



Sicurezza dei sistemi e delle reti¹

Mattia Monga

Dip. di Informatica
Università degli Studi di Milano, Italia
mattia.monga@unimi.it

a.a. 2014/15

¹ © 2011–15 M. Monga. Creative Commons Attribuzione — Condividi allo stesso modo 4.0 Internazionale. <http://creativecommons.org/licenses/by-sa/4.0/deed.it>. Derivato con permesso da © 2010 M. Cremonini.



Lezione I: Introduzione alla sicurezza delle reti



Di cosa parleremo

La sicurezza dei sistemi in rete

- I protocolli TCP/IP dal punto di vista della sicurezza
- Analisi delle possibilità di connessione e del traffico di rete
- La sicurezza “perimetrale”
- Rilevamento delle intrusioni
- Protezione di servizi critici e dell’infrastruttura Internet



Di cosa parleremo

La sicurezza **nelle** reti

- Misure di protezione in una rete untrusted
- VPN
- Anonimato
- Specificità delle reti wireless



Sicurezza delle
reti

Monga

Gli argomenti
del corso

- Il sito del corso:

<https://mameli.docenti.di.unimi.it/sicureti>



SHA-1 fingerprint:

0E:06:D3:0B:63:71:6A:5D:1C:7D:2F:DC:41:17:4B:89:E6:DE:46:3D

- Testi di riferimento:
 - "Security Engineering" R. Anderson, Wiley 2008 (Disponibile anche gratuitamente:
<http://www.cl.cam.ac.uk/~rja14/book.html>)
 - "The Tao of Network Security Monitoring – Beyond Intrusion Detection" R. Bejtlich Pearson Education Inc., 2004
 - "Silence on the Wire. A Field Guide to Passive Reconnaissance and Indirect Attacks", M. Zalewski, No Starch Press, 2005
- Articoli scientifici indicati a lezione (e sul sito)

5



Sicurezza delle
reti

Monga

Gli argomenti
del corso

- prova scritta + prova di laboratorio: il voto finale 75% scritto + 25% laboratorio (entrambe devono essere sufficienti).
- Scritto: domande e svolgere esercizi sul programma trattato a lezione e gli approfondimenti indicati.
- Laboratorio: esercizio da risolvere con i tool trattati a lezione

6



Sicurezza delle
reti

Monga

Gli argomenti
del corso

Il titolo del corso è assai vasto... Ci concentreremo su:

- Reti TCP/IP
- Le misure classiche di protezione "perimetrale"
- La sicurezza nelle reti

7



Sicurezza delle
reti

Monga

Concetti
generali

Internet worm
Malware
Lo scenario
attuale

Storicamente il grande pubblico ha iniziato a parlare di **sicurezza informatica** in congiunzione con la diffusione delle reti.

L'evento simbolo Rete/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*.

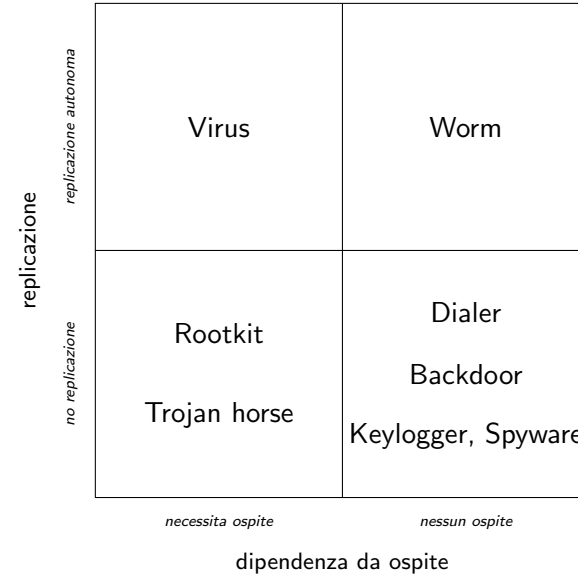
8



In realtà il problema era già ben noto: la legge grazie alla quale R. Morris fu condannato era del 1986.

Letture obbligatorie:

- Joyce Reynolds; *The Helminthiasis of the Internet*; RFC 1135; Dec. 1989.



malware: codice progettato per danneggiare intenzionalmente un sistema, alterandone funzionalità o dati.



<http://www.symantec.com/threatreport/>

- 42% increase in targeted attacks in 2012.
- 6787 (2012: 5291) new vulnerabilities discovered in 2013, 127 (2012: 416) of them on mobile operating systems.
- Spam volume continued to decrease, with 66% of all email being spam (-3%)
- Number of bots detected (2.3M) decreasing (-33%)



Secondo *Verizon 2014 Data Breach Investigations Report* (contiene anche i dati dell'USSS, e di varie polizie) 63437 incidenti + 1367 *data breaches*. Il report è molto cambiato: nel 2013 conteneva solo 621 incidenti.

2010	2011	2012	2013	
70%	92%	98%	92%	causato da agenti esterni
48%	17%	4%	14%	causato da interni
11%	< 1%	< 1%	1%	causato da business partner
40%	17%	21%	25%	attacchi mirati
38%	49%	69%	40%	causato da malware

19% 'state-affiliated'...

Geni del crimine?



Sicurezza delle reti

Monga

Concetti generali

Internet worm

Malware

Lo scenario attuale

Altri dati interessanti (dal report 2013): 99% delle compromissioni iniziali non è da considerarsi *molto difficile* e la grande maggioranza (78%) usa tecniche di base o strumenti automatici...

13

Lettura obbligatoria



Sicurezza delle reti

Monga

Concetti generali

Internet worm

Malware

Lo scenario attuale

Verizon Data Breach Investigations Report
<http://www.verizonenterprise.com/DBIR/2014/>

14

Un'altra data simbolo?



Sicurezza delle reti

Monga

Concetti generali

Internet worm

Malware

Lo scenario attuale

Una nuova data simbolo: il 7 giugno 2013 Edward J. Snowden rivela che NSA ha raccolto informazioni riguardanti comunicazioni private con l'aiuto di Microsoft, Yahoo, Google, Facebook, PalTalk, YouTube, Skype, AOL, Apple (programma PRISM). Seguono decine di altre rivelazioni:
<http://www.lawfareblog.com/catalog-of-the-snowden-revelations/>.
Per approfondire: "No place to hide" Glenn Greenwald (in italiano: "Sotto controllo", Rizzoli).

15

Riassumendo



Sicurezza delle reti

Monga

Concetti generali

Internet worm

Malware

Lo scenario attuale

Sicurezza informatica è sempre più un problema con risvolti sociali, oltre che tecnologici

- Non solo da attacchi mirati, ma comunque attacchi con obiettivi commerciali
- Malware "di massa"
- Spionaggio industriale e attacchi alle libertà civili

16