THE ITALIAN RESEARCH & EDUCATION NETWORK

Consortium GARR

DDoS e dintorni

Roberto Cecchini

Workshop GARR 2014, Roma, 2-4 Dicembre

Incidenti: spam

- Si mantiene ad un livello costante
- La tecnica principale è il furto di credenziali via campagne di *phishing*
  - i mailer ufficiali finiscono nelle blacklist
- Gli APM sono rapidi nel rilevare e bloccare gli account compromessi.

Incidenti: probe & brute force

- Molto in calo i probe verso porte Windows (135-138 e 445). Attualmente (in ordine di frequenza):
  - 22 (ssh)
  - 80 (http)
  - 8080
  - 21 (ftp)
  - 3389 (rdp)
  - 23 (telnet)
- Brute force
  - principalmente **ssh**, ma anche qualche **IMAP/POP3**, servizi web/CMS (**Wordpress** e **phpMyAdmin**) e **ftp**

Incidenti: D(R)DoS

- La ricerca di nodi sfruttabili è continua
- Si usano dispositivi che non corrispondono al concetto classico di “nodo infetto” che ha l'utente medio (ma anche alcuni admin)
  - marcatempo, NAS, Access Point, stampanti, fotocopiatrici, sistemi di webconferencing (Aethra)

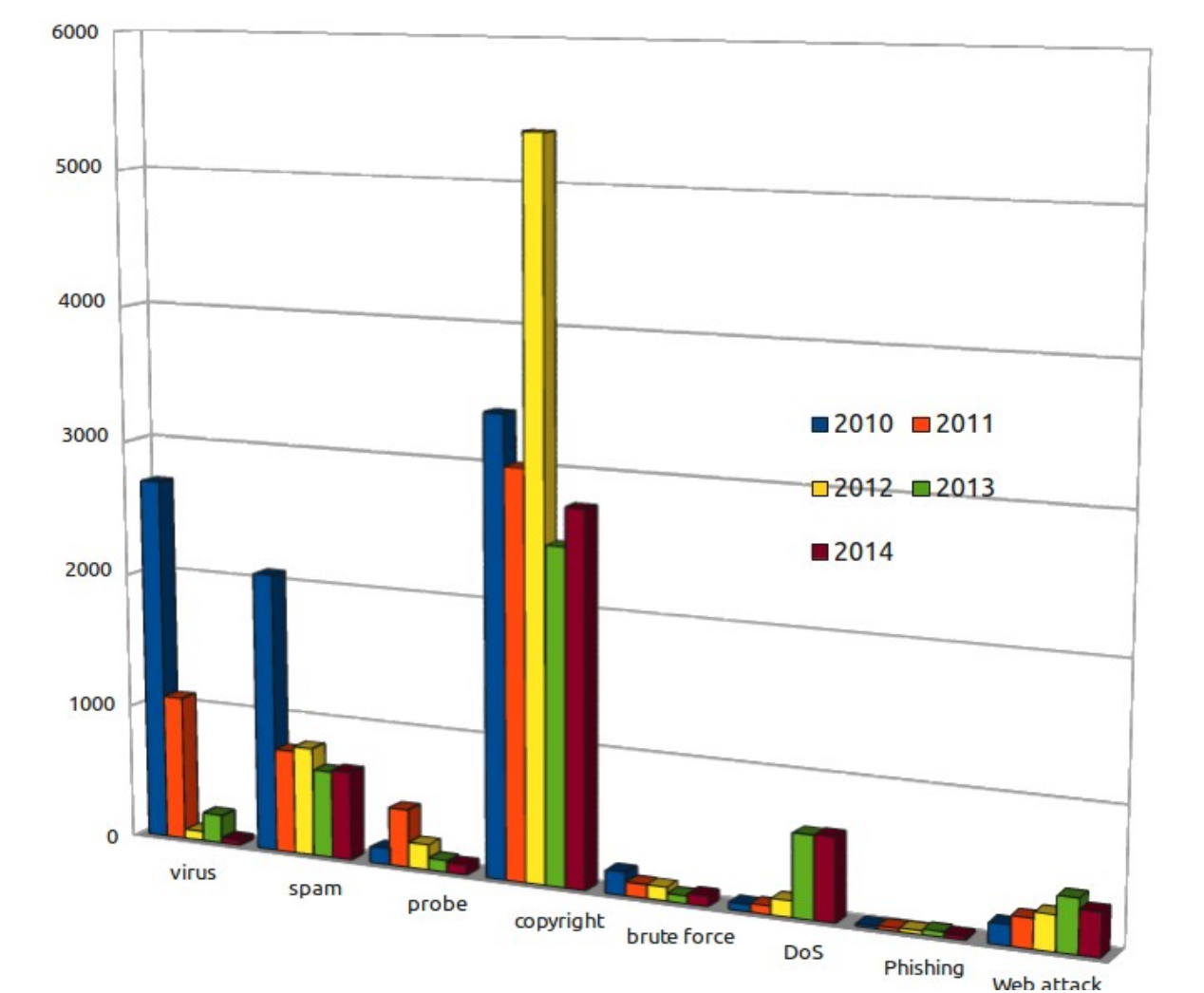
Incidenti: siti web

- Quasi tutte le compromissioni di siti web sfruttano vecchie installazioni di CMS (Joomla, Drupal, Wordpress o altri) o **plug-in**
  - La mancanza di aggiornamenti li porta nel giro di poco più di un anno ad essere facilmente attaccabili
- Da un'analisi a campione di Dario Vettore su 130 siti:
  - PHP: 35%
  - CMS: 15%
  - Apache: 73%

Joomla: un esempio

CMS Version	Available	Support		End of Life	Upgrade Type	Notes	Latest Release
		Bugs	Security				
1.5	✗	✗	✗	Sept 2012	Migration to 2.5	Plan to migrate to 2.5 now Joomla 1.5 version history	**EOL** at 1.5.26
1.6	✗	✗	✗	Aug 2011	One-click to 2.5	Upgrade to 2.5 now Joomla 1.6 version history	1.6.6
1.7	✗	✗	✗	Feb 2012	One-click to 2.5	Upgrade to 2.5 now Joomla 1.7 version history	1.7.5
2.5	✓	✓	✓	December 31st, 2014	One-click core to 3.x	Start planning for an upgrade to 3.3.6 Joomla 2.5 version history	**2.5.27**
3.0	✗	✗	✗	May 2013	One-click to 3.1	You should use the one click upgrade Joomla 3.0 version history	3.0.4
3.1	✗	✗	✗	Dec 2013	One-click to 3.2	You should use the one click upgrade Joomla 3.1 version history	3.1.6
3.2	✗	✗	✗	Oct 2014[1]	One-click to 3.3	You should upgrade your server's PHP to 5.3.10 or greater and upgrade to 3.3 Joomla 3.2 version history	3.2.7
3.3	✓	✓	✓	3.4 release	One-click	Recommended for all new installs Joomla 3.3 version history	**3.3.6**
3.4[2]	Nov 2014[2][3]	-	-	3.5 release	One-click		
3.5[2]	Jan 2015[2][3]	-	-	3.6 release	One-click		

Statistiche incidenti



Andamento DDoS

- A settembre 2014
  - 133 attacchi > 100 Gbps; 22 in Q3
  - forte aumento **ssdp**: 42% > 10 Gbps in Settembre
  - **ntp** in 50% > 100Gbps in Q3
  - 16.5% > 1 Gbps in Q3 (15.3% in Q2)
- Attacco medio in Q3: **859 Mbps**; massimo **264.6 Gbps**

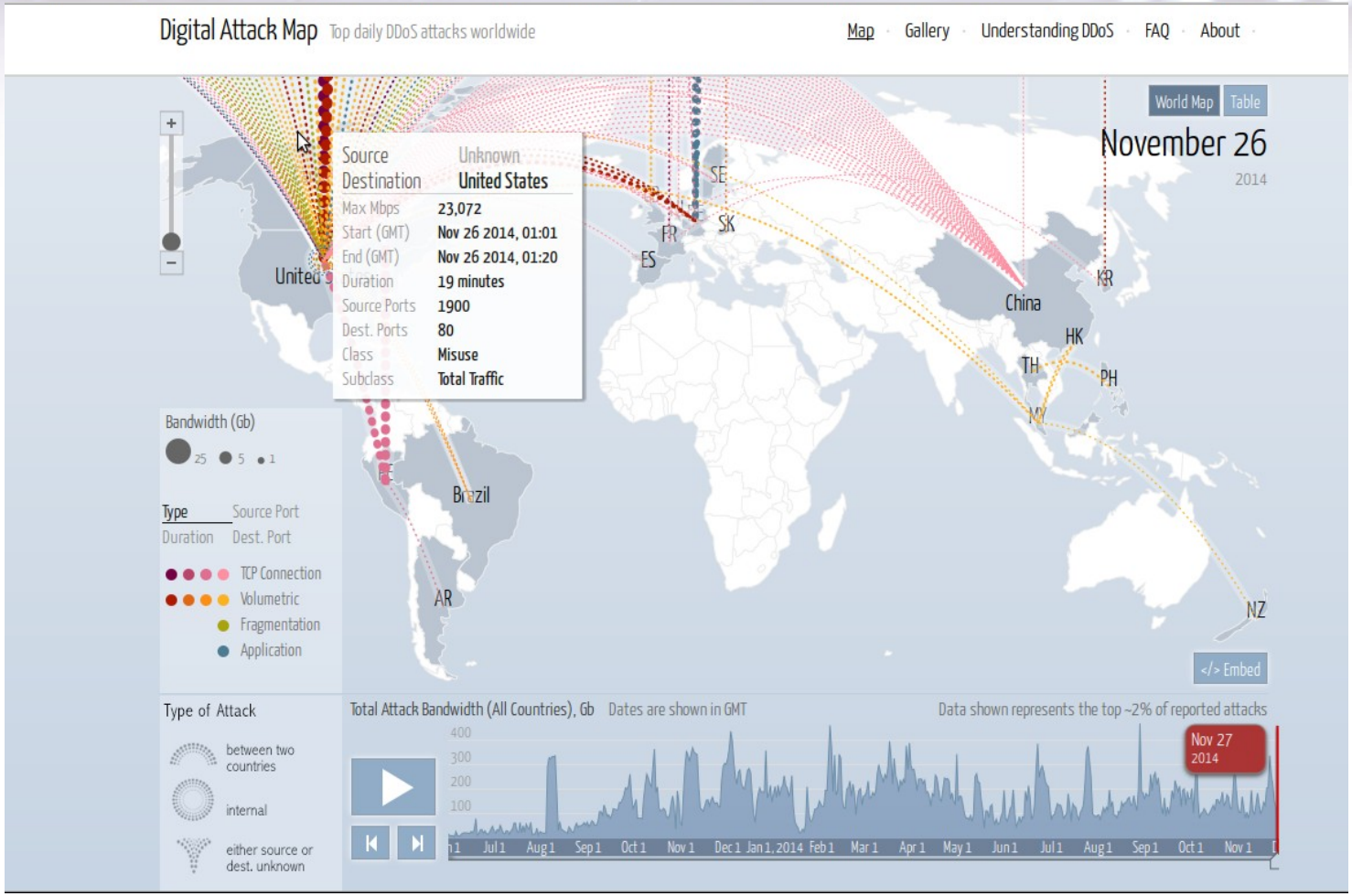
DRDoS: fattori di amplificazione

Protocol	BAF *all*	BAF 50%	BAF 10%	PAF *all*	Scenario
SNMP v2	6.3	8.6	11.3	1.00	*GetBulk* request
NTP	556.9	1083.2	4670.0	3.84	Request client statistics
DNS_{NS}	54.6	76.7	98.3	2.08	ANY lookup at author. NS
DNS_{OR}	28.7	41.2	64.1	1.32	ANY lookup at open resolv.
NetBios	3.8	4.5	4.9	1.00	Name resolution
SSDP	30.8	40.4	75.9	9.92	*SEARCH* request
CharGen	358.8	n/a	n/a	1.00	Character generation request
QOTD	140.3	n/a	n/a	1.00	Quote request
BitTorrent	3.8	5.3	10.3	1.58	File search
Kad	16.3	21.5	22.7	1.00	Peer list exchange
Quake 3	63.9	74.9	82.8	1.01	Server info exchange
Steam	5.5	6.9	14.7	1.12	Server info exchange
ZAv2	36.0	36.6	41.1	1.02	Peer list and cmd exchange
Sality	37.3	37.9	38.4	1.00	URL list exchange
Gameover	45.4	45.9	46.2	5.39	Peer and proxy exchange

TABLE III: Bandwidth amplifier factors per protocols. *all* shows the average BAF of all amplifiers, 50% and 10% show the average BAF when using the worst 50% or 10% of the amplifiers, respectively.

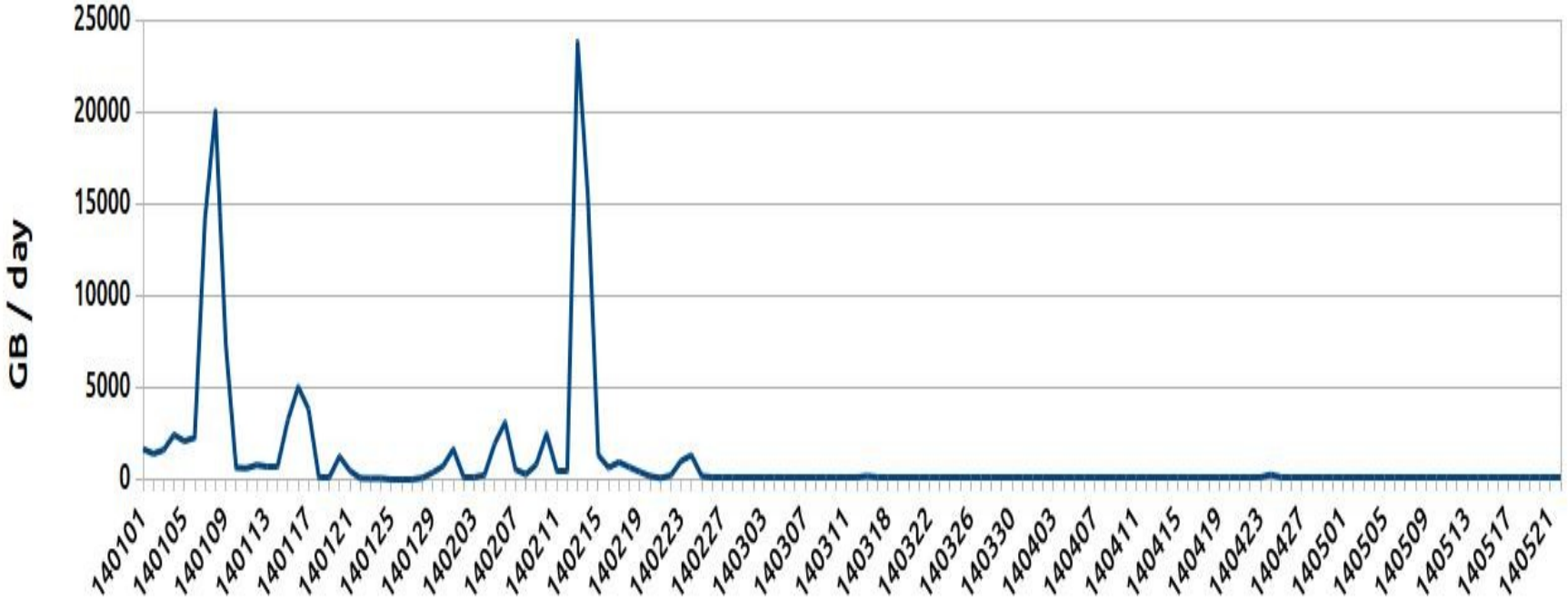
Christian Rossow, *Amplification Hell: Revisiting Network Protocols for DDoS Abuse*, v.gd/Z55h7y

I DDoS nel mondo



www.digitalattackmap.com/#anim=1&color=0&country=ALL&time=16400&view=map

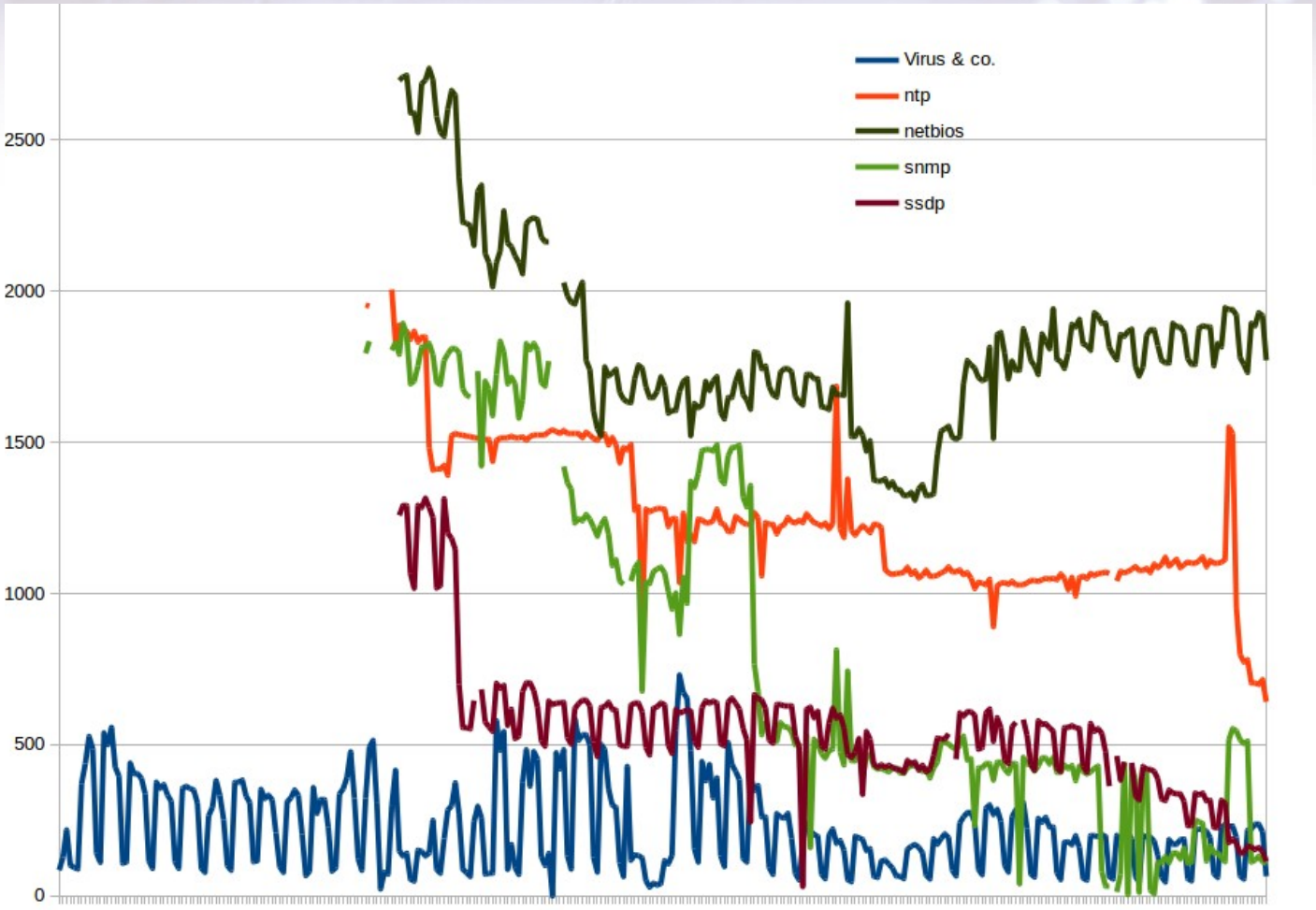
I nostri momenti di gloria



Segnalazioni automatiche

- Dal 2012, su indicazione di varie fonti, principalmente **shadowserver**
- Nodi infetti o compromessi
- Nodi utilizzabili per attacchi DRDoS
  - dns
  - ntp
  - snmp
  - ecc. ecc.

Segnalazioni ricevute nel 2014



Spediti 26000 mail

Poodle

- Utilizzando un attacco MITM è possibile recuperare dati da una connessione SSL/TLS
  - sistemi e applicazioni devono supportare SSL 3.0 CBC
  - 97% server vulnerabili a ottobre (Netcraft)
- Dettagli in alert GARR-CERT **GCSA-14038**
- Circa 8000 server web GARR vulnerabili **oggi** (dati **shadowserver**)

Altre vulnerabilità gravi

- **heartbleed** (**openssl**, aprile 2014)
  - recupero di dati nella memoria del server
  - http://heartbleed.com/
- **shellshock** (**bash**, settembre 2014)
  - esecuzione di comandi arbitrari
  - https://shellshocker.net/

Principali rischi

- Server
  - applicazioni web
  - D(R)DoS
- Utenti
  - phishing e spear phishing
  - mobile
  - SO operativi obsoleti / non mantenuti (windows xp?)
  - botnet