Homo homini virus. Il fattore umano nella sicurezza informatica

Andrea Rossetti

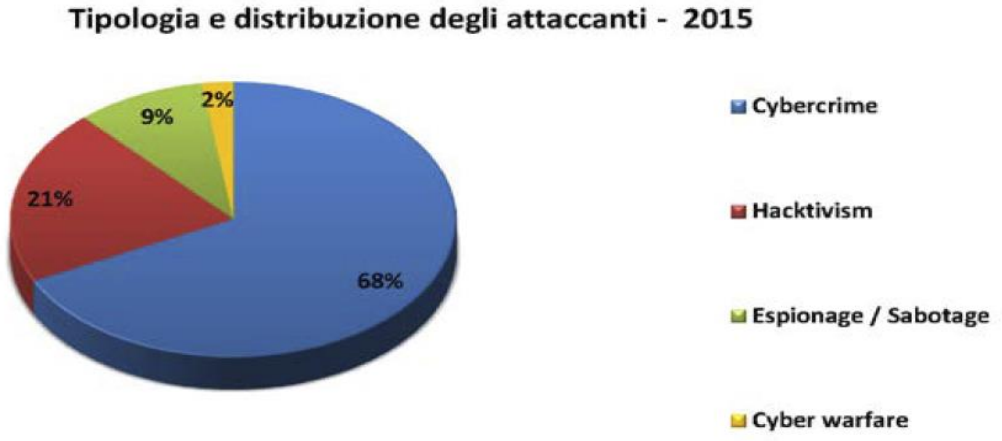
BiS Lab – Università di Milano Bicocca


INTEGRITY
AVAILABILITY
INFORMATION SECURITY
CONFIDENTIALITY

UNIVERSITÀ DEGLI STUDI DI MILANO BICOCCA

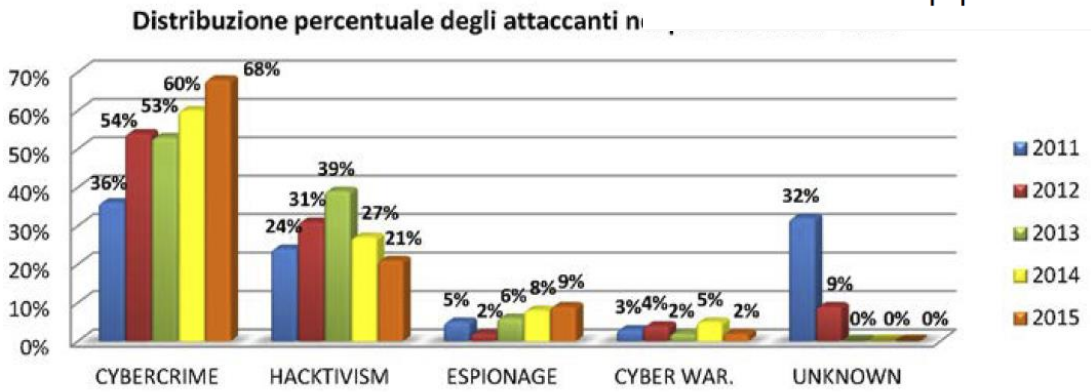
Bicocca Security Lab – Università Milano-Bicocca

BiS Lab



ATTACCANTI	2011	2012	2013	2014	2015	2012 su 2011	2013 su 2012	2014 su 2013	2015 su 2014	Trend 2015
Cybercrime	170	633	609	526	684	272,35%	-3,79%	-13,63%	30,04%	↑
Hacktivism	114	368	451	236	209	222,81%	22,55%	-47,67%	-11,44%	↓
Espionage	23	29	67	69	96	26,09%	131,03%	2,99%	39,13%	↑
Information Warfare	14	43	25	42	23	207,14%	-41,86%	68,00%	-45,24%	↓

© Clusit - Rapporto 2016 sulla Sicurezza ICT in Italia – *Aggiornamento al 31 dicembre 2015*



TECNICHE DI	[illegible]	[illegible]	[illegible]	[illegible]	2015	2012 su 2011	2013 su 2012	2014 su 2013	2015 su 2014	Trend 2015
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	84	120,81%	-50,11%	-49,31%	67,27%	↑
Unknown	73	294	239	199	232	302,74%	-18,71%	-16,74%	16,58%	↑
DDoS	27	165	191	81	101	511,11%	15,76%	-57,59%	24,69%	↑
Known Vuln/ Misconfig	107	142	256	195	184	32,71%	80,28%	-23,83%	-5,64%	→
Malware	34	61	57	127	106	79,41%	-6,56%	122,81%	-16,54%	↓
Account Cracking	10	41	115	86	91	310,00%	180,49%	-25,22%	5,81%	→
Phishing/Social Engineering	10	21	3	4	6	110,00%	-85,71%	33,33%	50,00%	↑
Multiple Techniques/APT	6	13	71	60	104	116,67%	446,15%	-15,49%	73,33%	↑
0-day	5	8	3	8	3	60,00%	-62,50%	166,67%	-62,50%	↓
Phone Hacking	0	3	0	3	1	-	-	-	-66,67%	↓

Che cosa è il **phishing**

Non è un problema di antivirus (e di misure tecnologiche)

supporto	mezzo	distro target	fine
fisico	email	tutti	denaro
	malware	organizzazioni	
rete	server	personale	dati

Deceptive Phishing

Malware-Based Phishing.

Data Theft

Search Engine Phishing

Hosts File Poisoning

Keyloggers

Session Hijacking

Web Trojans

Content-Injection Phishing

Screenloggers

DNS-Based Phishing

System Reconfiguration Attacks

Man-in-the-Middle Phishing

principianti

insiders

cyber punk

criminali professionisti

guerrieri informatici

vecchia guardia

ladruncoli


Prendere di mira un singolo obiettivo dentro una specifica organizzazione
Cercare di guardagnare un punto d'appoggio nell'ambiente
APT
advanced persistent threat
Usare il sistema compromesso per accedere alla rete obiettivo
Installare ulteriori strumenti per poter a termine l'attacco
Coprire le tracce e mantenere l'accesso per futuri attacchi
UNIVERSITÀ DEGLI STUDI DI MILANO BICOCCA
Bicocca Security Lab – Università Milano-Bicocca
BiS Lab

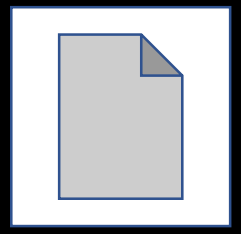
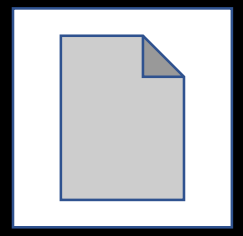
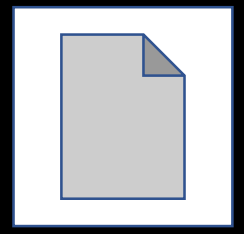
L'e-mail viene da qualcuno che conosco?

Stavo aspettando questa e-mail?

Cerca di farmi fare qualche cosa?

Sono le richieste ragionevoli?

Il contenuto ha un contenuto emotivo?
Fa leva sulla paura, avidità curiosità?

Regolamento UE n. 2016/679

riconosce espressamente il "diritto all'oblio"

stabilisce il diritto alla "portabilità dei dati"

sancisce il principio di "accountability"

introduce il principio della "privacy by design"

introduce il principio della "privacy by default"

Data Protection Officer

(i) informare e consigliare il titolare o il responsabile del trattamento, nonché i dipendenti, in merito agli obblighi derivanti dal Regolamento

(ii) verificare l'attuazione e l'applicazione della normativa, oltre alla sensibilizzazione e formazione del personale e dei relativi auditors

Data Protection Officer

(iii) fornire, se richiesto, pareri in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliare i relativi adempimenti

(iv) fungere da punto di contatto per gli "interessati", in merito a qualunque problematica connessa al trattamento dei loro dati nonché all'esercizio dei loro diritti

(v) fungere da punto di contatto per il Garante per la protezione dei dati personali oppure, eventualmente, consultare il Garante di propria iniziativa

Security is a process, not a product.

Bicocca Security Lab – Università Milano-Bicocca


Università degli Studi di Milano-Bicocca
Dipartimento di Giurisprudenza
Andrea Rossetti
Filosofia del Diritto / Informatica Giuridica
Piazza dell'Ateneo Nuovo 1
Edificio U6 - II piano
20126 Milano (MI)
Italia (I)
Tel.: (+39) 02.6448.4047
Fax: (+39) 02.6448.4110
Cell.: (+39) 392.310.7443
andrea.rossetti@unimib.it