Consortium GARR

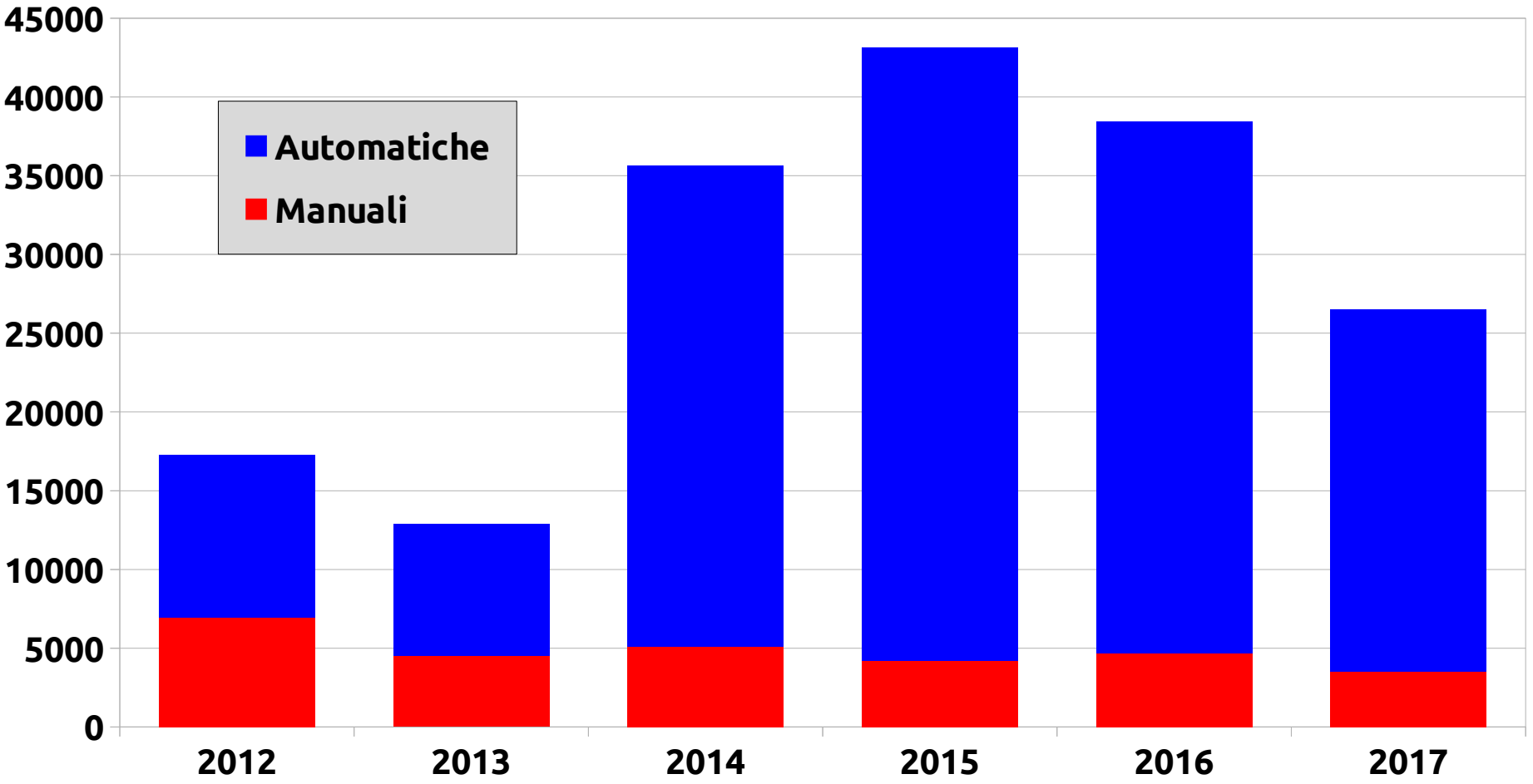
GARR-CERT: un aggiornamento

Roberto Cecchini & Simona Venuti

Workshop GARR 2017
Roma, 5-7 Aprile

Consortium GARR

Segnalazioni



Tendenze (2016)

- Violazione copyright (2884, 60%): leggero aumento
- spam (587): leggero calo
  - credenziali via **phishing** o brute force
- DoS e DRDoS (423): stazionari
  - rilevazione via GINS DoS Monitor
- Servizi web (120): in crescita
  - principalmente CMS (Wordpress per primo)

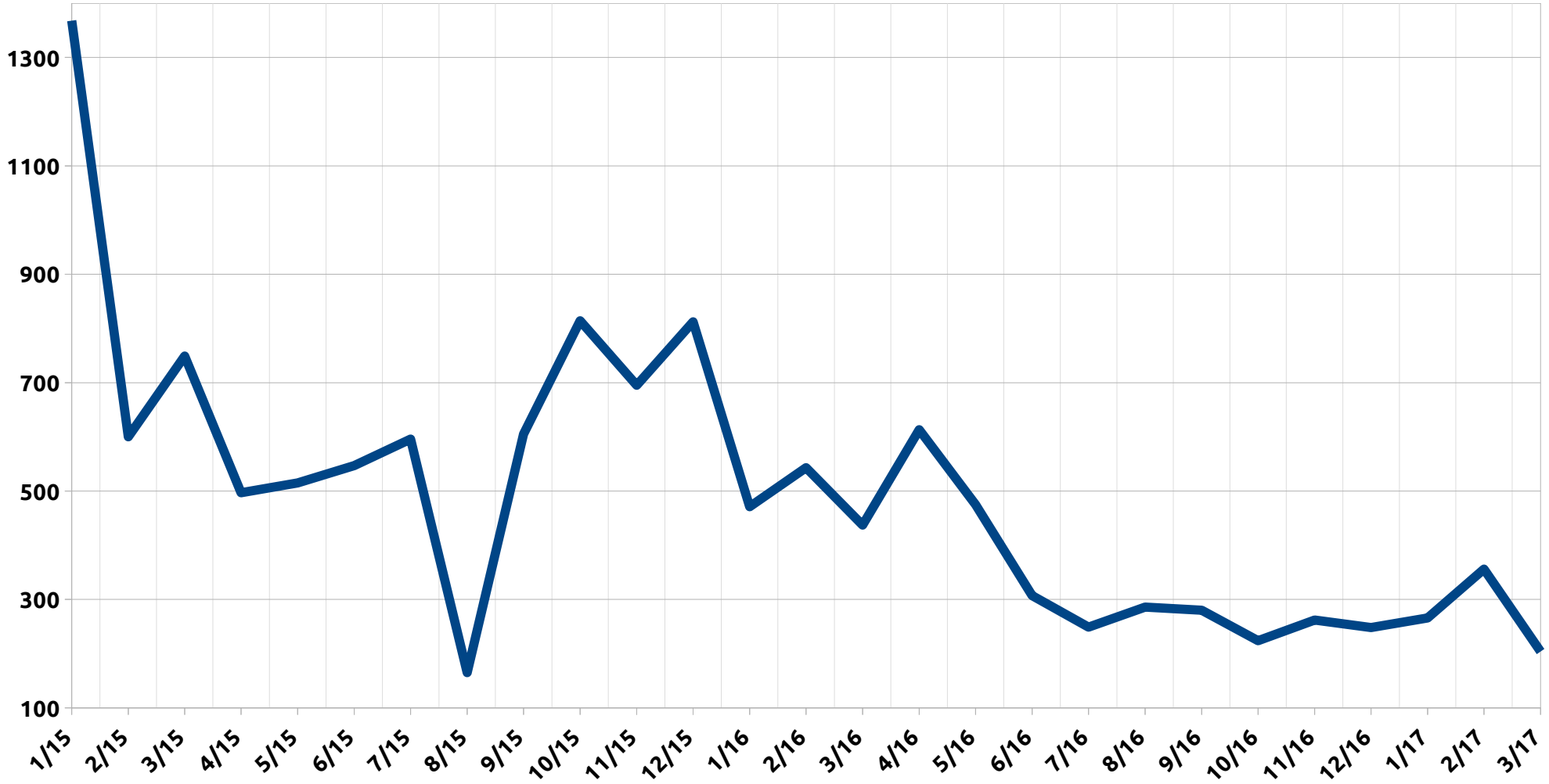
Segnalazioni automatiche: tipologia 1/2

- Soggetto del tipo: **`GARR-CERT-A...`**
- La macchina **potrebbe** essere usata per attacchi DRDoS
  - Character Generator Protocol (**cq**);
  - Domain Name System (**dns**);
  - Network Time Protocol (**ntp** & **ntpmon**);
  - MS-SQL Server resolution service (**mssql**);
  - Simple Network Management Protocol (**snmp**);
  - Simple Service Discovery Protocol (**ssdp**);
  - X Display Manager (**xdmcp**).

Segnalazioni automatiche: tipologia 2/2

- La macchina **potrebbe** essere infetta
- La macchina **potrebbe** esporre dati
  - Mongo DB (**mongo**)
  - Intelligent Platform Management Interface (**ipmi**)
- La macchina è stata inserita in una o più blacklist (**BL**)
- RDP mal configurato? [a richiesta]

Segnalazioni automatiche spedite



GARR Certification Service

- TCS:
  - Multi-Domain SSL
  - EV Multi-Domain
  - Digital Signature Plus
  - Email Security Plus
  - Premium
  - Grid Premium
  - Grid Robot
  - Grid Host Multi-Domain SSL
  - Code Signing
  - EV Code Signing

Gruppi di lavoro

- Istituiti al WS 2016
  - **Contrasto ai DDoS**: Nino Ciurleo
  - **Network auditing**: Ermann Ripepi
  - **Best practice sicurezza**: Marco Pirovano
  - **802.1x wired**: Valentino Gratton
- Altre proposte:
  - Analisi malware
  - Contrasto al phishing