# Gli attacchi


Massimo Carnevali



Massimo Carnevali
posta@massimocarnevali.com
https://it.linkedin.com/in/massimocarnevali

## Gli attacchi

- Tipi di attacco



..

## Tipi di attacco

# (Crypto)Kidnapper
# Ransomware
# Cryptolocker



Prende in ostaggio i dati dell’utente e chiede un riscatto.

Esempio di cattivo professionale molto attivo ultimamente.

Tecniche:

Spingere l'utente a lanciare un applicativo infetto o a clickare su un link malevolo (normalmente sfruttando zero-day vulnerability).

Bloccargli il PC o cifrargli i file chiedendo un riscatto per sbloccarlo o per avere la chiave di decifratura.

Pagamenti in bitcoin.

## Tipi di attacco




C’è chi combatte il Ransomware come missione
https://www.nomoreransom.org/

https://www.propublica.org/article/the-ransomware-superhero-of-normal-illinois

https://id-ransomware.malwarehunterteam.com/

## Tipi di attacco

# Ransomware – quanto rende?

| Data | Campagna | Wallet | Bitcoin |
|---|---|---|---|
| 29-11-2016<br>15-12-2016 | stopper | 1FwHxzFFGbAmmdkxhUUTEjocuDhEowDyuU | 67.56167621 |
| 29-11-2016<br>20-12-2016 | worm01 | 1KQhTbj9sGrQ596wBPZLQTpbiN1gBXwAny | 28.53519378 |
| 10-12-2016<br>15-12-2016 | mkgoro | 1swAqc6dAyqcSaKdx8VnuJhhE9vaYLHFb | 8.09468500 |
| 12-12-2016<br>15-12-2016 | payforhelp | 1GKpUP4SWC7TiiX7BkeST4i9bFNVyyPTjb | 4.00000000 |
| 13-12-2016<br>16-12-2016 | bitcoin143 | 19PuzW2WwD4jnhQLLvHun7cCeJq8HZux4 | 9.00000000 |
| 20-12-2016<br>21-12-2016 | amagnus | 1DaeQHLUbckx2tnshQrmcE45tEMB1UxjPS | 4.00000000 |
| 07-01-2017<br>11-01-2017 | bitcoin143 | 1AJa5kZY1LDzSLrYJ3SDq3CubX8qHwpjEN | 12.50000000 |
| 05-01-2017<br>16-01-2017 | cryptsvc | 116CZ4y4mHs9ruzmYCufrwk4t17dsNEnAJ | 26.00070000 |
| | | Totale Bitcoin | 159.69225499 |

"Fonte: CRAM di TG Soft https://www.tgsoft.it"

Esempio di guadagni con una campagna di un mese e mezzo di Ransomware.

"Fonte: CRAM di TG Soft https://www.tgsoft.it "

Attacchi a pioggia, si punta a tanti piccoli incassi, diversi sono gli attacchi mirati che puntano al colpo grosso.

## Tipi di attacco

# Campagne mirate

### Attacco hacker alla Bonfiglioli. "Chiesto riscatto di 2,4 milioni"

L'azienda decide di non pagare: "Abbiamo scelto di non assoggettarci al ricatto e non alimentare un meccanismo criminale"

Ultimo aggiornamento il **2 luglio 2019 alle 19:37**

### Gruppo Iris, attacco hacker. Chiesti 950mila euro di riscatto

Due settimane fa il sistema dell'azienda è stato 'tenuto in ostaggio' Federica Minozzi: "Non abbiamo ceduto, i nostri tecnici hanno risolto tutto"

Ultimo aggiornamento il **28 dicembre 2018 alle 11:51**



Campagne mirate molto complesse.

## Tipi di attacco

# Rischio chiusura aziendale

### Azienda chiude i battenti a causa del ransomware e licenzia 300 dipendenti

Primo Piano  Sabato, 04 Gennaio 2020 09:10

E' stato un inizio del nuovo anno amaro per trecento lavoratori che prima di Natale hanno ricevuto una lettera dalla direzione, che non voleva però fare i tradizionali auguri, bensì comunicare loro che dopo 61 anni di onorata attività l'azienda era costretta a chiudere i battenti a causa dei danni subìti a seguito di un attacco **ransomware**.



Ci sono aziende che sono saltate per aria (anche in Italia, nel bergamasco 80 persone a casa).

## Tipi di attacco

# Danni collaterali (attacco NotPetya)

Logistica Maersk (**300M$**)

Chimica-farmaceutica Merck (**870M$**)

Logistica FedEx-TNT (**400M$**)

Industria Saint-Gobain (**384M$**)



Attacco NotPetya del 2017, sfugge di mano agli attaccanti (probabilmente)
https://en.wikipedia.org/wiki/Petya_(malware)
Maersk (17 porti bloccati per 10 giorni) 150/150 domain controller bloccati contemporaneamente, salvi perché uno in Ghana era offline, hard disk portato a Londra a mano (problema “visti”).
10 giorni per ripartire con 4.000 Server e 45.000 PC, 600 persone al lavoro, full recovery dopo due mesi.
Considerato atto di guerra, l’assicurazione non paga?
https://www.bloomberg.com/news/features/2019-12-03/merck-cyberattack-s-1-3-billion-question-was-it-an-act-of-war

## Tipi di attacco

# DOS - DDOS

## (agenti esterni o interni)

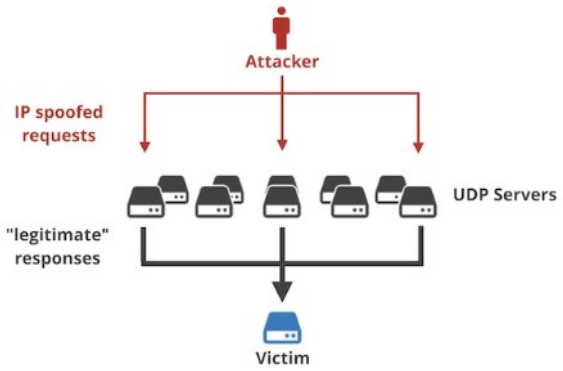


(Distributed) Denial of Service
https://en.wikipedia.org/wiki/Denial-of-service_attack
Impedire il funzionamento di un servizio con attacchi che possono partire anche da punti distribuiti della rete. Cui prodest?
Può essere un puro atto “vandalico” (Hacktivism), può servire per chiedere un riscatto oppure può essere il preludio di un altro attacco (blocco un servizio di difesa oppure blocco il servizio vero per attivarne uno falso).
Può essere fatto a diversi livelli (fisico, trasporto, applicativo, umano) anche algoritmico (mail bomb o pdf “complicati” ad esempio).
Acquistabile in service in rete: “the cost to power a DDoS attack using a cloud-based botnet of 1,000 desktops is about $7 per hour.”
http://securityaffairs.co/wordpress/57429/cyber-crime/cost-ddos-attack-service.html

## Tipi di attacco

# DOS - DDOS

## Riflesso e amplificazione






Se non ho tanti attaccanti posso usare il metodo del riflesso e dell'amplificazione.
Ip spoofing del target poi richieste con poco input e tanto output di riflesso.
https://arstechnica.com/information-technology/2018/02/in-the-wild-ddoses-use-new-way-to-achieve-unthinkable-sizes/

DNS moltiplica per 50
NTP per 60
Protocollo memcache (cache db per web e reti) 50K

1.1Tbps di picco dell'attacco

Mail bomb come attacco DOS alla posta. Allegato zip che si espande (es. da 42KB a 5.5GB)
https://www.bamsoftware.com/hacks/zipbomb/

## Tipi di attacco

# Man in the middle
# Connection hijacking

Man in the Middle attack
https://en.wikipedia.org/wiki/Man-in-the-middle_attack

Può avvenire a vari livelli:
- Fisico (ethernet, wifi)
- Trasporto (TCP/IP)
- Applicativo (http)
- Umano (vedi “Social Engineering”)

Connection Hijacking: inserirsi all’interno di una conversazione oppure modificarne il flusso o i dati
Anche questo può avvenire a vari livelli.
E’ una generalizzazione del Man in the Middle.

## Tipi di attacco

# Privilege Escalation
# Buffer Overflow
# Backdoor
# Keylogging
# IP Spoofing



Privilege escalation: accedere ad un sistema/servizio con privilegi maggiori di quelli previsti per l'utenza. Sfrutta vulnerabilità, crash o errori di programmazione.
https://en.wikipedia.org/wiki/Privilege_escalation
Buffer overflow: accedere ad aree di memoria che non dovrei vedere. Lettura dati o esecuzione programmi.
https://en.wikipedia.org/wiki/Buffer_overflow
Backdoor: una porta di servizio ai miei sistemi/software di cui non sono a conoscenza. Errori di programmazione o lasciata volutamente (produttore, governi, criminali)
https://en.wikipedia.org/wiki/Backdoor_(computing)
Keylogging: intercettare i tasti che vengono premuti sulla tastiera, via software o hardware. Attacchi "over the shoulder".
https://en.wikipedia.org/wiki/Keystroke_logging
IPSpoofing: impersonificare un altro IP, sia per ingannare utente che per mettere in difficoltà l'IP spoofato
https://en.wikipedia.org/wiki/IP_address_spoofing

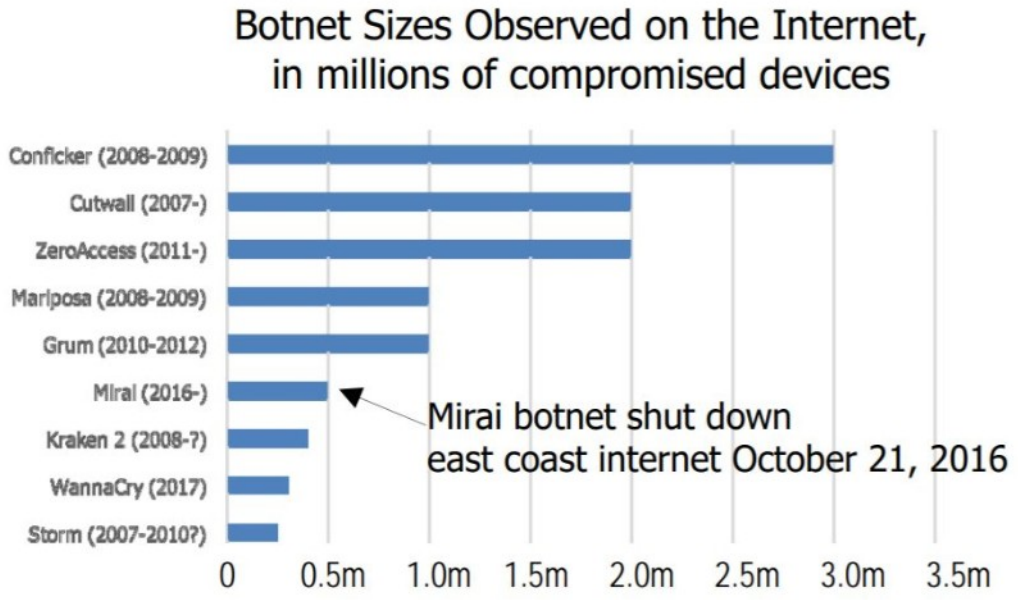
## Tipi di attacco

# Command & control



Command & control
https://en.wikipedia.org/wiki/Command_and_control_(malware)
Termine di derivazione militare.
Rete di server che controllano macchine infette, zombie, botnet ecc.
Cercano di spostarsi velocemente (DNS) e utilizzano reti o macchine compromesse. A volte anche macchine reali ospitate in paesi “amici”.
Reti gerarchiche (multiserver) o P2P.
Utilizzano protocolli standard (IRC, TOR) e connessioni crittografate.
Difficili da tracciare e da fermare, richiedono un’organizzazione complessa dietro (governi, criminalità organizzata ecc.).

## Tipi di attacco



Command & control
https://en.wikipedia.org/wiki/Command_and_control_(malware)

Termine di derivazione militare.

Rete di server che controllano macchine infette, zombie, botnet ecc.

Cercano di spostarsi velocemente (DNS) e utilizzano reti o macchine compromesse. A volte anche macchine reali ospitate in paesi “amici”.

Reti gerarchiche (multiserver) o P2P.

Utilizzano protocolli standard (IRC, TOR) e connessioni crittografate.

Difficili da tracciare e da fermare, richiedono un’organizzazione complessa dietro (governi, criminalità organizzata ecc.).

## Tipi di attacco

# Advanced Persistent Threat



Advanced Persistent Threat
https://en.wikipedia.org/wiki/Advanced_persistent_threat

Identifica tutti gli attacchi che non mirano ad un risultato immediato ma sono complessi (Advanced) e mirano ad installarsi permanentemente nella rete dell'obiettivo (persistent) facendo movimenti orizzontali. Solitamente esfiltrano dati per lungo tempo oppure rimangono nascosti fino al momento di "esplodere".

## Tipi di attacco

# Kill Chain militare

1. Reconnaissance
2. Weaponization
3. Delivery
4. Exploitation
5. Installation
6. Command and control
7. Action on objectives



1. Reconnaissance: ottenimento di informazioni sulla vittima
2. Weaponization: creazione del payload malevolo (exploit/documento/malware) che sarà usato per compromettere la rete del cliente
3. Delivery: invio del payload alla vittima. Nel caso di un’azienda la vittima può essere un particolare utente ritenuto vulnerabile.
4. Exploitation: esecuzione del payload malevolo sulla vittima
5. Installation: persistenza del malware o dell’attaccante all’interno della vittima.
6. Command and control: instaurazione della connettività con il centro di controllodel malware.
7. Action on objectives: esecuzioni di azioni per il raggiungimento dell’obiettivo, come esfiltrazione dati o propagazione orizzontale.

# Fasi dell'attacco

- Raccolta informazioni (Sniffing, Port Scanning oppure OSINT)
- Raccolta/costruzione armi
- Spedizione carico maligno o intrusione
- Sfruttare il carico maligno o l'intrusione
- Installare persistenza (APT)
- Command & control
- Azioni su obiettivo

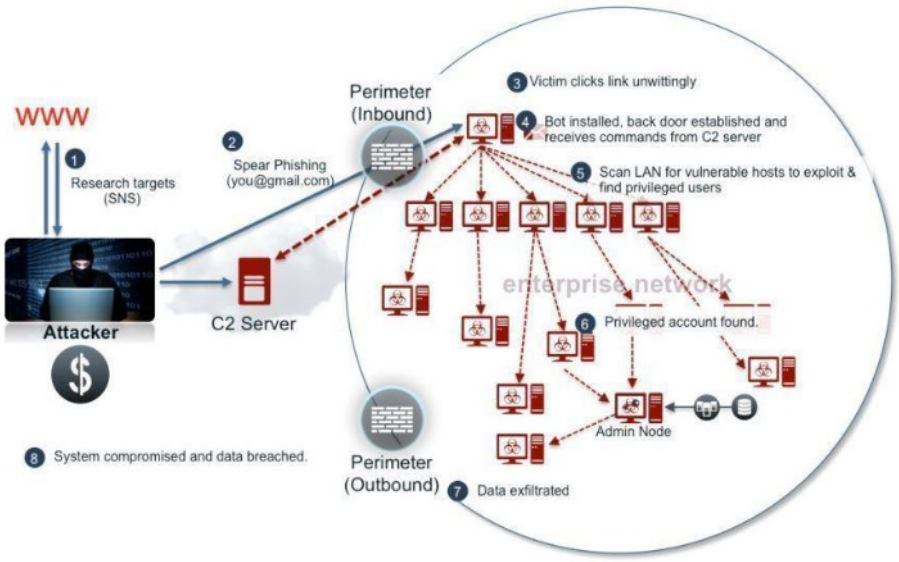
 

Preparare un attacco: prima fase raccolta di informazioni.

Sniffing (packet analyzing) https://en.wikipedia.org/wiki/Packet_analyzer raccolta di dati sul tipo e contenuto del traffico. Utile anche come strumento di Problem Determination. (Wireshark)

Port Scanning https://en.wikipedia.org/wiki/Port_scanner raccolta di informazioni su un host, servizi usati, livelli di software, vulnerabilità ecc. Molto utile ma espone al rischio di essere scoperti. (Nmap)

## Tipi di attacco






Scavalcare il perimetro e muoversi “orizzontalmente”.

La storia visuale dei più grandi data breach: https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

## Tipi di attacco

## Qualche consiglio per MITIGARE il rischio

- Antivirus
- Patch
- Plugin
- Browser+AD-blocker
- Backup
- Utenti non amministratori del PC
- Antivirus sulla posta
- Filtri di navigazione
- Bloccare cartelle sistema
- NO Windows Script Host



- Antivirus buono e sempre aggiornato
- Patch all'ultimo livello (soprattutto windows)
- Plugin aggiornati (Java, Adobe)
- Browser aggiornati con AD-blocker
- Backup protetti non in linea (e provare restore)
- Utenti non amministratori del PC
- Antivirus solidi sulla posta (Bloccare src,exe,com,vbs,js)
- Filtri aggiornati di navigazione
- Bloccare cartelle sistema con policy e permessi
- Disabilitare Windows Script Host
- Ecc.
- Ecc.