Analisi dei Malware

Alfredo De Santis

Dipartimento di Informatica
Università degli Studi di Salerno

ads@unisa.it

Giugno 2020

Outline

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

Outline

- **Analisi dei Malware**
- Analisi Statica
- Analisi Dinamica
  - White Box
  - Black Box
- Malware su Dispositivi Mobile
- Strumenti per l'Analisi dei Malware

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

Outline

- Analisi dei Malware
- **Analisi Statica**
- Analisi Dinamica
  - White Box
  - Black Box
- Malware su Dispositivi Mobile
- Strumenti per l'Analisi dei Malware

Analisi dei Malware
Analisi Statica – 1/4

- L'**analisi statica** definisce le metodologie per l'analisi del codice e della 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

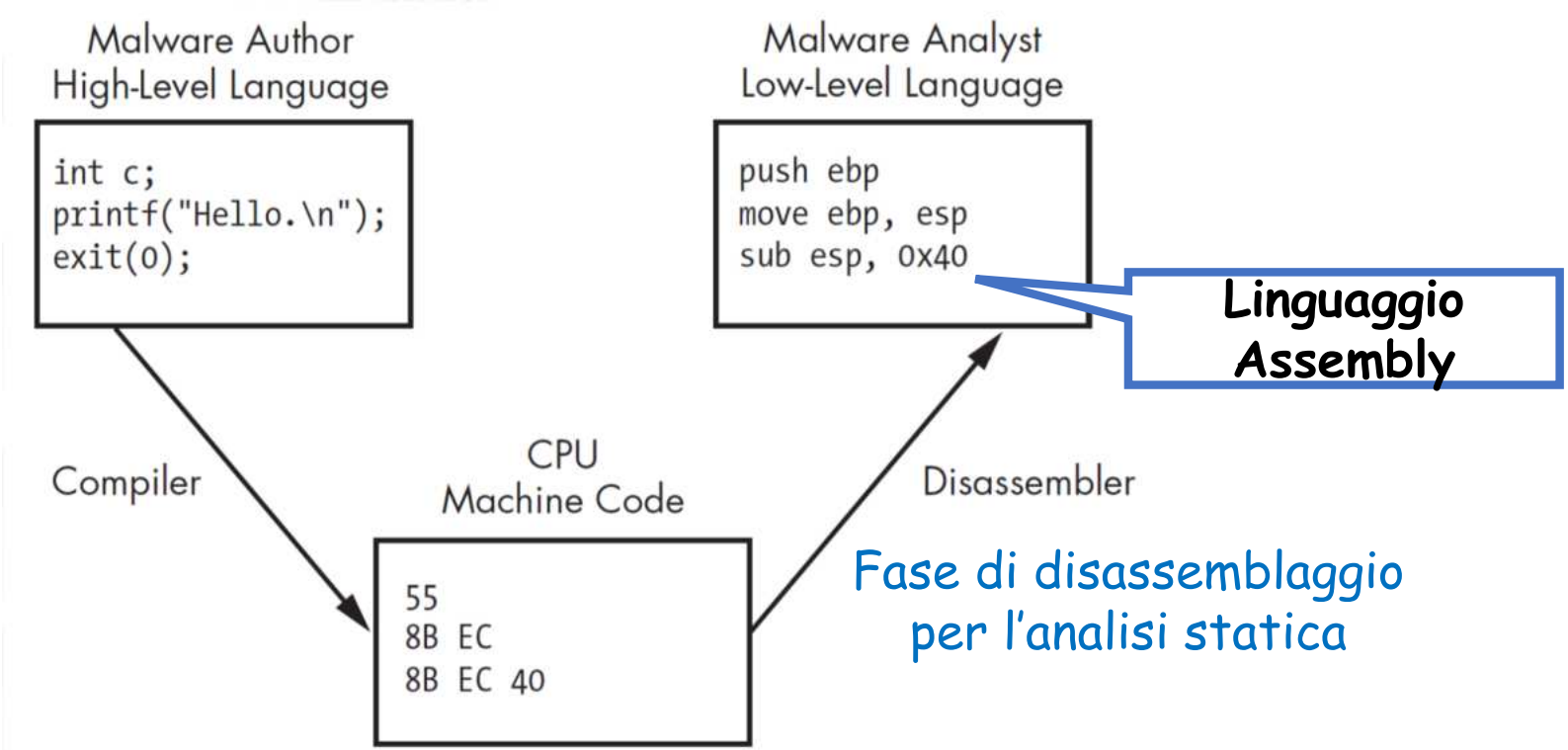
- Esistono vari modi per farlo
  - Utilizzando software anti-virus/anti-malware per confermare la natura maliziosa del malware
  - Utilizzando funzioni hash per identificare il malware
  - Analizzando stringhe, funzioni e header presenti nel file

Analisi dei Malware
Analisi Statica – 3/4

- I malware sono generalmente programmati mediante linguaggi di alto livello
  - Il codice eseguito dalla CPU (linguaggio di basso livello) è generato dal compilatore
- L'analisi dei malware viene di solito 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***



Fase di disassemblaggio per l'analisi statica

Outline

- Analisi dei Malware
- Analisi Statica
- **Analisi Dinamica**
  - White Box
  - Black Box
- Malware su Dispositivi Mobile
- Strumenti per l'Analisi dei Malware

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 quella 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 altri sistemi 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

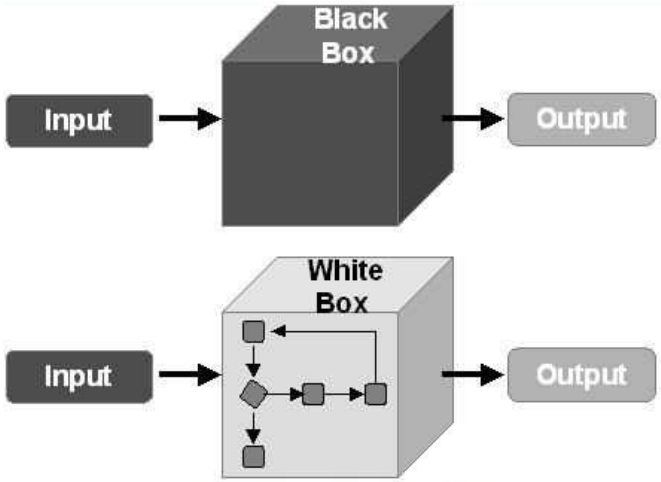
- Per l'analisi dinamica generalmente si utilizza una macchina virtuale, o eventualmente una macchina fisica dedicata
  - La macchina virtuale è connessa ad una rete *air-gapped* (*air-gap*, letteralmente vuoto d'aria)
    - Protetta dall'accesso ad Internet per evitare possibili diffusioni del malware 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



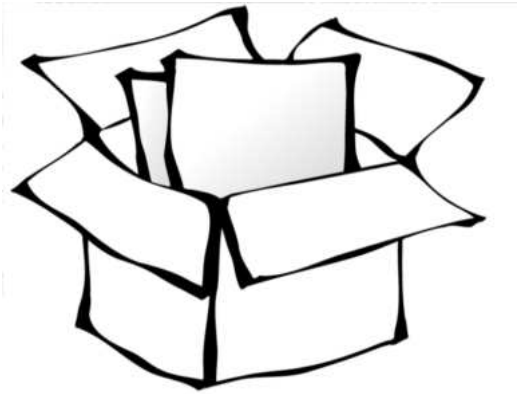
Outline

- Analisi dei Malware
- Analisi Statica
- Analisi Dinamica
  - **White Box**
  - Black Box
- Malware su Dispositivi Mobile
- Strumenti per l'Analisi dei Malware

Analisi dei Malware
Analisi Dinamica – White Box - 1/3

- A differenza dell'approccio Black Box, l'approccio **White Box** è più profondo

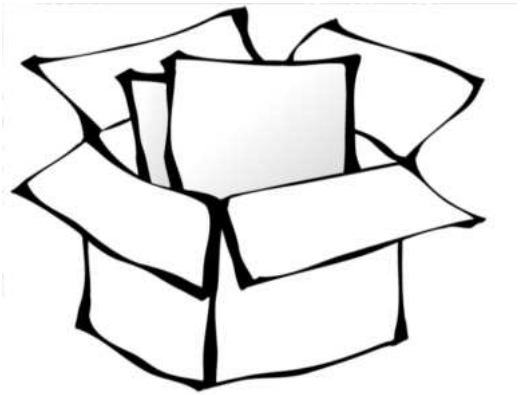
- È necessario conoscere dettagli sulle caratteristiche e sul codice del malware in esame



Analisi dei Malware
Analisi Dinamica – White Box - 2/3

- Durante l'analisi White Box vengono analizzati tutti gli aspetti relativi all'esecuzione del malware

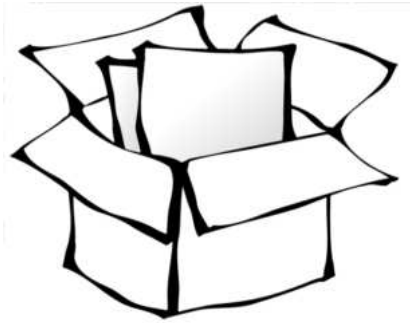
- Vengono analizzati tutti quegli aspetti che conducono
  - **Dallo stato del sistema prima dell'infezione** del malware
  - Allo stato del **sistema dopo l'esecuzione** del malware stesso



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

- Per l'analisi possono essere necessari strumenti specifici
  - Debugger
  - Editor
  - Etc.



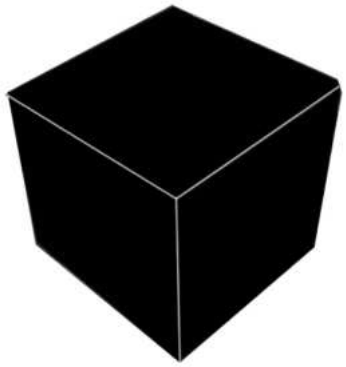
Outline

- Analisi dei Malware
- Analisi Statica
- Analisi Dinamica
  - White Box
  - **Black Box**
- Malware su Dispositivi Mobile
- Strumenti per l'Analisi dei Malware

Analisi dei Malware
Analisi Dinamica – Black Box - 1/2

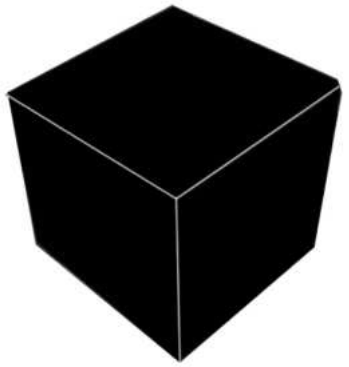
- L'approccio *Black Box* si focalizza sull'analisi degli effetti derivanti dall'esecuzione del malware
  - Senza soffermarsi sulla comprensione del comportamento e sui meccanismi che innescano effettivamente le attività malevole

- L'approccio Black Box è quindi un approccio "superficiale"



Analisi dei Malware
Analisi Dinamica – Black Box – 2/2

- 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.



Outline

- Analisi dei Malware
- Analisi Statica
- Analisi Dinamica
  - White Box
  - Black Box
- **Malware su Dispositivi Mobile**
- Strumenti per l'Analisi dei Malware

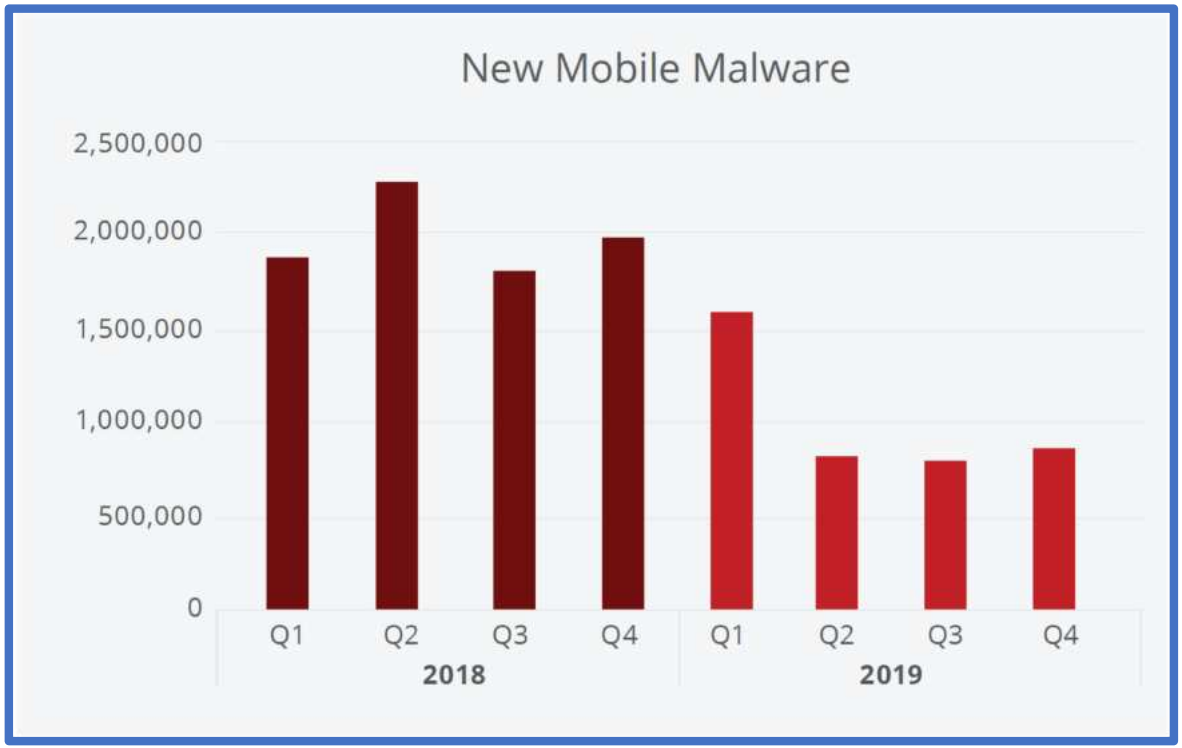
Analisi dei Malware su Dispositivi Mobile – 1/8

- 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

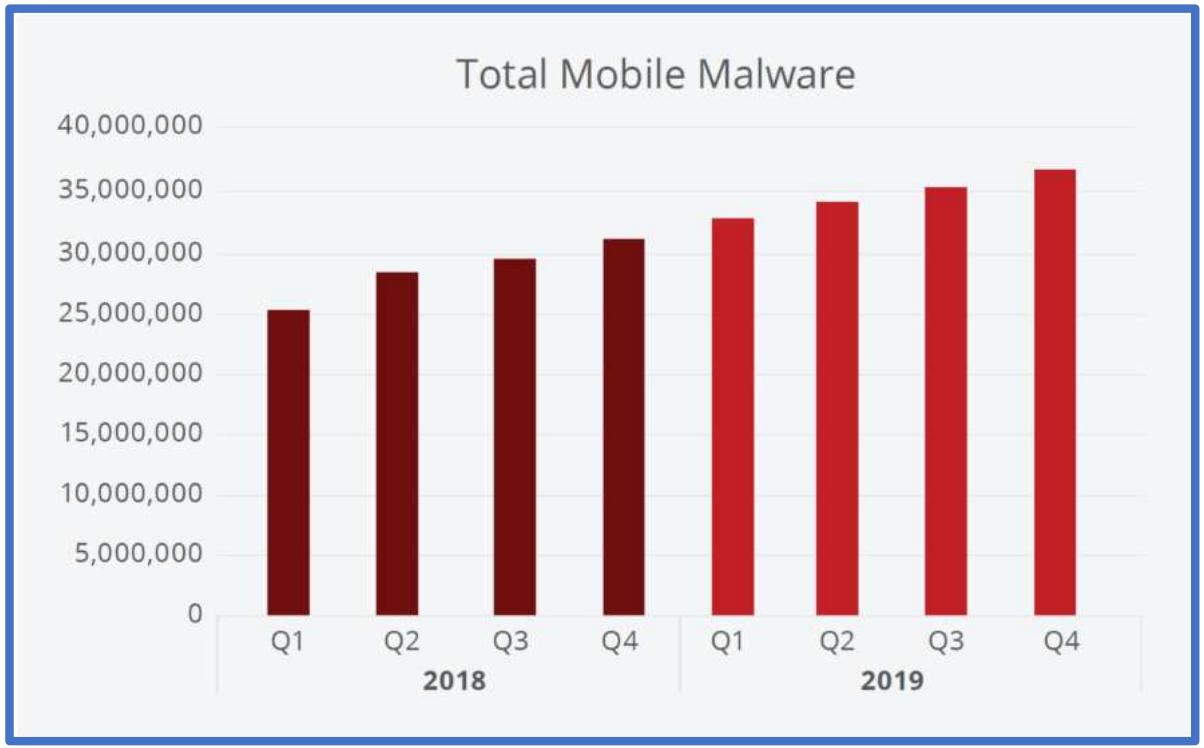
- Nuovi malware identificati su dispositivi mobile
  - Anni considerati: 2018 e 2019



Fonte
https://www.mcafee.com/content/dam/consumer/en-us/docs/2020-Mobile-Threat-Report.pdf

Analisi dei Malware su Dispositivi Mobile – 2/8

- Malware identificati su dispositivi mobile
  - Anni considerati: 2018 e 2019

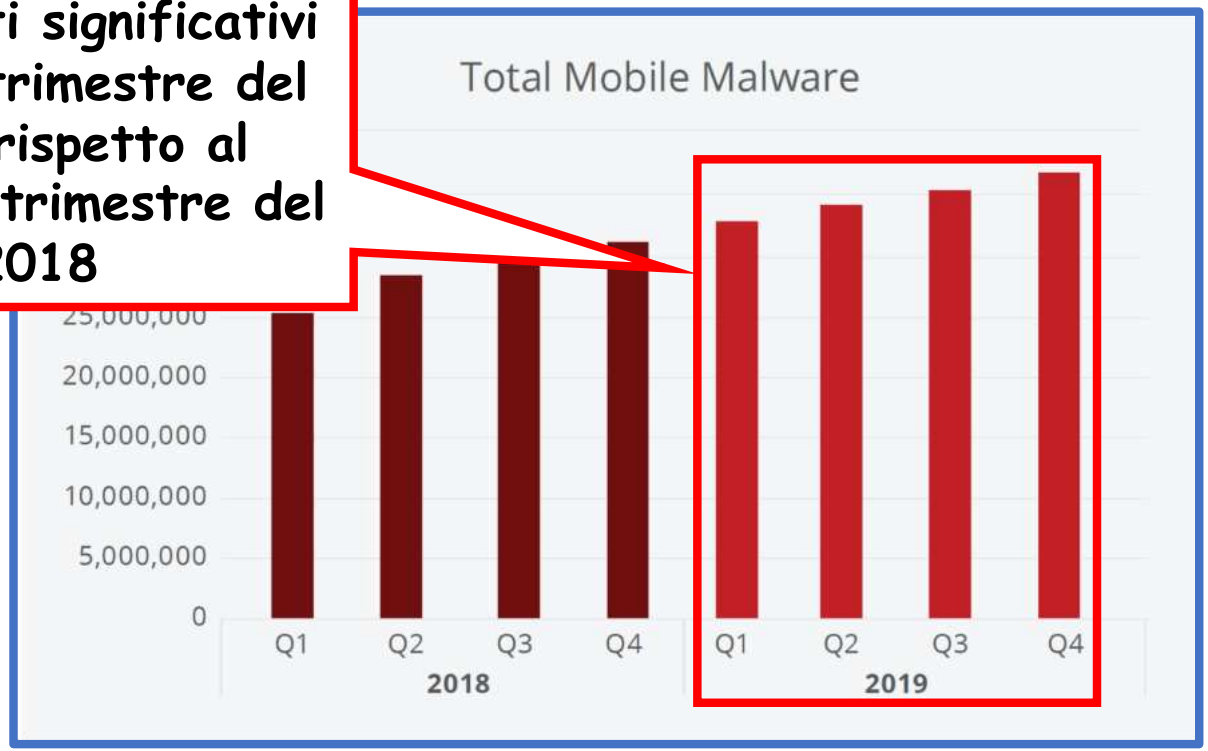


Fonte
https://www.mcafee.com/content/dam/consumer/en-us/docs/2020-Mobile-Threat-Report.pdf

Analisi dei Malware su Dispositivi Mobile – 2/8

- Malware identificati su dispositivi mobile
  - Anni considerati: 2018 e 2019

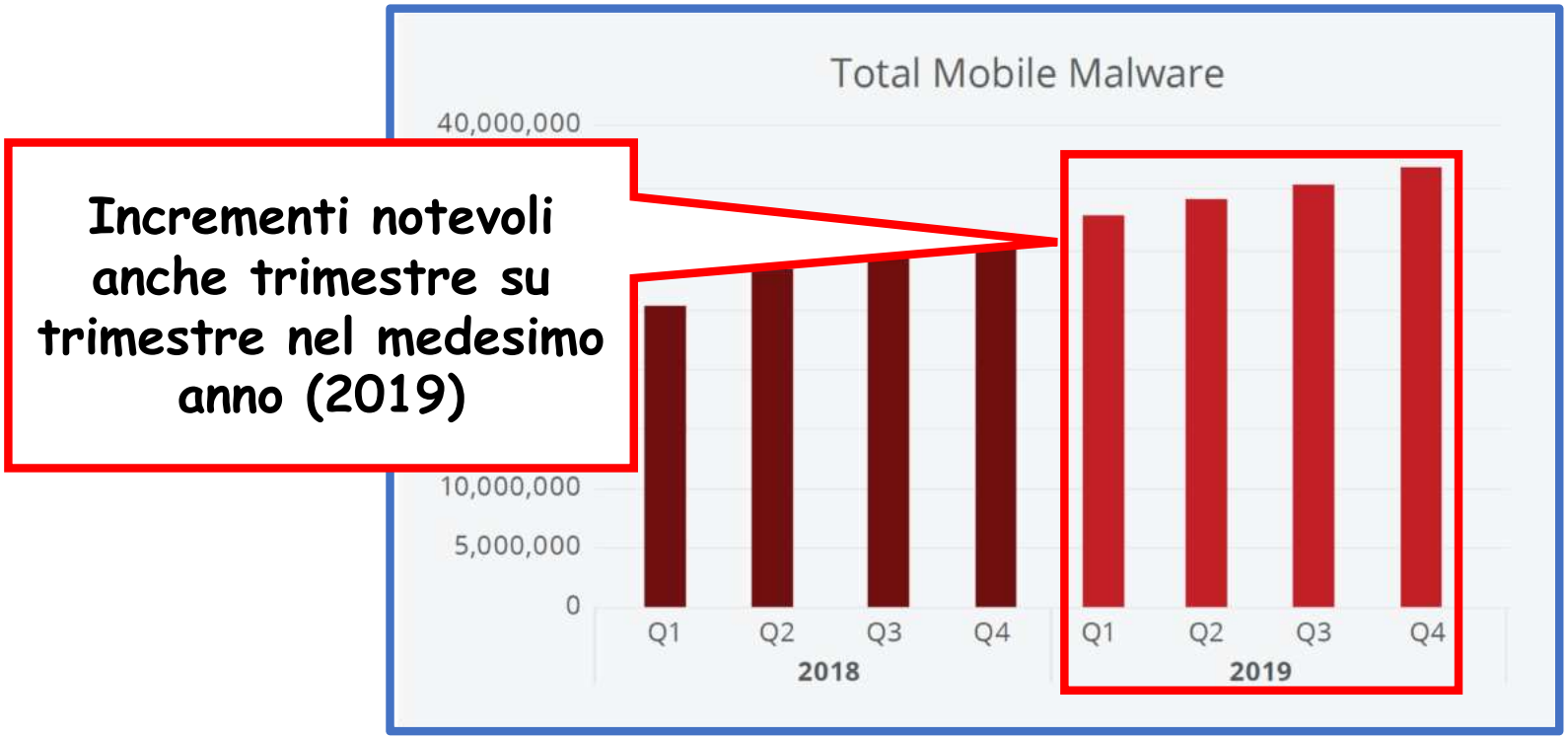
Incrementi significativi per ogni trimestre del 2019, rispetto al medesimo trimestre del 2018



Fonte
https://www.mcafee.com/content/dam/consumer/en-us/docs/2020-Mobile-Threat-Report.pdf

Analisi dei Malware su Dispositivi Mobile – 2/8

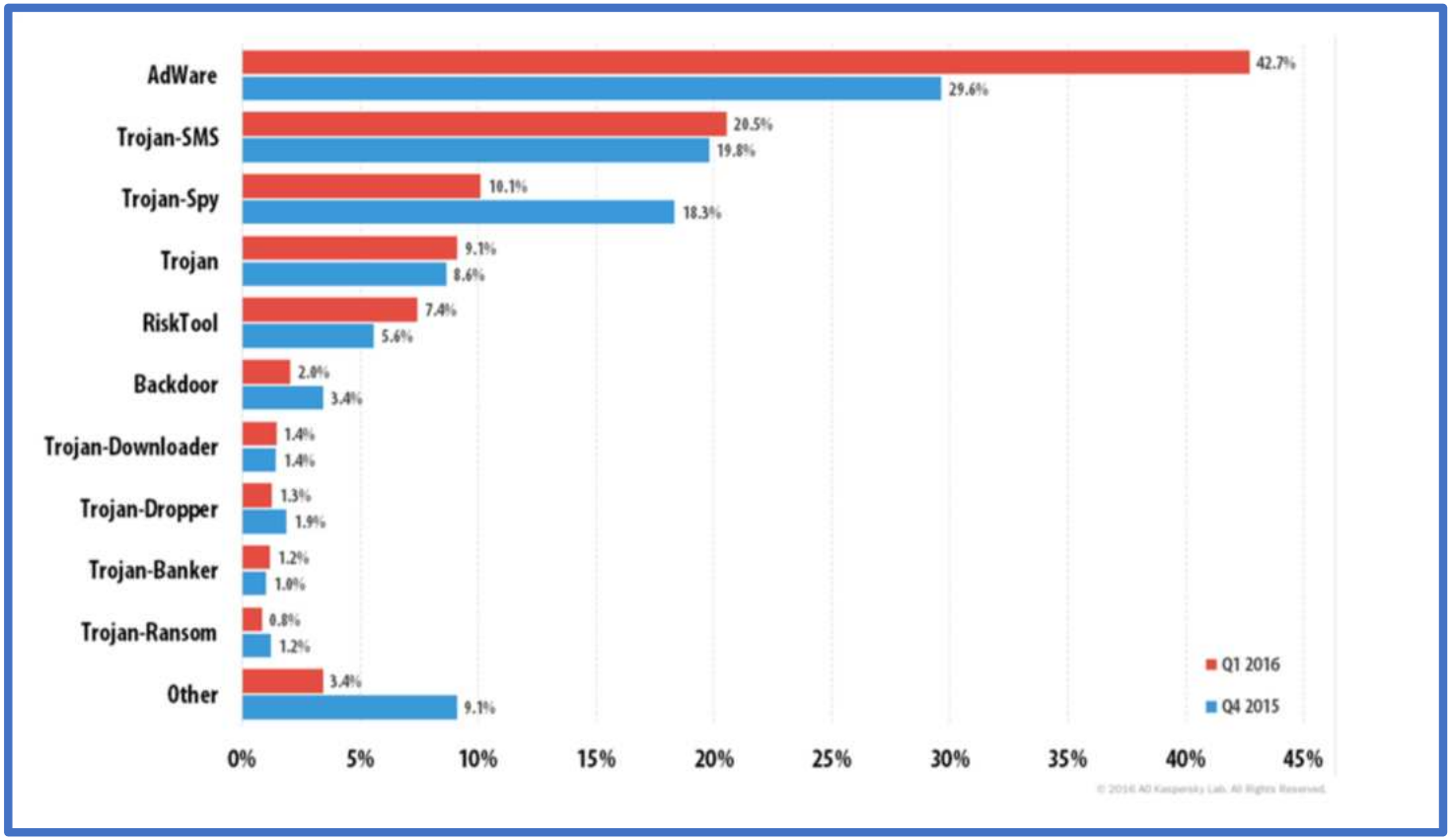
- Malware identificati su dispositivi mobile
  - Anni considerati: 2014 e 2015



Fonte
https://www.mcafee.com/content/dam/consumer/en-us/docs/2020-Mobile-Threat-Report.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

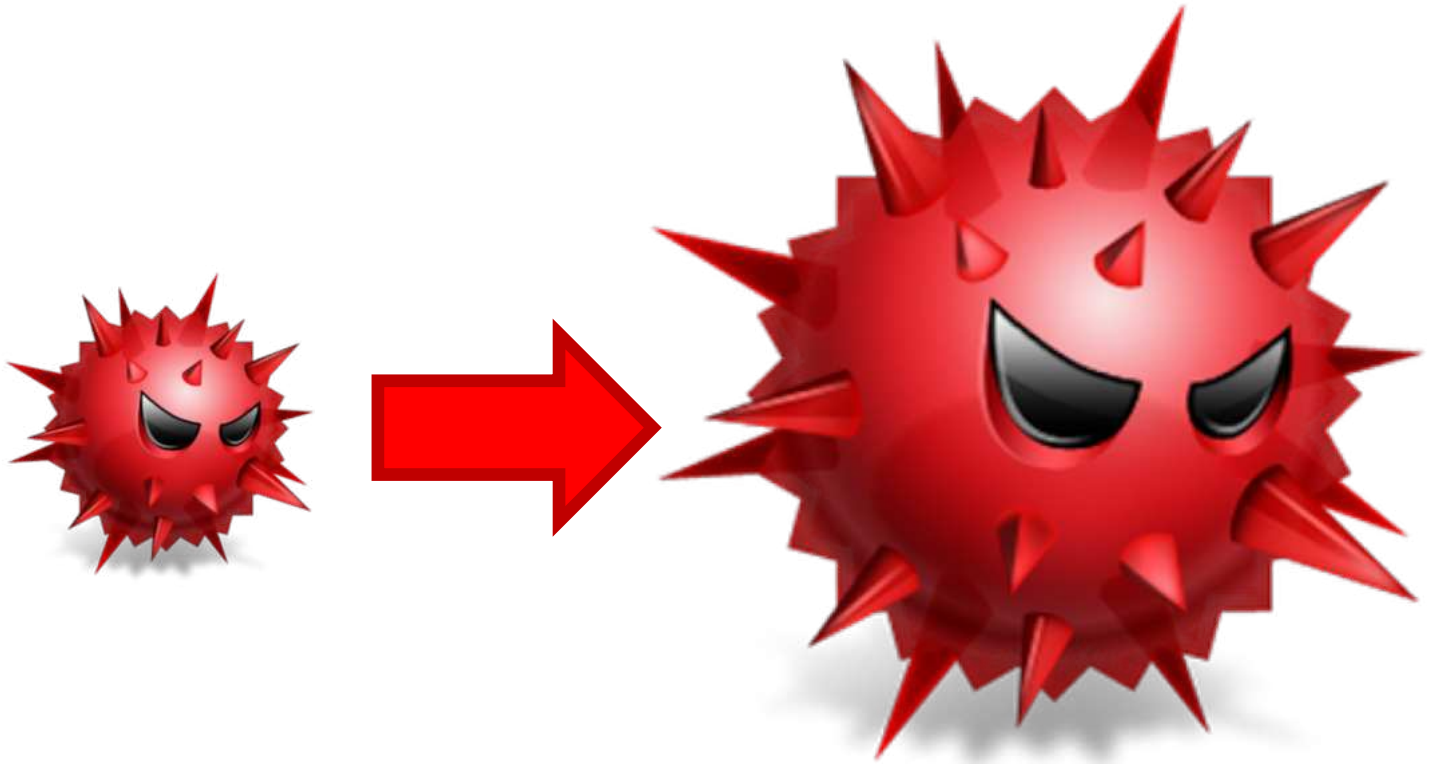
Analisi dei Malware su Dispositivi Mobile – 3/8

- 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

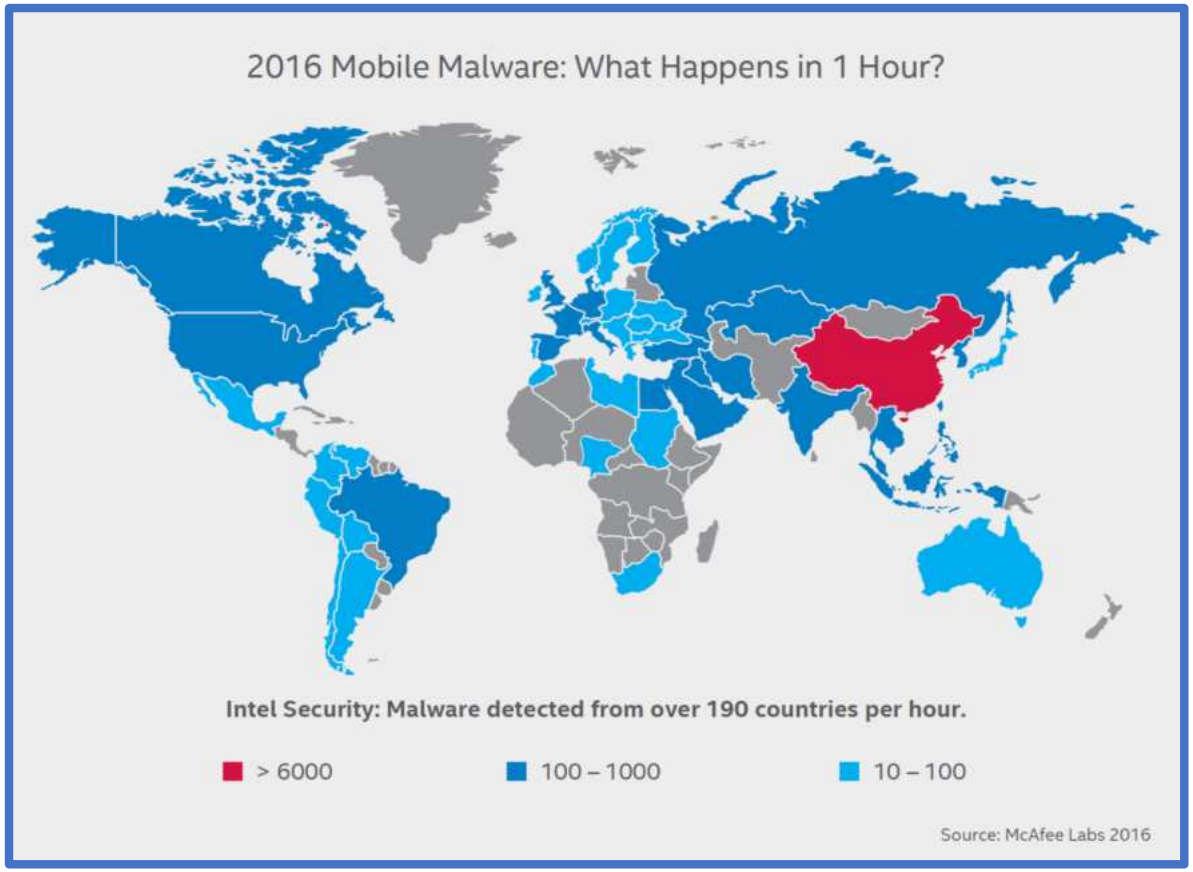
Analisi dei Malware su Dispositivi Mobile – 4/8

- Oltre al significativo e preoccupante incremento del numero di nuovi malware identificati
  - C'è stato anche un notevole incremento della loro **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 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 migliorate, così come le prestazioni delle reti da essi utilizzate, le quali permettono di accedere rapidamente a contenuti multimediali, etc.
  - *Sistemi Operativi Complessi*
    - I moderni SO 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

Outline

- Analisi dei Malware
- Analisi Statica
- Analisi Dinamica
  - White Box
  - Black Box
- Malware su Dispositivi Mobile
- **Strumenti per l'Analisi dei Malware**

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 dell'analisi dei malware
  - Disassembla l'intero eseguibile
    - Individua le funzioni usate
    - Analizza lo stack
    - Analizza lo stato delle variabili locali
    - Etc.
  - Risulta essere molto utile nell'ambito dell'analisi statica di un malware

Strumenti – 1/10

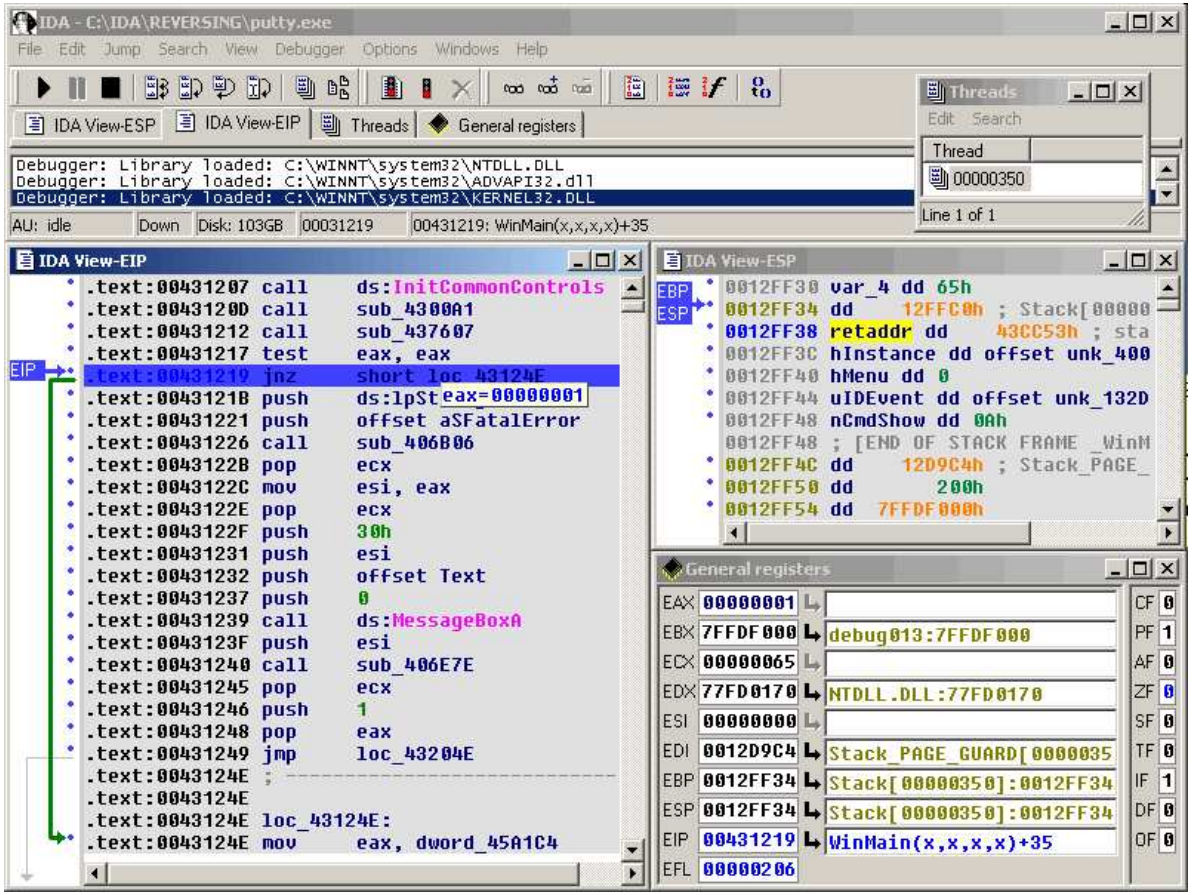
IDA PRO – 2/6

- **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

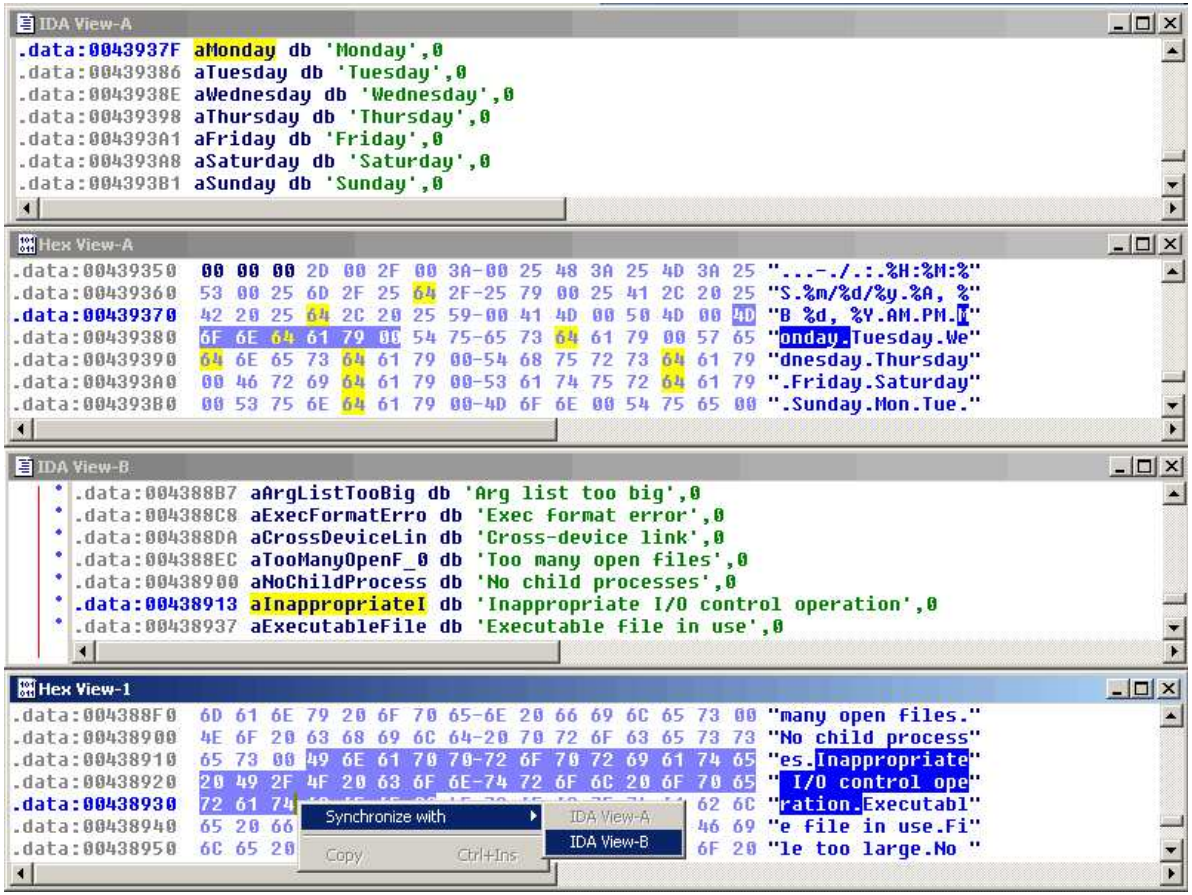
- Interactive Disassembler Professional



Strumenti - 1/10

IDA PRO - 4/6

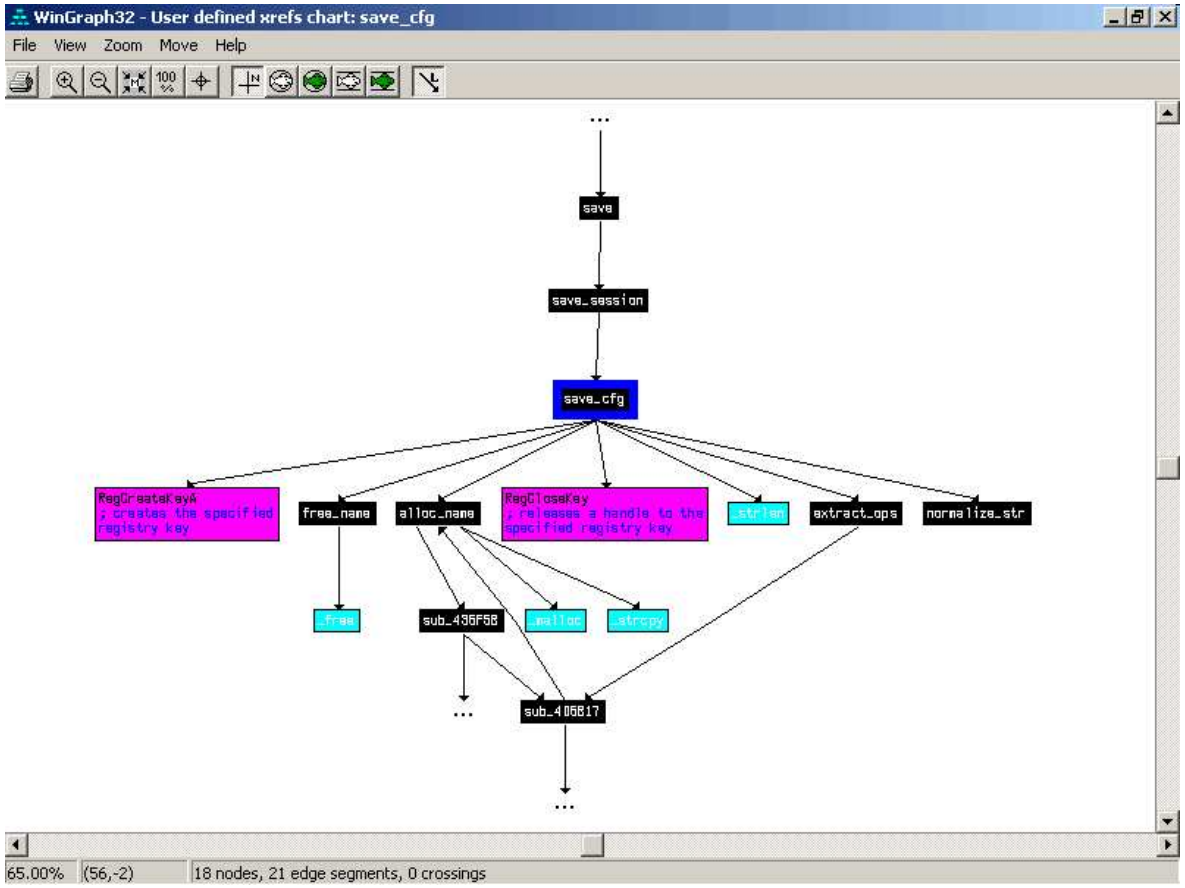
- Interactive Disassembler Professional



Strumenti - 1/10

IDA PRO - 5/6

- Interactive Disassembler Professional



Strumenti - 1/10

IDA PRO - 6/6

- **Interactive Disassembler Professional**
  - Link Utile
    - 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 Utile
  - 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 Utile
  - 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 dei registri di sistema
      - Segnalando le varie modifiche nei contenuti
  - Disponibile solo per sistemi basati su Microsoft Windows

Strumenti - 4/10

OllyDBG - 2/2

- OllyDBG
  - Link Utile
    - 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 Utile
  - 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 Utile
  - 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 Utile
  - 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 Utile
  - 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 nell'analisi dinamica per individuare richieste/risposte a/da un host da parte di eventuali malware
  - Open-Source

- Link Utile
  - 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

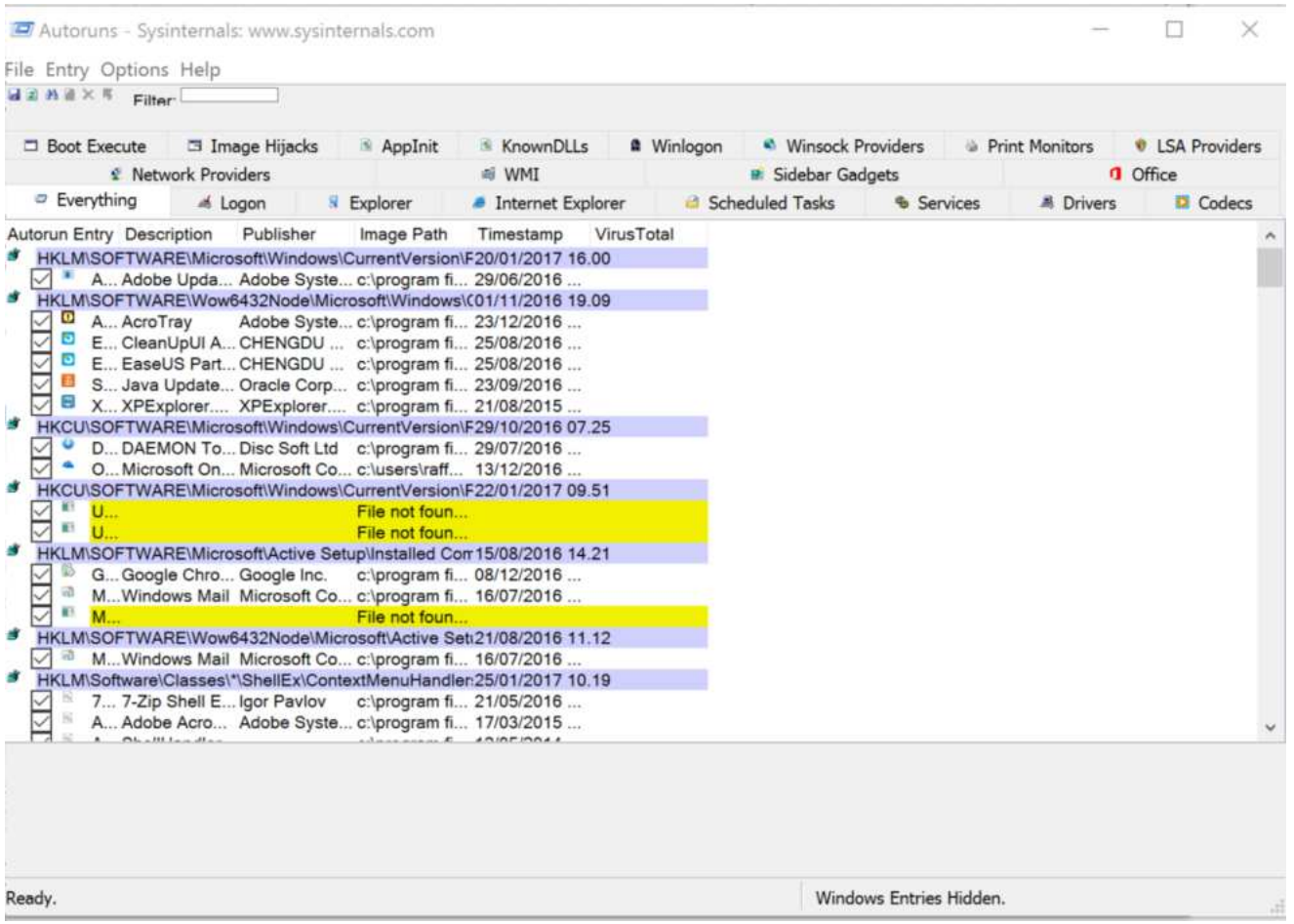
Strumenti – 10/10
(Autoruns – 2/3)

- **Autoruns**
  - Link Utile
    - https://technet.microsoft.com/it-it/sysinternals/bb963902

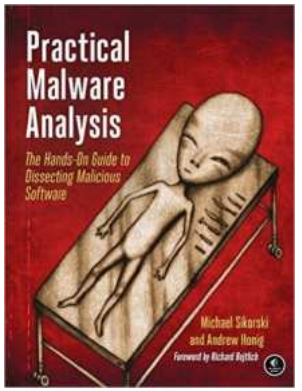
Strumenti – 10/10

(Autoruns – 3/3)

- **Autoruns**



Bibliografia



- **Sikorski, Michael, and Andrew Honig. Practical malware analysis: the hands-on guide to dissecting malicious software. no starch press, 2012. ISBN: 978-1593272906**
  - Malware Analysis Primer [pp. 1-5]
  - Basic Static Techniques [pp. 9-18]
  - Basic Dynamic Analysis [pp. 39-59]
  - Malware Behaviour [pp. 231-250]
    - *Solo Cenni*