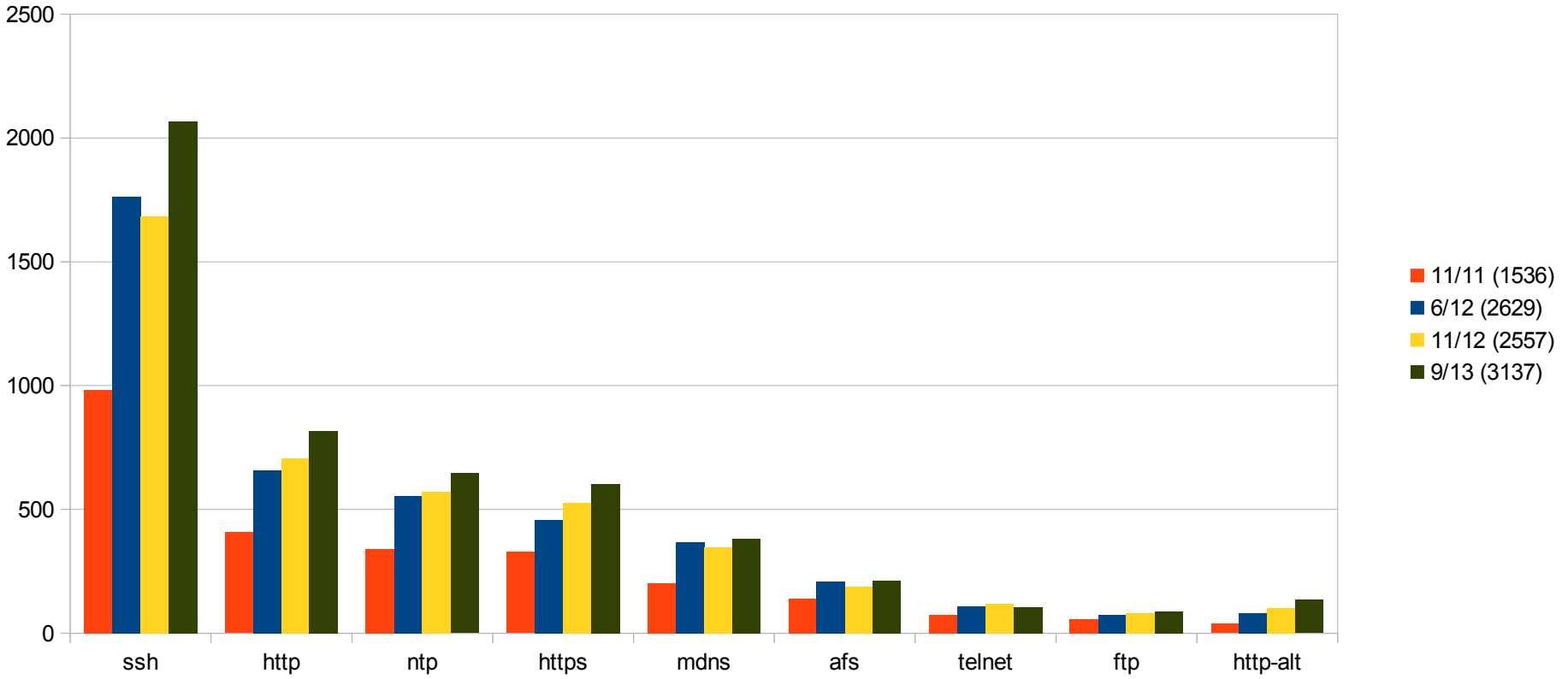
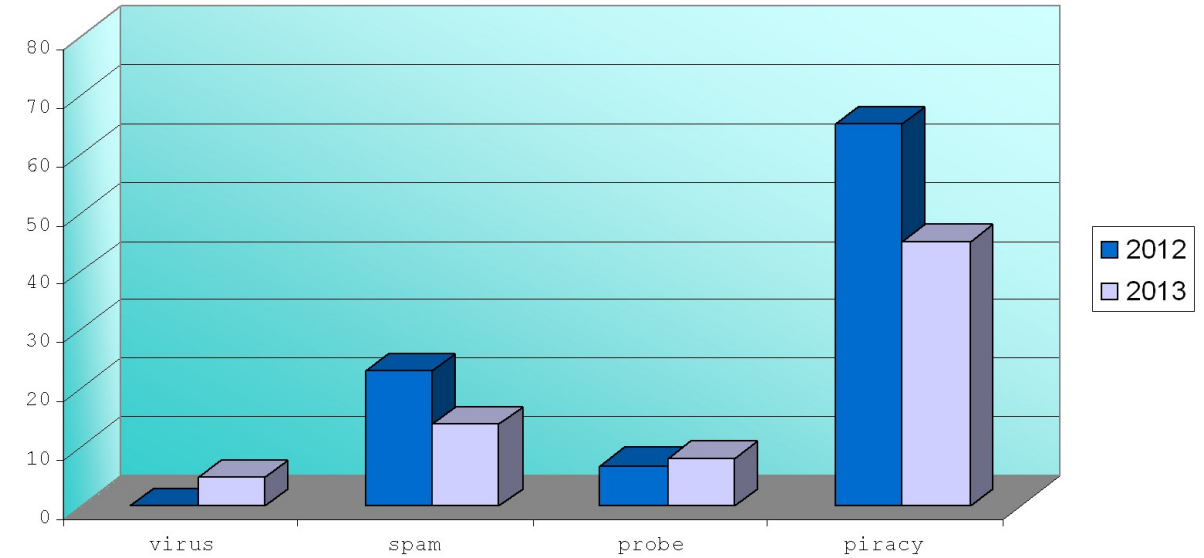
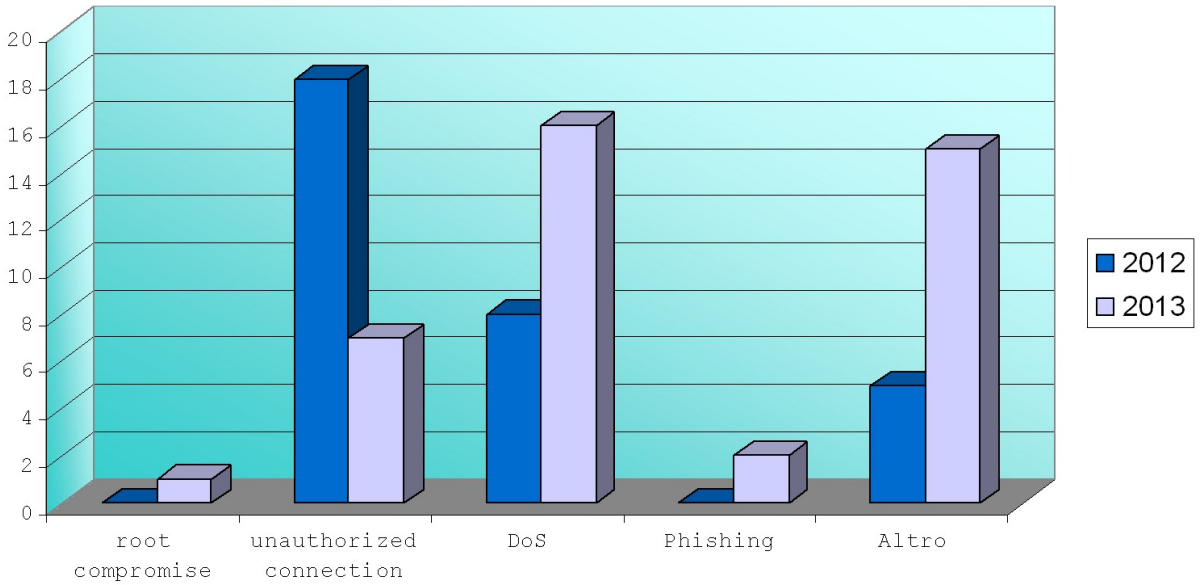
L'irresistibile ascesa dei servizi

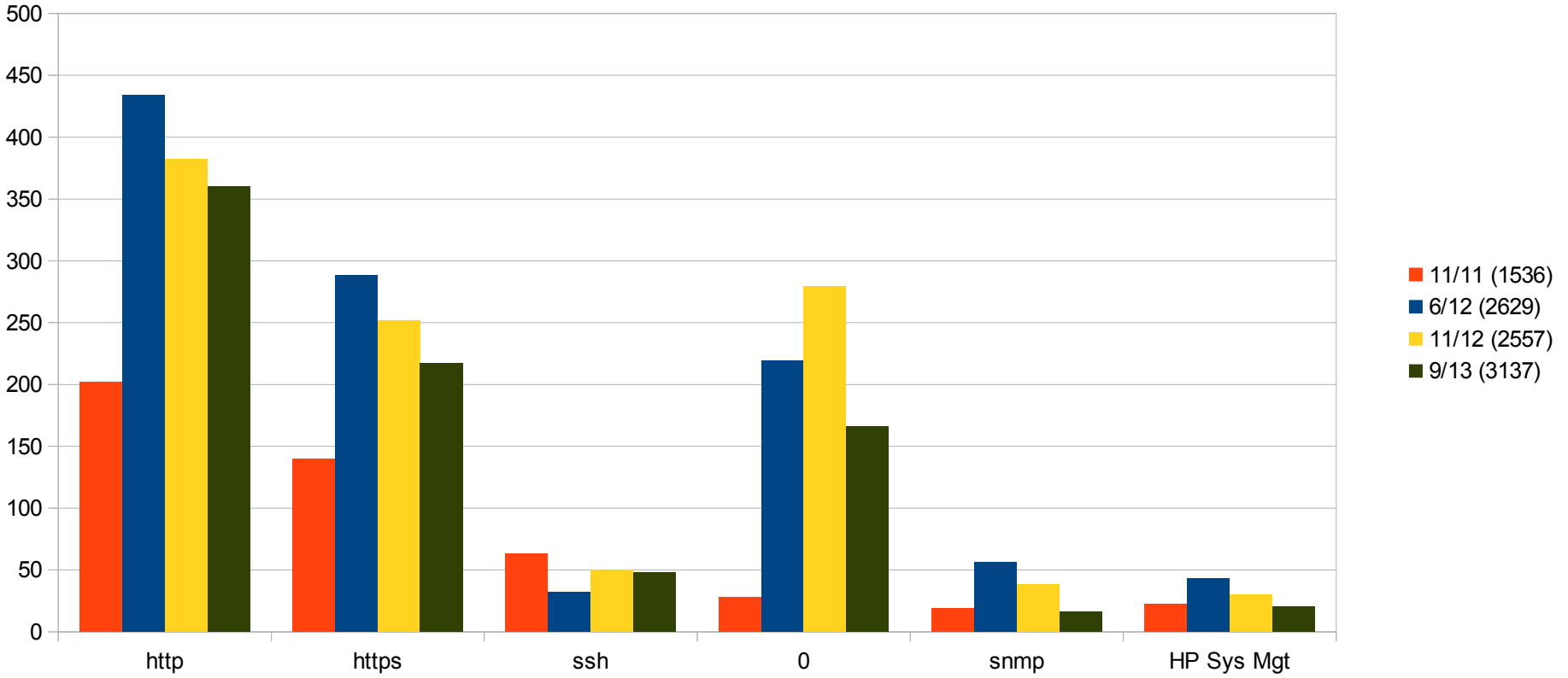


Dati GARR-CERT





L'andamento delle vulnerabilità



Totali vulnerabilità gravi

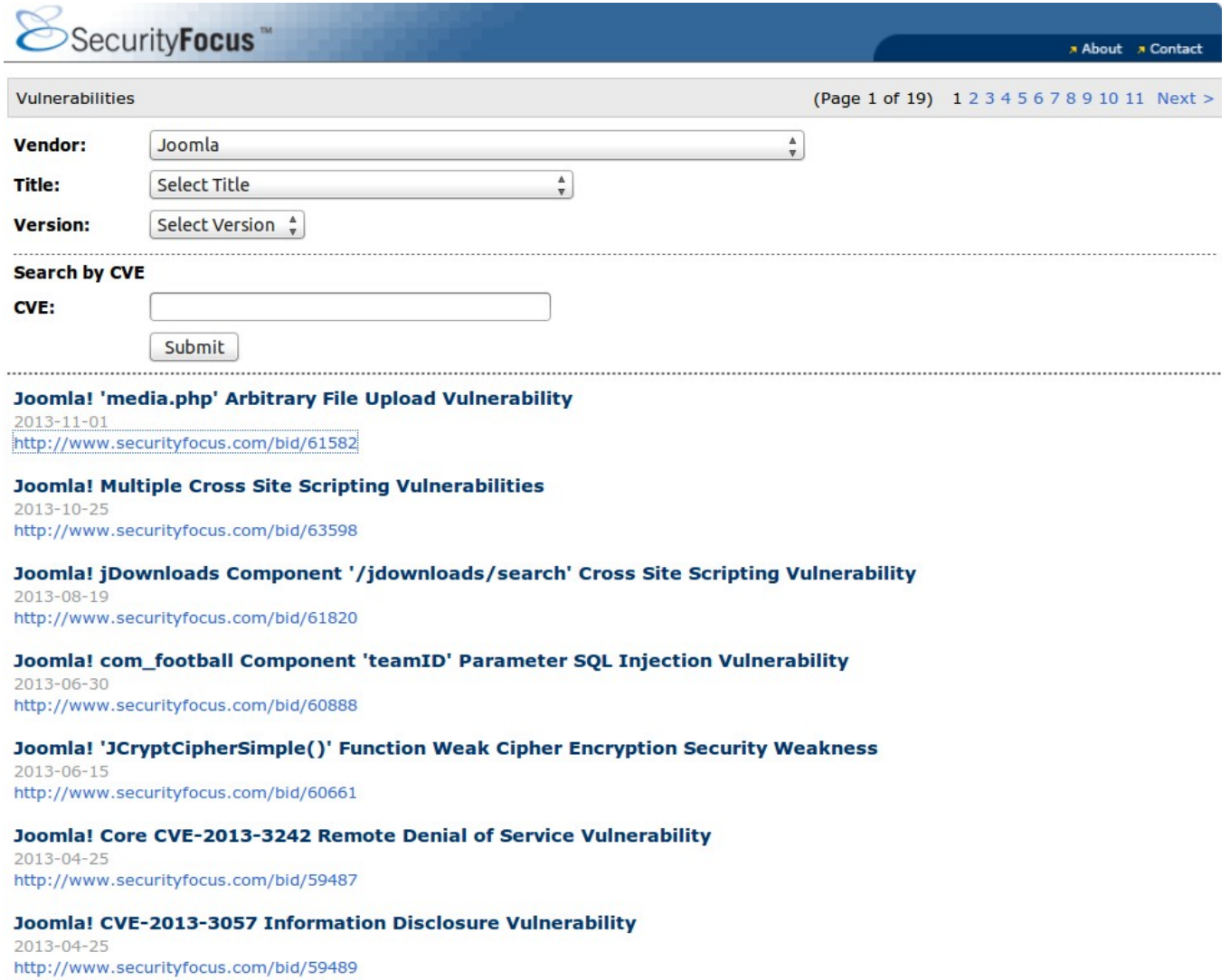
#	Tipo
382	PHP
186	Apache
94	Unsupported OS
62	CISCO IOS
31	SSH
20	HP system mgt
13	SNMP
5	Liferay default credentials
4	ISC Bind

Vulnerabilità plugin Joomla

Title	Created Date
My Blog, 2.0.1 Build 286,	26 September 2013
Master Password,	01 June 2013
ag google analytic	20 February 2013
JTag [joomlatag]	20 February 2013
RSGallery2	20 February 2013
ownbiblio 1.5.3	20 February 2013
bearleague	20 February 2013
Quickl Form	20 February 2013
com_advert	20 February 2013
Dshop	20 February 2013
QContacts 1.0.6	20 February 2013
Jobprofile 1.0	20 February 2013
JX Finder 2.0.1	20 February 2013
wdbanners	20 February 2013
JB Captify Content J1.5 and J1.7	20 February 2013
JB Microblog	20 February 2013
JB Slideshow <3.5.1,	20 February 2013
JB Bamboobox	20 February 2013
Vik Real Estate 1.0	20 February 2013
Time Returns	20 February 2013
acajoom	20 February 2013
alpharegistration	20 February 2013
Sobi	20 February 2013
xmap	20 February 2013
myApi	20 February 2013
mdigg	20 February 2013
Scriptegrator Plugin 1.5.5	20 February 2013
Joomnik Gallery	20 February 2013
JMS fileseller	20 February 2013
sh404SEF	20 February 2013

Page 1 of 5

Vulnerabilità Joomla



Versioni di Joomla

	1.0	1.5	1.6	1.7	2.5	3.0	3.1	3.2	3.5
Rilasciata nel	settembre 2005	gennaio 2008	gennaio 2011	luglio 2011	gennaio 2012	settembre 2012	aprile 2013	novembre 2013	marzo 2014
Supporto ufficiale	✖	✖	✖	✖	✔	✖	✔	✔	-
Termina nel	luglio 2009	settembre 2012	agosto 2011	febbraio 2012	dicembre 2014	maggio 2013	dicembre 2013	aprile 2014	-
Ultima stabile	1.0.15	1.5.26	1.6.6	1.7.5	**2.5.16**	3.0.4	3.1.6	3.2.0	-
Possibili nuovi aggiornamenti?	✖	✖	✖	✖	✔	✖	✔	✔	-
Presenza Bug di sicurezza noti?	SI	SI	SI	SI	NO	SI	NO	NO	-
Supporto a lungo o breve periodo?	LUNGO	LUNGO	BREVE	BREVE	LUNGO	BREVE	BREVE	BREVE	LUNGO
Aggiornamento semplice alla ver. successiva	no	no	si	si	no	si	si	si	-

da www.joomla.it

CMS INFN

Joomla	1.0.x	1 + 1
	1.5.x	9 + 3
	1.6.x	1
	2.5.x	8
	2.5.16	2
Wordpress	3.2.1	2
	3.3.2	1
	3.4.2	1
	3.5.1	1
	3.7.1	2
Drupal	7.17	1
	7.22	2 + 1
Dokuwiki		3
Plone		3

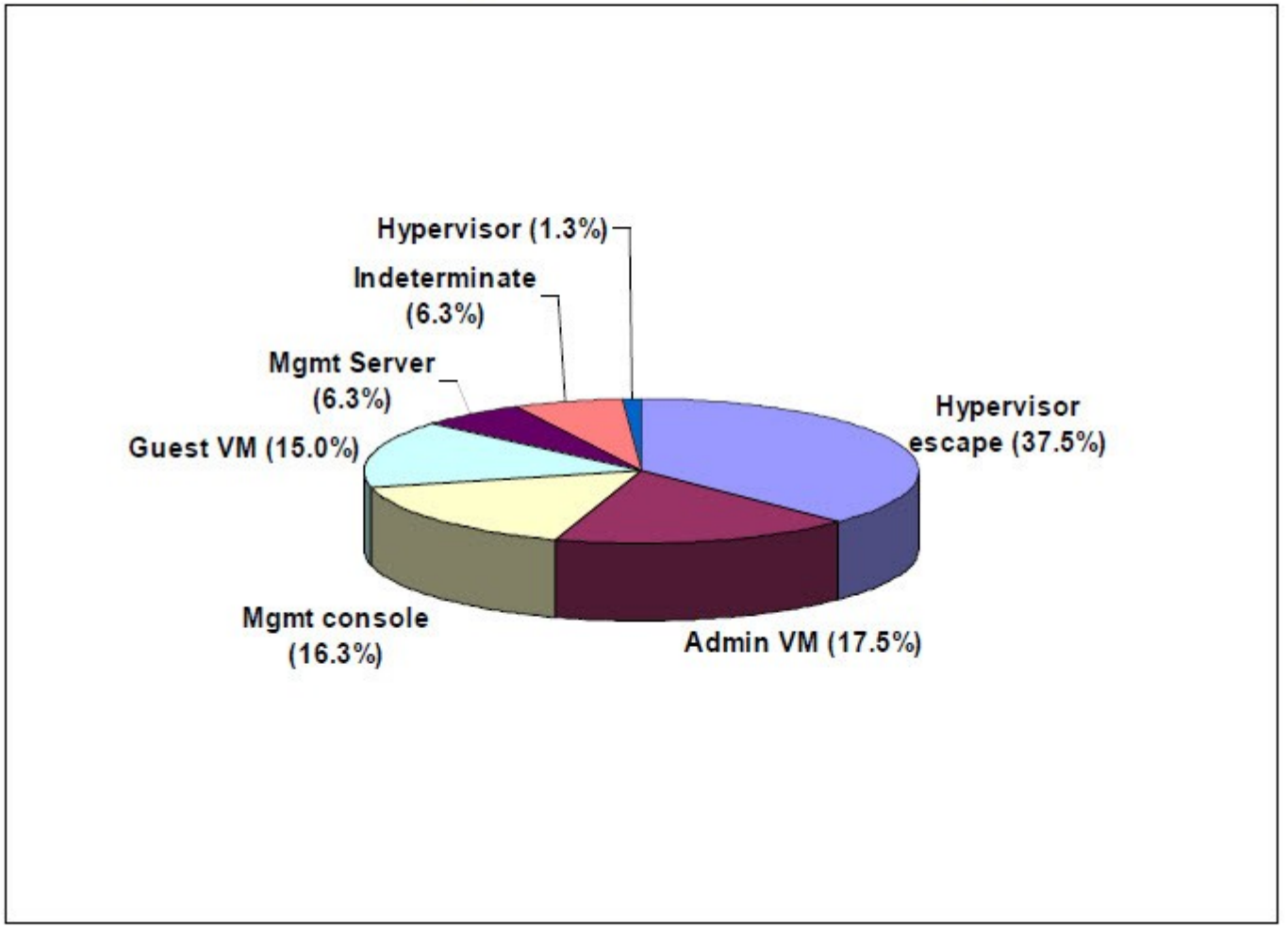
Evoluzione minacce (ENISA)

Top Threats	Current Trends	Top 10 Emerging Trends					
		Mobile Computing	Social Technology	Critical Infrastr.	Trust Infrastr.	Cloud	Big Data
1. Drive-by exploits	↑	↑	↑	↑		↑	↑
2. Worms/Trojans	↑	↑	↑	↑		→	↑
3. Code Injection	↑	→		↑		↑	
4. Exploit Kits	↑	↑	→	↑			↑
5. Botnets	↑	↑		→		→	
6. Denial of Service	→			→	↑	→	
7. Phishing	→	↑	↑	→			→
8. Compromising Confidential Information	↑	↑		↑	→	↑	↑
9. Rogueware/ Scareware	→		→				
10. Spam	↓		→				→
11. Targeted Attacks	↑		↑	↑	→	↑	→
12. Physical Theft/Loss/Damage	↑	↑	↑	↑	→	→	
13. Identity Theft	↑	↑	↑		→	↑	↑
14. Abuse of Information Leakage	↑	→	↑		→	↑	↑
15. Search Engine Poisoning	→						
16. Rogue Certificates	↑				↑		

Legend: ↓ Declining, → Stable, ↑ Increasing

Vulnerabilità nella virtualizzazione

Production Virtualization System Vulnerabilities By Class



Virtualization security

Guide to Security for Full Virtualization and Technologies, NIST (2011)

- Hypervisor
- Guest OS
  - attenzione al disk sharing
- Virtualized Infrastructure
  - accesso ad hw virtuale strettamente limitato agli OS che lo usano
- Desktop Virtualization
  - può non essere possibile controllare la “qualità” del SO utilizzato dall'utente

Vulnerabilità CVE con CVSS score > 7

- XEN
  - 8 (ultima il 23/11/2013)
- Vmware
  - 87 (ultima il 18/11/2013)
- Virtualbox (Oracle & SUN)
  - 3 (ultima il 17/7/2013)

Minacce al cloud computing (ENISA)

- Attacchi all'architettura dell'infrastruttura cloud (ad es. alle API delle macchine virtuali);
- rischi dovuti all'aumento dei device mobili (ad es. furto di credenziali per l'accesso ai servizi cloud);
- co-hosting di informazioni sensibili;
- utilizzo di servizi cloud come malware tool:
  - storage di malware
  - lancio di attacchi
  - vicinanza a potenziali vittime

Cybercrime-As-A-Service