

# I Malware

**Alfredo De Santis**

Dipartimento di Informatica  
Università di Salerno

**ads@unisa.it**



**Giugno 2020**

# Outline

- Definizione e Caratteristiche
- Ciclo di Vita
- Tipologie di Malware
- Casi di Studio
  - Il Worm di Morris
  - Backdoor ed il caso dell'iPhone® di San Bernardino
  - Malware su Mobile: Le vulnerabilità di Stagefright (Android)

# Outline

- Definizione e Caratteristiche
- Ciclo di Vita
- Tipologie di Malware
- Casi di Studio
  - Il Worm di Morris
  - Backdoor ed il caso dell'iPhone® di San Bernardino
  - Malware su Mobile: Le vulnerabilità di Stagefright (Android)

# Definizione e Caratteristiche - 1/5

- Un malware (malicious software) è una sequenza di codice (o programma) nocivo
  - Progettato per provocare intenzionalmente danni o alterare il normale comportamento di un sistema informatico e i dati in esso contenuti
- Un malware agisce in modo subdolo
  - Viene eseguito all'insaputa dell'utente

# Definizione e Caratteristiche - 2/5

- Spesso vengono utilizzati meccanismi di **offuscamento** o di **packing** per rendere i malware difficili da rilevare ed analizzare
- Con i meccanismi di **offuscamento** si cerca di occultare l'esecuzione di un malware
- Con i meccanismi di **packing** si comprime (impacchetta) il programma malevolo

# Definizione e Caratteristiche - 2/5

- Spesso vengono utilizzati meccanismi di **offuscamento** o di **packing** per rendere i malware difficili da rilevare ed analizzare
  - Con i meccanismi di **offuscamento** si cerca di occultare l'esecuzione di un malware
  - Con i meccanismi di **packing** si comprime (impacchetta) il programma malevolo
- Entrambe le tecniche **limitano significativamente** la probabilità che il malware venga rilevato mediante alcune tipologie di analisi
  - Ad esempio, *l'analisi statica*

# Definizione e Caratteristiche - 3/5

- I programmi legittimi (non malevoli) includono generalmente **molte stringhe**, che possono essere estratte in fase di analisi
- Un malware compresso (meccanismo di packing) o offuscato contiene **pochissime stringhe**
- Se in seguito dell'analisi di un programma vengono individuate poche stringhe, **probabilmente il programma è compresso o offuscato (e potrebbe quindi essere malevolo)**

# Definizione e Caratteristiche - 4/5

- Uno degli obiettivi dei malware è spesso quello di **rubare le credenziali della vittima**
  - Malware che attendono l'accesso della vittima per rubare le proprie credenziali
  - Malware che effettuano il dump delle informazioni archiviate nel S.O.
    - Informazioni quali hash delle password, etc.
  - Malware il cui compito è quello di registrare alcuni comportamenti della vittima
    - Battiture di tasti, screenshot del S.O., etc.



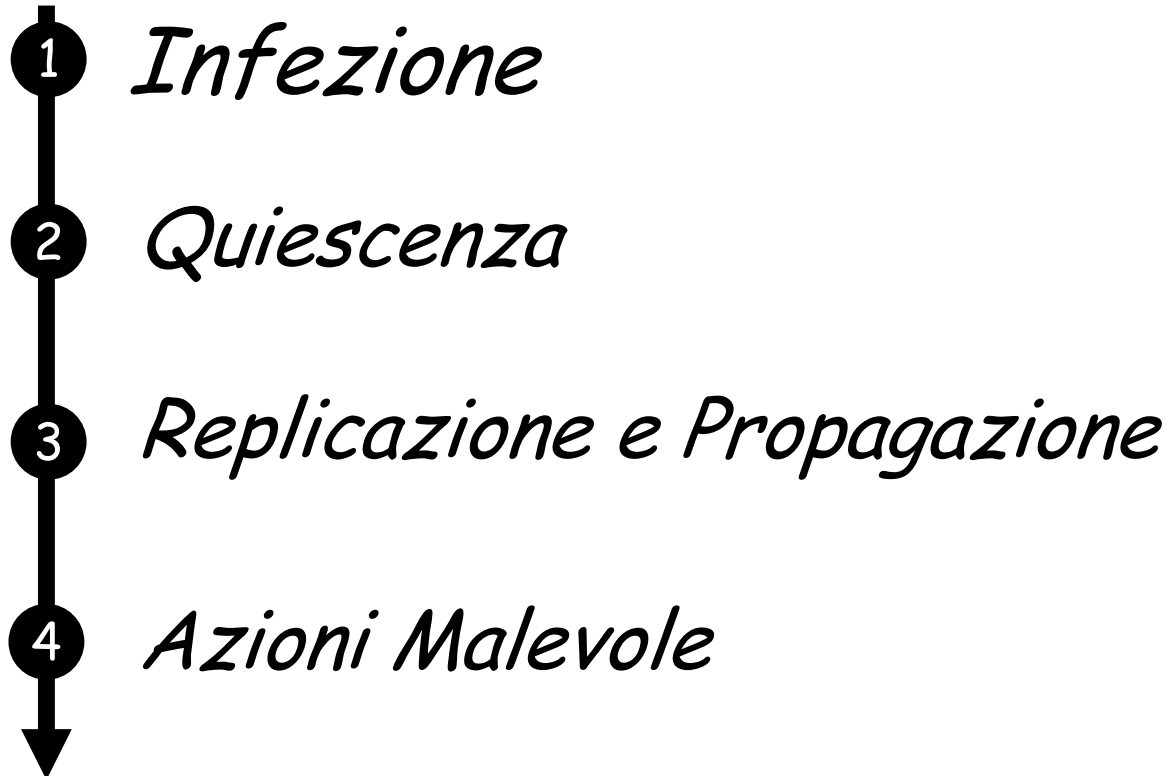
# Definizione e Caratteristiche - 5/5

- L'esecuzione del codice malevolo contenuto in un malware è possibile grazie a vari fattori
  - Utenti inesperti
  - Infrastrutture di rete deboli
  - Misure di sicurezza inadeguate/non sufficienti
  - Falle nel sistema informatico
  - Etc.

# Outline

- Definizione e Caratteristiche
- Ciclo di Vita
- Tipologie di Malware
- Casi di Studio
  - Il Worm di Morris
  - Backdoor ed il caso dell'iPhone® di San Bernardino
  - Malware su Mobile: Le vulnerabilità di Stagefright (Android)

# Ciclo di Vita - 1/5



# Ciclo di Vita - 2/5

## ➤ Infezione

- Fase nella quale il malware penetra e si installa nel sistema, superando eventuali barriere difensive
- I canali principali attraverso i quali avviene l'infezione sono
  - Web
  - Dispositivi Esterni (Penne USB, HDD esterni, SD Card, etc.)
  - E-mail
  - Etc.

# Ciclo di Vita - 3/5

## ➤ Quiescenza

- Il codice malevolo è memorizzato all'interno del sistema (ad es., su memorie di massa, etc.), ma non è attivo
  - Per attivarsi attende che si verifichi una determinata condizione
- Durante questa fase il malware è vulnerabile ad eventuali controlli anti-malware
  - Tuttavia, i malware si sono sempre più specializzati per rendersi difficilmente individuabili anche durante questa fase

# Ciclo di Vita - 4/5

## ➤ **Replicazione e Propagazione**

- Il malware, al verificarsi di determinati eventi o condizioni, si replica e seleziona i bersagli su cui replicarsi
  - Altri sistemi, etc.
- Questa fase è tipica della maggior parte dei software malevoli

# Ciclo di Vita - 5/5

## ➤ Azioni Malevole

- Non si limitano ad una specifica o singola operazione
- Sono caratterizzate dalla combinazione di numerose problematiche (ad es., furto di dati/file, etc.)
  - Che tendono a generarsi in cascata
- Vengono eseguite al verificarsi di determinati eventi o condizioni

# Outline

- Definizione e Caratteristiche
- Ciclo di Vita
- Tipologie di Malware
- Casi di Studio
  - Il Worm di Morris
  - Backdoor ed il caso dell'iPhone® di San Bernardino
  - Malware su Mobile: Le vulnerabilità di Stagefright (Android)



# Tipologie di Malware

- Malware a Diffusione
  - Virus, Worm, Rabbit, ...
- Malware Strumentali
  - Trojan, Backdoor, Spyware, ...
- Malware per il Controllo e l'Attacco
  - Rootkit, Ransomware, Botnet, ...

# Tipologie di Malware

- Malware a Diffusione

- Virus, Worm, Rabbit, ...

- Malware Strumentali

- Trojan, Backdoor, Spyware, ...

- Malware per il Controllo e l'Attacco

- Rootkit, Ransomware, Botnet, ...

A composite image showing various microscopic organisms. The top half features a large, complex virus with many thin, radiating spikes. The bottom half shows several other viruses, some with prominent spikes and others more rounded, along with some rod-shaped bacteria. The background is a soft, out-of-focus green and blue.

# Malware a Diffusione Virus - 1/2

- Il **virus** è una delle tipologie più note e diffuse di malware
- L'obiettivo principale di un virus è quello di danneggiare file o parti del S. O.
  - È solitamente in grado di replicarsi

# Malware a Diffusione Virus - 2/2

- Un virus necessita di un software ospite in cui inserirsi e tramite il quale iniziare l'infezione
  - Da qui l'analogia con i virus in ambito biologico
- Probabilmente i virus sono stati la prima forma di malware



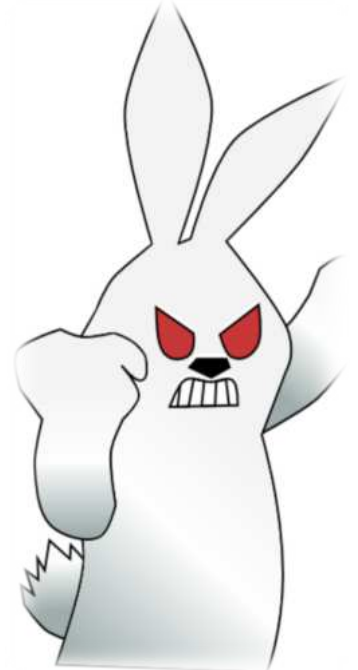
# Malware a Diffusione Worm

- Un **worm** non necessita di un software ospite
- È in grado di auto-propagarsi
  - Sfrutta le vulnerabilità di software installati o del Sistema Operativo
- Il primo Worm diffuso via Internet è stato il *Worm di Morris*
  - Maggiori dettagli in seguito...



# Malware a Diffusione Rabbit

- I malware di tipo **rabbit** sono caratterizzati da una rapidissima auto-propagazione
  - Da qui l'analogia con i conigli...
- L'obiettivo principale di un rabbit è quello di rendere inutilizzabili le risorse di sistema
  - Memoria
  - CPU
  - Etc.



# Tipologie di Malware

- Malware a Diffusione

- Virus, Worm, Rabbit, ...

- Malware Strumentali

- Trojan, Backdoor, Spyware, ...

- Malware per il Controllo e l'Attacco

- Rootkit, Ransomware, Botnet, ...

# Malware Strumentali

## Trojan

- I **trojan**, noti anche come "Cavalli di Troia", celano la loro identità
  - Appaiono all'utente come software utili o comunque non nocivi
- Possono avere molteplici obiettivi malevoli
  - Ad esempio l'esecuzione di ulteriori malware più dannosi
- Non presentano però obiettivi di auto-propagazione





# Malware Strumentali

## Backdoor

- Una **backdoor** può nascondersi in un software, similmente ad un trojan
- Le backdoor vengono solitamente usate per fornire accessi non convenzionali e privilegiati a determinate parti del software
  - Utilizzate dai programmatori per accessi al sistema in casi di emergenza o di manutenzione ordinaria e straordinaria
  - Utilizzate anche durante casi giudiziari
    - Maggiori dettagli in seguito...



# Malware Strumentali

## Spyware

- L'obiettivo principale di uno **spyware** è quello di ottenere informazioni e dati sensibili all'insaputa dell'utente
- Una volta infettato il sistema, lo spyware registra e trasmette informazioni riguardanti le attività effettuata dell'utente
- Non presenta obiettivi di auto-propagazione



# Tipologie di Malware

- Malware a Diffusione

- Virus, Worm, Rabbit, ...

- Malware Strumentali

- Trojan, Backdoor, Spyware, ...

- Malware per il Controllo e l'Attacco

- Rootkit, Ransomware, Botnet, ...

# Malware per il Controllo e l'Attacco

## Rootkit

- L'obiettivo di un **rootkit** è di permettere l'accesso ed il controllo di un sistema
  - Il controllo può essere ottenuto da locale o da remoto
- I rootkit non si auto-propagano



# Malware per il Controllo e l'Attacco

## Ransomware

- Un **ransomware** è una tipologia di malware in grado di cifrare, mediante una chiave complessa, i dati contenuti nel sistema infettato
  - Talvolta può essere cifrato il contenuto dell'intero hard disk
- Di solito è richiesto il pagamento di un riscatto per poter decifrare i dati



# Malware per il Controllo e l'Attacco Ransomware - Esempio 1



# Malware per il Controllo e l'Attacco Ransomware - Esempio 2



## Your computer has been locked!

**Your computer has been locked due to suspicion of illegal content downloading and distribution.**  
Mentioned illegal content (414 Mb of video files) was automatically classified as child pornographic materials. Such actions, in whole or in part, violate following U.S. Federal Laws:

- 18 U.S.C. § 2251- Sexual Exploitation of Children (Production of child pornography)
- 18 U.S.C. § 2252- Certain activities relating to material involving the sexual exploitation of minors (Possession, distribution and receipt of child pornography)
- 18 U.S.C. § 2252A- certain activities relating to material constituting or containing child pornography

**Any individual who violates, or attempts to violate, or conspires to violate mentioned laws shall be sentenced to a mandatory term of imprisonment from 4 to 30 years and shall be fined up to \$250,000.**

**Technical details:**  
Involved IP address: [REDACTED]  
Involved host name: [REDACTED]  
Source or intermediary sites: <http://pornerbros.com>

All suspicious files from your computer were transmitted to a special server and shall be used as evidences. Don't try to corrupt any data or unblock your account in an unauthorized way.

Your case can be classified as occasional/unmotivated, according to title 17 (U. S. Code) § 512. Thus it may be closed without prosecution. Your computer will be unblocked automatically.

**In order to resolve the situation in an above-mentioned way you should pay a fine of \$300.**

### HOW TO UNLOCK YOUR COMPUTER:

-  Take your cash to one of this retail locations:  

-  Get a MoneyPak and purchase it with cash at the register
-  Come back and enter your MoneyPak code to unlock your computer (5 attempts available)


Code:

1	2	3
4	5	6
7	8	9
Delete	0	Enter

Permanent lock on 05/01/2013 5:20 p.m. EST




# Malware per il Controllo e l'Attacco Ransomware - Esempio 3



## Guardia di Finanza

*insieme per la legalità*



### Attenzione!!!

È stata rivelata un'attività illegale. Il sistema operativo è stata bloccata per una violazione delle leggi della Repubblica Italiana!  
È stata fissata una seguente violazione: Dal tuo indirizzo IP "151.50.120.125" era eseguito un accesso alle web-pagine contenenti la pornografia, la pornografia minorile, zoofilia, nonché la violenza dei bambini. Nel tuo computer sono stati trovati video-file contenenti la pornografia, elementi di violenza e la pornografia minorile.  
**Dalla posta elettronica era effettuato anche la distribuzione dello spam con un senso recondito terroristico.**  
**Il bloccaggio di computer serve per troncare l'attività illegale dalla parte tua.**

I tuoi dati

**IP:** [redacted]  
**Posizione:** Italy, [redacted]  
**ISP:** [redacted]

**Per togliere il bloccaggio devi pagare una multa di 100 euro. Hai due seguenti varianti di pagamento:**

1) Effettuare il pagamento tramite l'Ukash.

Per questo inserisci il numero ricevuto nella colonna di pagamento, dopodiché premi OK (se hai più numeri, allora inseriscili uno dopo l'altro, dopodiché premi OK)

Se il sistema segnalerà un errore, allora dovrai mandare il numero per la posta elettronica [deposito@cyber-gdf.net](mailto:deposito@cyber-gdf.net).

2) Effettuare il pagamento tramite il Paysafecard:



Per questo inserisci per favore il numero ricevuto (nel caso di necessità insieme con la password) nella colonna di pagamento, dopodiché premi OK (se hai più numeri, allora inseriscili uno dopo l'altro, dopodiché premi OK).


Se il sistema segnalerà un errore, allora dovrai mandare il numero per la posta elettronica [deposito@cyber-gdf.net](mailto:deposito@cyber-gdf.net).

### Ukash Dove passo trovare Ukash?

Puoi richiedere e ottenere Ukash presso migliaia di punti vendita, edicole, stazioni di servizio, bar e tabacchi e negozi di telefonia mobile dotati di terminale **Epay, Epipoli**.

Recati presso il punto vendita dotato di terminale **Epay, Epipoli** a te più vicino. Richiedi un voucher in contanti al negoziante. Il negoziante dovrà stampare e consegnarti un voucher Ukash con codice PIN da 19 cifre.







# Malware per il Controllo e l'Attacco Ransomware - Esempio 4

- Nel gennaio 2017 l'hotel austriaco *Romantik Seehotel Jägerwir* ha subito un attacco
  - Operato da un gruppo di hacker mediante un ransomware
- Tale attacco ha impedito il normale funzionamento della struttura, bloccando tra l'altro
  - Chiusura e Apertura delle Stanze
  - Sistema per il check-in e check-out
- La direzione dell'hotel è stata costretta al pagamento di un riscatto pari a 1500€
  - Effettuato tramite BitCoin

## Fonte

[https://thenextweb.com/security/2017/01/30/hackers-use-ransomware-to-lock-hotel-guests-in-their-rooms/?utm\\_source=feedburner&utm\\_medium=feed&utm\\_campaign=Feed%3A+TheNextWeb+%28The+Next+Web+All+Stories%29](https://thenextweb.com/security/2017/01/30/hackers-use-ransomware-to-lock-hotel-guests-in-their-rooms/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+TheNextWeb+%28The+Next+Web+All+Stories%29)

# Malware per il Controllo e l'Attacco

## Botnet - 1/2

- Una **botnet** è costituita da un insieme di host compromessi
  - Detti anche *zombie*
- Tali host sono controllati da un server centrale
  - Detto *Botnet Controller*



# Malware per il Controllo e l'Attacco

## Botnet - 2/2

- L'obiettivo principale di una botnet è di quello di creare una rete di zombie che sia il più vasta possibile, al fine di
  - Diffondere su larga scala software malevolo
  - Inviare spam
  - Realizzare attacchi di *Distributed Denial of Service (DDoS)*
    - Per rendere inutilizzabili servizi di rete
  - Etc.

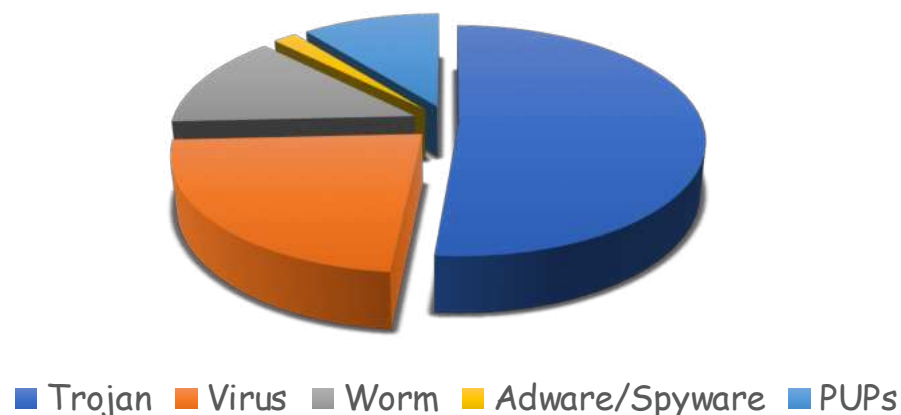


# Malware e Diffusione - 1/4

- Nel 2015 sono stati identificati mediamente 230000 nuovi malware al giorno

Tipologia	Percentuale
Trojan	51,45%
Virus	22,79%
Worm	13,22%
Adware/Spyware	1,83%
Potentially Unwanted Programs (PUPs)	10,71%

Nuovi Malware Creati nel 2015

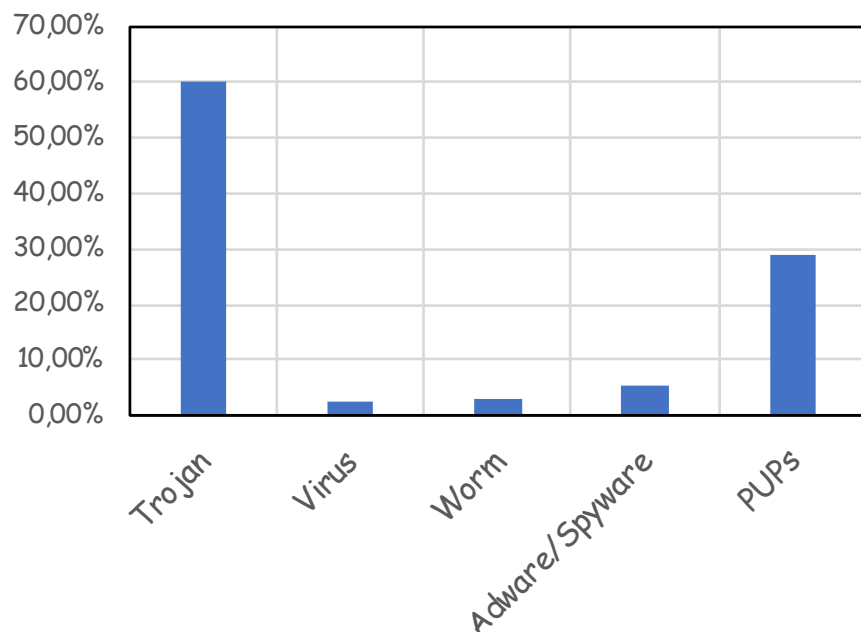


- Dati provenienti dal Rapporto Annuale del 2015 di PandaLab
  - <http://www.pandasecurity.com/mediacenter/src/uploads/2014/07/Pandalabs-2015-anual-EN.pdf>

# Malware e Diffusione - 2/4

- La percentuale dei PC infetti è pari al 32,13% e le infezioni sono distribuite come segue

Percentuale Infezioni per Tipo di Malware nel 2015



Tipologia	Percentuale
Trojan	60,30%
Virus	2,55%
Worm	2,98%
Adware/Spyware	5,19%
Potentially Unwanted Programs (PUPs)	28,98%

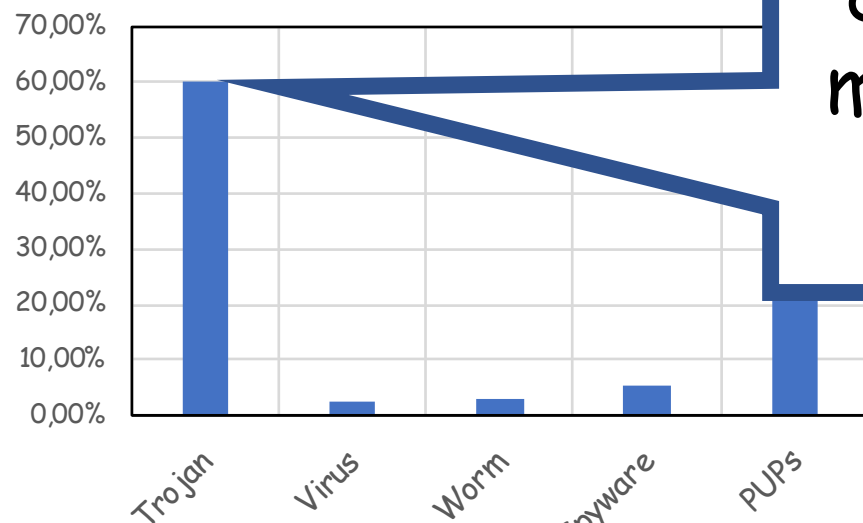
- Dati provenienti dal Rapporto Annuale del 2015 di PandaLab

➤ <http://www.pandasecurity.com/mediacenter/src/uploads/2014/07/Pandalabs-2015-anual-EN.pdf>

# Malware e Diffusione - 2/4

- La percentuale dei PC infetti è pari al 32,13% e le infezioni sono distribuite come segue

Percentuale Infezioni per Tipo di Malware



È possibile osservare che i trojan hanno la maggiore percentuale di infezione

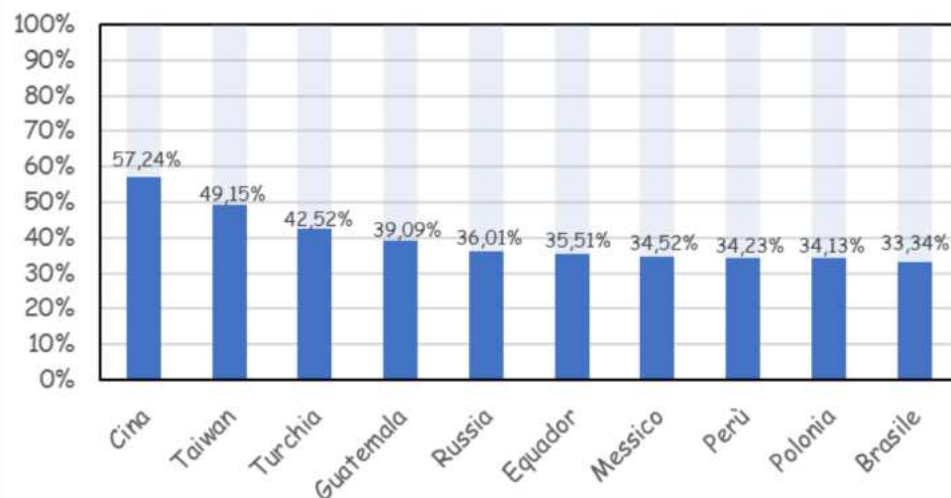
	Percentuale
Trojan	60,30%
Virus	2,55%
Worm	2,98%
Adware/Spyware	5,19%
Potentially Unwanted Programs (PUPs)	28,98%

- Dati provenienti dal Rapporto Annuale del 2015 di PandaLab

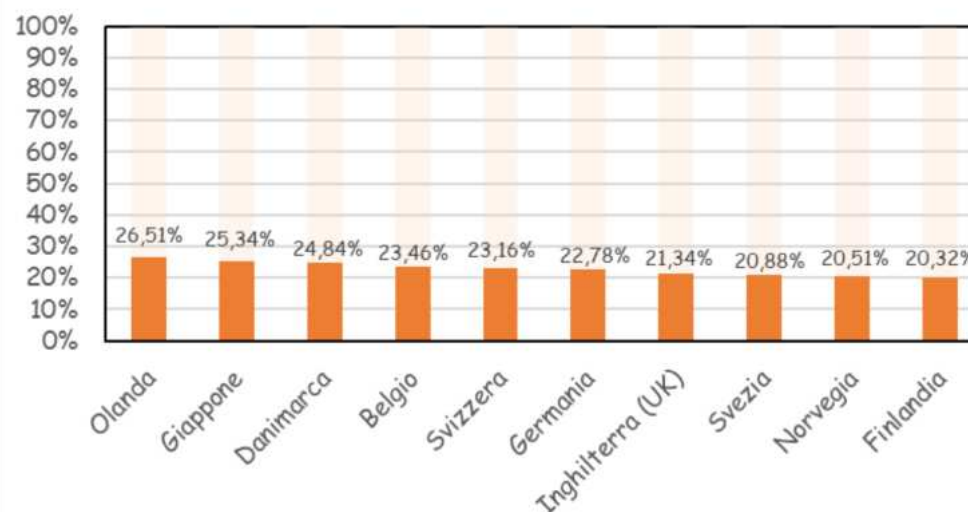
➤ <http://www.pandasecurity.com/mediacenter/src/uploads/2014/07/Pandalabs-2015-anual-EN.pdf>

# Malware e Diffusione - 3/4

Paesi con il Tasso di Infezione più Alto nel 2015



Paesi con il Tasso di Infezione più Basso nel 2015

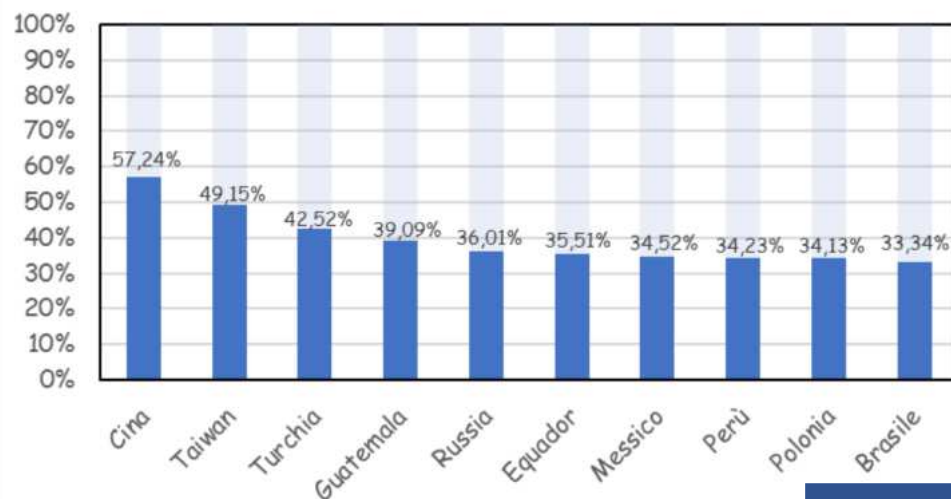


➤ Dati provenienti dal Rapporto Annuale del 2015 di PandaLab

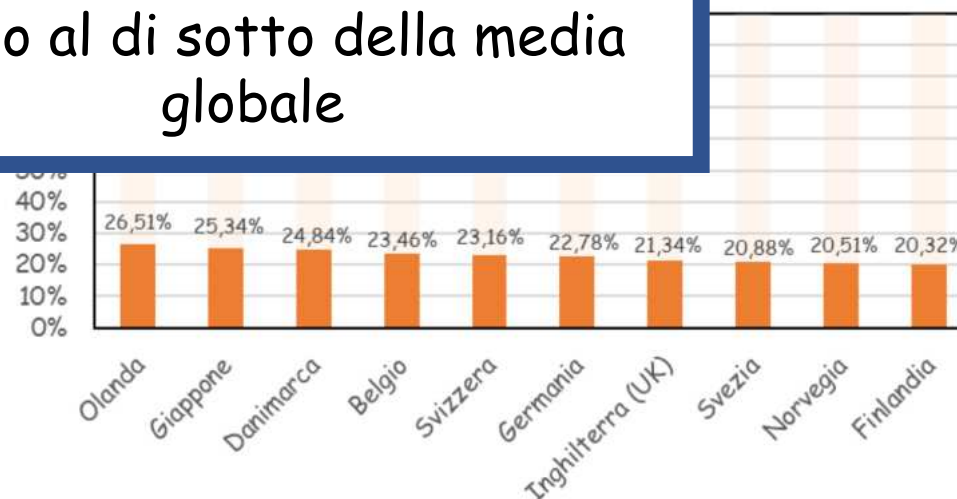
➤ <http://www.pandasecurity.com/mediacenter/src/uploads/2014/07/Pandalabs-2015-anual-EN.pdf>

# Malware e Diffusione - 3/4

Paesi con il Tasso di Infezione più Alto nel 2015



Paesi con il Tasso di Infezione più Basso nel 2015



Tasso al di sotto della media globale



➤ Dati provenienti dal Rapporto Annuale del 2015 di PandaLab

➤ <http://www.pandasecurity.com/mediacenter/src/uploads/2014/07/Pandalabs-2015-anual-EN.pdf>



# Malware e Diffusione - 4/4

(Pandalab - Rapporto Annuale 2015)

- Il Rapporto Annuale 2015 di PandaLab mette in evidenza i seguenti punti
  - La percentuale di attacchi è cresciuta come mai registrato prima
  - È necessario investire maggiori risorse per migliorare la protezione da malware
    - Soprattutto in ambito business

# Malware e Diffusione - 4/4

- In futuro sarà necessario prestare grande attenzione
  - Ai dispositivi dell'**Internet of Things (IoT)**
    - Sempre connessi ad Internet e quindi potenziali bersagli
  - Al mondo dell'industria e **della sanità**
    - Potrebbero essere il prossimo obiettivo dei ransomware
    - Come evidenziato alla RSA Conference del 2017, le infrastrutture di tali enti spesso non godono di sistemi di sicurezza adeguati

➤ Fonti:

- <http://www.pandasecurity.com/mediacenter/src/uploads/2014/07/Pandalabs-2015-anual-EN.pdf>
- [http://www.infoworld.com/article/3169606/security/infrastructure-under-attack-the-next-ransomware-wave.html#tk.rss\\_all](http://www.infoworld.com/article/3169606/security/infrastructure-under-attack-the-next-ransomware-wave.html#tk.rss_all)

# Outline

- Definizione e Caratteristiche
- Ciclo di Vita
- Tipologie di Malware
- Casi di Studio
  - Il Worm di Morris
  - Backdoor ed il caso dell'iPhone® di San Bernardino
  - Malware su Mobile: Le vulnerabilità di Stagefright (Android)

# Outline

- Definizione e Caratteristiche
- Ciclo di Vita
- Tipologie di Malware
- Casi di Studio
  - Il Worm di Morris
  - Backdoor ed il caso dell'iPhone® di San Bernardino
  - Malware su Mobile: Le vulnerabilità di Stagefright (Android)

# Caso di Studio 1

## Il Worm di Morris (Morris Worm) - 1/4

- Il worm di Morris è stato scritto da Robert Morris
  - Rilasciato il 2 Novembre 1988
- È stato uno dei primi worm ad essere diffusi via Internet
  - È stato diffuso da un elaboratore del *Massachusetts Institute of Technology (MIT)*



Robert Morris

# Caso di Studio 1

## Il Worm di Morris (Morris Worm) - 2/4

- Le finalità del worm di Morris non erano dannose
  - L'obiettivo principale era quello di individuare la dimensione di Internet
  - A tal fine il worm sfruttava diverse vulnerabilità di
    - Unix
    - Comando *sendmail*
    - Comando *password*
    - Etc.



Codice Sorgente del  
Worm Morris

# Caso di Studio 1

## Il Worm di Morris (Morris Worm) – 3/4

- Il Worm di Morris è costituito da poche centinaia di linee di codice
  - Scritto in C
- Il codice sorgente si articola in 9 file
  - 7 file .c (C source-file)
  - 2 file .h (C header-file)
  - 1 makefile (direttive di compilazione)
- Il codice del worm è disponibile al link seguente
  - <https://github.com/arialdomartini/morris-worm>

```
cracksome.c  
hs.c  
makefile  
net.c  
stubs.c  
worm.c  
worm.h  
wormdes.c  
x8113550.c
```

File del codice  
sorgente

# Caso di Studio 1

## Il Worm di Morris (Morris Worm) - 4/4

```
main(argc, argv)          /* 0x20a0 */
{
    int argc;
    char **argv;

    int i, l8, pid_arg, j, cur_arg, unused;
    long key;                /* -28(fp) */
    struct rlimit rl;

    l8 = 0;                  /* Unused */

    strcpy(argv[0], XS("sh")); /* <env+52> */
    time(&key);
    srand(key);
    rl.rlim_cur = 0;
    rl.rlim_max = 0;
    if (setrlimit(RLIMIT_CORE, &rl))
    ;
    signal(SIGPIPE, SIG_IGN);
    pid_arg = 0;
    cur_arg = 1;
    if (argc > 2 &&
        strcmp(argv[cur_arg], XS("-p")) == 0) { /* env55 == "-p" */
        pid_arg = atoi(argv[2]);
        cur_arg += 2;
    }
    for(i = cur_arg; i < argc; i++) { /* otherwise <main+286> */
        if (loadobject(argv[i]) == 0)
            exit(1);
        if (pid_arg)
            unlink(argv[i]);
    }
    if ((nobjects < 1) || (getobjectbyname(XS("l1.c")) == NULL))
        exit(1);
    if (pid_arg) {
        for(i = 0; i < 32; i++)
            close(i);
        unlink(argv[0]);
        unlink(XS("sh")); /* <env+63> */
        unlink(XS("/tmp/.dumb")); /* <env+66>"/tmp/.dumb"
    }
}
```

Funzione main  
del Worm di Morris  
(file: worm.c)



# Outline

- Definizione e Caratteristiche
- Ciclo di Vita
- Tipologie di Malware
- Casi di Studio
  - Il Worm di Morris
  - Backdoor ed il caso dell'iPhone® di San Bernardino
  - Malware su Mobile: Le vulnerabilità di Stagefright (Android)

# Caso di Studio 2

## Backdoor ed il Caso dell'iPhone® nella Strage di San Bernardino - 1/6

### La Strage (Sintesi)

- 2 Dicembre 2015, *Inland Regional Center*, Centro Sociale per Disabili, San Bernardino (California, USA)
  - Syed Farook e Tashfeen Malik (marito e moglie) hanno compiuto una strage di stampo terroristico dove hanno perso la vita 14 persone e 24 sono rimaste ferite



# Caso di Studio 2

## Backdoor ed il Caso dell'iPhone® nella Strage di San Bernardino - 2/6

### Il coinvolgimento di Apple

- Farook era possessore di un iPhone 5C
  - Tale dispositivo non ha il TouchID® di Apple
    - Sensore biometrico per impronte digitali
  - È possibile accedere al dispositivo solo mediante un codice numerico
- L'FBI aveva necessità di accedere al dispositivo per procedere con l'indagine
  - Per carpire eventuali informazioni su cellule terroristiche, etc.



# Caso di Studio 2

## Backdoor ed il Caso dell'iPhone® nella Strage di San Bernardino - 3/6

- Risultò impossibile per l'FBI accedere al dispositivo
  - A causa del codice di protezione
- Gli attacchi a forza bruta (*brute force*) furono scartati
  - Avrebbero potuto compromettere l'indagine
  - iOS®, il Sistema Operativo dell'iPhone, ha un'opzione di sicurezza
    - **Auto-cancella i dati** presenti sul dispositivo dopo un certo numero (10) di fallimenti nell'inserimento del codice di protezione
    - Tale opzione era attiva nell'iPhone in questione



# Caso di Studio 2

## Backdoor ed il Caso dell'iPhone® nella Strage di San Bernardino - 4/6

- Un'ordinanza del Giudice Federale di Los Angeles richiese ad Apple di aggiungere in iOS, solo sul dispositivo oggetto di indagine, le seguenti funzionalità
  - Disabilitare (o bypassare) la funzione di auto-cancellazione a seguito dei 10 tentativi errati
  - Consentire all'FBI di inserire il codice di protezione tramite una porta fisica del dispositivo
  - Eliminare eventuali ritardi tra l'inserimento di un codice di protezione errato ed un altro codice



# Caso di Studio 2

## Backdoor ed il Caso dell'iPhone® nella Strage di San Bernardino - 4/6

Stralcio dell'ordinanza  
emessa nel Febbraio 2016

1 "SUBJECT DEVICE") pursuant to a warrant of this Court by providing  
2 reasonable technical assistance to assist law enforcement agents in  
3 obtaining access to the data on the SUBJECT DEVICE.

4 2. Apple's reasonable technical assistance shall accomplish  
5 the following three important functions: (1) it will bypass or  
6 disable the auto-erase function whether or not it has been enabled;  
7 (2) it will enable the FBI to submit passcodes to the SUBJECT DEVICE  
8 for testing electronically via the physical device port, Bluetooth,  
9 Wi-Fi, or other protocol available on the SUBJECT DEVICE; and (3) it  
10 will ensure that when the FBI submits passcodes to the SUBJECT  
11 DEVICE, software running on the device will not purposefully  
12 introduce any additional delay between passcode attempts beyond what  
13 is incurred by Apple hardware.

14 3. Apple's reasonable technical assistance may include, but is  
15 not limited to: providing the FBI with a signed iPhone Software  
16 file, recovery bundle, or other Software Image File ("SIF") that can  
17 be loaded onto the SUBJECT DEVICE. The SIF will load and run from



# Caso di Studio 2

## Backdoor ed il Caso dell'iPhone® nella Strage di San Bernardino - 5/6

- Nonostante l'ordinanza, il CEO di Apple, Tim Cook, dispose di non voler "forzare" il codice di sblocco, perché ciò avrebbe creato un precedente pericoloso
  - L'eventuale tecnica di sblocco avrebbe potuto essere applicata su altre unità di iPhone
    - Creando, di fatto, una sorta di backdoor
- L'FBI dichiarò in seguito di essere riuscita a sbloccare l'iPhone senza l'aiuto di Apple
  - Secondo indiscrezioni, il costo complessivo di tale sblocco fu di circa 1,3 milioni di dollari



# Caso di Studio 2

## Backdoor ed il Caso dell'iPhone® nella Strage di San Bernardino - 6/6

- Questo caso è stato emblematico
  - Ha messo in luce le criticità ed i vantaggi delle backdoor, in relazione al loro utilizzo
- Ha anche suscitato diverse polemiche e scontri mediatici fra FBI, Governo USA, Apple ed aziende terze
  - Che si sono schierate a favore (ad es., Microsoft) o contro





# Caso di Studio 2

## Backdoor ed il Caso dell'iPhone® nella Strage di San Bernardino - 6/6

### Bari come San Bernardino: bloccato l'iPhone di uno degli indagati

*Gli inquirenti sono riusciti ad entrare nei cellulari di Qari Khesta Mir Ahmadzai e Surgul Ahmadzai. Non in quello di Mansoor Ahmadzai.*

*Una situazione analoga a quella affrontata dall'Fbi con lo smartphone usato dal killer californiano*

di GIULIANO FOSCHINI e FABIO TONACCI



Lo leggo dopo

11 maggio 2016



Cronaca

Maggio 2016

#### Fonte

[http://www.repubblica.it/cronaca/2016/05/11/news/bari\\_come\\_san\\_bernardino\\_bloccato\\_l\\_iphone\\_e\\_di\\_uno\\_degli\\_indagati-139556905/](http://www.repubblica.it/cronaca/2016/05/11/news/bari_come_san_bernardino_bloccato_l_iphone_e_di_uno_degli_indagati-139556905/)



# Caso di Studio 2

## Backdoor ed il Caso dell'iPhone® nella Strage di San Bernardino - 6/6

**IL**  **MATTINO.it**

Febbraio 2017

Il Mattino > Napoli > Cronaca

### Video hot, sbloccato l'iPhone di Tiziana: si fa luce sul suicidio

I carabinieri sono stati precisi: hanno «scavato» in maniera chirurgica perché già sapevano che in quell'iPhone 5 ci sarebbe stata la verità. L'hanno trovata intatta, tra i messaggi vocali di Tiziana Cantone registrati prima che si lasciasse morire impiccata all'attrezzo da ginnastica della tavernetta. E per aprire il cellulare di Tiziana Cantone è stato usato un trucco informatico **identico a quello utilizzato dall'Fbi per accedere allo smartphone del killer di San Bernardino**. Niente spedizioni di telefoni oltreoceano, niente richieste di aiuto alla Apple. Solo tecnica e algoritmi.

#### Fonte

[http://www.ilmattino.it/napoli/cronaca/video\\_hot\\_sbloccato\\_l\\_iphone\\_di\\_tiziana\\_si\\_fa\\_luce\\_sul\\_suicidio-2259325.html](http://www.ilmattino.it/napoli/cronaca/video_hot_sbloccato_l_iphone_di_tiziana_si_fa_luce_sul_suicidio-2259325.html)



# Outline

- Definizione e Caratteristiche
- Ciclo di Vita
- Tipologie di Malware
- Casi di Studio
  - Il Worm di Morris
  - Backdoor ed il caso dell'iPhone® di San Bernardino
  - Malware su Mobile: Le vulnerabilità di Stagefright (Android)

# Caso di Studio 3

## Malware su Mobile: Le Vulnerabilità di Stagefright (Android) - 1/5

- Letteralmente *strage fright* significa *panico da palcoscenico*
- È un insieme di librerie per la gestione dei contenuti multimediali in Android
  - Si occupa di file video e file audio
  - Permette di estrarre metadati da tali file
  - Etc.



# Caso di Studio 3

## Malware su Mobile: Le Vulnerabilità di Stagefright (Android) - 2/5

- Sono state rilevate delle vulnerabilità in Stagefright
  - Individuate da Joshua Drake, vice presidente di *Platform Research and Exploitation*, Agosto 2015
- Queste vulnerabilità esposero milioni di dispositivi al rischio di attacchi
  - Alcuni attacchi potevano infettare il dispositivo senza alcun intervento da parte dell'utente



# Caso di Studio 3

## Malware su Mobile: Le Vulnerabilità di Stagefright (Android) – 3/5

- È stato mostrato come infettare un dispositivo
  - Con il semplice invio, tramite MMS, di un breve video contenente il codice malevolo
- Al momento della ricezione dell'MMS, il dispositivo processa il video ed attiva il codice malevolo
  - Spesso automaticamente e senza l'intervento dell'utente
- Esponendo tale dispositivo al possibile accesso remoto dei dati
  - Operazioni di copia/cancellazione, etc.



# Caso di Studio 3

## Malware su Mobile: Le Vulnerabilità di Stagefright (Android) - 4/5

- Al momento dell'individuazione della vulnerabilità, circa il 95% dei dispositivi basati su Android® era esposto a tali attacchi
- Google ha prontamente preparato una patch correttiva
  - Tuttavia, non tutti i produttori hanno rilasciato aggiornamenti per i propri dispositivi



# Caso di Studio 3

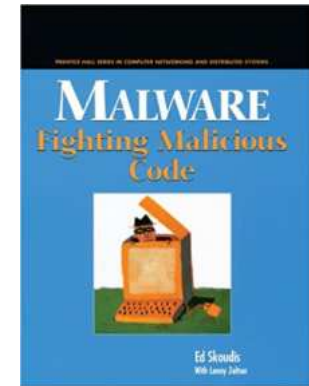
## Malware su Mobile: Le Vulnerabilità di Stagefright (Android) - 5/5

- RSA Conference 2017
  - Adrian Ludwig, direttore della sicurezza Android in Google
    - Sottolineò che non ci furono casi "confermati" di infezione tramite questa vulnerabilità





# Bibliografia



- Ed Skoudis, Lenny Zeltser. **Malware: Fighting Malicious Code**. Prentice Hall PTR, 2003. ISBN: 0-13-101405-6
  - Capitoli 1, 2, 3, 5, 6, 7, 8, 9

# Sitografia San Bernardino

## ➤ La vicenda riportata dai Mass Media

- [https://www.nytimes.com/interactive/2016/09/09/us/document-Review-of-the-San-Bernardino-Terrorist-Shooting.html?\\_r=0](https://www.nytimes.com/interactive/2016/09/09/us/document-Review-of-the-San-Bernardino-Terrorist-Shooting.html?_r=0)
- [http://www.repubblica.it/esteri/2015/12/04/news/usa\\_storag\\_e\\_di\\_san\\_bernardino\\_storie\\_vittime-128763486/](http://www.repubblica.it/esteri/2015/12/04/news/usa_storag_e_di_san_bernardino_storie_vittime-128763486/)
- [http://www.repubblica.it/tecnologia/sicurezza/2016/02/17/news/iphone\\_e\\_sicurezza\\_la\\_chiave\\_e\\_ios\\_un\\_sistema\\_blinato-133645581/](http://www.repubblica.it/tecnologia/sicurezza/2016/02/17/news/iphone_e_sicurezza_la_chiave_e_ios_un_sistema_blinato-133645581/)

## ➤ Ordinanza

- <https://assets.documentcloud.org/documents/2714005/SB-Shooter-Order-Compelling-Apple-Asst-iPhone.pdf>

# Sitografia

## Vulnerabilità Stagefright

- <https://www.blackhat.com/docs/us-15/materials/us-15-Drake-Stagefright-Scary-Code-In-The-Heart-Of-Android.pdf>
- [https://www.theregister.co.uk/2017/02/15/google\\_stagefright\\_android\\_bug\\_zero\\_success/](https://www.theregister.co.uk/2017/02/15/google_stagefright_android_bug_zero_success/)