



Sistemi  
Operativi e  
informatica

Massimo  
Marchi

Sicurezza e  
malware

Introduzione  
Malware &  
underground  
economy

# Sistemi Operativi e informatica<sup>1</sup>

Massimo Marchi

Dip. Scienze dell'Informatica  
Università degli Studi di Milano, Italia

[marchi@dsi.unimi.it](mailto:marchi@dsi.unimi.it)

a.a. 2011/12





# Malware

Sistemi  
Operativi e  
Informatica

Massimo  
Marchi

Sicurezza e  
malware

Introduzione  
Malware &  
underground  
economy

*Sequenza di codice progettata per danneggiare intenzionalmente un sistema, i dati che contiene o comunque alterare il suo normale funzionamento, all'insaputa dell'utente*



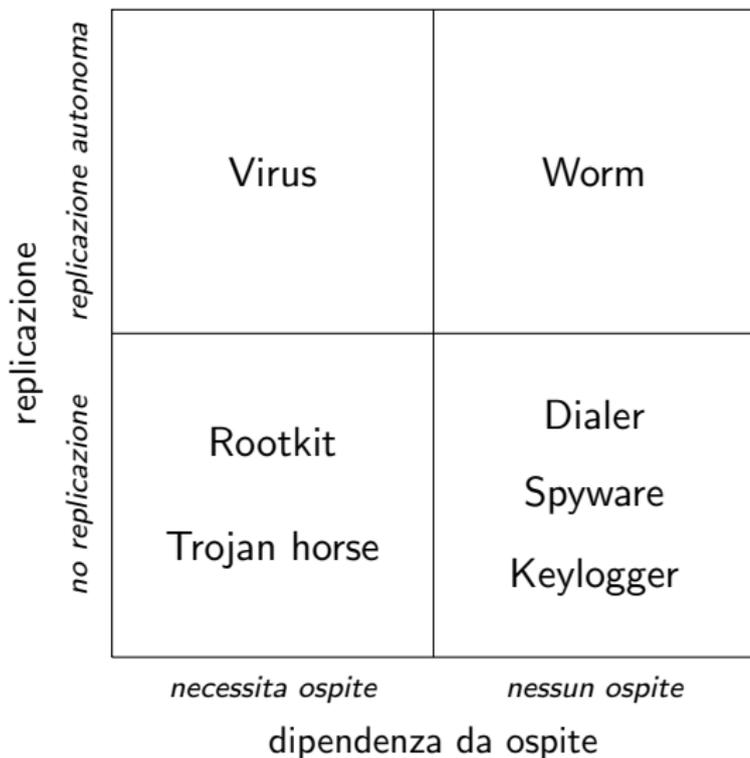
# Tipologie di malware

Sistemi  
Operativi e  
informatica

Massimo  
Marchi

Sicurezza e  
malware

Introduzione  
Malware &  
underground  
economy





# Tipologie di malware

## Virus & worm

Sistemi  
Operativi e  
informatica

Massimo  
Marchi

Sicurezza e  
malware

Introduzione  
Malware &  
underground  
economy

### Virus

- replicazione autonoma
- necessitano di un *ospite* in cui inserirsi
- propagazione attraverso la *diffusione dell'ospite*

### Worm

- *non* necessitano di un ospite
- propagazione autonoma attraverso la *rete*
- capacità di propagarsi in sistemi altrui sfruttando delle vulnerabilità



# Tipologie di malware

## Virus & worm

Sistemi  
Operativi e  
informatica

Massimo  
Marchi

Sicurezza e  
malware

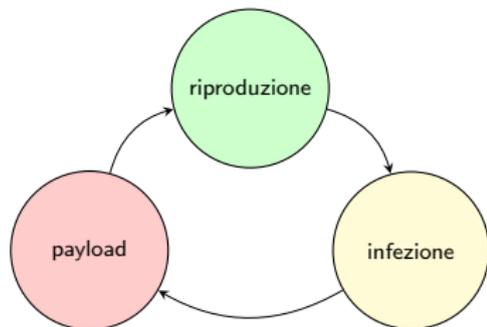
Introduzione  
Malware &  
underground  
economy

### Virus

- replicazione autonoma
- necessitano di un *ospite* in cui inserirsi
- propagazione attraverso la *diffusione dell'ospite*

### Worm

- *non* necessitano di un ospite
- propagazione autonoma attraverso la *rete*
- capacità di propagarsi in sistemi altrui sfruttando delle vulnerabilità





# Tipologie di malware

## Trojan horse & backdoor

Sistemi  
Operativi e  
Informatica

Massimo  
Marchi

Sicurezza e  
malware

Introduzione  
Malware &  
underground  
economy

### Trojan horse

- funzionalità maligne camuffate tra altre benigne
- propagazione manuale: diffusione di applicazioni con funzionalità “secondarie” o inserimento di nuove funzionalità in applicazioni esistenti
- rientrano in questa categoria *adware* e *spyware*

### Backdoor

- per assicurare l'accesso ad un sistema compromesso
- rientrano in questa categoria i *RAT (Remote Access Trojan)*

### Rootkit

- strumenti utilizzati per mantenere l'accesso ad un sistema compromesso senza fare nascere sospetti
- utilizzati per nascondere file, processi, connessioni di rete, ...
- sia a livello kernel che a livello utente



# Tipologie di malware

## Trojan horse & backdoor

Sistemi  
Operativi e  
Informatica

Massimo  
Marchi

Sicurezza e  
malware

Introduzione  
Malware &  
underground  
economy

### Trojan horse

- funzionalità maligne cammuffate tra altre benigne
- propagazione manuale: diffusione di applicazioni con funzionalità “secondarie” o inserimento di nuove funzionalità in applicazioni esistenti
- rientrano in questa categoria *adware* e *spyware*

### Backdoor

- per assicurare l'accesso ad un sistema compromesso
- rientrano in questa categoria i *RAT (Remote Access Trojan)*

### Rootkit

- strumenti utilizzati per mantenere l'accesso ad un sistema compromesso senza fare nascere sospetti
- utilizzati per nascondere file, processi, connessioni di rete, ...
- sia a livello kernel che a livello utente



# Tipologie di malware

## Trojan horse & backdoor

### Trojan horse

- funzionalità maligne cammuffate tra altre benigne
- propagazione manuale: diffusione di applicazioni con funzionalità “secondarie” o inserimento di nuove funzionalità in applicazioni esistenti
- rientrano in questa categoria *adware* e *spyware*

### Backdoor

- per assicurare l'accesso ad un sistema compromesso
- rientrano in questa categoria i *RAT (Remote Access Trojan)*

### Rootkit

- strumenti utilizzati per mantenere l'accesso ad un sistema compromesso senza fare nascere sospetti
- utilizzati per nascondere file, processi, connessioni di rete, ...
- sia a livello kernel che a livello utente



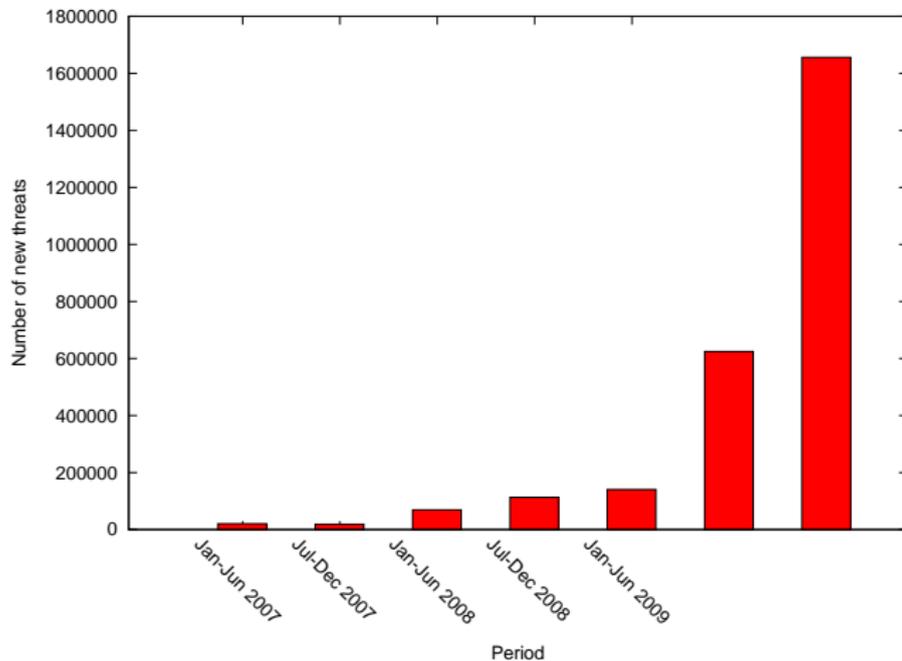
# Nuove minacce

Sistemi  
Operativi e  
informatica

Massimo  
Marchi

Sicurezza e  
malware

Introduzione  
Malware &  
underground  
economy



Fonte: Symantec



# Phishing

Sistemi Operativi e Informatica

Massimo Marchi

Sicurezza e malware

Introduzione Malware & underground economy

Poste Italiane - Accedi a Poste.it - Iceweasel

History Bookmarks Tools Help

http://demo.livestore.com.mx/cuentas/5318/assets/personale/login.html

**Posteitaliane** Home | Chi siamo | Sala stampa | English . Registrazione . Accedi

DI COSA HAI BISOGNO? PRODOTTI BUSINESS SERVIZI ONLINE

**Servizi online**

- Scopri i servizi online
- Negozi online
- Registrazione
- Accedi ai servizi online
- Codice di attivazione
- Utenti pre-registrati
- Hai dimenticato la password?
- Privacy
- Sicurezza dei dati

**Accedi a Poste.it**

Per poter usufruire dei servizi online di Poste.it occorre prima identificarsi. Inserisci negli appositi spazi il tuo nome utente e la password.

**Privati Business**

Servizi online **Privati**

Nome utente

Password

**Accedi**

Per utilizzare i servizi online e in caso di mancato accesso o non funzionamento dei servizi è necessario:

- verificare il corretto inserimento del nome utente e della password.
- Il nome utente va inserito come nome cognome più l'eventuale estensione (mario.rossi-1234) richiesta durante la registrazione.
- La password va inserita rispettando la sequenza di caratteri maiuscolo o minuscolo come inseriti in fase di registrazione o in occasione dell'ultimo cambio.
- verificare che il browser consenta connessioni con protocollo SSL e accetti i cookie della sessione;
- eseguire periodicamente la pulizia dei file temporanei e dei cookie;
- verificare le proprietà data/ora e fuso orario del computer.



# Phishing

Sistemi Operativi e Informatica

Massimo Marchi

Sicurezza e malware

Introduzione Malware & underground economy

Poste Italiane - Accedi a Poste.it - Iceweasel

History Bookmarks Tools Help

http://demo.livestore.com.mx/cuentas/5318/assets/personale/login.html

Posteitaliane

Home | Chi siamo | Sala stampa | English . Registrazione . Accedi

DI COSA HAI BISOGNO? PRODOTTI BUSINESS SERVIZI ONLINE

Servizi online

- Scopri i servizi online
- Negozi online
- Registrazione
- Accedi ai servizi online
- Codice di attivazione
- Utenti pre-registrati
- Hai dimenticato la password?
- Privacy
- Sicurezza dei dati

**Privati Business**

Servizi online **Privati**

Nome utente

Password

Accedi

**Accedi a Poste.it**

Per poter usufruire dei servizi online di Poste.it occorre prima identificarsi. Inserisci negli appositi spazi il tuo nome utente e la password.

Per utilizzare i servizi online e in caso di mancato accesso o non funzionamento dei servizi è necessario:

- verificare il corretto inserimento del nome utente e della password.
- Il nome utente va inserito come nome cognome più l'eventuale estensione (mario.rossi-1234) richiesta durante la registrazione.
- La password va inserita rispettando la sequenza di caratteri maiuscolo o minuscolo come inseriti in fase di registrazione o in occasione dell'ultimo cambio.
- verificare che il browser consenta connessioni con protocollo SSL e accetti i cookie della sessione;
- eseguire periodicamente la pulizia dei file temporanei e dei cookie;
- verificare le proprietà data/ora e fuso orario del computer.



# Come funziona?

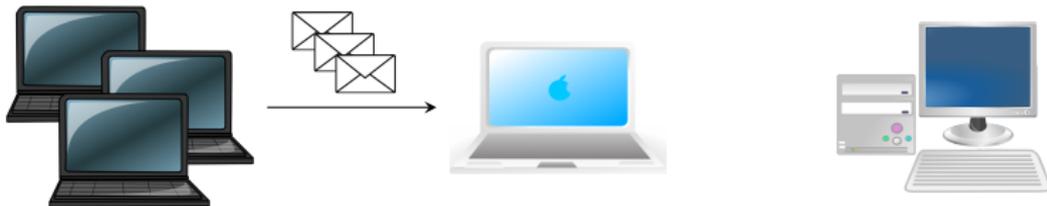
Sistemi  
Operativi e  
Informatica

Massimo  
Marchi

Sicurezza e  
malware

Introduzione  
Malware &  
underground  
economy

- 1 **campagna di spam**
- 2 social engineering
- 3 furto credenziali & malware
- 4 infezione macchine





# Come funziona?

Sistemi  
Operativi e  
Informatica

Massimo  
Marchi

Sicurezza e  
malware

Introduzione  
Malware &  
underground  
economy

- 1 campagna di spam
- 2 **social engineering**
- 3 furto credenziali & malware
- 4 infezione macchine



GET /...





# Come funziona?

Sistemi  
Operativi e  
Informatica

Massimo  
Marchi

Sicurezza e  
malware

Introduzione  
Malware &  
underground  
economy

- 1 campagna di spam
- 2 social engineering
- 3 furto credenziali & malware
- 4 infezione macchine





# Come funziona?

Sistemi  
Operativi e  
Informatica

Massimo  
Marchi

Sicurezza e  
malware

Introduzione  
Malware &  
underground  
economy

- 1 campagna di spam
- 2 social engineering
- 3 furto credenziali & malware
- 4 **infezione macchine**





# Underground economy

Vendita informazioni rubate

Sistemi  
Operativi e  
informatica

Massimo  
Marchi

Sicurezza e  
malware

Introduzione  
Malware &  
underground  
economy

<b>Goods &amp; services</b>	<b>Percentage</b>	<b>Range of prices</b>
Bank accounts	22%	\$10-\$1000
Credit cards	13%	\$0.40-\$20
Full identities	9%	\$1-\$15
Online auction site accounts	7%	\$1-\$8
Scams	7%	\$2.50-\$50/week (hosting)
Mailers	6%	\$1-\$10
Email addresses	5%	\$0.83/MB-\$10/MB
Email passwords	5%	\$4-\$30
Drop (request or offer)	5%	10%-20% of drop amount
Proxies	5%	\$1.50-\$30

Fonte: Symantec



# Underground economy

Furto credenziali – Portata del fenomeno

Sistemi  
Operativi e  
Informatica

Massimo  
Marchi

Sicurezza e  
malware

Introduzione  
Malware &  
underground  
economy

- Università di Mannheim – Limbo & ZeuS
- ~ 70 dropzone
- **33 GB** di dati
- 11000 account bancari, 150000 account mail

Dropzone	# Machines	Data amount	Country
webpinkXXX.cn	26,150	1.5 GB	China
coXXX-google.cn	12,460	1.2 GB	Malaysia
77.XXX.159.202	10,394	503 MB	Russia
finXXXonline.com	6,932	438 MB	Estonia
<i>Other</i>	108,122	24.4 GB	
<b>Total</b>	<b>164,058</b>	<b>28.0 GB</b>	

Fonte: Learning More About the Underground Economy – T. Holz, M. Engelberth, F. Freiling, 2008



# Underground economy

*"Malware as a service"*

Sistemi Operativi e Informatica

Massimo Marchi

Sicurezza e malware

Introduzione Malware & underground economy

- Bot in affitto (~ \$1000-\$2000/mese)
- MPACK: exploit toolkit a ~ \$1000

**Cx Stats**  
ADVANCED STATISTIC

STATISTICS bots exploits

Advanced select

SELECT: by Language **Any**  
 and by Version **3**  
 and by FQuery **RU | Russia (7099)**  
 and by FExecuted **US | United States (1641)**  
 and by FExecuted **DE | Germany (1504)**  
 and by FExecuted **NL | Netherlands (492)**  
 and by FExecuted **UA | Ukraine (237)**  
 and by FExecuted **BR | Brazil (196)**  
 and by FExecuted **GB | United Kingdom (152)**  
 and by FExecuted **ES | Spain (138)**  
 and by FExecuted **BE | Belgium (126)**  
 and by FExecuted **TR | Turkey (101)**  
 and by FExecuted **FR | France (100)**  
 and by FExecuted **CZ | Czech Republic (64)**  
 and by FExecuted **PL | Poland (63)**  
 and by FExecuted **TW | Taiwan (62)**  
 and by FExecuted **IT | Italy (57)**  
 and by FExecuted **HU | Hungary (57)**  
 and by FExecuted **MX | Mexico (39)**  
 and by FExecuted **HK | Hong Kong (38)**  
 and by FExecuted **SA | Saudi Arabia (36)**

ORDER: by **Bot ID**

SHOW: **30** records

30 records in DB. [Hint: SQL Query.](#)

Navigation: > >> **Jump on page** << <

	#	Common	Land	IP Address	Bot Version	Rep. Count	Days	First report
<input type="checkbox"/>	1				5.1.86	0	10	[31/07/08] 02:04:...
<input type="checkbox"/>	2				5.1.86	0	11	[30/07/08] 23:55:2...
<input type="checkbox"/>	3				5.1.86	0	11	[30/07/08] 20:42:1...



# Underground economy

The spam business

Sistemi  
Operativi e  
Informatica

Massimo  
Marchi

Sicurezza e  
malware

Introduzione  
Malware &  
underground  
economy

## CAPTCHA?

- OCR, Fuzzy OCR, ...
- Soluzioni migliori?
- "Human computation"!



# Underground economy

The spam business

Sistemi  
Operativi e  
Informatica

Massimo  
Marchi

Sicurezza e  
malware

Introduzione  
Malware &  
underground  
economy

## CAPTCHA?

- OCR, Fuzzy OCR, ...
- **Soluzioni migliori?**
- “Human computation”!



# Underground economy

The spam business

Sistemi  
Operativi e  
informatica

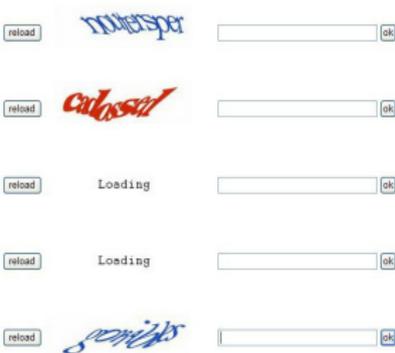
Massimo  
Marchi

Sicurezza e  
malware

Introduzione  
Malware &  
underground  
economy

## CAPTCHA?

- OCR, Fuzzy OCR, ...
- Soluzioni migliori?
- **“Human computation”!**



> 100K captcha al giorno, \$1.5-\$8 per 1000 captcha



# Underground economy

## The spam business

Sistemi  
Operativi e  
informatica

Massimo  
Marchi

Sicurezza e  
malware

Introduzione  
Malware &  
underground  
economy

## CAPTCHA?

- OCR, Fuzzy OCR, ...
- Soluzioni migliori?
- **“Human computation”!**

The screenshot shows a web browser window titled "Free gallery" with a URL of "http://". The main content area displays a CAPTCHA challenge. At the top, the word "wlnzyhlp" is written in a stylized font. Below it, a green arrow points to a small image of a green character. The text "To view next image type the chars, please" is displayed. The main image shows a woman with blonde hair (Melissa) in a room with a window and plants. Below the browser window, a chat window titled "Melissa strip" is open. It contains the following text:

Hil  
My name is Melissa. I'm 18 years old and you have come to the right place to play :)

How to play?  
Easy, enter the code that you will see and I'm taking off 1 of my things. :) Want to start strip me? Then what are you waiting for? Click the start play.



# Funzionalità del malware

## Click fraud

Sistemi Operativi e Informatica

Massimo Marchi

Sicurezza e malware

Introduzione Malware & underground economy

- *Google*: 10% dei “click” sono fraudolenti (~ \$1B)
- Clickbot.A (~ 50k host infetti)
- molti “clickbot” commerciali
- ClickJacking

IP	Country	Time	Clicks	Version	Manage
		03:30:05	0	v0.007	Block
		03:30:04	Holded	v0.007	Allow
		03:30:04	8	v0.007	Block





# Funzionalità del malware

## Anti-anti-virus

Sistemi  
Operativi e  
Informatica

Massimo  
Marchi

Sicurezza e  
malware

Introduzione  
Malware &  
underground  
economy

- kill processi in esecuzione
- vari hook per auto-start prima dell'AV
- impedire aggiornamento AV
- corruzione DB signature
- kernel-level callback via  
`PsSetLoadImageNotifyRoutine()`
- ...



# Funzionalità del malware

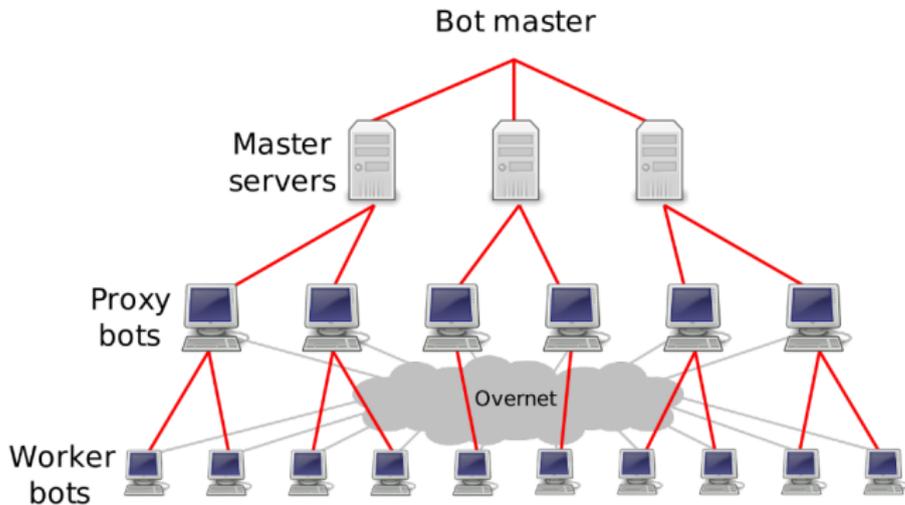
## Botnet

Sistemi  
Operativi e  
Informatica

Massimo  
Marchi

Sicurezza e  
malware

Introduzione  
Malware &  
underground  
economy





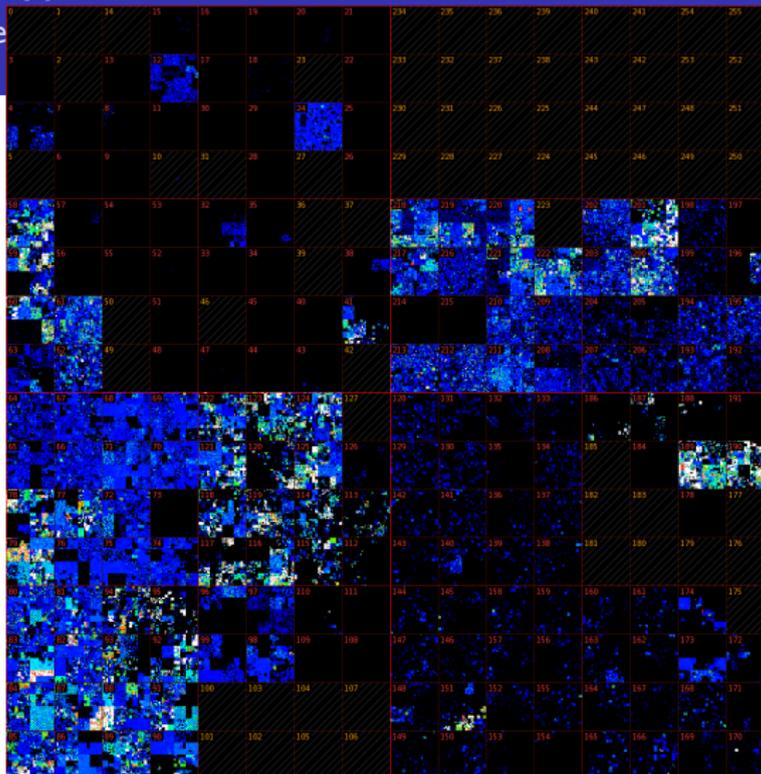
# Botnet Interne

Sistemi  
Operativi e  
Informatica

Massimo  
Marchi

Sicurezza e  
malware

Introduzione  
Malware &  
underground  
economy

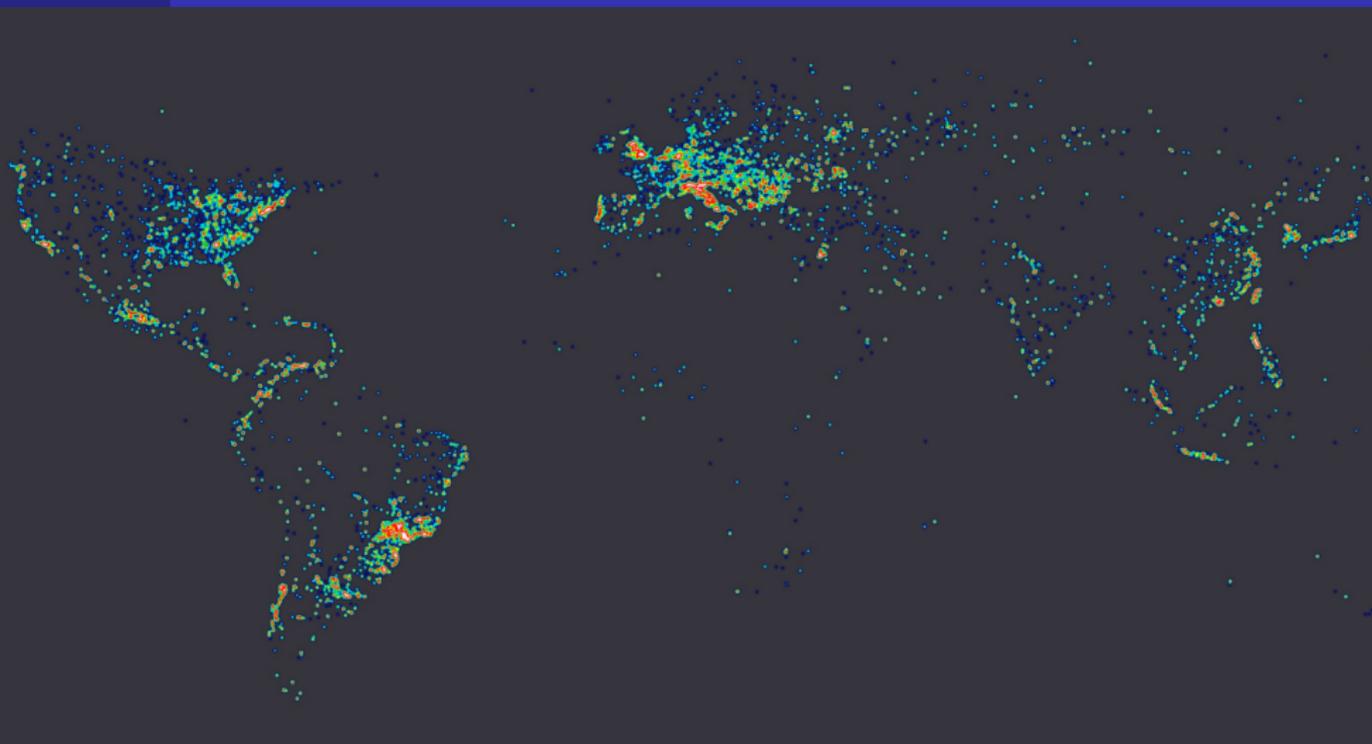


Fonte: Team Cymru



# Botnet

Conficker (29/01/2009)



1.7 milioni di host compromessi

*Fonte: Team Cymru*



# Botnet

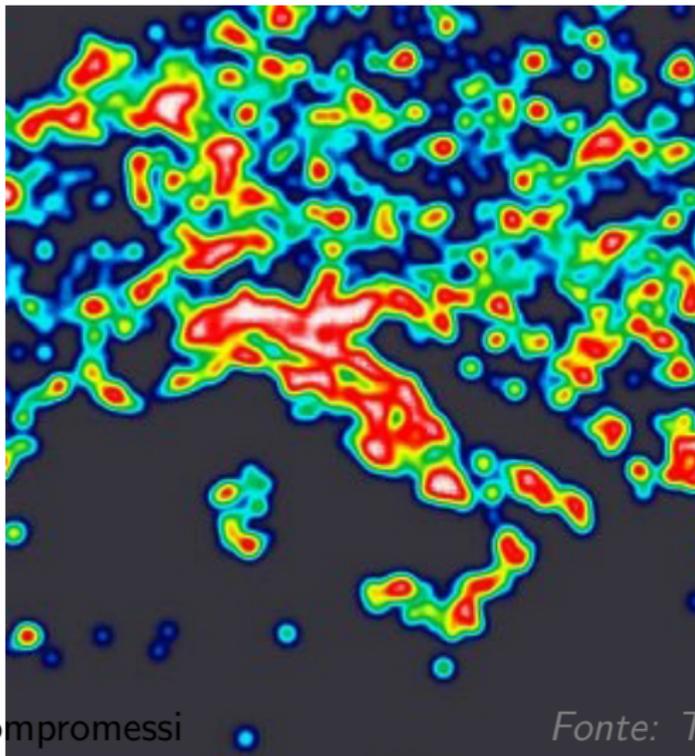
Conficker (29/01/2009)

Sistemi  
Operativi e  
Informatica

Massimo  
Marchi

Sicurezza e  
malware

Introduzione  
Malware &  
underground  
economy



1.7 milioni di host compromessi

Fonte: Team Cymru



# Botnet

## Botnet & spam

Sistemi  
Operativi e  
Informatica

Massimo  
Marchi

Sicurezza e  
malware

Introduzione  
Malware &  
underground  
economy

Nome	Dimensione	Capacità di spam
Conficker	9.000.000	10G/giorno
Kraken	495.000	9G/giorno
Srizbi	450.000	60G/giorno
Rustock	150.000	30G/giorno
Cutwail	125.000	16G/giorno
Storm	> 1.000.000	3G/giorno
Grum	50.000	2G/giorno
Mega-D	35.000	10G/giorno



# Botnet

Non solo spam...

Sistemi  
Operativi e  
Informatica

Massimo  
Marchi

Sicurezza e  
malware

Introduzione  
Malware &  
underground  
economy

Analisi di 10 giorni di traffico di rete generato da Torpig:

Unique IP Count	1.148.264
Unique Torpig keys (machines)	180.835
POP accounts	415.206
Email addresses	1.235.122
Passwords	411.039
Unique credit cards	875
Unique ATM pins	141
Unique social security numbers	21



# Tecniche di propagazione

Sistemi  
Operativi e  
Informatica

Massimo  
Marchi

Sicurezza e  
malware

Introduzione  
Malware &  
underground  
economy

<b>Propagation mechanisms</b>	<b>Percentage</b>
File sharing executables	40%
File transfer/email attachment	32%
File transfer/CIFS	28%
File sharing/P2P	19%
Remotely exploitable vulnerability	17%
SQL	3%
Back door/Kuang2	3%
Back door/SubSeven	3%
File transfer/embedded HTTP URI/Yahoo! Messenger	2%
Web	1%

*Fonte: Symantec, 2007*



# Tecniche di propagazione

## Rogue Antivirus

Sistemi Operativi e Informatica

Massimo Marchi

Sicurezza e malware

Introduzione Malware & underground economy

The screenshot shows a Windows XP desktop environment. At the top, a browser window titled "mplayer dump dvd - Links brought you by GreenMan - Iceweasel" is open. The desktop background is blue and features several icons: Local Disk (C:), Local Disk (D:), DVD-RAM Drive (E:), and Shared Documents. A "Security threat" warning is visible on the Local Disk (D:) icon. On the left side, the "System Tasks" and "Other Places" panels are visible. The "System Tasks" panel includes options like "View system information", "Add or remove programs", and "Change a settings". The "Other Places" panel includes "My Network Places", "My Documents", "Shared Documents", and "Control Panel". The "Details" panel shows "My Computer" and "System Folder". In the center, a progress bar indicates an "81% files - System scan" of "C:\Documents and Settings\My Documents", with a total of 3831 files. At the bottom, a security warning window titled "Your Computer is Infected" displays a "WARNING! Spyware threat has been detected on your PC." Below the warning, a table lists detected threats:

C:\Documents and Settings\user\Local Set...	Spyware	System Soap Pro
C:\Documents and Settings\user...	Spyware	AntiLamer Light
C:\Documents and Settings\user\Cookies	Virus	MC 30 Day
C:\Documents and Settings\user\Cookies	Virus	SoftEther

A "Full system cleanup" button is located at the bottom of the warning window. The taskbar at the bottom of the screen shows standard Windows XP navigation icons.



# Tecniche di propagazione

## Rogue Antivirus

Sistemi Operativi e Informatica

Massimo Marchi

Sicurezza e malware

Introduzione Malware & underground economy

The screenshot shows a Windows XP desktop environment. In the background, a web browser window titled "mplayer dump dvd - Links brought you by GreenMan - Iceweasel" is open. The desktop background displays "Local Disk (C:)", "Local Disk (D:)", and "DVD-RW".

In the foreground, two windows are visible:

- Opening MalwareDefender2009.exe**: A dialog box asking for action on a file. The file is identified as "MalwareDefender2009.exe", a Windows Executable from "http://78.159.122.156". The "Open with" dropdown is set to "wine-safe (default)".
- WARNING!!! Scan results**: A security warning window with a red header. It contains a table of scan results and a red banner at the bottom stating "364 infected files found".

Type	Alert level
Spyware	Average
Spyware	Average
Spyware	Danger
Spyware	High
Virus	High
Virus	High
Virus	Critical
Spyware	Critical
Spyware	Critical
Virus	Critical

! 364 infected files found

Click the "Erase all threats" button to erase all spyware and viruses from Windows

Erase all threats



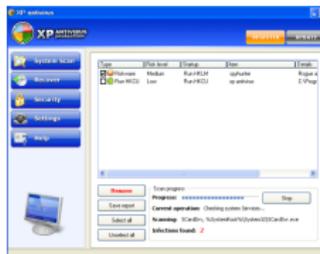
# Tecniche di propagazione Rogue Antivirus

Sistemi Operativi e Informatica

Massimo Marchi

Sicurezza e malware

Introduzione  
Malware & underground economy





# Situazione attuale

Sistemi  
Operativi e  
Informatica

Massimo  
Marchi

Sicurezza e  
malware

Introduzione  
Malware &  
underground  
economy

- malware vs AV
- AV in posizione svantaggiata

*The amount of new malware has never been higher.  
Our labs are receiving an average of **25,000**  
malware samples every day, seven days a week.*

F-Secure, 2008



# Perchè una così grande diffusione?

Sistemi  
Operativi e  
Informatica

Massimo  
Marchi

Sicurezza e  
malware

Introduzione  
Malware &  
underground  
economy

- omogeneità, connettività e configurazione
- scarsa attenzione
- incentivo economico



## Removing admin rights stymies 92% of Microsoft's bugs

Bulk of IE's bugs in '08 could have been blocked, says vendor

By Gregg Keizer



# Perchè una così grande diffusione?

- omogeneità, connettività e configurazione
- **scarsa attenzione**
- incentivo economico

Sistemi Operativi e Informatica

Massimo Marchi

Sicurezza e malware

Introduzione Malware & underground economy



What is means "Downloadable Software"?



# Perchè una così grande diffusione?

Sistemi  
Operativi e  
Informatica

Massimo  
Marchi

Sicurezza e  
malware

Introduzione  
Malware &  
underground  
economy

- omogeneità, connettività e configurazione
- scarsa attenzione
- **incentivo economico**



## Global ATM Caper Nets Hackers \$9 Million in One Day

By Kevin Poulsen February 03, 2009 | 2:43:39 PM Categories: [Crime](#)

A carefully coordinated global ATM heist last November resulted in a one-day haul of \$9 million in cash, after a hacker penetrated a server at payment processor RBS WorldPay, New York's Fox 5 reports.

RBS WorldPay announced on December 23 that they'd been hacked, and personal information on approximately 1.5 million payroll-card and gift-card customers had been stolen. (Payroll cards are debit cards issued and recharged by employers as an alternative to paychecks and direct-deposit.) Now we know that account numbers and other mag-stripe data needed to clone the debit cards were also



00:11 / 03:39





# Situazione malware detector

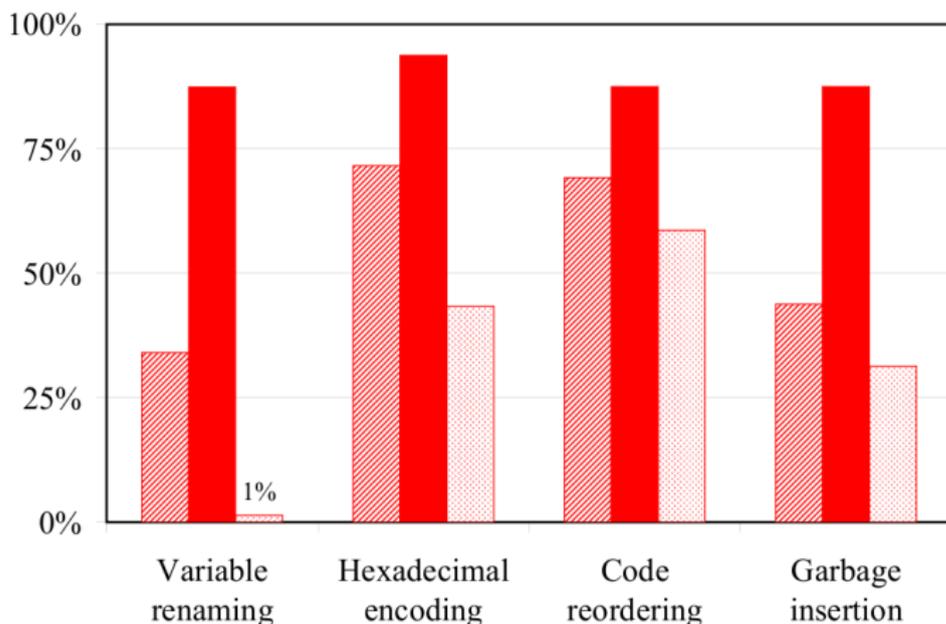
## Signature-based detectors

Sistemi Operativi e Informatica

Massimo Marchi

Sicurezza e malware

Introduzione Malware & underground economy



Fonte: *Testing Malware Detectors* – M. Christodorescu, S. Jha, 2004



# Situazione malware detector

... qualche dato più recente

Sistemi  
Operativi e  
Informatica

Massimo  
Marchi

Sicurezza e  
malware

Introduzione  
Malware &  
underground  
economy

Rank	Detected	Missed	Product
1	91%	178	Sophos
2	91%	179	AntiVir
3	90%	194	Microsoft
4	90%	195	AVG
5	90%	202	Ikarus
6	89%	213	BitDefender
7	88%	241	Norman
8	88%	247	TrendMicro
9	87%	259	Kaspersky
10	87%	268	F-Secure

Fonte: SRI International + VirusTotal, campione di 2064 malware



# Tecniche di *self-defense*

## Packing

Sistemi  
Operativi e  
Informatica

Massimo  
Marchi

Sicurezza e  
malware

Introduzione  
Malware &  
underground  
economy

- codice maligno nascosto da 1<sup>+</sup> layer di compressione/cifratura
- decompressione/decrifatura a runtime

Malicious  
code



# Tecniche di *self-defense*

## Packing

Sistemi  
Operativi e  
Informatica

Massimo  
Marchi

Sicurezza e  
malware

Introduzione  
Malware &  
underground  
economy

- codice maligno nascosto da 1<sup>+</sup> layer di compressione/cifratura
- decompressione/decrifatura a runtime

Malicious  
code



# Tecniche di *self-defense*

## Packing

Sistemi  
Operativi e  
Informatica

Massimo  
Marchi

Sicurezza e  
malware

Introduzione  
Malware &  
underground  
economy

- codice maligno nascosto da 1<sup>+</sup> layer di compressione/cifratura
- decompressione/decrifatura a runtime

Unpacking  
routine

Malicious  
code



# Tecniche di *self-defense*

## Packing

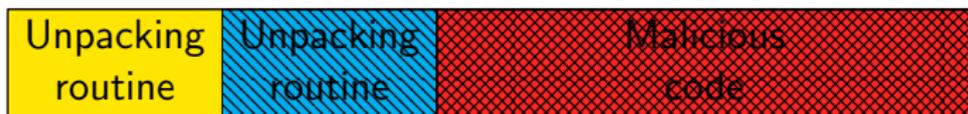
Sistemi  
Operativi e  
Informatica

Massimo  
Marchi

Sicurezza e  
malware

Introduzione  
Malware &  
underground  
economy

- codice maligno nascosto da 1<sup>+</sup> layer di compressione/cifratura
- decompressione/decrifatura a runtime





# Tecniche di *self-defense*

## Packing

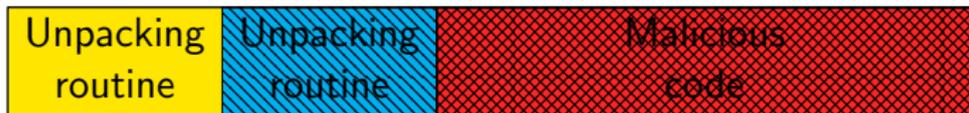
Sistemi  
Operativi e  
informatica

Massimo  
Marchi

Sicurezza e  
malware

Introduzione  
Malware &  
underground  
economy

- codice maligno nascosto da 1<sup>+</sup> layer di compressione/cifratura
- decompressione/decrifatura a runtime



### Problema

- ~ 80% del malware è “packed”
- 200 famiglie di packer, 2000 varianti
- backlog di ~ 90 famiglie

Fonte: Symantec, 2008



# Tecniche di *self-defense*

## Polimorfismo

Sistemi  
Operativi e  
Informatica

Massimo  
Marchi

Sicurezza e  
malware

Introduzione  
Malware &  
underground  
economy

- ancora corpo cifrato
- il malware è in grado di mutare la routine di cifratura

### Esempio

```
1  lea si, corpo_virus
2  nop
3  mov sp, 0682h
4  sub ax, bx
5  ciclo:
6  xor [si],si
7  inc cx
8  xor [si],sp
9  inc si
10 add bx, cx
11 dec sp
12 jnz ciclo
13 corpo_virus:
14 ...
```

- le istruzioni evidenziate sono “junk code”
- possibile anche *instruction reordering*, *instruction substitution*, *register replacement*, ...
- elevato numero di mutazioni possibili
- difficile individuare una *signature* costante



# Tecniche di *self-defense*

## Metamorfismo

- “*metamorphics are body-polymorphics*” (Igor Muttik)

### W95/Regswap

1	5A <b>pop</b> edx	1	58 <b>pop</b> eax
2	BF04000000 <b>mov</b> edi,0004h	2	BB04000000 <b>mov</b> ebx,0004h
3	8BF5 <b>mov</b> esi,ebp	3	8BD5 <b>mov</b> edx,ebp
4	B80C000000 <b>mov</b> eax,000Ch	4	BF0C000000 <b>mov</b> edi,000Ch
5	81C288000000 <b>add</b> edx,0088h	5	81C088000000 <b>add</b> eax,0088h
6	8B1A <b>mov</b> ebx,[edx]	6	8B30 <b>mov</b> esi,[eax]

### W32/Evol

1	BF0F000055 <b>mov</b> edi,5500000Fh	1	BB0F000055 <b>mov</b> ebx,5500000Fh
2	893E <b>mov</b> [esi],edi	2	891E <b>mov</b> [esi],ebx
3	5F <b>pop</b> edi	3	<del>5B <b>pop</b> ebx</del>
4	52 <b>push</b> edx	4	51 <b>push</b> ecx
5	B640 <b>mov</b> dh,40	5	B9CB00C05F <b>mov</b> ecx,5FC000CBh
6	BA8BEC5151 <b>mov</b> edx,5151EC8Bh	6	81C1C0EB91F1 <b>add</b> ecx,F191EBC0h
7	53 <b>push</b> ebx	7	894E04 <b>mov</b> [esi+0004],ecx
8	8BDA <b>mov</b> ebx,edx		
9	895E04 <b>mov</b> [esi+0004],ebx		

Sistemi  
Operativi e  
Informatica

Massimo  
Marchi

Sicurezza e  
malware

Introduzione  
Malware &  
underground  
economy



# Tecniche di *self-defense*

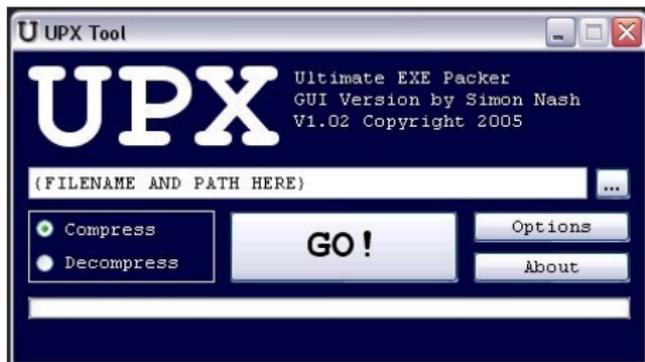
Implementazione difficile?

Sistemi  
Operativi e  
Informatica

Massimo  
Marchi

Sicurezza e  
malware

Introduzione  
Malware &  
underground  
economy





# Tecniche di *self-defense*

Implementazione difficile?

Sistemi Operativi e Informatica

Massimo Marchi

Sicurezza e malware

Introduzione Malware & underground economy

The screenshot displays the Themida v1.0.0.0 application window. The title bar reads "Themida v1.0.0.0 | Project: E:\Projects\Tests\test.tmd \*". The main window features a menu bar with "New", "Open...", "Save", "Save As...", "Protect", "Help", and "About...". A left sidebar contains "Options" and "Help" sections. The "Options" section lists: Application Information, Protection Options, Code Replace, Customized Dialogs, and Software Updates. The "Help" section lists: Protection Options, Protect Now, and SecureEngine Technology. The main area is titled "Protection Options" and contains a grid of settings, all of which are checked and enabled:

- Memory Guard**: Enable Protection
- Advanced API-Wrapping**: Enable Protection
- Anti Dumpers**: Enable Protection
- Virtual Machine Emulation**: Enable Protection
- Entry Point Obfuscation**: Enable Protection
- Metamorph Security**: Enable Protection
- Resources Encryption**: Enable Encryption
- Advanced Debugger Mon.**: Enable Protection
- Debug Interrupts**: Enable Protection
- When Debugger Found**: Display Message
- Compression**: Application, Resources, SecureEngine®
- Monitor Blockers**: Files Monitors, Registry Monitors
- Delphi/BCB Form Protection**: Enable Protection

At the bottom left, there is a "Microsoft .net compatible" logo and the version number "1.0.0.0".



# Next-generation malware detector

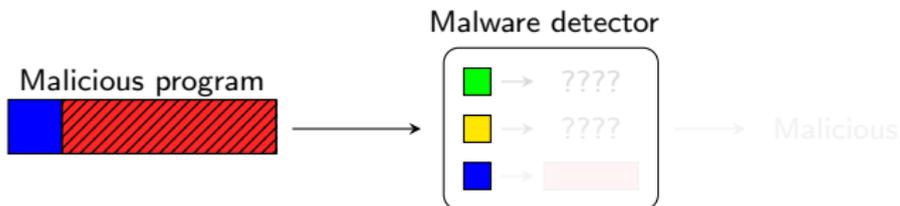
Situazione attuale: Algorithmic unpacking

Sistemi Operativi e Informatica

Massimo Marchi

Sicurezza e malware

Introduzione  
Malware & underground economy



## Problemi

- ogni packer richiede un unpacker specifico
- troppe famiglie di packer
- Symantec: da 6 ore a 6 mesi per packer
- multi-layer packing



# Next-generation malware detector

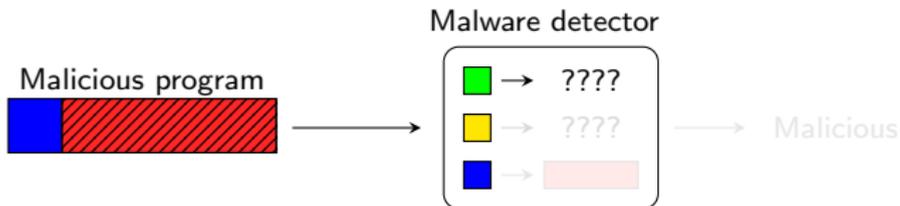
Situazione attuale: Algorithmic unpacking

Sistemi Operativi e Informatica

Massimo Marchi

Sicurezza e malware

Introduzione  
Malware & underground economy



## Problemi

- ogni packer richiede un unpacker specifico
- **troppe** famiglie di packer
- Symantec: da 6 ore a **6 mesi** per packer
- multi-layer packing



# Next-generation malware detector

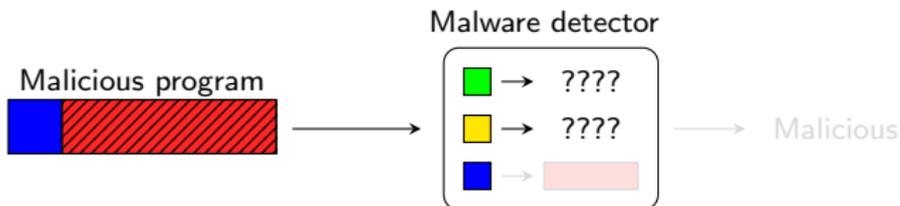
Situazione attuale: Algorithmic unpacking

Sistemi  
Operativi e  
Informatica

Massimo  
Marchi

Sicurezza e  
malware

Introduzione  
Malware &  
underground  
economy



## Problemi

- ogni packer richiede un unpacker specifico
- **troppe** famiglie di packer
- Symantec: da 6 ore a **6 mesi** per packer
- multi-layer packing



# Next-generation malware detector

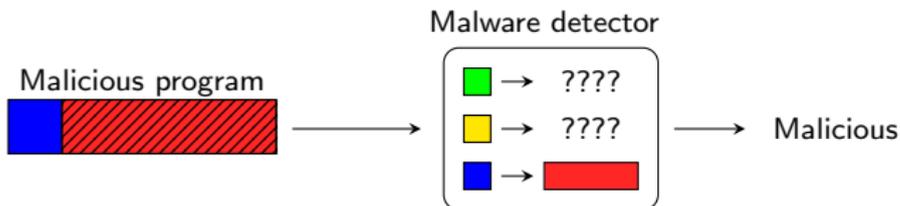
Situazione attuale: Algorithmic unpacking

Sistemi  
Operativi e  
Informatica

Massimo  
Marchi

Sicurezza e  
malware

Introduzione  
Malware &  
underground  
economy



## Problemi

- ogni packer richiede un unpacker specifico
- **troppe** famiglie di packer
- Symantec: da 6 ore a **6 mesi** per packer
- multi-layer packing



# Next-generation malware detector

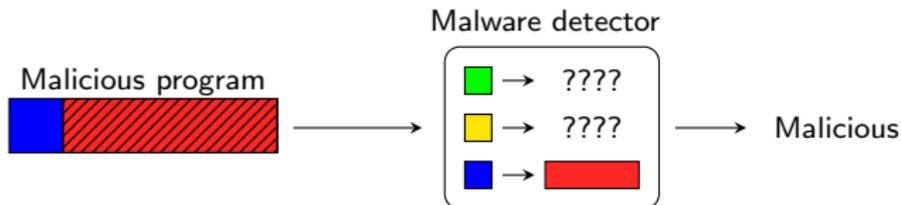
Situazione attuale: Algorithmic unpacking

Sistemi  
Operativi e  
Informatica

Massimo  
Marchi

Sicurezza e  
malware

Introduzione  
Malware &  
underground  
economy



## Problemi

- ogni packer richiede un unpacker specifico
- **troppe** famiglie di packer
- Symantec: da 6 ore a **6 mesi** per packer
- multi-layer packing



# Next-generation malware detector

Unpacking generico

Sistemi  
Operativi e  
Informatica

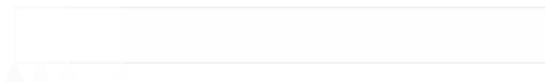
Massimo  
Marchi

Sicurezza e  
malware

Introduzione  
Malware &  
underground  
economy

## Idea

- analisi dinamica
- emulazione/tracing dell'esecuzione fino al termine della routine di unpacking



## Unpackatori

- *OmniUnpack*
- *Justin*
- *Renovo*
- *PolyUnpack*



# Next-generation malware detector

Unpacking generico

Sistemi  
Operativi e  
Informatica

Massimo  
Marchi

Sicurezza e  
malware

Introduzione  
Malware &  
underground  
economy

## Idea

- analisi dinamica
- emulazione/tracing dell'esecuzione fino al termine della routine di unpacking



## Unpackers

- *OmniUnpack*
- Justin
- Renovo
- PolyUnpack



# Next-generation malware detector

Unpacking generico

Sistemi  
Operativi e  
Informatica

Massimo  
Marchi

Sicurezza e  
malware

Introduzione  
Malware &  
underground  
economy

## Idea

- analisi dinamica
- emulazione/tracing dell'esecuzione fino al termine della routine di unpacking



Un po' di nomi...

- *OmniUnpack*
- Justin
- Renovo
- PolyUnpack



# Next-generation malware detector

Unpacking generico

Sistemi  
Operativi e  
Informatica

Massimo  
Marchi

Sicurezza e  
malware

Introduzione  
Malware &  
underground  
economy

## Idea

- analisi dinamica
- emulazione/tracing dell'esecuzione fino al termine della routine di unpacking



Un po' di nomi...

- *OmniUnpack*
- Justin
- Renovo
- PolyUnpack



# Next-generation malware detector

Unpacking generico

Sistemi  
Operativi e  
Informatica

Massimo  
Marchi

Sicurezza e  
malware

Introduzione  
Malware &  
underground  
economy

## Idea

- analisi dinamica
- emulazione/tracing dell'esecuzione fino al termine della routine di unpacking



## Un po' di nomi...

- *OmniUnpack*
- Justin
- Renovo
- PolyUnpack



# Next-generation malware detector

Unpacking generico

Sistemi Operativi e Informatica

Massimo Marchi

Sicurezza e malware

Introduzione Malware & underground economy

## Idea

- analisi dinamica
- emulazione/tracing dell'esecuzione fino al termine della routine di unpacking



## Un po' di nomi...

- *OmniUnpack*
- Justin
- Renovo
- PolyUnpack



# Next-generation malware detector

Analisi comportamentale

Sistemi  
Operativi e  
Informatica

Massimo  
Marchi

Sicurezza e  
malware

Introduzione  
Malware &  
underground  
economy

- signature-based detection è troppo debole
- ⇒ verso tecniche più “*semantiche*”

## Soluzioni

- analisi dinamica
- granularità a livello di system call
- NovaShield, ThreatFire, Sana Security, ...

## Problemi

- performance
- falsi positivi
- information leakage
- ...



# Next-generation malware detector

Analisi comportamentale

Sistemi  
Operativi e  
Informatica

Massimo  
Marchi

Sicurezza e  
malware

Introduzione  
Malware &  
underground  
economy

- signature-based detection è troppo debole
- ⇒ verso tecniche più “*semantiche*”

## Soluzioni

- analisi dinamica
- granularità a livello di system call
- NovaShield, ThreatFire, Sana Security, ...

## Problemi

- performance
- falsi positivi
- information leakage
- ...



# Remediation

Sistemi  
Operativi e  
informatica

Massimo  
Marchi

Sicurezza e  
malware

Introduzione  
Malware &  
underground  
economy

- detection non è sempre possibile
- **remediation** dell'infezione
- ... *ma funziona?*



# Remediation

Sistemi Operativi e Informatica

Massimo Marchi

Sicurezza e malware

Introduzione Malware & underground economy

- detection non è sempre possibile
- **remediation** dell'infezione
- ... *ma funziona?*

