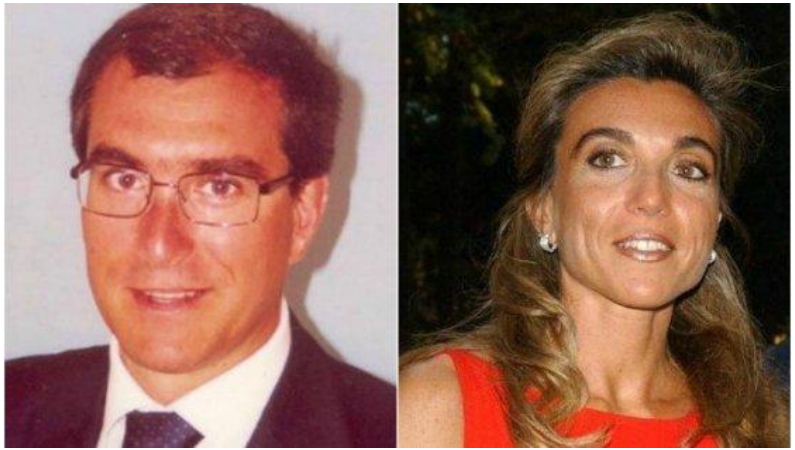
Analisi di malware

Reverse engineering di malware e realizzazione di una signature

Toure Pape Alpha
Esame di Stato 2017

RICORDATE ?

- Fratelli Occhionero
- Elezioni USA
- Snowden e NSA
- WannaCry
- Petya



COME SONO SUCCESSI ?

- Ingegneria sociale
- Vulnerabilità di software
- Malware

...

COME SONO SUCCESSI ?

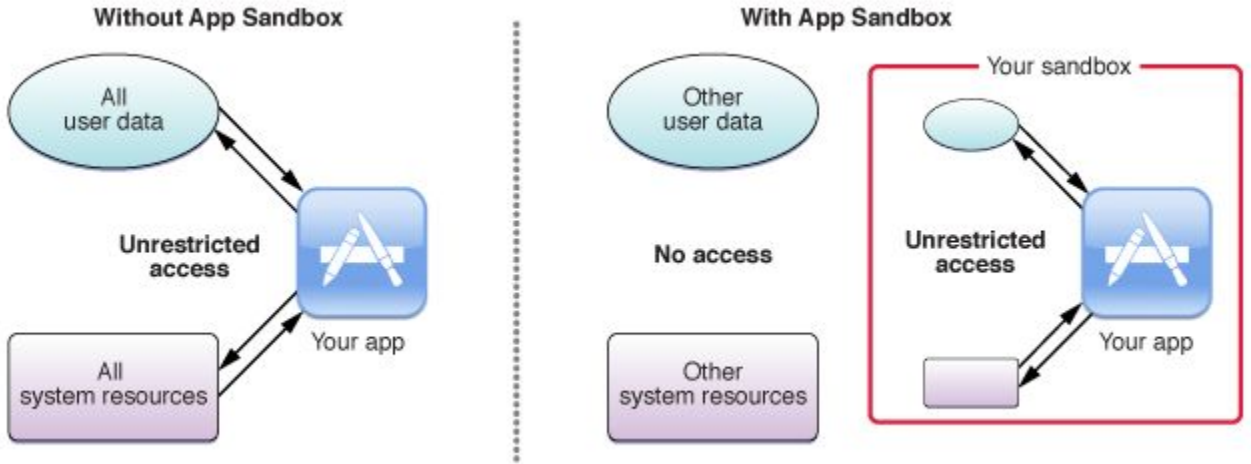
- Ingegneria sociale
- Vulnerabilità di software
- **Malware**

...

COME RICONOSCERLI ?

- Effettuando analisi automatiche
- Effettuando analisi manuali

SANDBOX


Without App Sandbox
All
user data
Unrestricted
access
Your app
All
system resources
With App Sandbox
Other
user data
No access
Other
system resources
Your sandbox
Unrestricted
access
Your app

COME INDIVIDUARLI ?

- ~~Effettuando analisi automatiche~~
- Effettuando analisi **manuali**

REVERSE ENGINEERING

- Analisi statica
- Analisi dinamica

WIRENET

- **Primo malware cross-platform**
- Probabilmente utilizza e-mail come vettore d’attacco
- Progettato per attacchi su piccola scala
- ~ 64 funzionalità a disposizione
- Programmato da principianti

WIRENET

- Primo malware cross-platform
- **Probabilmente utilizza e-mail come vettore d’attacco**
- Progettato per attacchi su piccola scala
- ~ 64 funzionalità a disposizione
- Programmato da principianti

WIRENET

- Primo malware cross-platform
- Probabilmente utilizza e-mail come vettore d’attacco
- **Progettato per attacchi su piccola scala**
- ~ 64 funzionalità a disposizione
- Programmato da principianti

WIRENET

- Primo malware cross-platform
- Probabilmente utilizza e-mail come vettore d’attacco
- Progettato per attacchi su piccola scala
- **~ 64 funzionalità a disposizione**
- Programmato da principianti

WIRENET

- Primo malware cross-platform
- Probabilmente utilizza e-mail come vettore d’attacco
- Progettato per attacchi su piccola scala
- **~ 64 funzionalità a disposizione**
  - Keylogger
  - Furto di credenziali
  - Connessioni sicure con il C&C
  - Reverse bind shell
- Programmato da principianti

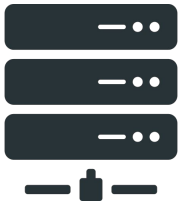
WIRENET

- Primo malware cross-platform
- Probabilmente utilizza e-mail come vettore d’attacco
- Progettato per attacchi su piccola scala
- **~ 64 funzionalità a disposizione**
  - Keylogger
  - Furto di credenziali
  - Connessioni sicure con il C&C
  - Reverse bind shell
- Programmato da principianti

WIRENET

- Primo malware cross-platform
- Probabilmente utilizza e-mail come vettore d’attacco
- Progettato per attacchi su piccola scala
- **~ 64 funzionalità a disposizione**
  - Keylogger
  - Furto di credenziali
  - Connessioni sicure con il C&C
  - Reverse bind shell
- Programmato da principianti

ARCHITETTURA

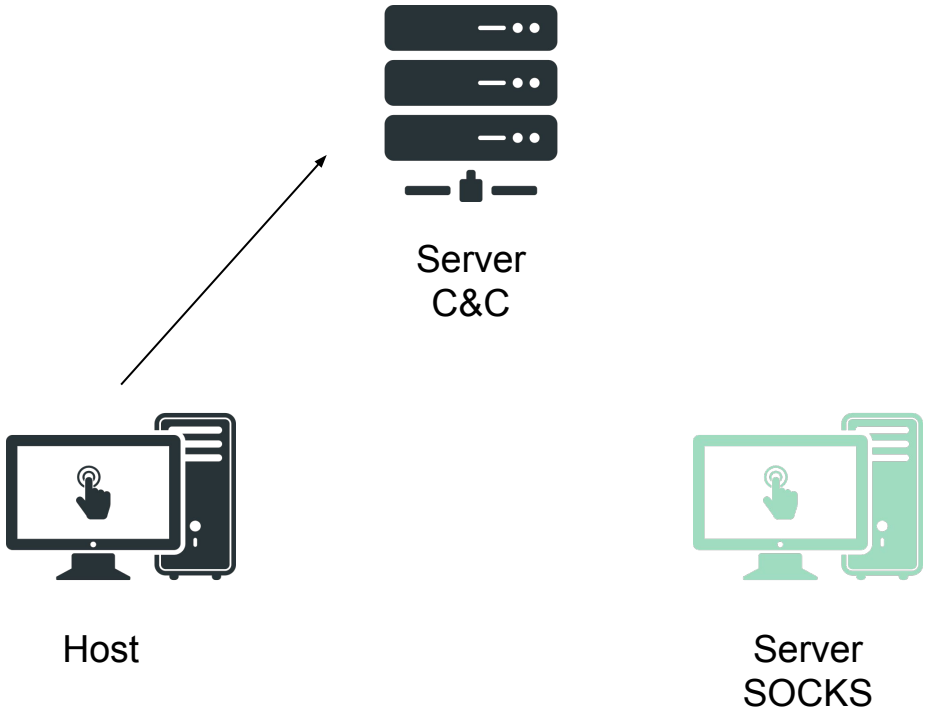


Server
C&C

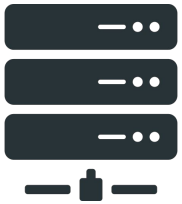
Host

Server
SOCKS

ARCHITETTURA



ARCHITETTURA

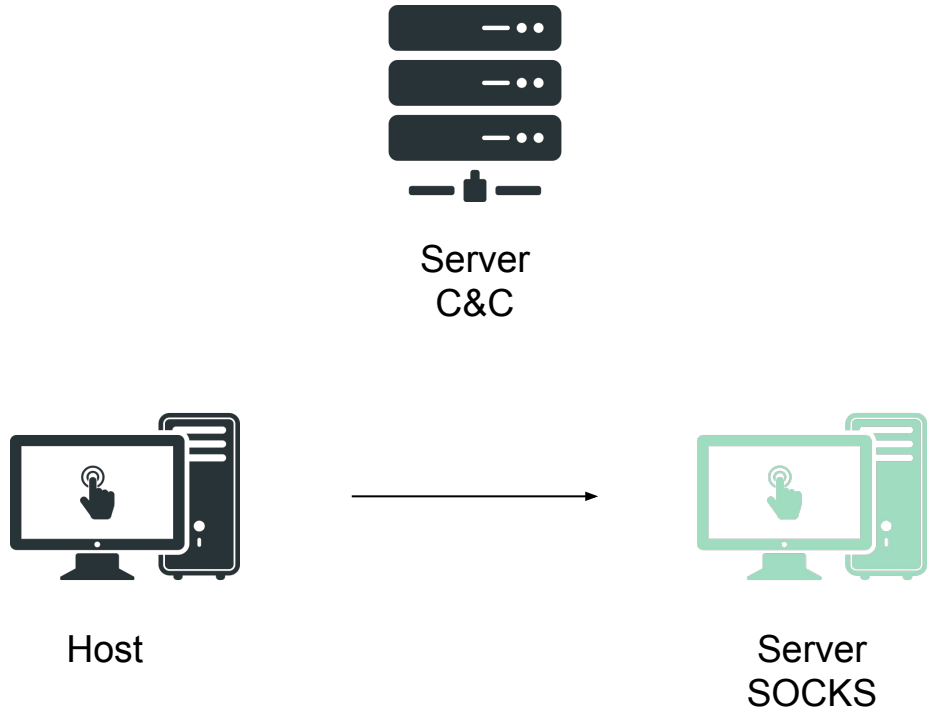


Server
C&C

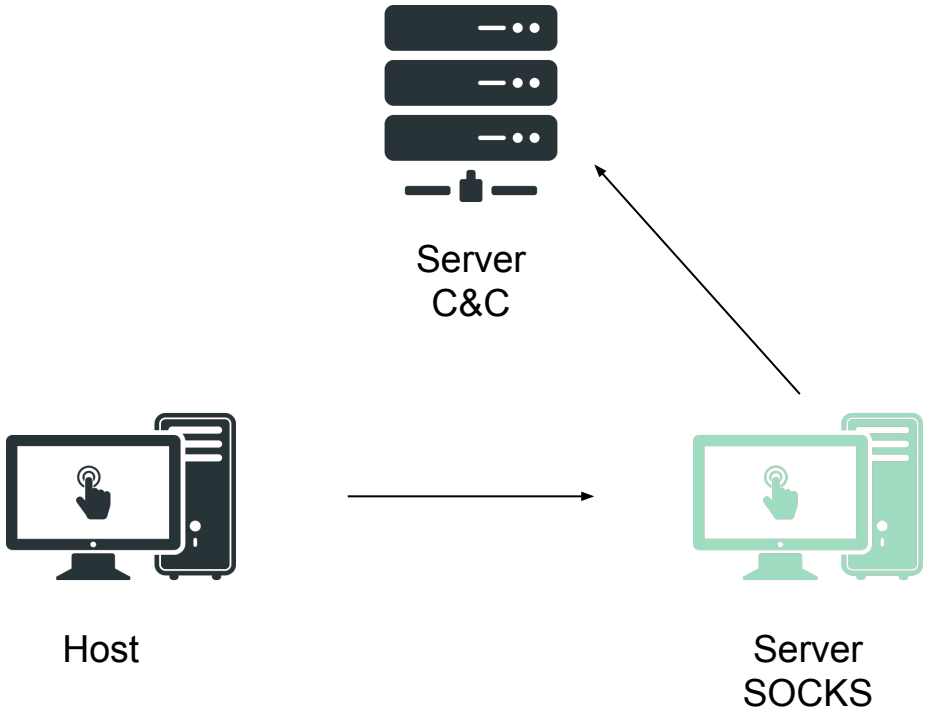
Host

Server
SOCKS

ARCHITETTURA



ARCHITETTURA



WIRENET

- Primo malware cross-platform
- Probabilmente utilizza e-mail come vettore d’attacco
- Progettato per attacchi su piccola scala
- **~ 64 funzionalità a disposizione**
  - Keylogger
  - Furto di credenziali
  - Connessioni sicure con il C&C
  - Reverse bind shell
- Programmato da principianti

WIRENET

- Primo malware cross-platform
- Probabilmente utilizza e-mail come vettore d’attacco
- Progettato per attacchi su piccola scala
- ~ 64 funzionalità a disposizione
- **Programmato da principianti**

COME RICONOSCERLI ?

- ~~Effettuando analisi automatiche~~
- Effettuando analisi manuali **per creare signatures**

SIGNATURE

- I blocchi colorati sono file
- Le forme sono le regole
- Più regole formano una firma

YARA

- Programma di ricerca di pattern
- Regole composte da stringhe testuali e byte
- Operatori logici
- Hash (di file interi o sezioni)

YARA

- Programma di ricerca di pattern
- Regole composte da stringhe testuali e byte
  - `$str  = “signons.sqlite”`
  - `$hex = { 55 B9 C7 D6 AC 4A }`
- Operatori logici
- Hash (di file interi o sezioni)

YARA

- Programma di ricerca di pattern
- Regole composte da stringhe testuali e byte
- Operatori logici
  - `any of ($str, $hex), and, or ...`
- Hash (di file interi o sezioni)

YARA

- Programma di ricerca di pattern
- Regole composte da stringhe testuali e byte
- Operatori logici
  - `any of ($str, $hex), and, or ...`
- Hash (di file interi o sezioni)

“1984 was not supposed to be an instruction manual”

ED ORA ?

- Canale di distribuzione sicuro