

Analisi dei Malware

Alfredo De Santis

Dipartimento di Informatica
Università di Salerno

ads@dia.unisa.it

<http://www.dia.unisa.it/professori/ads>



Maggio 2017

Sommario

- Analisi dei Malware
 - Analisi Statica
 - Analisi Dinamica
 - White Box
 - Black Box
 - Malware su Dispositivi Mobile
 - Strumenti

Analisi dei Malware - 1/3

- Analizzare un malware significa cercare di comprenderne il comportamento, al fine di
 - **Identificare il malware**
 - **Difendersi dal malware**
 - **Eliminare il malware**
 - **Sviluppare adeguate contromisure verso il malware**



Analisi dei Malware - 2/3

- Durante l'analisi di un malware è necessario tener ben presente che si sta analizzando software dannoso
 - Sono necessarie opportune precauzioni
- In alcuni contesti è possibile effettuare un'infezione "controllata"
 - Al fine di reperire informazioni utili sul malware stesso



Analisi dei Malware - 3/3

- Esistono diverse metodologie per l'analisi di software malevolo
 - Analisi Statica
 - Analisi Dinamica
- Analisi *statica* e *dinamica* rappresentano due approcci diversi, ma complementari
 - Di solito devono essere usati entrambi per un'analisi approfondita di un malware



Analisi dei Malware

Analisi Statica - 1/4

- L'analisi statica definisce le metodologie per l'analisi del codice e/o la struttura di un malware
 - Per determinarne il suo funzionamento
- Durante l'analisi statica il malware **non viene eseguito**

Analisi dei Malware

Analisi Statica - 2/4

- Partendo dall'eseguibile di un malware si possono ottenere diverse informazioni
- Esistono vari modi per farlo
 - Utilizzando software anti-virus/anti-malware per confermare la natura maliziosa del malware
 - Utilizzando funzioni hash per identificare il malware
 - Analizzando stringhe, funzioni e header presenti nel file

Analisi dei Malware

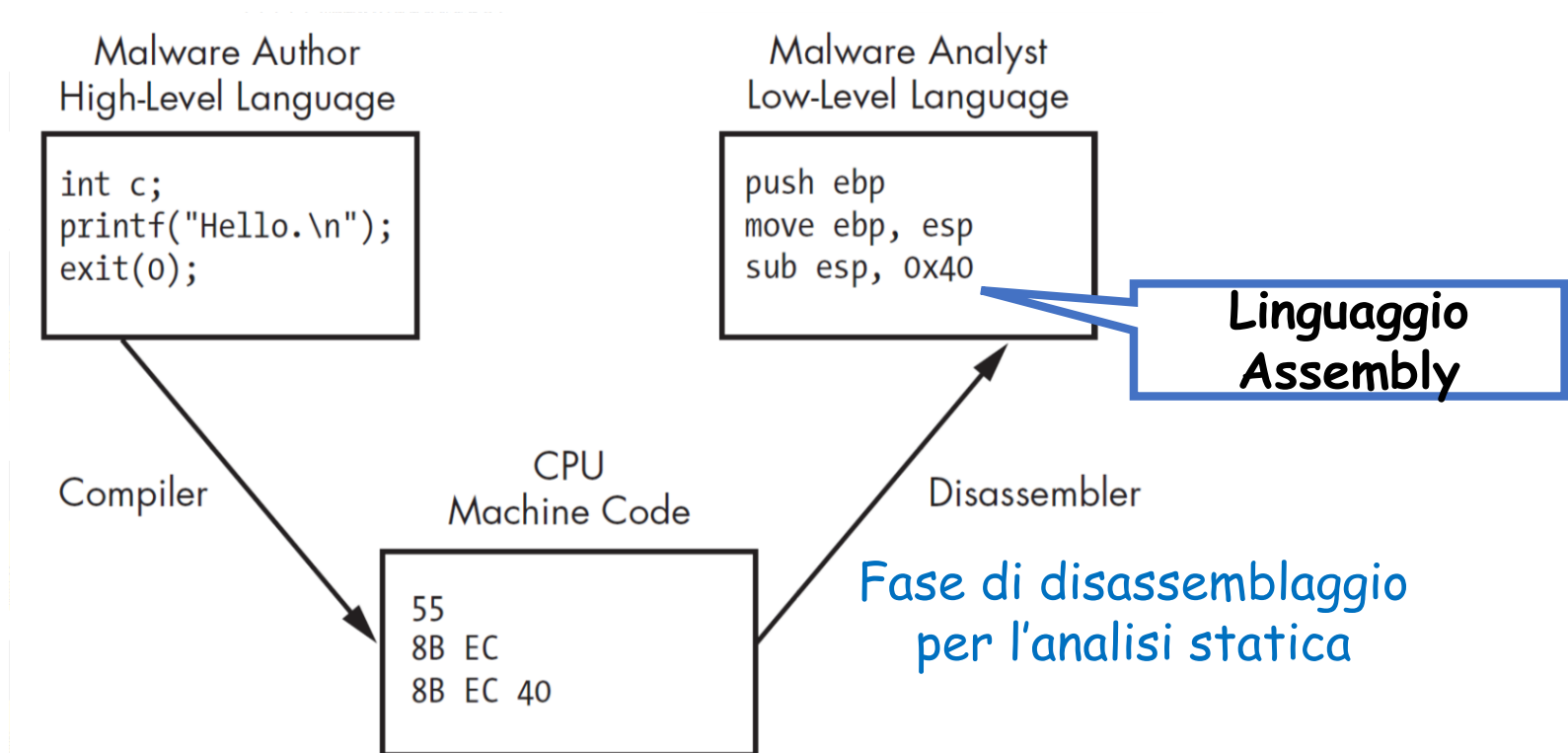
Analisi Statica - 3/4

- I malware sono generalmente programmati mediante linguaggi di alto livello
 - Il codice effettivamente eseguito dalla CPU (linguaggio di basso livello) è generato dal compilatore
- L'analisi dei malware viene eseguita su linguaggi di basso livello
 - Codice assembly
- Mediante i *disassemblatori* è possibile generare codice assembly
 - Tale codice può essere analizzato e compreso durante l'analisi statica

Analisi dei Malware

Analisi Statica - 4/4

➤ Esempio di Disassemblatore



Analisi dei Malware

Analisi Dinamica - 1/4

- L'analisi dinamica viene di solito effettuata dopo quella statica
- L'analisi dinamica consiste nell'esaminare un malware durante la sua esecuzione
 - Osservandone il comportamento in maniera analoga a quello che risulterebbe all'utente
- Mediante l'analisi dinamica è possibile ottenere informazioni riguardanti il funzionamento del malware in esame
- **Esempio**
 - Analizzando un malware appartenente alla categoria dei KeyLogger è possibile individuare in quale file ed in che modo vengono memorizzate e trasmesse le informazioni

Analisi dei Malware

Analisi Dinamica - 2/4

- Quando si effettua l'analisi dinamica è necessario procedere con attenzione
 - L'esecuzione del malware senza le adeguate protezioni potrebbe portare
 - Alla diffusione del malware su altre macchine o sistemi informatici mediante la rete
 - Alla contaminazione del sistema stesso su cui il malware viene eseguito e dei dati in esso presenti



Analisi dei Malware

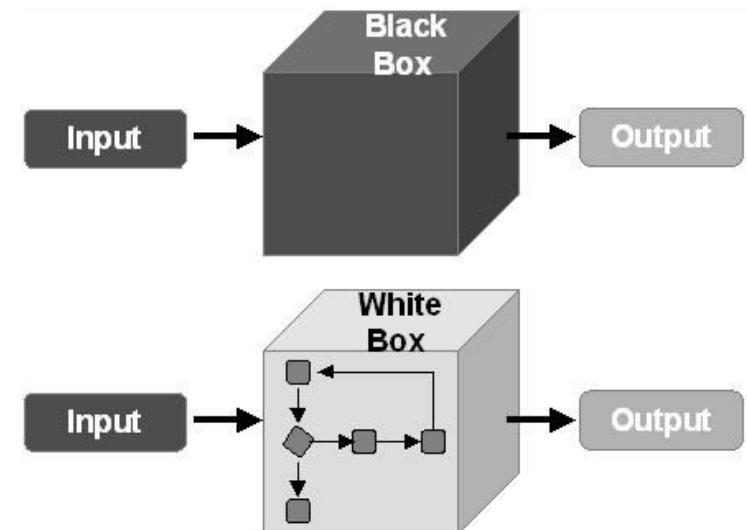
Analisi Dinamica - 3/4

- Per l'analisi dinamica generalmente si utilizza una macchina virtuale, o eventualmente una macchina fisica dedicata
 - La macchina virtuale è connessa ad una rete *air-gapped* (*air-gap*, letteralmente vuoto d'aria)
 - Protetta dall'accesso ad Internet per evitare possibili diffusioni del malware su altre macchine
- Senza l'analisi dinamica sarebbe estremamente difficile determinare i reali effetti dannosi prodotti dal malware

Analisi dei Malware

Analisi Dinamica - 4/4

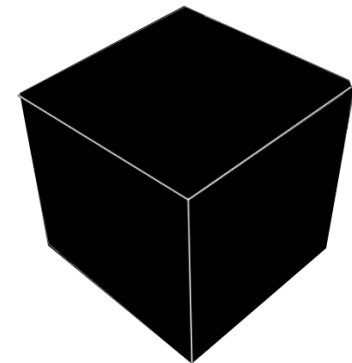
- Durante l'analisi dinamica si utilizzano *strumenti di debugging*
 - Per analizzare *step by step* il comportamento del malware e la sua influenza sul sistema
- Esistono due approcci per l'analisi dinamica di un malware
 - Black Box
 - White Box



Analisi dei Malware

Analisi Dinamica - Black Box - 1/2

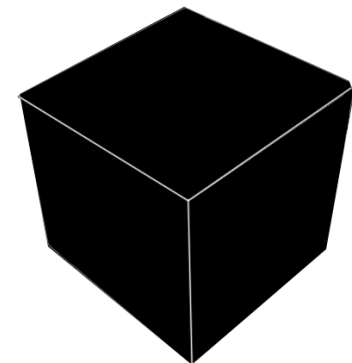
- L'approccio *Black Box* si focalizza sull'analisi degli effetti derivanti dall'esecuzione del malware
 - Senza soffermarsi sulla comprensione del comportamento e sui meccanismi che innescano effettivamente le attività malevole
- L'approccio Black Box è quindi un approccio "superficiale"



Analisi dei Malware

Analisi Dinamica - Black Box - 2/2

- Essenzialmente, l'approccio Black Box rappresenta una sorta di monitoraggio del malware
- Non può essere usato per ottenere informazioni dettagliate
- Ha notevoli vantaggi
 - Tempistiche brevi di analisi
 - Poco dispendioso
 - Etc.



Analisi dei Malware

Analisi Dinamica - White Box - 1/3

- A differenza dell'approccio Black Box, l'approccio **White Box** è più profondo
- È necessario conoscere dettagli sulle caratteristiche e sul codice del malware in esame



Analisi dei Malware

Analisi Dinamica - White Box - 2/3

- Durante l'analisi White Box vengono analizzati tutti gli aspetti dell'esecuzione del malware
- In particolare, vengono analizzati tutti quegli aspetti che conducono
 - Dallo stato del sistema prima dell'infezione del malware
 - Allo stato del sistema dopo l'esecuzione del malware stesso



Analisi dei Malware

Analisi Dinamica - White Box - 3/3

- Per l'approccio White Box è necessario
 - Conoscere e comprendere il codice di esecuzione del malware
 - Osservare il malware per un certo lasso di tempo
- N.B. Per l'analisi possono essere necessari strumenti specifici
 - Debugger
 - Editor
 - Etc.



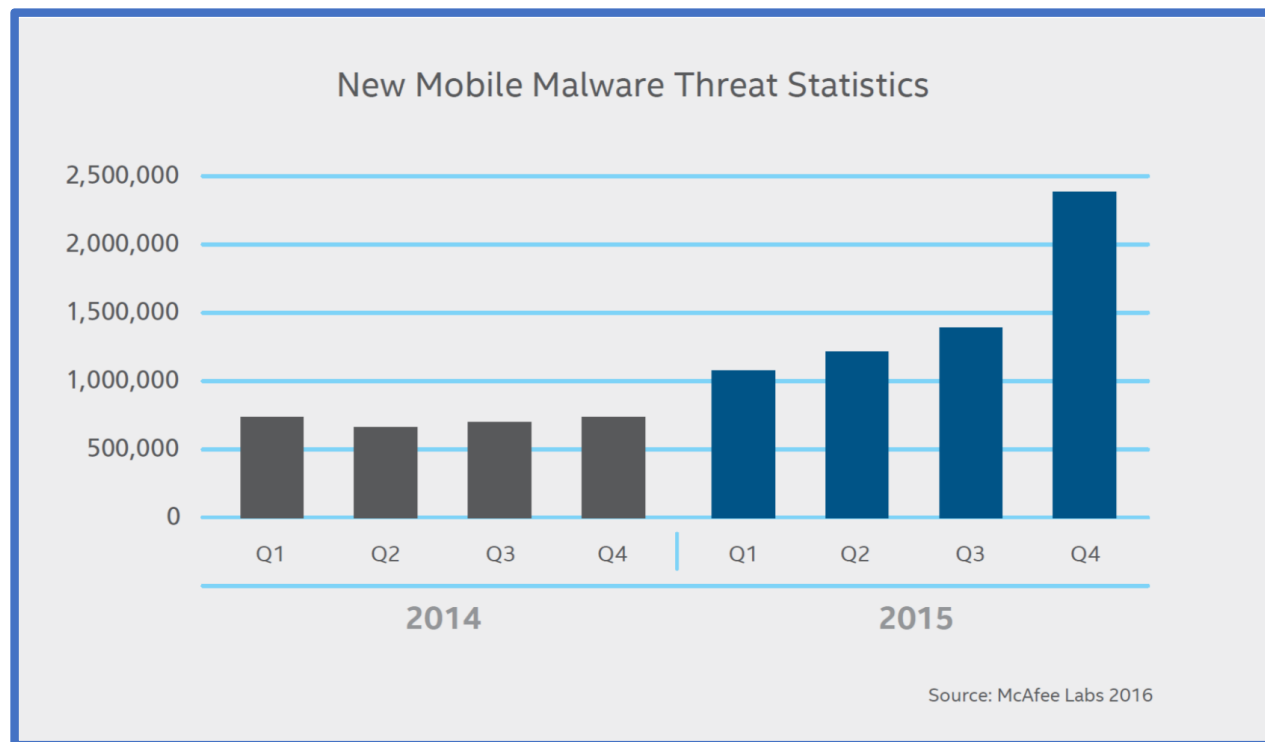
Analisi dei Malware su Dispositivi Mobile - 1/8

- I malware per dispositivi mobile hanno struttura e meccanismi di diffusione diversi rispetto a quelli per piattaforme desktop
- Con la sempre crescente diffusione dei dispositivi mobile a livello globale, si è verificato un significativo aumento anche per quanto riguarda i malware su tali dispositivi



Analisi dei Malware su Dispositivi Mobile - 2/8

- Malware identificati su dispositivi mobile
 - Anni considerati: 2014 e 2015



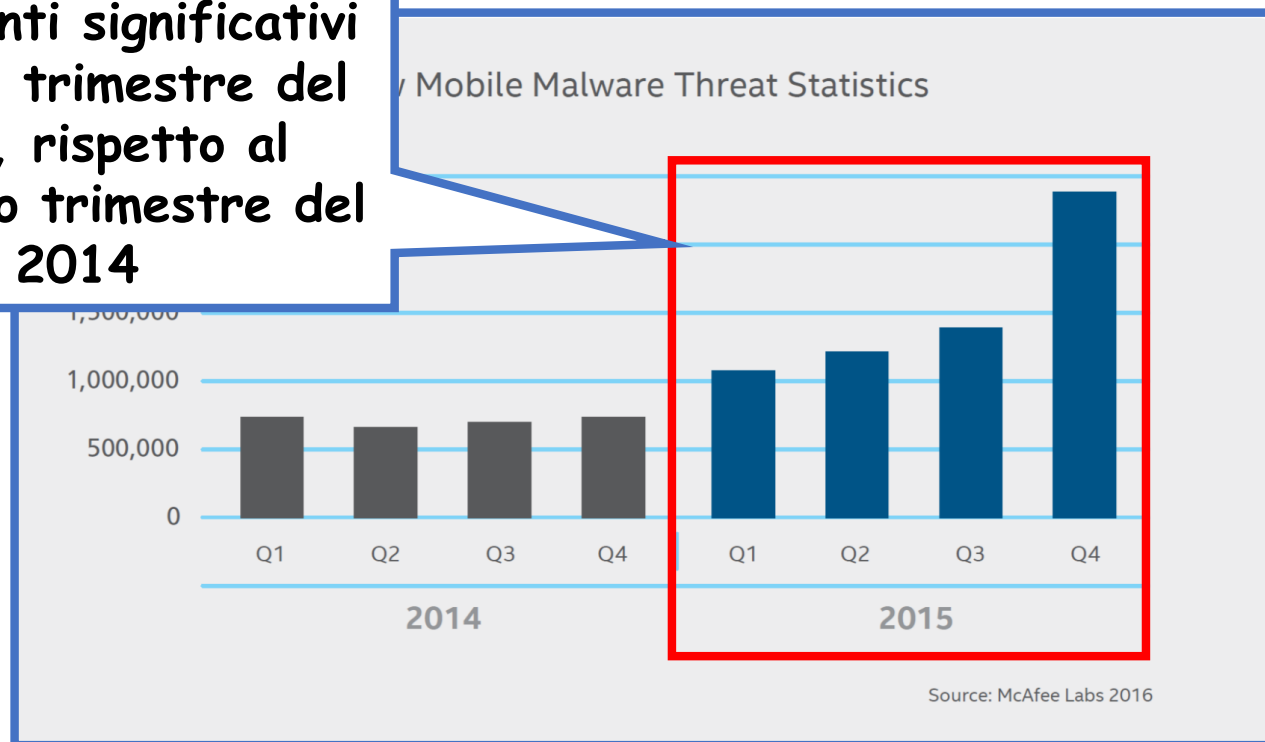
Fonte

<http://www.mcafee.com/us/resources/reports/rp-mobile-threat-report-2016.pdf>

Analisi dei Malware su Dispositivi Mobile - 2/8

- Malware identificati su dispositivi mobile
 - Anni considerati: 2014 e 2015

Incrementi significativi per ogni trimestre del 2015, rispetto al medesimo trimestre del 2014

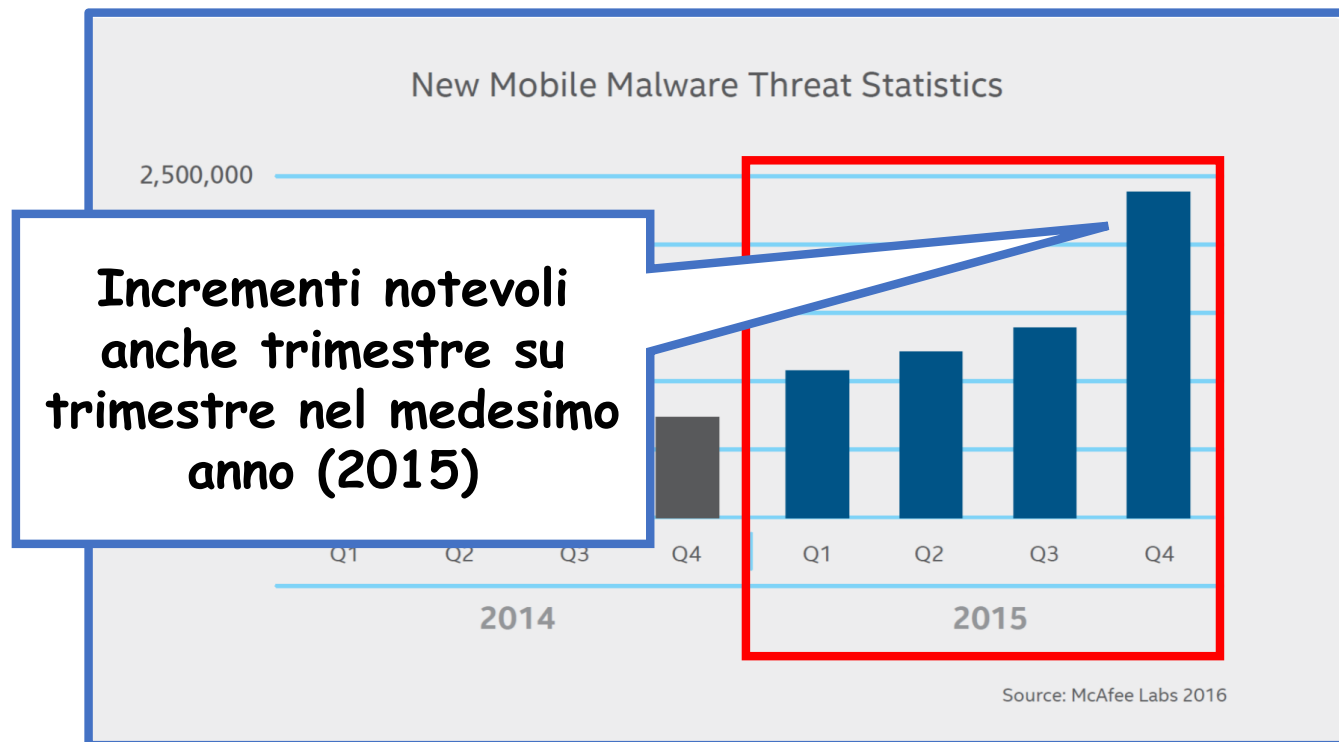


Fonte

<http://www.mcafee.com/us/resources/reports/rp-mobile-threat-report-2016.pdf>

Analisi dei Malware su Dispositivi Mobile - 2/8

- Malware identificati su dispositivi mobile
 - Anni considerati: 2014 e 2015

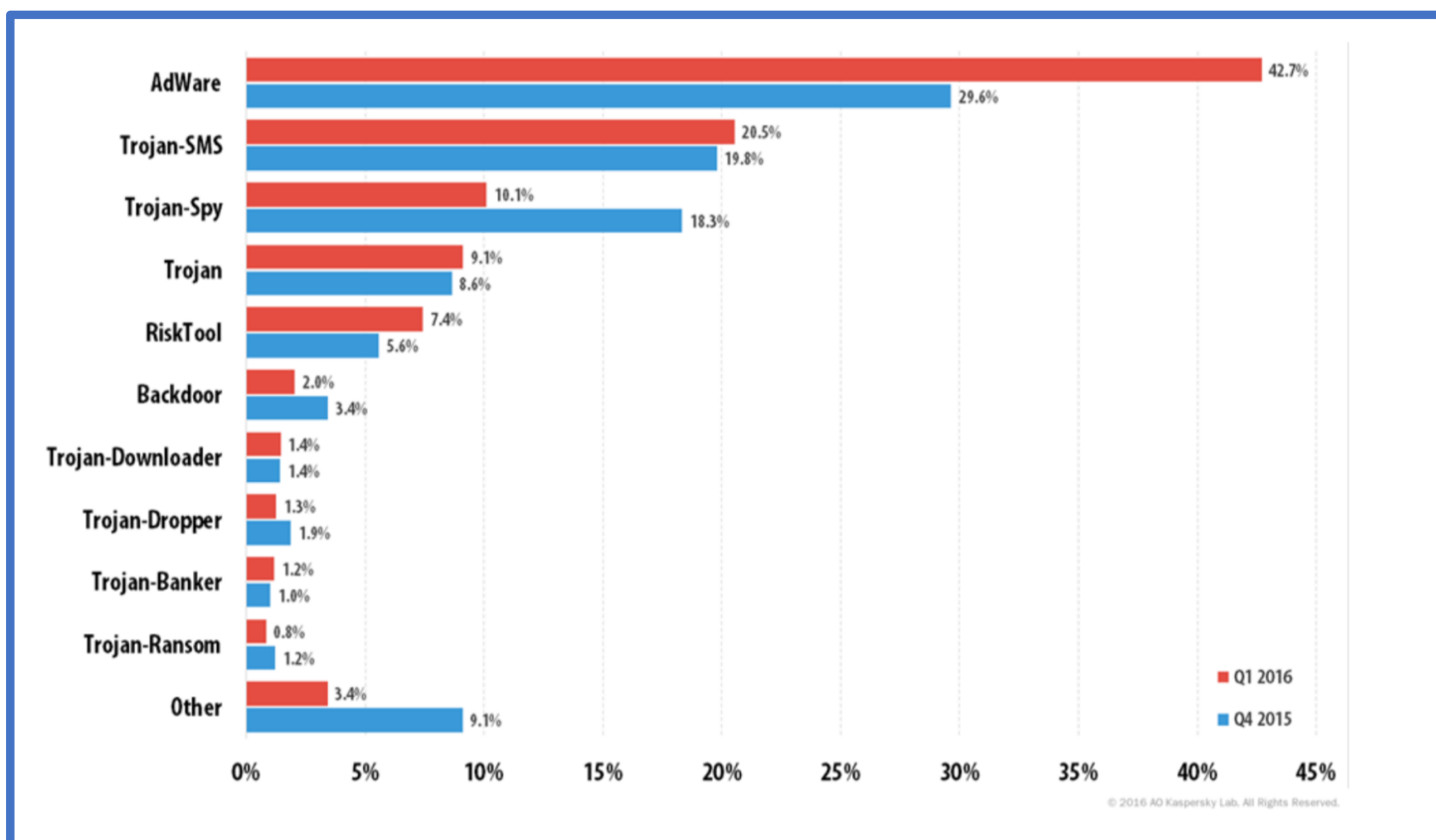


Fonte

<http://www.mcafee.com/us/resources/reports/rp-mobile-threat-report-2016.pdf>

Analisi dei Malware su Dispositivi Mobile - 3/8

- Distribuzione dei nuovi malware per tipologia
 - Q1 2016 vs Q4 2015



Fonte

https://securelist.com/files/2016/05/Q1_2016_MW_report_FINAL_eng.pdf

Analisi dei Malware su Dispositivi Mobile - 3/8

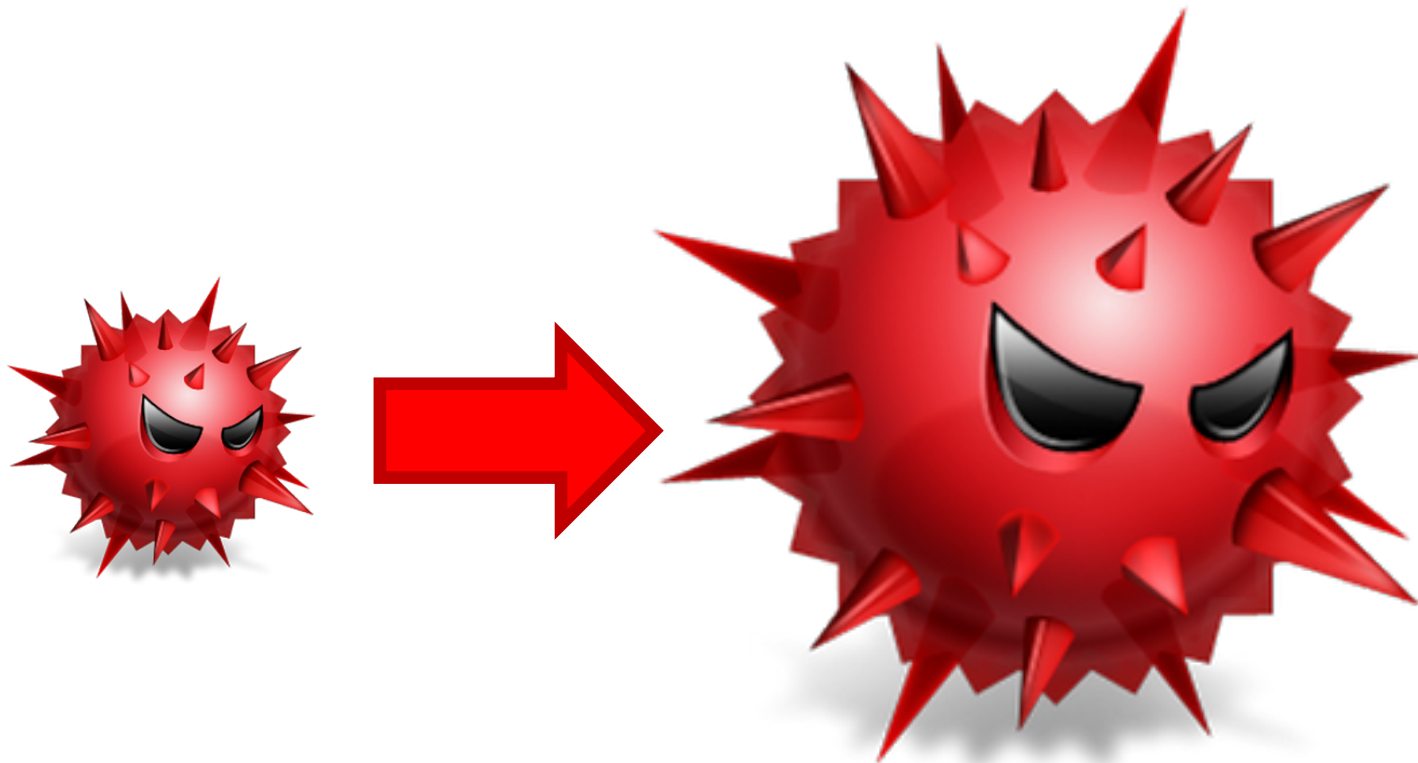
- Il rapporto annuale di Kaspersky Lab, denominato "*Mobile Virusology*", ha evidenziato che
 - Il numero di malware per dispositivi mobile nel 2016 è triplicato rispetto al 2015
 - Sono stati individuati **40 milioni di tentativi di attacco**
 - Sono stati rilevati **260000** pacchetti di installazione per **ransomware**
 - È aumentato di **1,6 volte** il numero di **utenti presi di mira dai ransomware mobile**
 - Circa **153000** utenti

Fonte

http://www.ansa.it/sito/notizie/tecnologia/software_app/2017/03/02/smartphone-malware-triplicati-nel-2016_c811517a-fb83-4b26-b28b-4e9c91b6e9b6.html

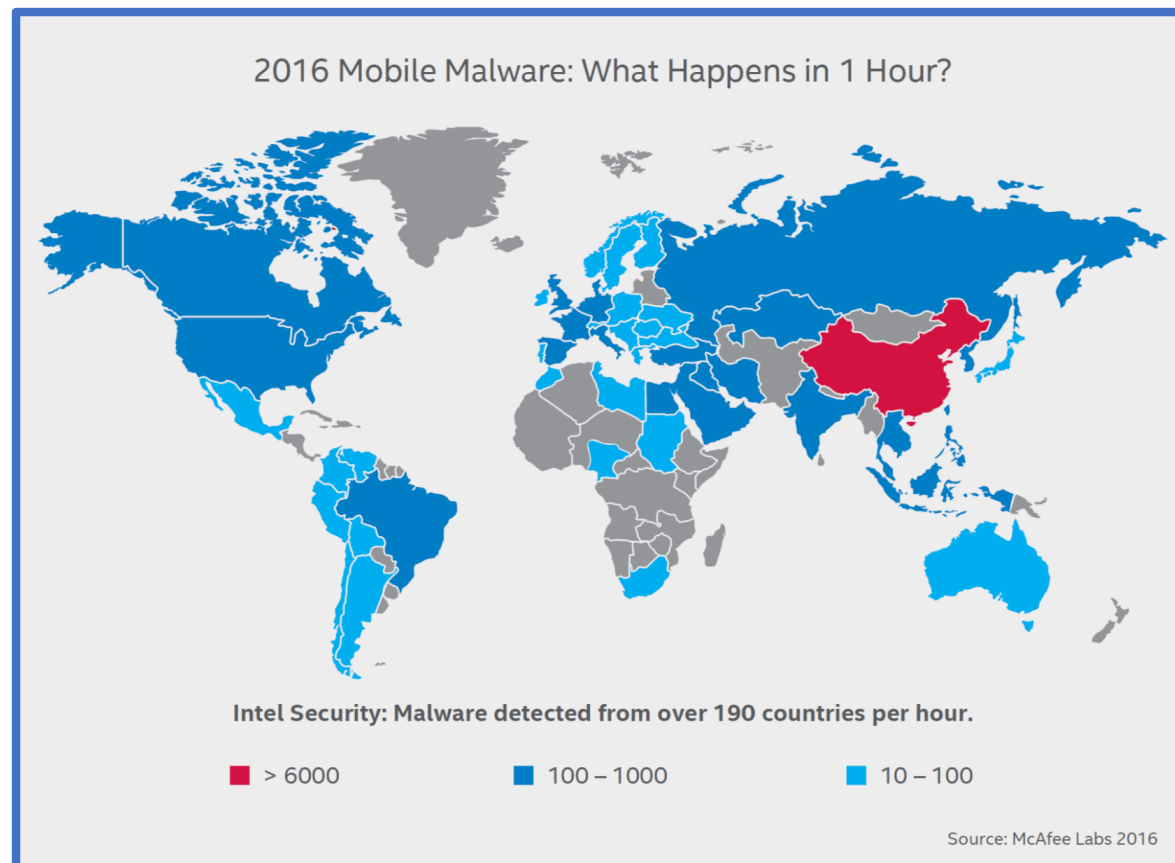
Analisi dei Malware su Dispositivi Mobile - 4/8

- Oltre il significativo e preoccupante incremento del numero di nuovi malware identificati
 - Vi è un notevole incremento anche della relativa complessità



Analisi dei Malware su Dispositivi Mobile - 5/8

- Numero di minacce da malware identificate nel corso di un'ora su 190 paesi



Fonte

<http://www.mcafee.com/us/resources/reports/rp-mobile-threat-report-2016.pdf>

Analisi dei Malware su Dispositivi Mobile - 6/8

- Numerosi sono i fattori che inducono a realizzare nuovi malware per dispositivi mobile
 - *Aumento delle vendite*
 - Le vendite degli smartphone hanno ampiamente superato quelle di PC e laptop
 - *Incremento Prestazionale/Velocità Reti*
 - Le prestazioni degli smartphone sono notevolmente aumentate, così come le prestazioni delle reti da essi utilizzate, le quali permettono di accedere rapidamente a contenuti multimediali, etc.
 - *Sistemi Operativi Complessi*
 - I moderni OS mobile hanno un grado di complessità elevato
 - *Presenza Nuovi Sensori*
 - Fotocamere, GPS, microfoni, etc. sono solo alcuni dei sensori di cui sono dotati gli smartphone/tablet odierni

Analisi dei Malware su Dispositivi Mobile - 7/8

- Uno dei principali obiettivi dei malware per dispositivi mobile è il furto di dati sensibili (o credenziali)
- I dispositivi mobile utilizzano principalmente due sistemi operativi
 - Android® di Google
 - iOS® di Apple
- Entrambi offrono diversi livelli di protezione
 - Cifratura dei dati
 - Protezione contro accessi fisici
 - Firma delle app
 - Etc.

Analisi dei Malware su Dispositivi Mobile - 8/8

- L'analisi di un malware in ambito mobile risulta molto complessa
 - Spesso le app contenenti malware sono distribuite in maniera illegale o tramite canali non ufficiali
 - Gli store da cui è possibile scaricare/acquistare app non permettono la pubblicazione di app malevole
 - Spesso gli strumenti necessari al rilevamento/analisi del malware potrebbero essere inadeguati
 - La maggior parte delle volte è possibile effettuare solo un'analisi statica

Strumenti - 1/10

(IDA PRO - 1/6)

- **Interactive Disassembler Professional**
 - IDA PRO è un disassemblatore estremamente potente
 - Grazie alle sue funzionalità è molto utilizzato nell'ambito della malware analysis
 - Disassembla l'intero eseguibile
 - Individua le funzioni usate
 - Analisi dello stack
 - Variabili locali
 - Etc.
 - Risulta essere molto utile nell'ambito dell'analisi statica di un malware



Strumenti - 1/10

(IDA PRO - 2/6)

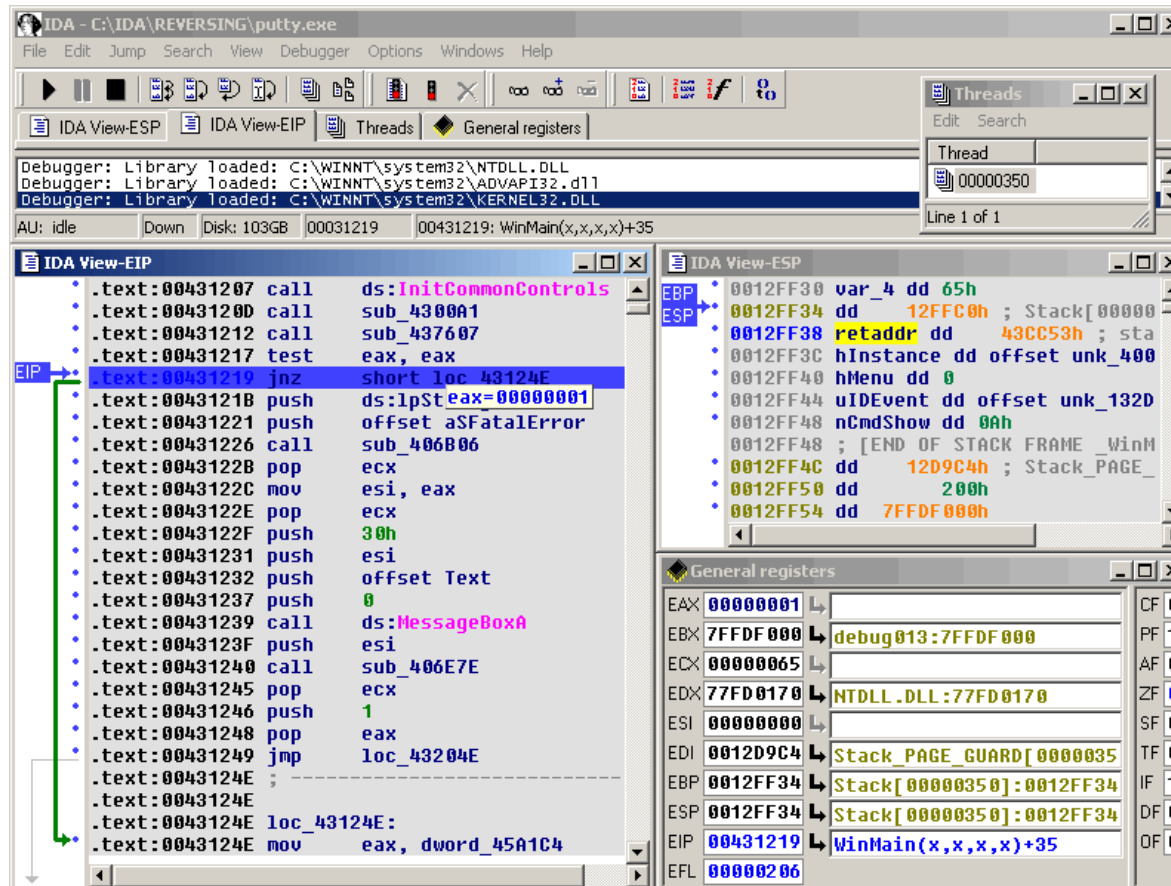
- **Interactive Disassembler Professional**
 - È pensato per essere **interattivo**
 - Tutte le parti del processo di disassembling possono essere manipolate, riscritte, etc.
 - È possibile memorizzare i progressi dell'analisi del malware
 - Inserendo note ed etichette su funzioni, variabili, etc.
 - Salvando tutto nell'*IDA PRO Database (idb)*
 - **Struttura modulare a Plug-in**
 - È possibile estendere le funzionalità di IDA PRO mediante appositi plug-in



Strumenti - 1/10

(IDA PRO - 3/6)

➤ Interactive Disassembler Professional



Strumenti - 1/10

(IDA PRO - 4/6)

➤ Interactive Disassembler Professional

```
IDA View-A
.data:0043937F aMonday db 'Monday',0
.data:00439386 aTuesday db 'Tuesday',0
.data:0043938E aWednesday db 'Wednesday',0
.data:00439398 aThursday db 'Thursday',0
.data:004393A1 aFriday db 'Friday',0
.data:004393A8 aSaturday db 'Saturday',0
.data:004393B1 aSunday db 'Sunday',0

Hex View-A
.data:00439350 00 00 00 2D 00 2F 00 3A-00 25 48 3A 25 4D 3A 25 "...-./.:%H:%M:%"
.data:00439360 53 00 25 6D 2F 25 6A 2F-25 79 00 25 41 2C 20 25 "S.%m/%d/%y.%A, %"
.data:00439370 42 20 25 6A 2C 20 25 59-00 41 4D 00 50 4D 00 4D "B %d, %Y.AM.PM."
.data:00439380 6F 6E 64 61 79 00 54 75-65 73 6A 61 79 00 57 65 "Monday.Tuesday.We"
.data:00439390 6A 6E 65 73 6A 61 79 00-54 68 75 72 73 6A 61 79 "nesday.Thursday"
.data:004393A0 00 46 72 69 6A 61 79 00-53 61 74 75 72 6A 61 79 ".Friday.Saturday"
.data:004393B0 00 53 75 6E 6A 61 79 00-4D 6F 6E 00 54 75 65 00 ".Sunday.Mon.Tue."

IDA View-B
.data:004388B7 aArgListTooBig db 'Arg list too big',0
.data:004388C8 aExecFormatErro db 'Exec format error',0
.data:004388DA aCrossDeviceLin db 'Cross-device link',0
.data:004388EC aTooManyOpenF_0 db 'Too many open files',0
.data:00438900 aNoChildProcess db 'No child processes',0
.data:00438913 aInappropriateI db 'Inappropriate I/O control operation',0
.data:00438937 aExecutableFile db 'Executable file in use',0

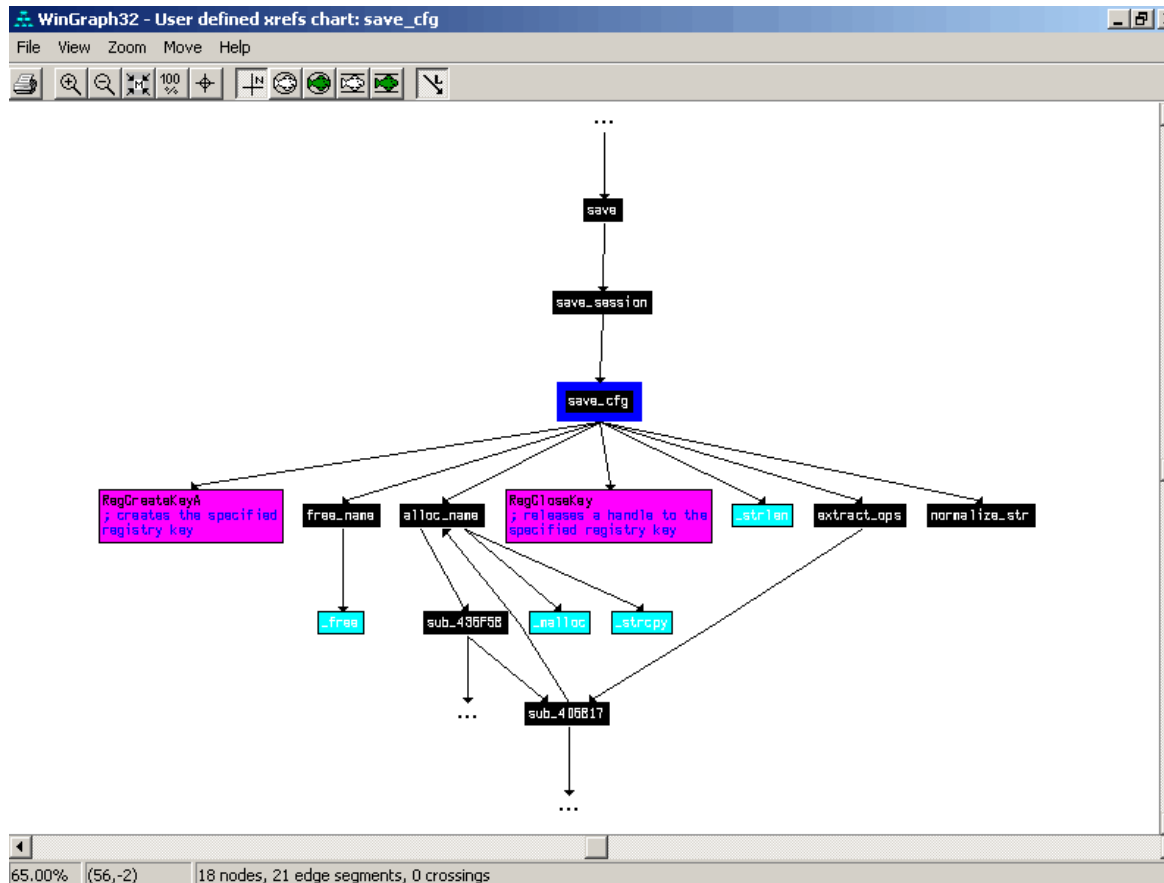
Hex View-1
.data:004388F0 6D 61 6E 79 20 6F 70 65-6E 20 66 69 6C 65 73 00 "many open files."
.data:00438900 4E 6F 20 63 68 69 6C 64-20 70 72 6F 63 65 73 73 "No child process"
.data:00438910 65 73 00 49 6E 61 70 70-72 6F 70 72 69 61 74 65 "es.Inappropriate"
.data:00438920 20 49 2F 4F 20 63 6F 6E-74 72 6F 6C 20 6F 70 65 "I/O control ope"
.data:00438930 72 61 74 65 6F 65 6F 65 6F 65 6F 65 6F 65 6F 65 62 6C "ration.Executabl"
.data:00438940 65 20 66 46 69 65 65 65 65 65 65 65 65 65 65 46 69 "e file in use.Fi"
.data:00438950 6C 65 20 6F 20 6F 20 6F 20 6F 20 6F 20 6F 20 6F 20 6F 20 "le too large.No"
```



Strumenti - 1/10

(IDA PRO - 5/6)

➤ Interactive Disassembler Professional



Strumenti - 1/10

(IDA PRO - 6/6)

- **Interactive Disassembler Professional**
 - Link Utili
 - <https://www.hex-rays.com/products/ida/>



Strumenti - 2/10

(WinHEX)

➤ WinHEX

- È un potente editor esadecimale
- Permette di esaminare un file, byte per byte, e di svolgere determinate operazioni su di esso
- Può essere usato per effettuare l'analisi statica e dinamica di un malware

➤ Link Utili

- <https://www.x-ways.net/winhex/>



Strumenti - 3/10

(Dependency Walker)

➤ Dependency Walker

- Permette di esaminare un qualsiasi modulo di Microsoft Windows
 - Exe, Dll, OCX, SYS, ...
- Costruisce un albero delle dipendenze relativo a tutti i moduli usati
- Può essere usato per effettuare l'analisi statica di un malware

➤ Link Utili

- <http://www.dependencywalker.com/>



Strumenti - 4/10

(OllyDBG - 1/2)

➤ OllyDBG

- Permette di osservare il comportamento di un malware durante la fase di analisi dinamica
 - Debugger per processori x86
 - Permette di osservare il flusso di esecuzione di ogni processo
 - Offre la possibilità di effettuare arbitrarie operazioni sul processo, quali riavvio, stop, etc.
 - Monitora lo stato del registro di sistema
 - Segnalando le varie modifiche nei contenuti
- Disponibile solo per Microsoft Windows



Strumenti - 4/10

(OlllyDBG - 2/2)

- OlllyDBG

- Link Utili

- <http://www.ollydbg.de/>





Strumenti - 5/10

(VirtualBox)

➤ VirtualBox

- Software per la creazione di macchine virtuali
 - Disponibile per Microsoft Windows, Apple OS X/macOS e Linux
- Permette di eseguire un malware su una macchina virtuale, al fine di studiarne il comportamento (analisi dinamica)
- Link Utili
 - <https://www.virtualbox.org/>



Strumenti - 6/10

(Process Monitor)

➤ Process Monitor

- Strumento di monitoraggio avanzato per Microsoft Windows
 - Permette il controllo di registri, file di sistema, processi e relativi thread, etc.
- Estremamente utile nell'analisi dinamica di un malware per la piattaforma Microsoft Windows
- Link Utili
 - <https://technet.microsoft.com/en-us/sysinternals/processmonitor.aspx>



Strumenti - 7/10

(HashMyFiles)

➤ HashMyFiles

- Strumento per la generazione del valore hash di un file
- Utilizzato principalmente per tenere traccia dell'auto-modifica dei malware
- Estremamente utile nell'analisi dinamica di un malware per la piattaforma Microsoft Windows
- Link Utili
 - http://www.nirsoft.net/utils/hash_my_files.html



Strumenti - 8/10

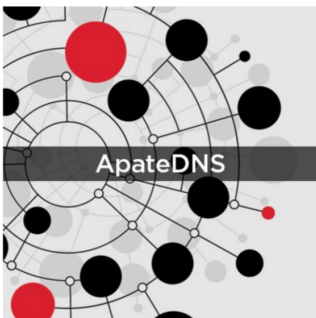
(ApateDNS)

➤ ApateDNS

- Strumento per controllare le risposte di un DNS
- Presenta un'interfaccia user-friendly
- Permette lo spoofing delle risposte del DNS verso un indirizzo IP specifico
- Utile nell'analisi dinamica di un malware per individuare richieste/risposte a/da un DNS da parte di eventuali malware

➤ Link Utili

- <https://www.fireeye.com/services/freeware/apatedns.html>



Strumenti - 9/10

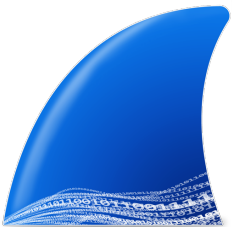
(WireShark)

➤ WireShark

- Permette il monitoraggio e lo sniffing
 - Cattura ed analizza i pacchetti singolarmente
- Utile per individuare richieste/risposte a/da un host da parte di eventuali malware, nell'analisi dinamica
- Open-Source

➤ Link Utili

- <https://www.wireshark.org/>



Strumenti - 10/10

(Autoruns - 1/3)

➤ Autoruns

- Utilizzato per la piattaforma Microsoft Windows
- Per mantenere la persistenza, il malware spesso si installa in diverse locazioni (registri, cartelle di autostart, etc.)
 - Autoruns è utile per individuare tali locazioni
- Permette di individuare le locazioni dove vengono memorizzati i programmi eseguiti automaticamente all'avvio di Windows (autostart)
- Fa parte della Suite chiamata *SysInternals* di Microsoft



Strumenti - 10/10

(Autoruns - 2/3)

- **Autoruns**

- Link Utili

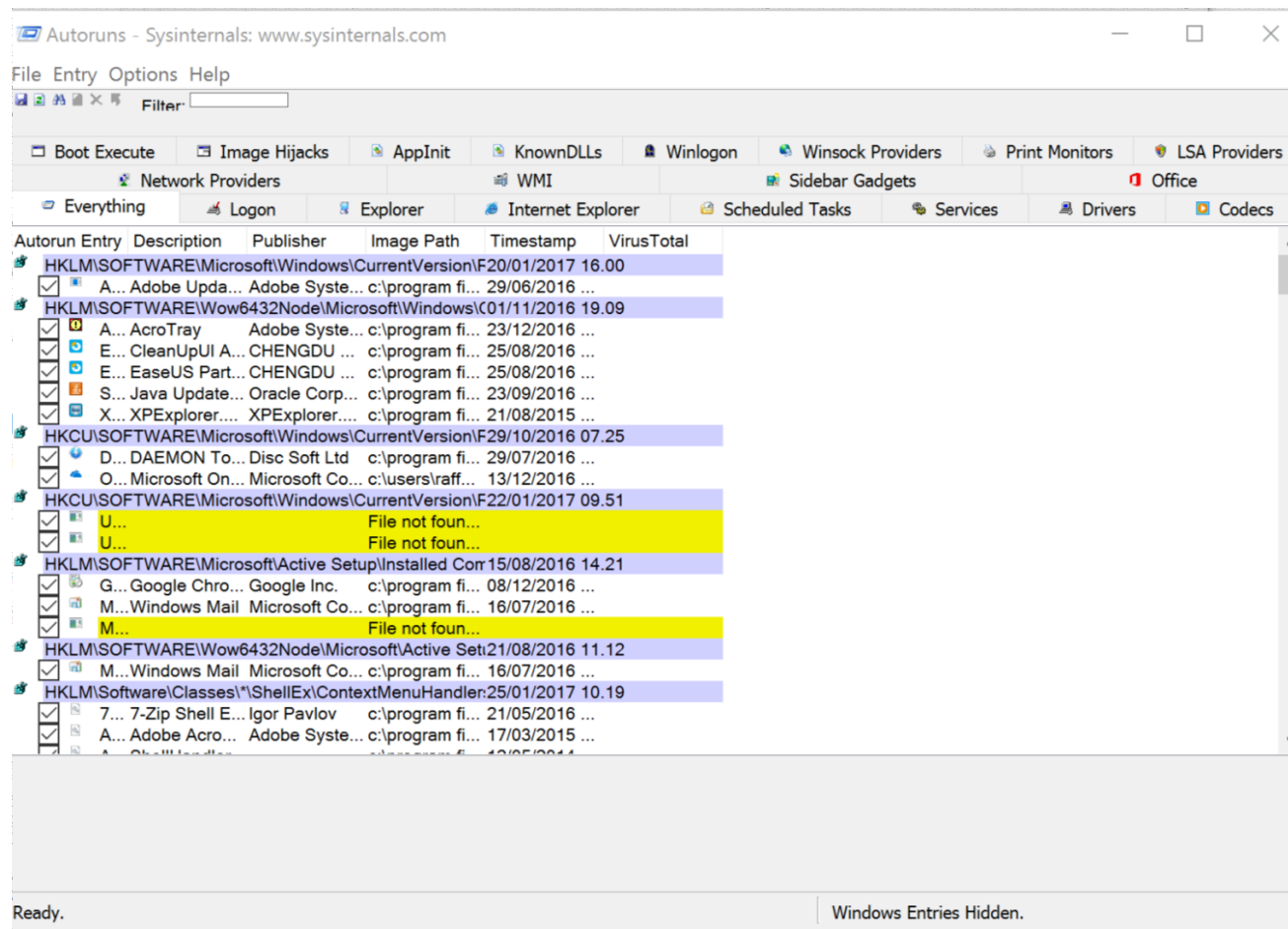
- <https://technet.microsoft.com/it-it/sysinternals/bb963902>



Strumenti - 10/10

(Autoruns - 3/3)

➤ Autoruns



The screenshot shows the Autoruns utility window from Sysinternals. The window title is "Autoruns - Sysinternals: www.sysinternals.com". The interface includes a menu bar (File, Entry, Options, Help), a toolbar with icons for various actions, and a filter input field. Below the toolbar are several tabs for different system components: Boot Execute, Image Hijacks, AppInit, KnownDLLs, Winlogon, Winsock Providers, Print Monitors, LSA Providers, Network Providers, WMI, Sidebar Gadgets, Office, Everything, Logon, Explorer, Internet Explorer, Scheduled Tasks, Services, Drivers, and Codecs. The main area displays a table of Autorun entries with columns for Autorun Entry, Description, Publisher, Image Path, Timestamp, and VirusTotal. The table contains various entries, some of which are highlighted in yellow, indicating they are selected or have a specific status. The status bar at the bottom shows "Ready." and "Windows Entries Hidden."

Autorun Entry	Description	Publisher	Image Path	Timestamp	VirusTotal
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\F20\01\2017				16.00	
<input checked="" type="checkbox"/> A...	Adobe Upda...	Adobe Syste...	c:\program fi...	29/06/2016	...
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\C01\11\2016				19.09	
<input checked="" type="checkbox"/> A...	AcroTray	Adobe Syste...	c:\program fi...	23/12/2016	...
<input checked="" type="checkbox"/> E...	CleanUpUI A...	CHENGDU ...	c:\program fi...	25/08/2016	...
<input checked="" type="checkbox"/> E...	EaseUS Part...	CHENGDU ...	c:\program fi...	25/08/2016	...
<input checked="" type="checkbox"/> S...	Java Update...	Oracle Corp...	c:\program fi...	23/09/2016	...
<input checked="" type="checkbox"/> X...	XPEXplorer...	XPEXplorer...	c:\program fi...	21/08/2015	...
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\F29\10\2016				07.25	
<input checked="" type="checkbox"/> D...	DAEMON To...	Disc Soft Ltd	c:\program fi...	29/07/2016	...
<input checked="" type="checkbox"/> O...	Microsoft On...	Microsoft Co...	c:\users\raff...	13/12/2016	...
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\F22\01\2017				09.51	
<input checked="" type="checkbox"/> U...			File not foun...		
<input checked="" type="checkbox"/> U...			File not foun...		
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Cor\15\08\2016				14.21	
<input checked="" type="checkbox"/> G...	Google Chro...	Google Inc.	c:\program fi...	08/12/2016	...
<input checked="" type="checkbox"/> M...	Windows Mail	Microsoft Co...	c:\program fi...	16/07/2016	...
<input checked="" type="checkbox"/> M...			File not foun...		
HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Set\21\08\2016				11.12	
<input checked="" type="checkbox"/> M...	Windows Mail	Microsoft Co...	c:\program fi...	16/07/2016	...
HKLM\Software\Classes*\ShellEx\ContextMenuHandler:25\01\2017				10.19	
<input checked="" type="checkbox"/> 7...	7-Zip Shell E...	Igor Pavlov	c:\program fi...	21/05/2016	...
<input checked="" type="checkbox"/> A...	Adobe Acro...	Adobe Syste...	c:\program fi...	17/03/2015	...
<input checked="" type="checkbox"/> A...	Shell Handl...		c:\program fi...	13/05/2014	...



Bibliografia

- Michael Sikorski, Andrew Honig - Practical Malware Analysis The Hands-On Guide to Dissecting Malicious Software-No Starch Press (2012)

