PRIMEUR

La sfida della sicurezza delle informazioni nel mondo della Moda

Damiano Peres
Damiano.peres@primeur.com

Le aziende della moda

- Il mondo della moda è un mondo che vive di tendenze e gusti che cambiano molto rapidamente. Tali imprese devono, quindi, adattarsi velocemente al mercato, puntare all'innovazione sia di processo che di prodotto, valorizzando la qualità, il servizio e la differenziazione.

- Tutto questo implica che le aziende devono essere costantemente connesse al fine di sfruttare e soddisfare le possibilità e le richieste del mercato moderno:
  - La produzione può avvenire in luoghi distanti dalla casa madre
  - I Fornitori possono essere dislocati in varie parti del mondo
  - Punti vendita che coprono l'intero mercato mondiale
  - Dipendenti dislocati in aree geografiche distanti tra loro
  - Collaboratori che necessitano di accedere ai dati aziendali in ogni momento, e con qualsiasi strumento (tablet, pc, smartphone etc..)

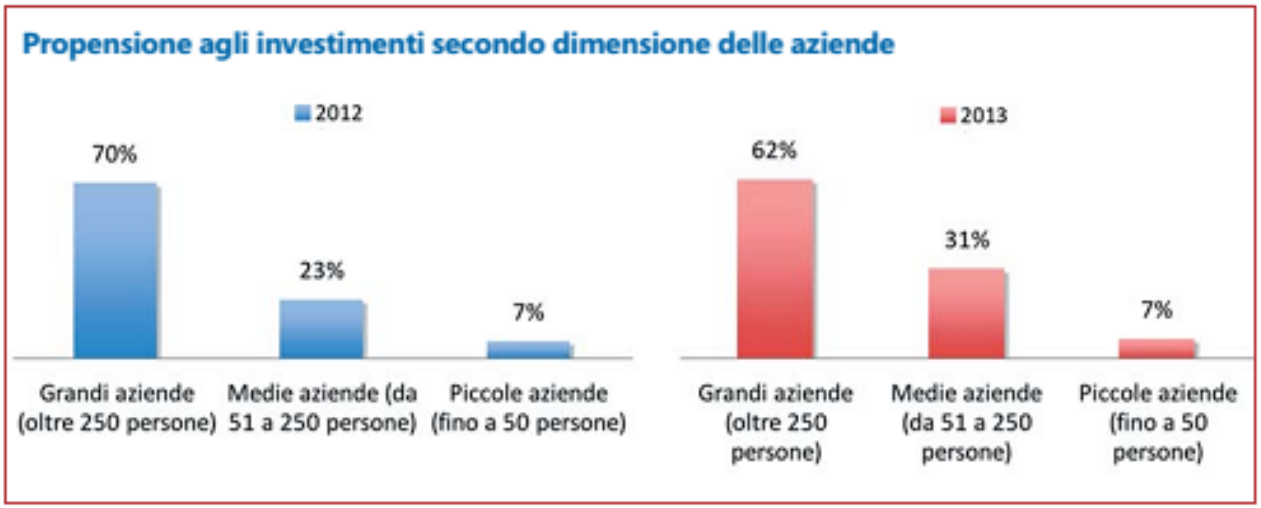
Marketing

- Il marketing riveste un ruolo importante per mantenere il posizionamento acquisito sul mercato, o per rinforzarlo, per questi motivi i nuovi canali di comunicazione vengono sfruttati al massimo:

- Le aziende quindi investono per mantenere dati, applicazioni, rete sempre:
  - Raggiungibili,
  - Disponibili,
  - Utilizzabili
- Investire per essere sempre più "attraenti" sui social.

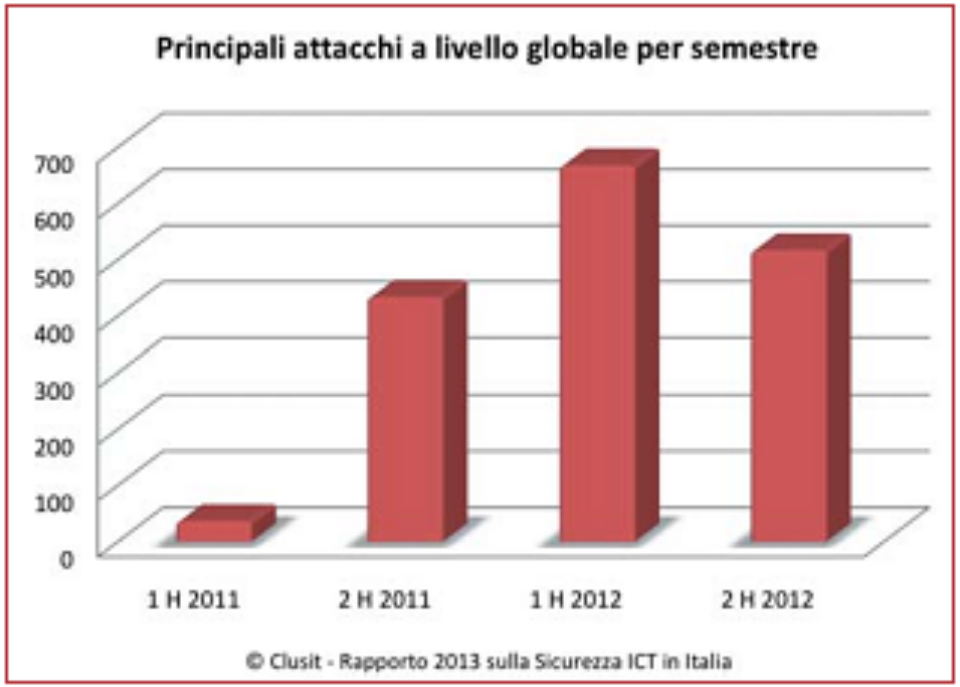
E la sicurezza?

(fonte clusit)



(fonte clusit)

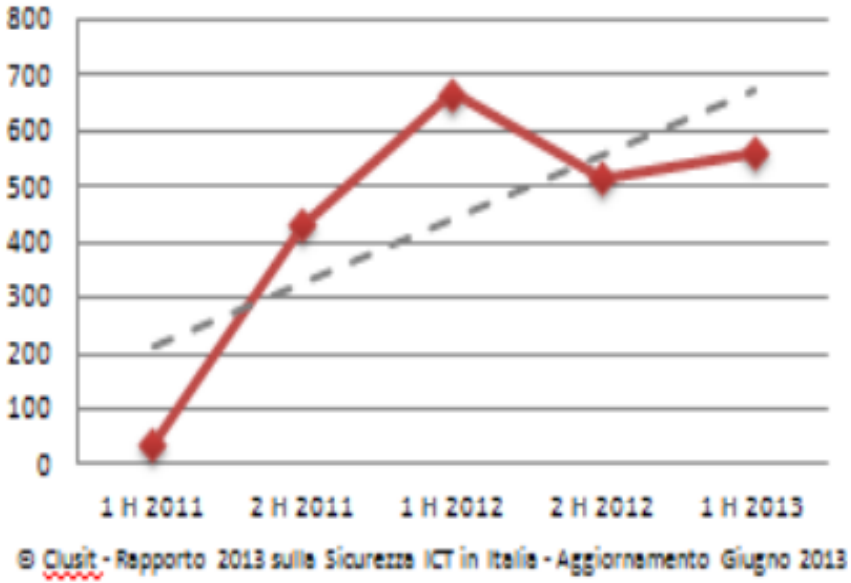
Questi sforzi sono sufficienti?



Fonte Clusit

Se fossero sufficienti il trend degli attacchi dovrebbero essere in diminuzione

Il trend è invece in crescita



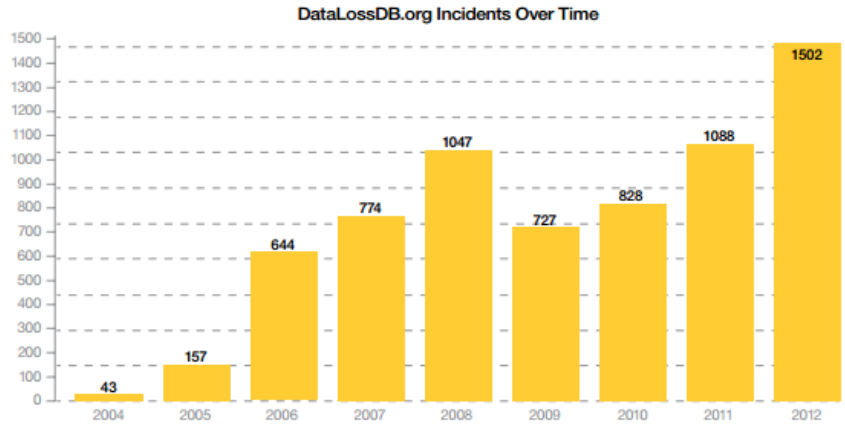
Questi sforzi sono sufficienti?

Report 2011-2012 (fonte Clusit)

VITTIME PER TIPOLOGIA	2011	2012	Variazioni 2012 su 2011
Institutions: Gov - Mil - LEAs - Intelligence	153	374	144,44%
Others	97	194	100,00%
Industry: Entertainment / News	76	175	130,26%
Industry: Online Services / Cloud	15	136	806,67%
Institutions: Research - Education	26	104	300,00%
Industry: Banking / Finance	17	59	247,06%
Industry: Software / Hardware Vendor	27	59	118,52%
Industry: Telco	11	19	72,73%
Gov. Contractors / Consulting	18	15	-16,67%
Industry: Security Industry:	17	14	-17,65%
Religion	0	14	-
Industry: Health	10	11	10,00%
Industry: Chemical / Medical	2	9	350,00%

Si può notare come nel 2012 gli attacchi sui e ai social network siano aumentati esponenzialmente

Le uniche aree in cui si è rilevata una diminuzione degli attacchi è nel Gov e Nella Security Industry… forse sono le uniche che hanno potenziato le loro difese

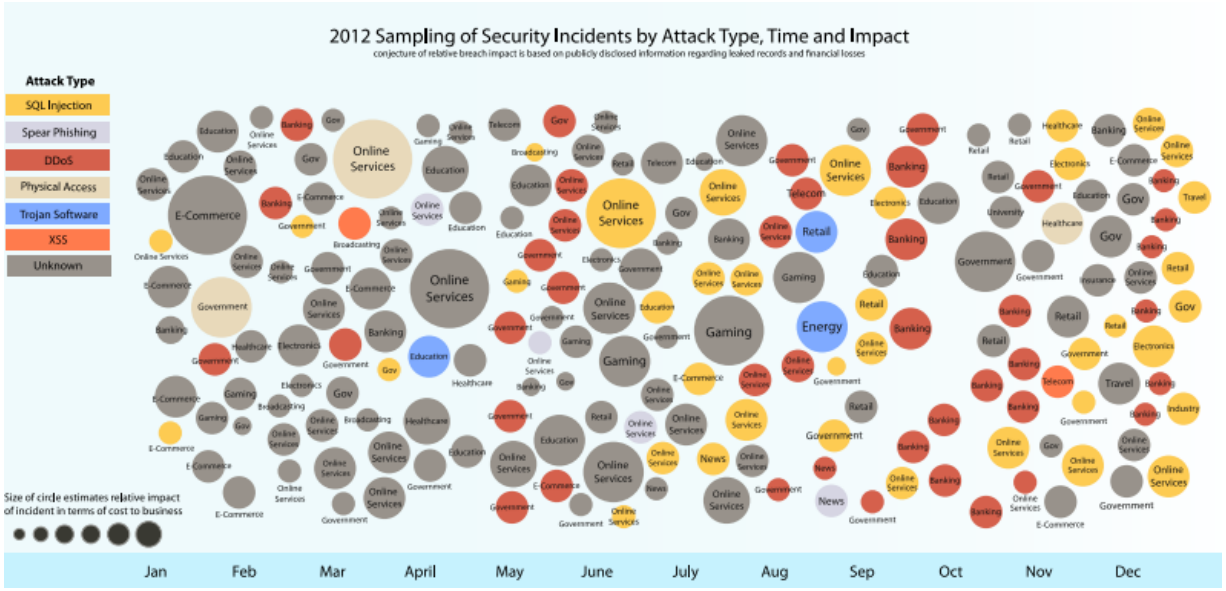


Tipologia di attacchi

Si nota come molti attacchi
Sfruttino metodi vecchi e conosciuti
SQL Injection, Misconfigurazioni, etc.. Che con poco sforzo di investimenti e di policy aziendali potrebbero essere risolti

TECNICHE PER TIPOLOGIA	2011	2012	Variazioni 2012 su 2011
SQL Injection[1]	197	435	120,81%
Unknown	73	294	302,74%
DDoS	27	165	511,11%
Known Vulnerabilities / Misconfig.	107	142	32,71%
Malware	34	61	79,41%
Account Cracking	10	41	310,00%
Phishing / Social Engineering	10	21	110,00%
Multiple Techniques / APT[2]	6	13	116,67%
0-day[3]	5	8	60,00%
Phone Hacking	0	3	-

Clusit



Ibm

Chi sono gli hacker oggi?

Fisionomia degli hacker

ATTACCANTI PER TIPOLOGIA	2011	2012	Variazioni 2012 su 2011
Cybercrime	170	633	272,35%
Unknown	148	110	-25,68%
Hacktivism	114	368	222,81%
Espionage / Sabotage	23	29	26,09%
Cyber warfare	14	43	207,14%

- CyberCrime
  - Hanno a disposizione elevate risorse monetarie e tecnologiche
  - Sono Molti, Organizzati , distribuiti

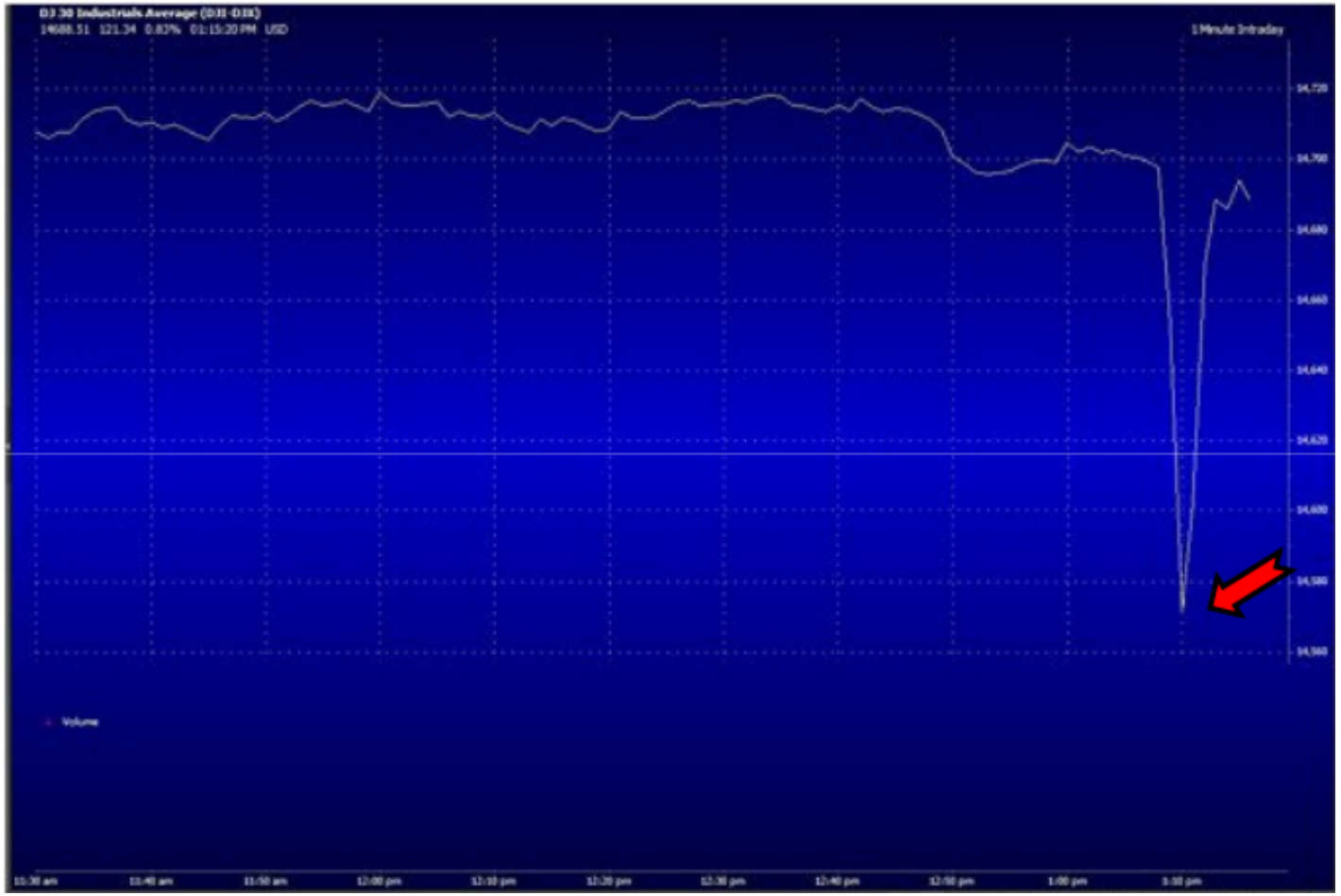
CyberCrime Perché ?

Semplice…è molto remunerativo

Hackerato l'account twitter di AP da "Syrian Elettronic Army"

Risultato

Ha causato in 5 min la perdita di circa 53 B$ alla NYSE



ROI

Anche le attività di CyberCrime hanno il loro ROI

Economical aspects for criminal organizations

Costs:

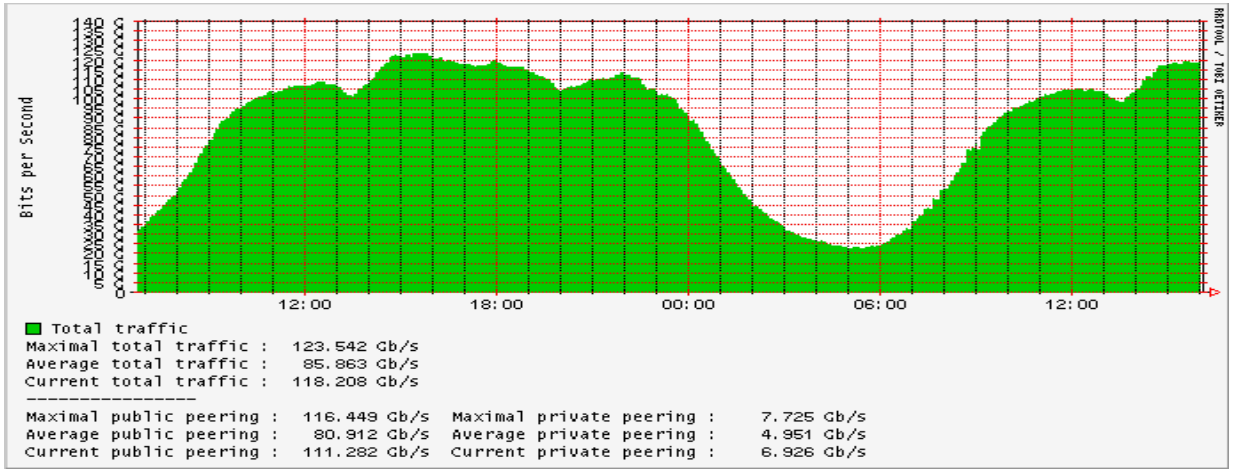
- Development of the malware on basis of the existing Zeus toolkit	$ 500
- Use of spam botnet	$ 50
- Hosting of command & control center	$ 2.000
- Use of the PC botnet for setting up sessions to Internet Banking	$ 500
- Translators for bank error pages	$ 500
- Cost of money mules in the Netherlands and Ukraine/Russia	$ 10.000

Benefits:

- 23 transactions	€ 116.000
- Return on investment:	**750%**

Sono molti e organizzati…
DDOS, Cyber Crime as a Service

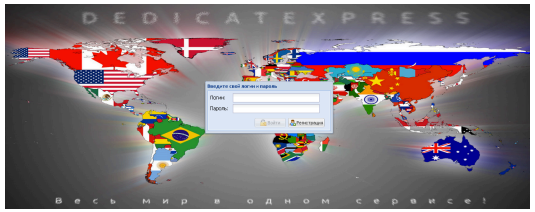
Attacchi strutturati: un recente attacco di tipo DDOS a Spamhaus ha generato banda per circa 300Gb

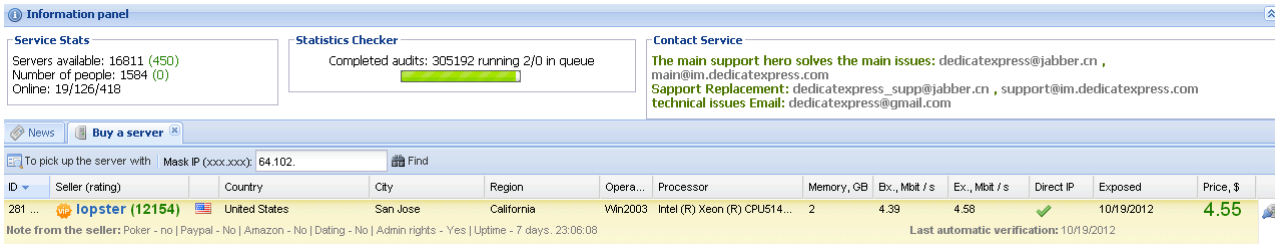


Il grafico riporta il traffico del MIX (31/10/2013).
Max total traffic 123,542 Gb.
Un DDOS di 300Gb potrebbe isolare gran parte delle comunicazioni Italiane

Cyber crime as a service

- Servizio di noleggio sistemi compromessi
- Tariffario 20$ per iscriversi
- Servizio di help-desk (se il Sistema non è più disponibile Ne viene fornito un'altro con le stesse caratteristiche)





Ma a me queste cose non succedono…

www.ilsole24ore.com/art/notizie/2012-03-26/rubano-firma-digitale-intestano-181133.shtml

ree Apps | Biz.nf Hosting | Google Traduttore | Login Page | pw_com_dwd_in | IBM Product Inform...

Rubano la firma digitale e si intestano l'azienda di un ignaro imprenditore: scovati dalla Guardia di Finanza

26 marzo 2012 Commenti (6)

Tweet 39 Consiglia 230 +1 2 My24

Rubano la firma digitale e si intestano l'azienda di un ignaro imprenditore: scovati dalla Guardia di Finanza

Si procurano una copia indebita della cosiddetta «firma digitale» e, con quella, scippano letteralmente l'azienda a un piccolo imprenditore. La truffa, prima nel suo genere, in Italia, è stata scoperta dagli 007 informatici del Gat, il Nucleo speciale frodi telematiche della Guardia di finanza, impegnati nelle indagini dirette dal procuratore aggiunto di Roma, Nello Rossi, e coordinate dal sostituto procuratore Eugenio Albamonte.

La scena del crimine

Tutto è avvenuto all'interno del sistema informatico delle Camere di Commercio. Protagonisti, un commercialista, un consulente per la sicurezza sul lavoro, una fantomatica società intestata a un'ottuagenaria defunta da circa un anno e facente capo in realtà a un soggetto sconosciuto al fisco da almeno 16 anni. Vittima, un imprenditore (vero, almeno lui), che riteneva di essere «protetto» dalla smart card obbligatoria per le comunicazioni societarie con il registro delle Imprese.

I capi d'accusa

Dopo perquisizioni e sequestri effettuati a Roma e provincia, i tre indagati devono ora rispondere - in concorso tra loro e con la continuazione della condotta - dei reati di sostituzione di persona, false dichiarazioni o attestazioni al certificatore di firma elettronica sull'identità o qualità personali proprie o di altri, falsità in atti pubblici, in scritture private e in documenti informatici.

La banda della firma digitale

Ma nel 2013 le cose saranno cambiate…

VITTIME PER TIPOLOGIA	2011	2012	Variazioni 2012 su 2011	2H 2012	1H 2013	Variazioni 1H 2013 su 2H 201
Institutions: Gov - Mil - LEAs - Intelligence	153	374	144,44%	156	168	7,69%
Others	97	194	100,00%	69	71	2,90%
Industry: Entertainment / News	76	175	130,26%	73	76	4,11%
Industry: Online Services / Cloud	15	136	806,67%	78	56	-28,21%
Institutions: Research - Education	26	104	300,00%	50	39	-22,00%
Industry: Banking / Finance	17	59	247,06%	33	65	96,97%
Industry: Software / Hardware Vendor	27	59	118,52%	35	24	-31,43%
Industry: Telco	11	19	72,73%	6	6	-
Gov. Contractors / Consulting	18	15	-16,67%	2	0	-100,00%
Industry: Security Industry:	17	14	-17,65%	2	5	150,00%
Religion	0	14	-	6	5	-16,67%
Industry: Health	10	11	10,00%	4	4	-
Industry: Chemical / Medical	2	9	350,00%	2	0	-100,00%
Critical Infrastructures	-	-	-	-	16	-
Industry: Automotive	-	-	-	-	16	-
Org / ONG	-	-	-	-	11	-

Si nota un notevole aumento di attacchi alle Banche e nel settore dell'Automotive (sempre più tecnologia a bordo delle vetture)

TECNICHE PER TIPOLOGIA	2011	2012	Variazioni 2012 su 2011	2H 2012	1H 2013	1H 2013 su 2H 2012
SQL Injection[1]	197	435	120,81%	212	162	-23,58%
Unknown	73	294	302,74%	120	106	-11,67%
DDoS	27	165	511,11%	67	97	44,78%
Known Vulnerabilities / Misconfig.	107	142	32,71%	56	78	39,29%
Malware	34	61	79,41%	30	8	-73,33%
Account Cracking	10	41	310,00%	17	46	170,59%
Phishing / Social Engineering	10	21	110,00%	5	2	-60,00%
Multiple Techniques / APT[2]	6	13	116,67%	6	61	916,67%
0-day[3]	5	8	60,00%	3	2	-33,33%
Phone Hacking	0	3	-	0	0	-

Cosa Fare

Vedremo nel pomeriggio qualcosa nel dettaglio ma

- La sicurezza della rete non è più sufficiente
- Vulnerability Assessment
- Penetretion Test
- Gestione delle informazioni (Log, trap Snmp etc..)
- Gestione delle Identità digitali
- Gestione delle politiche d'accesso
- Education, Formazione
- Policy Aziendali

- MA SOPRATTUTTO

...Sicurezza FAI DA TE....Ahl Ahl Ahl Ahl

I social sono molto utili ma anche molto pericolosi

Grazie