



# 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

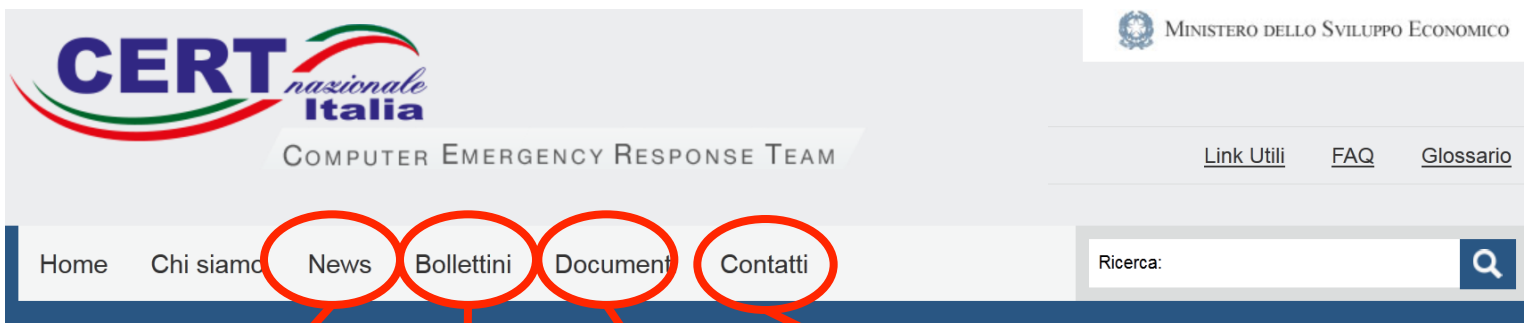
Specialized training in safety, training and awareness-raising campaigns aimed at citizens in order to raise awareness on the issues of computer security.

#### International Cooperation

Participation in international working groups in the field of prevention and response to cyber incidents



## Web site <https://www.certnazionale.it>



### 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

**Contacts**  
(PGP key, RFC-2350 etc)

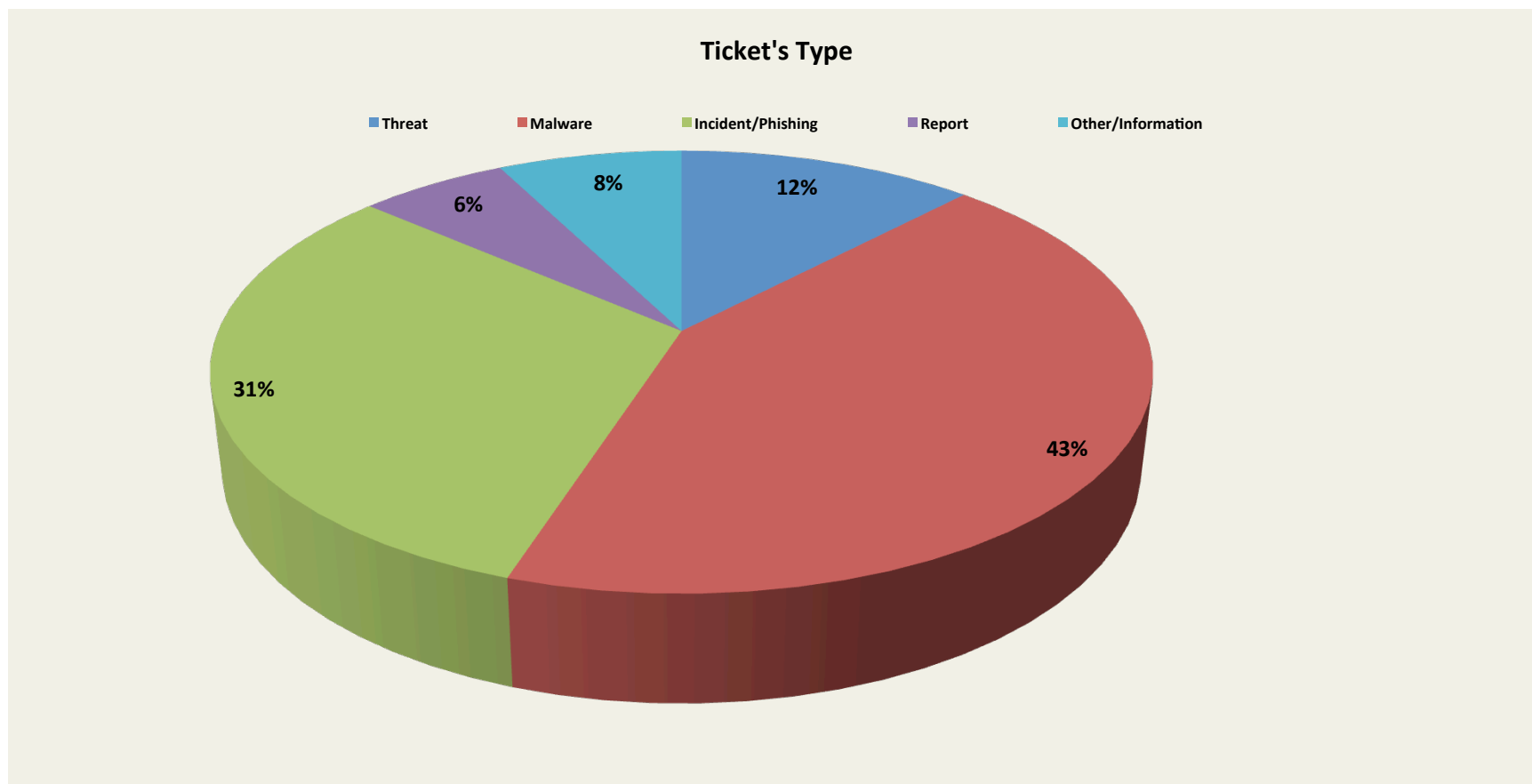
**Documents**  
(guidelines etc.)

### Technical 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 OPENSLL	6.8	10 giugno 2014



# Tipi di Ticket





## *Segnalazioni*

### Segnalazioni periodiche

ACDC – CIMBL - Ebury

- Fast Flux -

Mumblehard - Ramnit

- Shadowserver Report

### Altri tipi

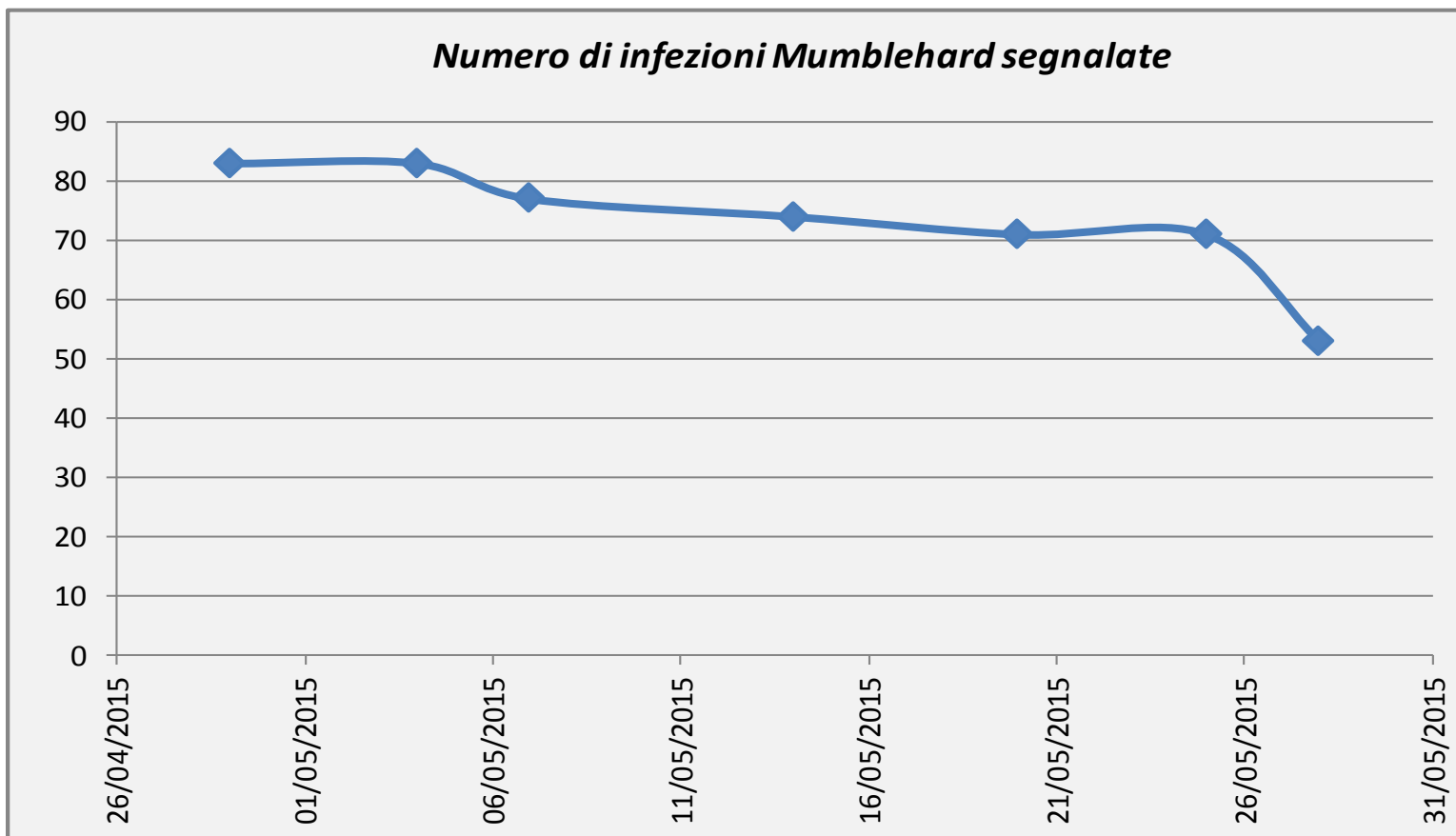
Leak - Malware/Compromissioni

DDoS - Phishing - Vulnerabilità



# Mumblehard

*Numero di infezioni Mumblehard segnalate*







## *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**



**Benvenuti nel sito dell'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione (ISCOM)**  
L'Istituto opera nell'ambito del Ministero dello Sviluppo Economico in qualità di organo tecnico-scientifico. La sua attività, rivolta specificatamente verso le aziende operanti nel settore ITC, le Amministrazioni pubbliche e l'utenza, riguarda fundamentalmente la normazione, la sperimentazione e la ricerca di base e applicata, la formazione e l'istruzione specializzata nel campo delle telecomunicazioni. [Leggi tutto...](#)

#### In Evidenza

[archivio »](#)

#### News

##### SPECIFICHE TECNICHE DI INTERCONNESSIONE

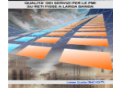
L'ISCOM, in collaborazione con altri Organi di questo Ministero e con la partecipazione di Operatori e Costruttori nel campo delle TLC, ha definito le Specifiche Tecniche di interconnessione tra reti di telecomunicazioni di Gestori diversi e altre Specifiche Tecniche utili a definire aspetti delle TLC non coperti da norme nazionali o internazionali.  
[Maggiori informazioni sulle Specifiche Tecniche...](#)

##### NUMERAZIONE NAZIONALE

L'ISCOM è dotato di una Sala di Numerazione Nazionale, all'interno

##### NUOVA PUBBLICAZIONE: LINEE GUI SERVIZI PER LE PMI SU RETI FISSE

La pubblicazione si propone di semplificare i processi utili all'individuazione del servizio di connettività (PMI) - offerta (Operatore).  
[Leggi tutto...](#)



**CERT Nazionale Italia**

[cert@mise.gov.it](mailto:cert@mise.gov.it)

<https://www.certnazionale.it>

# GRAZIE PER L'ATTENZIONE

[direttore.iscom@mise.gov.it](mailto:direttore.iscom@mise.gov.it)

