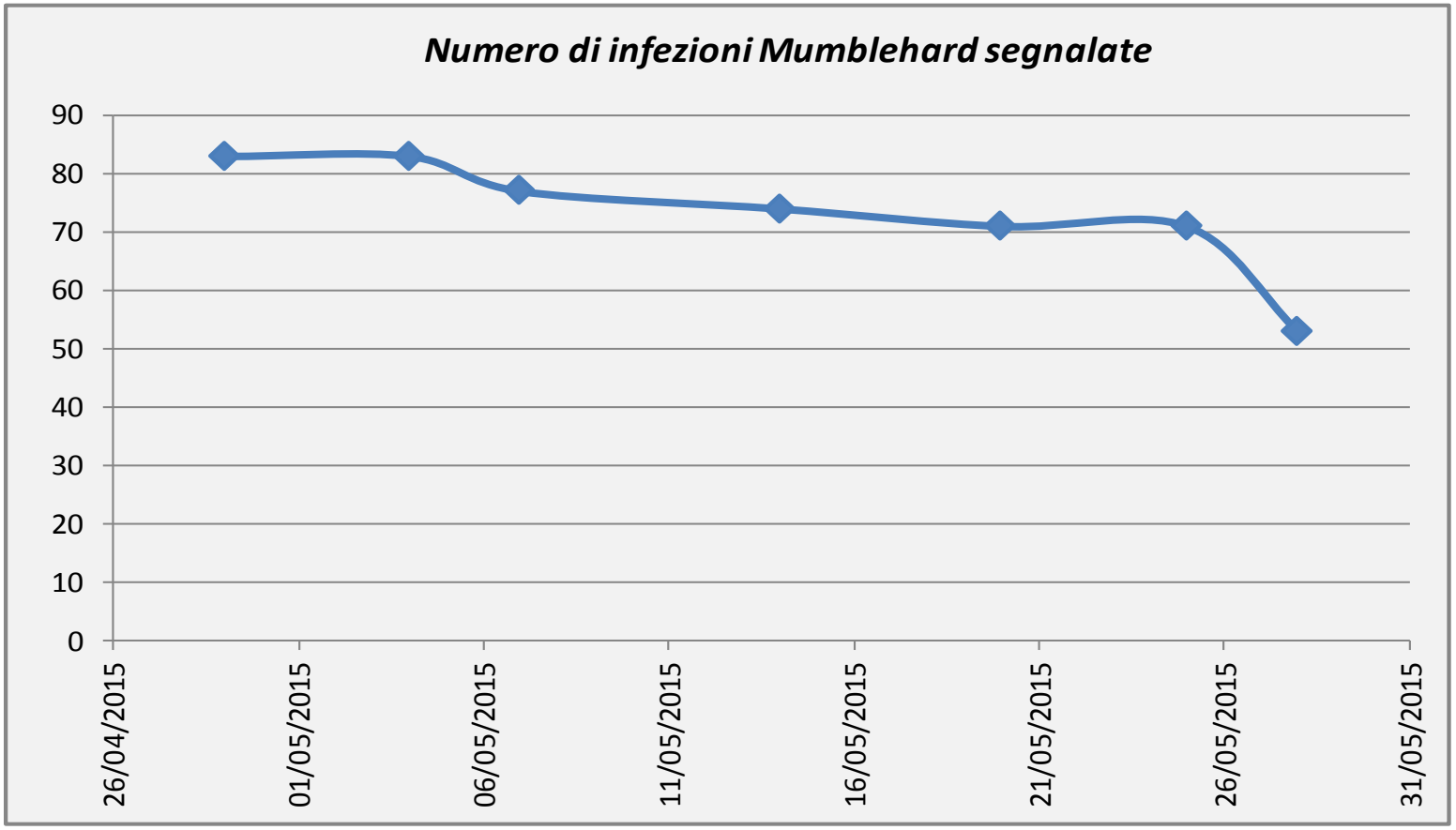
- **Segnalazioni periodiche**

  ACDC – CIMBL - Ebury - Fast Flux -
  Mumblehard - Ramnit - Shadowserver Report

- **Altri tipi**

  Leak - Malware/Compromissioni
  DDoS - Phishing - Vulnerabilità

Mumblehard


Numero di infezioni Mumblehard segnalate
90
80
70
60
50
40
30
20
10
0
26/04/2015
01/05/2015
06/05/2015
11/05/2015
16/05/2015
21/05/2015
26/05/2015
31/05/2015

Campagne Informative

- ***Compromised Website***, con oltre **4.500 eventi** notificati a circa **60 ISP**
- ***Sandbox URL***, con circa **540 eventi** notificati a **17 ISP**
- **DDoS *reflection/amplification***

  - **QOTD** (*Quote Of The Day*): **90 macchine** afferenti a **26 ISP**)
  - **Chargen** (*Character Generator Protocol*) : circa **830 macchine** afferenti a **40 ISP**)

CONCLUSIONI

- Importanza di una collaborazione intersettoriale
- Incremento dello scambio informazioni e coordinamento nella risposta agli incidenti

GRAZIE PER L'ATTENZIONE

direttore.Iscom@mise.gov.it

CERT Nazionale Italia
cert@mise.gov.it
https://www.certnazionale.it

CERT nazionale Italia