



## Sicurezza delle reti<sup>1</sup>

Mattia Monga

Dip. di Informatica e Comunicazione  
Università degli Studi di Milano, Italia  
[mattia.monga@unimi.it](mailto:mattia.monga@unimi.it)

a.a. 2010/11

<sup>1</sup> © 2011 M. Monga. Creative Commons Attribuzione-Condividi allo stesso modo 2.5 Italia License.  
<http://creativecommons.org/licenses/by-sa/2.5/it/>. Materiale derivato da © 2010 M. Cremonini.



## Lezione I: Introduzione



## Informazioni sul corso

- 2+2 ore di lezione settimanali (6 crediti), teoria e in laboratorio
- Esame Scritto e Prova pratica per la parte di laboratorio
- Libri di riferimento:
  - *Inside Network Perimeter Security*, 2nd Edition Northcutt, Zeltser, Winters, Kent, Ritchey, SAMS ed., 2005
  - *The Tao of Network Security Monitoring – Beyond Intrusion Detection* R. Beytlich, Pearson Education Inc., 2004
- Articoli specifici indicati di volta in volta
- <https://mameli.docenti.dico.unimi.it/sicureti>



## Sicurezza & reti

Storicamente si è iniziato a parlare di sicurezza informatica in congiunzione con la diffusione delle reti.

In particolare l'evento simbolo che ha chiarito l'impatto che la Rete può avere sulla sicurezza dei sistemi è l'Internet Worm (2 novembre 1988). Colpì qualche migliaio di macchine ed è considerato il giorno della *perdita dell'innocenza di Internet*. In realtà il problema era già ben noto: la legge grazie alla quale R. Morris fu condannato era del 1986.

- Joyce Reynolds; *The Helminthiasis of the Internet*; RFC 1135; Dec. 1989.
- Eugene H. Spafford; *The Internet Worm: Crisis and Aftermath*; Communications of the ACM; v. 32(6), pp. 678-687; June 1989.

## Tipologie di malware



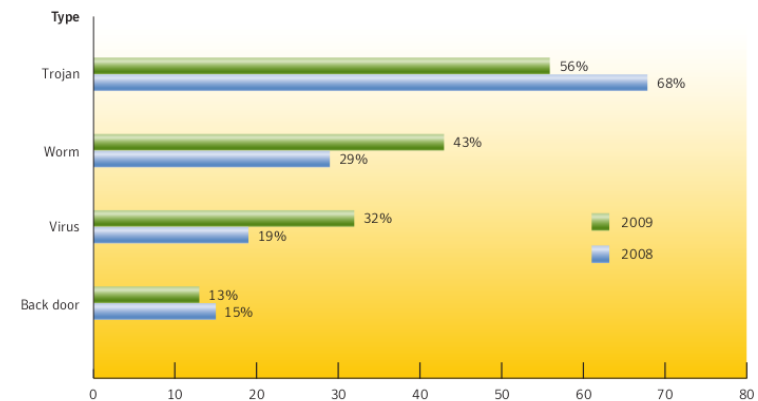
replicazione no replicazione	replicazione autonoma	Virus	Worm
	no replicazione	Rootkit Trojan horse	Dialer Spyware Keylogger
		necessita ospite	nessun ospite
		dipendenza da ospite	

malware: sequenza di codice progettata per danneggiare intenzionalmente un sistema, i dati che contiene o comunque alterarne il funzionamento, al di fuori delle intenzioni del progettista o degli amministratori.

5

Sicurezza delle reti  
Monga  
Concetti generali  
Gli argomenti del corso

## Proporzione fra le top 50 infezioni (Symantec)



6

Sicurezza delle reti  
Monga  
Concetti generali  
Gli argomenti del corso

## Chi ha interesse a colpire un sistema?



Secondo *Verizon 2010 Data Breach Investigations Report* (contiene anche i dati dell'USSS) 900 incidenti, 2/3 dei quali non sono mai stati resi pubblici.

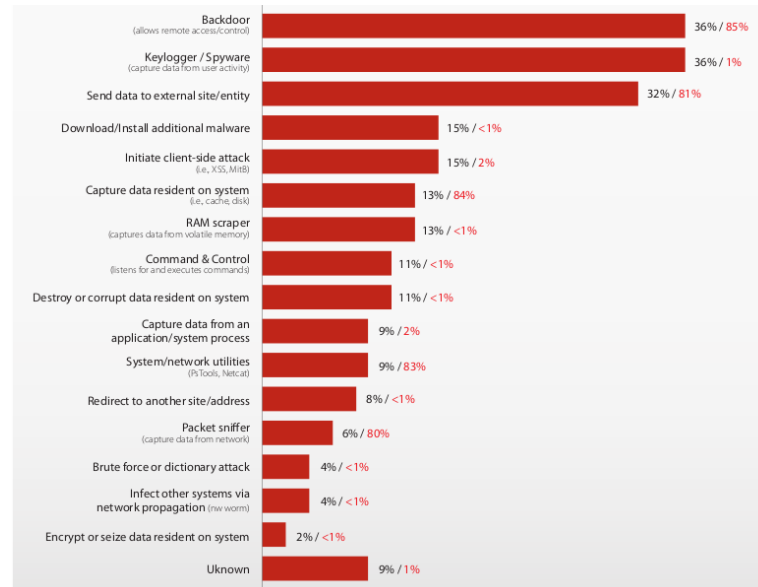
70%	causato da agenti esterni
48%	causato da interni
11%	causato da business partner
27%	coinvolge più attori
40%	attacchi mirati provenienti dalla rete
38%	causato da malware

Altri dati interessanti: 85% degli attacchi non è da considerarsi *molto difficile* e il 96% poteva essere evitato con semplici controlli...

7

Sicurezza delle reti  
Monga  
Concetti generali  
Gli argomenti del corso

## Funzionalità del malware (Verizon)



8

Sicurezza delle reti  
Monga  
Concetti generali  
Gli argomenti del corso

## Vettori di attacco (Verizon)

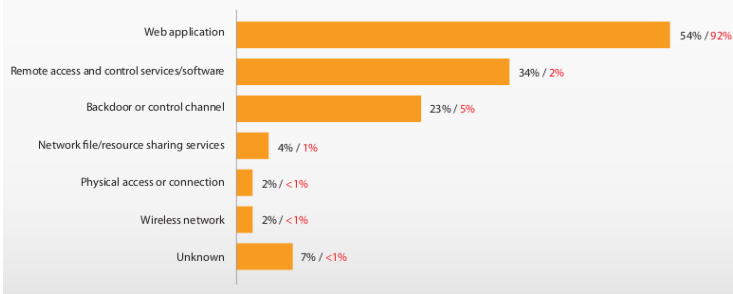


Sicurezza delle reti  
Monga

Concetti generali

Gli argomenti del corso

Figure 22. Attack pathways by percent of breaches within Hacking and percent of records



9

## Propagazione di malware (Symantec)



Sicurezza delle reti  
Monga

Concetti generali

Gli argomenti del corso

Rank	Propagation Mechanisms	2009 Percentage	2008 Percentage
1	File-sharing executables	72%	66%
2	File transfer, CIFS	42%	30%
3	File transfer, email attachment	25%	31%
4	Remotely exploitable vulnerability	24%	12%
5	File sharing, P2P	5%	10%
6	File transfer, HTTP, embedded URI, instant messenger	4%	4%
7	SQL	2%	3%
8	Back door, Kuang2	2%	3%
9	Back door, SubSeven	2%	3%
10	File sharing, data files	1%	1%

Table 18. Propagation mechanisms

Source: Symantec

10

## Motivazioni economiche (Symantec)



Sicurezza delle reti  
Monga

Concetti generali

Gli argomenti del corso

Overall Rank 2009	Overall Rank 2008	Item	Percentage 2009	Percentage 2008	Range of Prices
1	1	Credit card information	19%	32%	\$0.85-\$30
2	2	Bank account credentials	19%	19%	\$15-\$850
3	3	Email accounts	7%	5%	\$1-\$20
4	4	Email addresses	7%	5%	\$1.70/MB-\$15/MB
5	9	Shell scripts	6%	3%	\$2-\$5
6	6	Full identities	5%	4%	\$0.70-\$20
7	13	Credit card dumps	5%	2%	\$4-\$150
8	7	Mailers	4%	3%	\$4-\$10
9	8	Cash-out services	4%	3%	\$0-\$600 plus 50%-60%
10	12	Website administration credentials	4%	3%	\$2-\$30

Table 21. Goods and services advertised for sale on underground economy servers

Source: Symantec

Oltre a ciò, naturalmente ci sono gli attacchi mirati!

11

## Gli obiettivi del corso



Sicurezza delle reti  
Monga

Concetti generali

Gli argomenti del corso

- Definire l'ambito della sicurezza delle reti
- Rivedere i protocolli TCP/IP in un'ottica di sicurezza
- Conoscere le minacce più diffuse
- Saper analizzare il traffico e riconoscere gli attacchi
- Saper utilizzare le maggiori tecnologie di difesa
  - firewall
  - network intrusion detection system

12