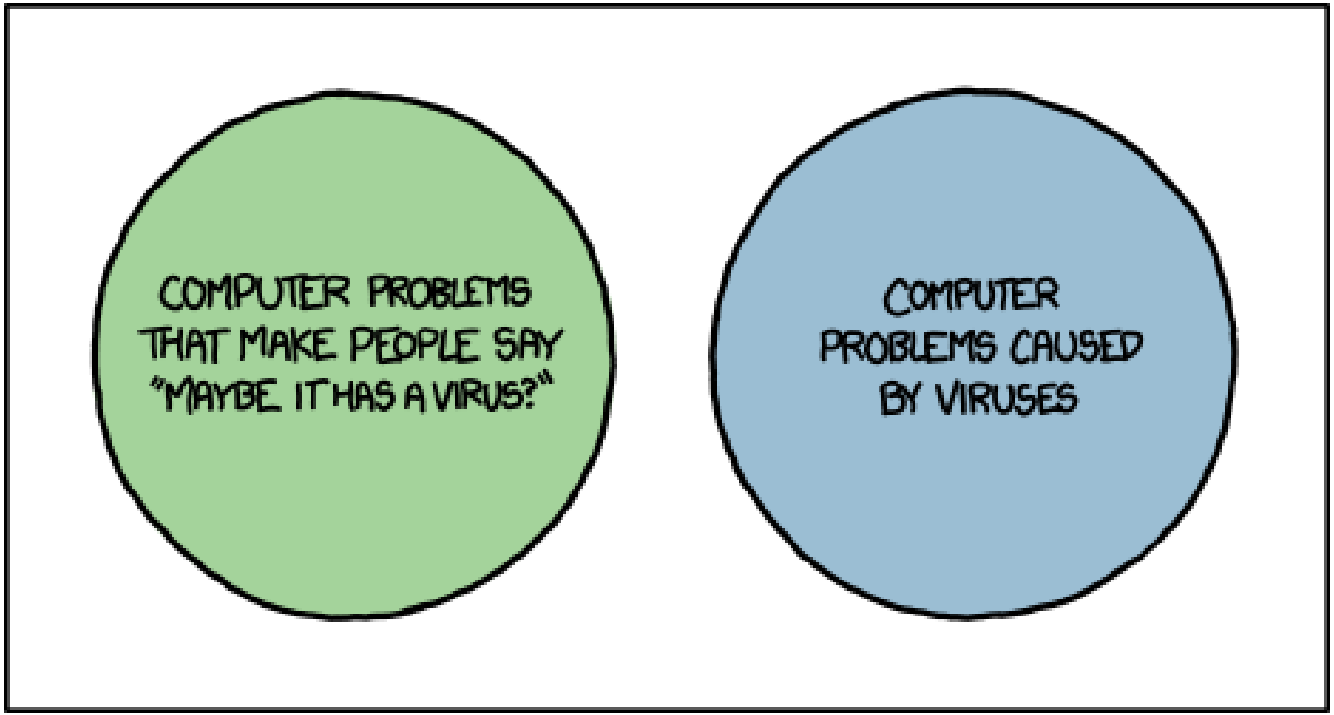
Malware

Cos’è un malware

- Letteralmente un “software malevolo”
  - Anche se “malevolo” è un concetto arbitrario
- Il malware viene catalogato in base alle sue caratteristiche e allo scopo per cui è programmato
- Molti malware appartengono a più categorie

Cos’è un malware



Malware

Alcuni Fatti

- **200,000** malware al giorno
- **80M** nuovi malware in un anno
- **700M+** malware in giro
- **Targeted**
- **Generati automaticamente**
- **Zero-day**

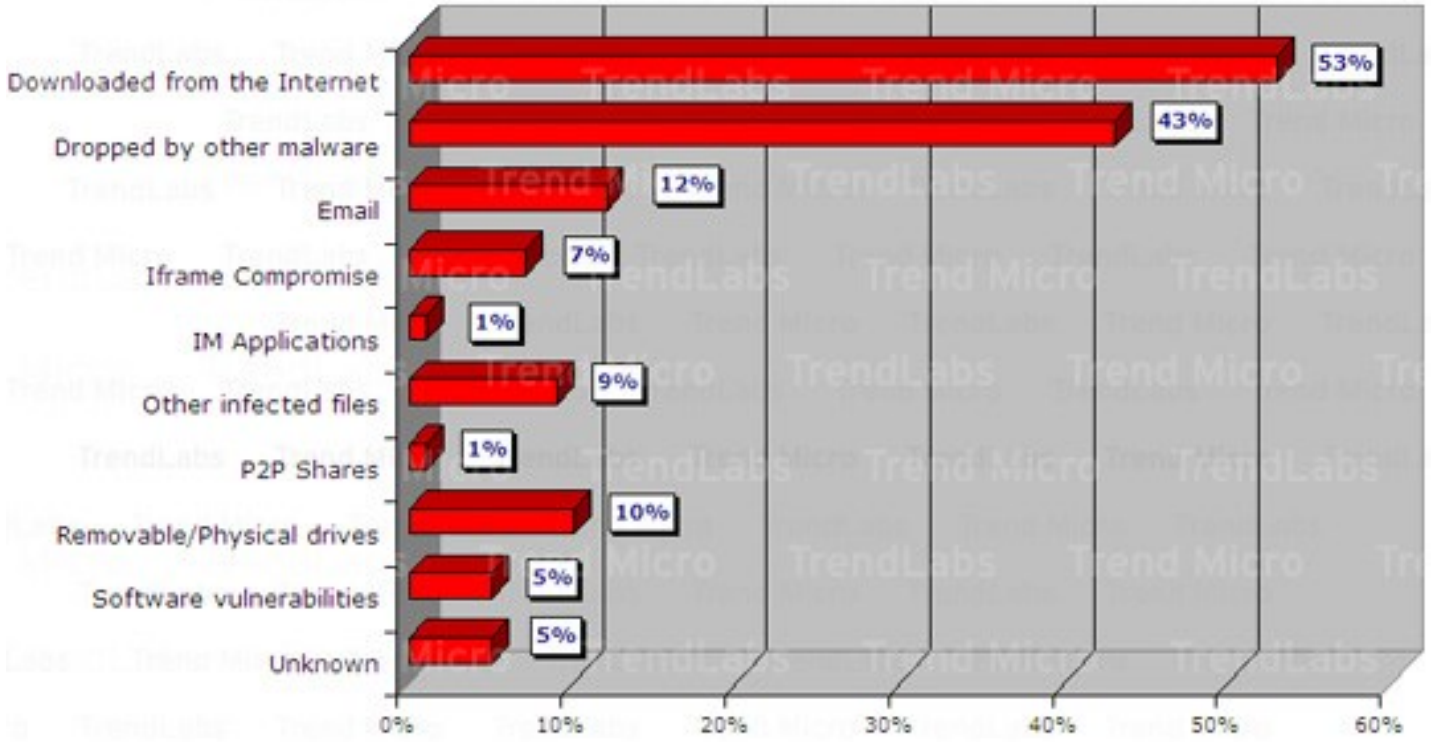
Pericolosità

- Creano problemi a una centrale nucleare (**Stuxnet**)
- Interrompono l'erogazione di energia elettrica (**BlackEnergy**)
- Si diffondono in 15 min. (**Warhol worm**)
- Controllano milioni di dispositivi per bloccare Internet (**Mirai**)
- Possono essere acquistato come servizio modulare (**GranCrab**)

Vettori di infezione

- Un vettore è il canale attraverso il quale viene trasmessa l'infezione di un malware
  - Applicazioni web
    - Es. via malvertisement o altre injection di codice malevolo
  - Macro di documenti
    - Excel, Word, Acrobat Reader, ...
  - Altri malware (trojan)
    - Allegati mail, software scaricati dalla rete, …
  - Direttamente caricati in memoria (Fileless)
  - Hardware

Vettori di infezione più comuni



IFrame = Internal Frame
IM = Instant Messaging

source: Trend Micro

Malvertisement

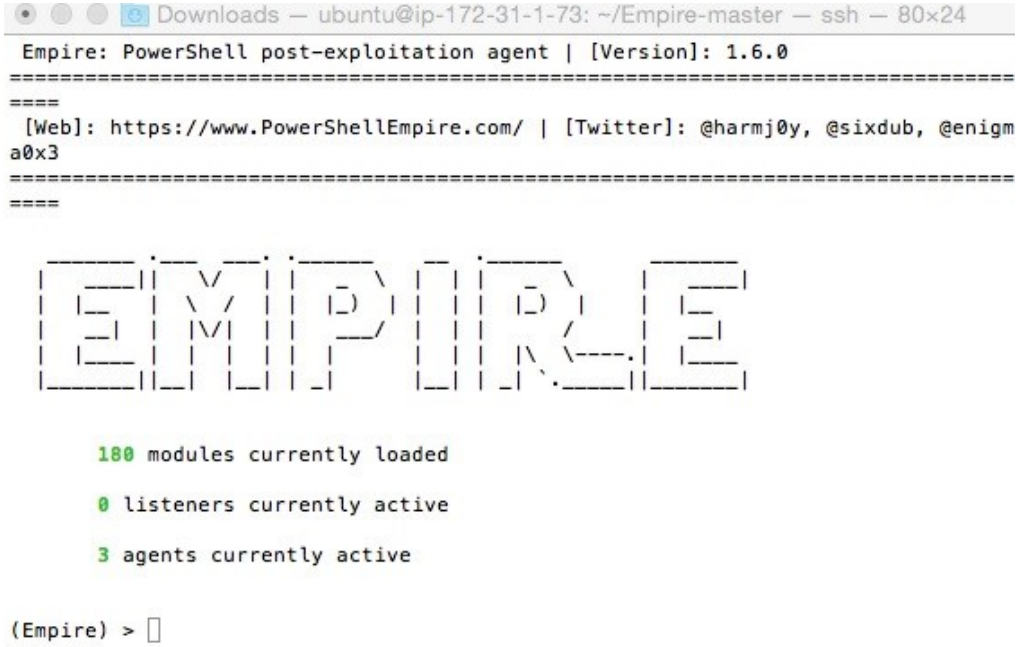
- Inserti pubblicitari (advertisement) che ridirigono l'utente verso servizi compromessi
  - Che, ad esempio, si occupano di distribuire il malware
- Appaiono all'interno di pagine note, in un contesto di cui l'utente si fida
  - Ad esempio, per la buona reputazione

Malvertisement

Macro

- Molti formati di documenti supportano linguaggi di scripting per operazioni complesse
  - Es. Documenti office
- Questi linguaggi permettono di definire delle procedure (macro) malevole
- La macro tipicamente si occupa di installare il malware vero e proprio (dropping)

PowerShell Empire



Trojan

- Un malware che viene distribuito e spacciato come un software legittimo
- Tipicamente installato direttamente dall'utente
  - Es. tramite un link o un allegato
- In alcuni casi si occupa solo della fase preparatoria dell'attacco
  - Configura il sistema ospite e installa altro malware

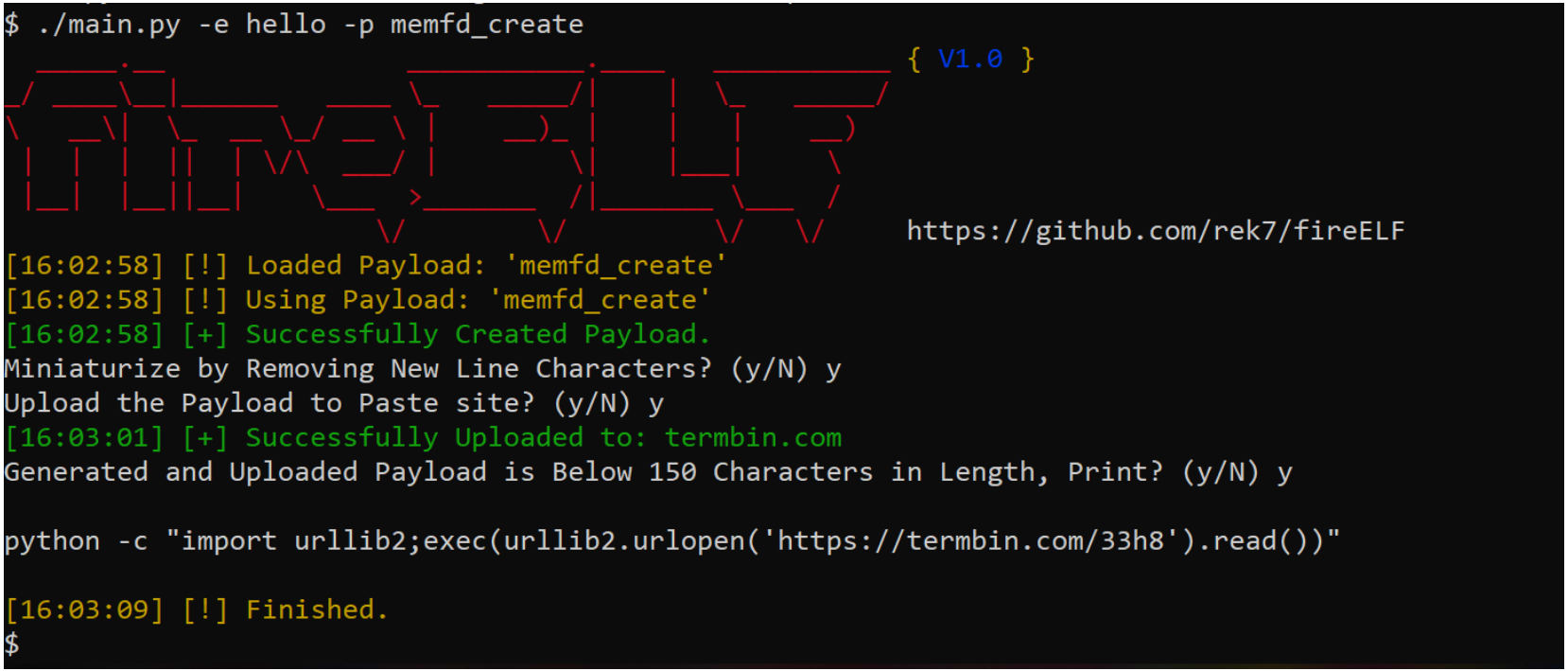
Fileless

- Un malware distribuito senza l'uso di un file vettore
  - Viene direttamente caricato ed eseguito in memoria (ad esempio tramite usb, o attacchi di social engineering)
  - Gli antivirus sono inermi se non hanno file da analizzare!
- Il malware viene caricato e lanciato direttamente dentro il terminale fornito con il Sistema Operativo:
  - Windows PowerShell
  - Linux e MacOS Terminal

FireELF: A fileless Linux malware

- Crea un file descriptor in memoria (`memfd`)
  - Non persistente, cancellato quando si riavvia il sistema
- Carica su `memfd` codice usando una clipboard online
  - `Termbin.com`
- Esegue memfd con una chiamata di sistema
  - `fexecve`

FireELF: A fileless Linux malware



Hardware

- In alcuni casi si può entrare in possesso di un hardware compromesso
  - Che esegue o contiene malware
- Un dispositivo USB può infettare i PC a cui viene collegato
  - Rubber ducky: dispositivo USB che si spaccia per una tastiera e digita comandi (e.g., per attacchi fileless)
- Uno smartphone può avere malware preinstallato

Alcune tipologie di malware

- I malware possono essere di vario tipo, spesso classificati in base a funzioni e obiettivi
- Adware
- Ransomware
- Spyware
- Command & Control
- ...

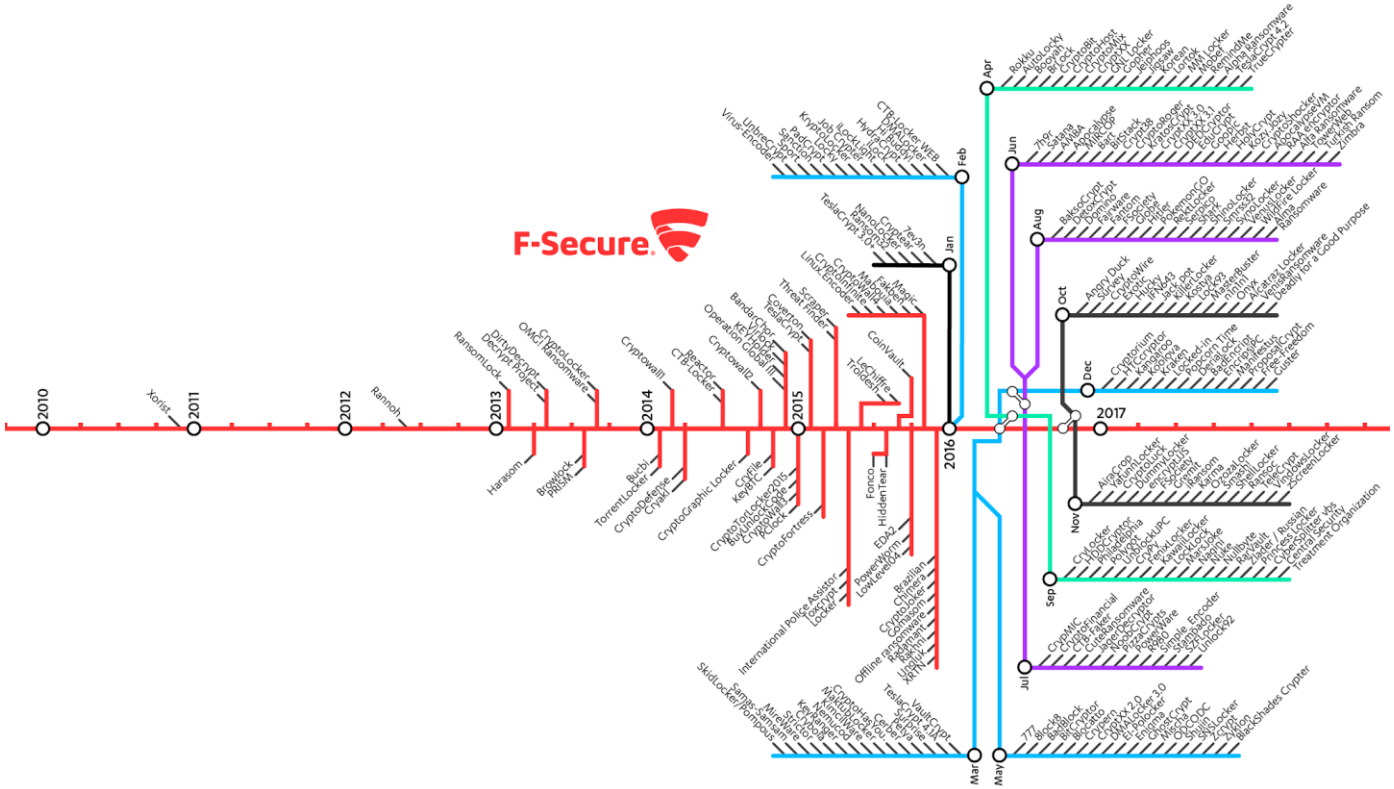
Adware

- Ha lo scopo di mostrare pubblicità all'utente
- Comunemente distribuito sotto forma di plugin del browser (es. toolbar) o come applicazione mobile
- Spesso generati modificando un'app esistente
  - repackaging

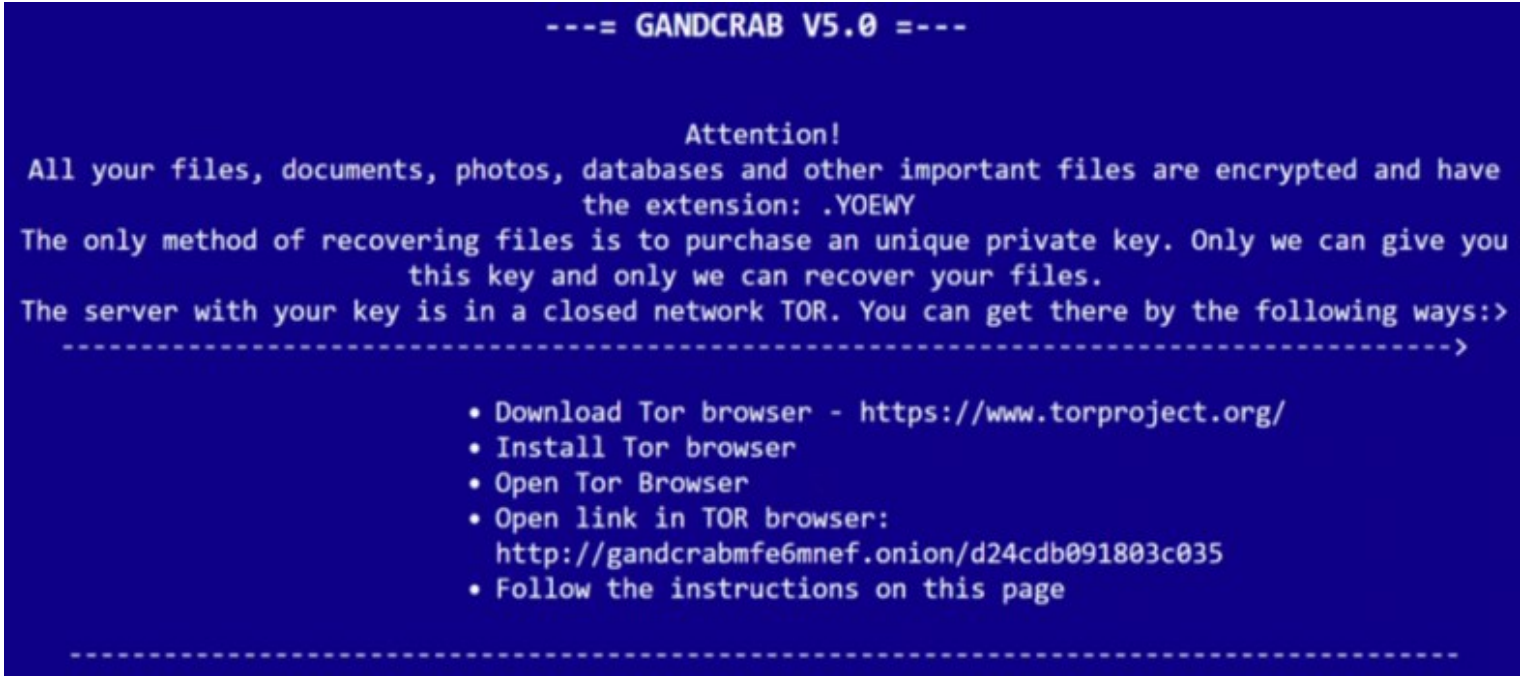
Ransomware

- Malware che ha lo scopo di estorcere un riscatto
- prendendo in ostaggio il filesystem
  - CryptoLocker, Wannacry
- minacciando di rivelare informazioni personali
  - GrandCrab
- minacciando di effettuare azioni irreversibili
  - Jigsaw

Ransomware: un mercato in crescita



Ransomware

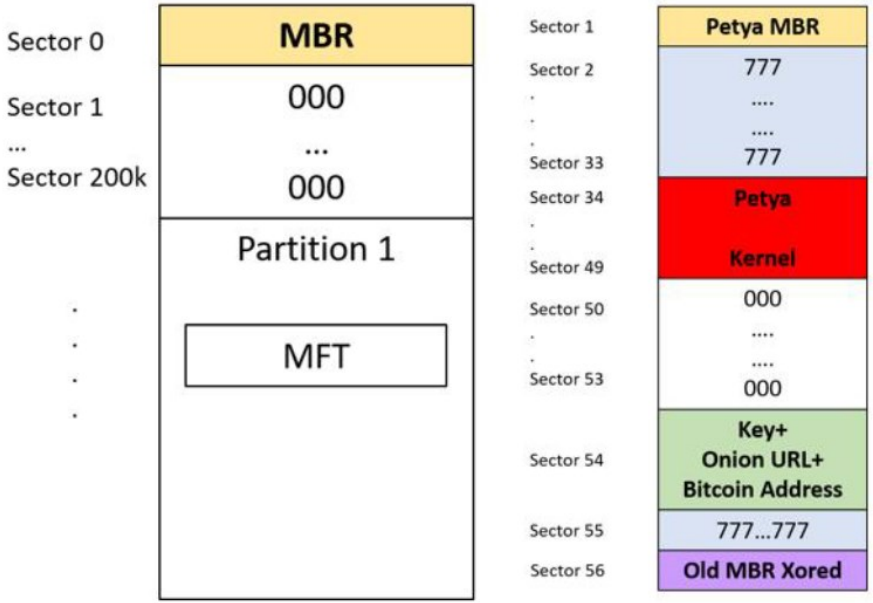

---= GANDCRAB V5.0 =---
Attention!
All your files, documents, photos, databases and other important files are encrypted and have the extension: .YOEWY
The only method of recovering files is to purchase an unique private key. Only we can give you this key and only we can recover your files.
The server with your key is in a closed network TOR. You can get there by the following ways:>
• Download Tor browser - https://www.torproject.org/
• Install Tor browser
• Open Tor Browser
• Open link in TOR browser:
http://gandcrabmfe6mnef.onion/d24cdb091803c035
• Follow the instructions on this page

Petya: un esempio

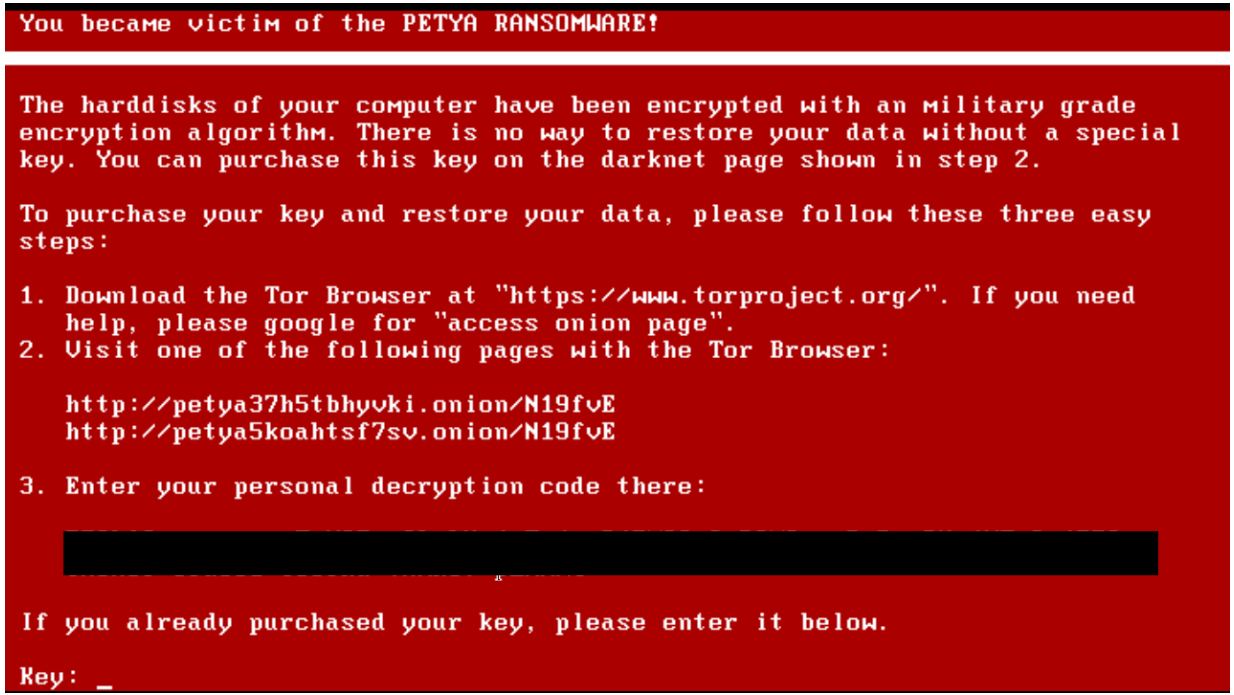
- Cripta la Master File Table (MFT) del filesystem impedendo l'avvio di Windows
- Il vecchio Master Boot Record (MBR)

1) viene messo in XOR con 0x37
2) viene spostato nel settore 56
3) viene sostituito con quello di Petya

- Viene generato *"NtRaiseHardError()"*
  - crash di sistema → reboot → Petya MBR



Petya: un esempio



RANSOMWARE

'Petya' ransomware attack strikes companies across Europe and US

Ukraine government, banks and electricity grid hit hardest, but companies in France, Denmark and Pittsburgh, Pennsylvania also attacked

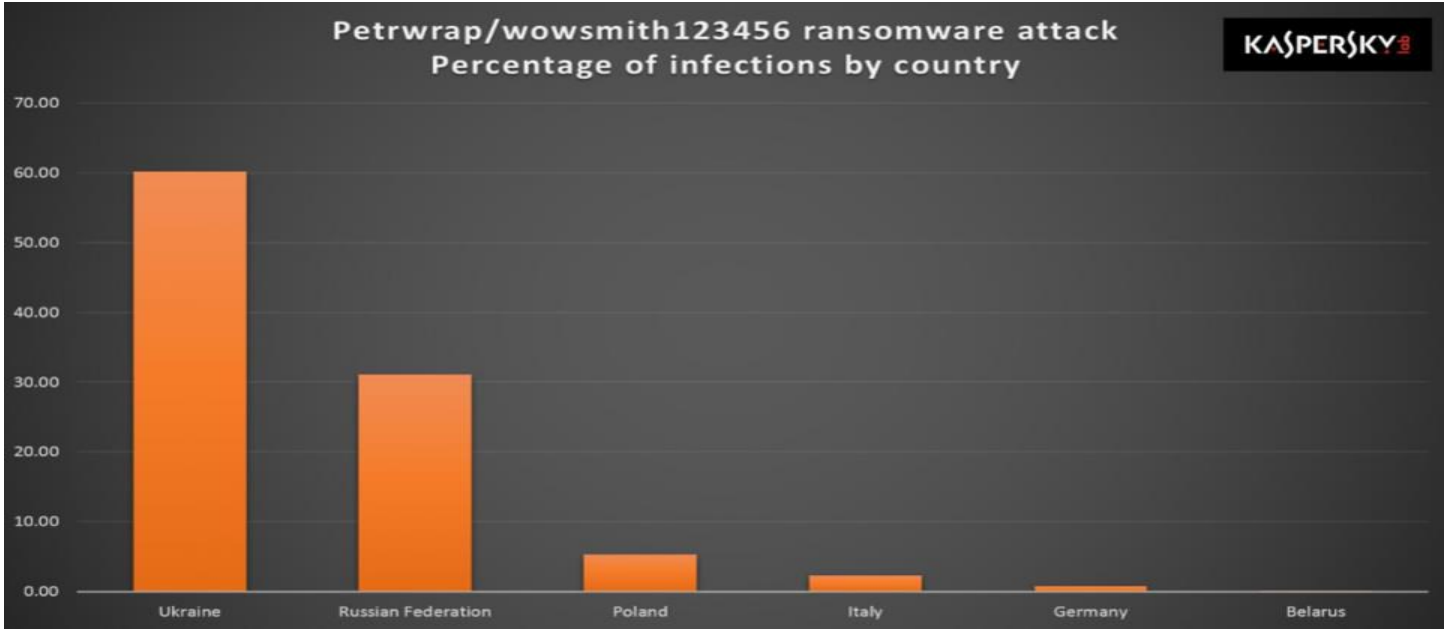
Not Petya: The evolution

- Utilizza l’exploit Eternalblue, trafugata all’NSA che le aveva utilizzate per 5 anni
- Sfrutta una vulnerabilità di SAMBA v.1, un software per condivisione file e stampanti usato da più di 900.000 sistemi Windows
- Cifra alcuni file utente prima del riavvio della macchina
- Programma un riavvio legale invece di forzarlo
- Dopo il riavvio presenta un'interfaccia utente diversa.

Popolarità dei Ransomware

- CryptoLocker, apparso a fine 2013, ha raccolto circa 3 milioni di dollari prima di essere disattivato.
- WannaCry, apparso a maggio 2017, ha infettato 230,000 computer in 150 paesi.
- Gli autori di ransomware hanno raccolto 209 milioni di $ nei primi 3 mesi del 2016 attraverso estorsioni ad aziende e istituzioni.

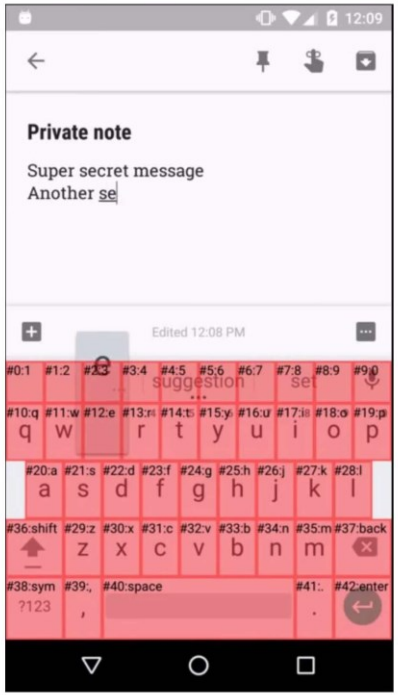
[CNN - April 15, 2016]


Petrwrap/wowsmith123456 ransomware attack
Percentage of infections by country
KASPERSKY lab
70.00
60.00
50.00
40.00
30.00
20.00
10.00
0.00
Ukraine
Russian Federation
Poland
Italy
Germany
Belarus

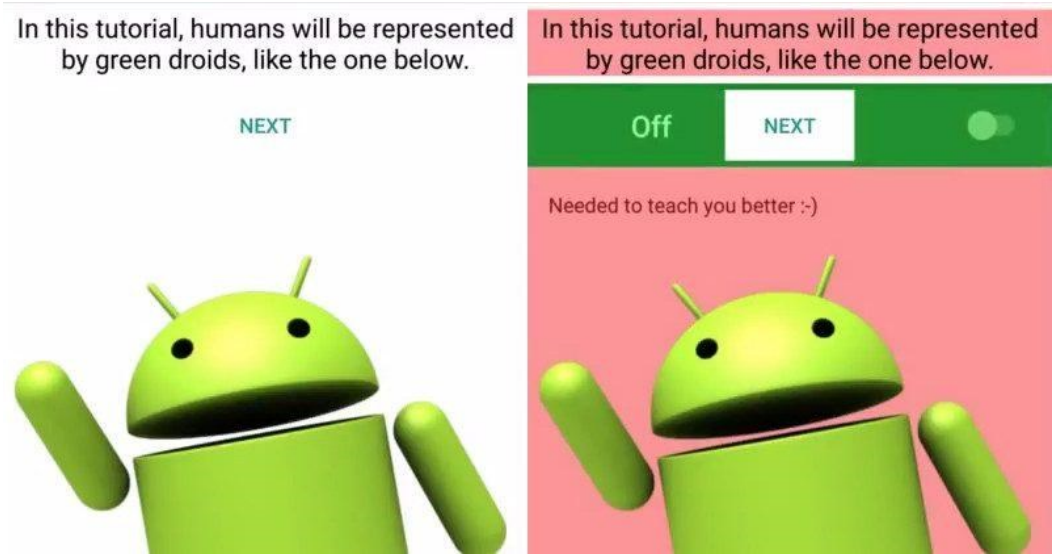
Spyware

- Malware che ha lo scopo di raccogliere informazioni sensibili dal dispositivo infettato
  - intercettando gli input dell'utente (Keylogger: software che rileva e memorizza la sequenza dei tasti digitata per poi eventualmente trasmetterli in remoto).
  - analizzando traffico dati e altre comunicazioni (Exodus: nascosto in applicazioni che l'utente viene indotto a scaricare; una volta installato, registra e trasmette conversazioni telefoniche)

Keylogger: Cloak & Dagger



Le parti in rosa non sono visibili all'utente, sfruttando la possibilità di configurare il livello di trasparenza



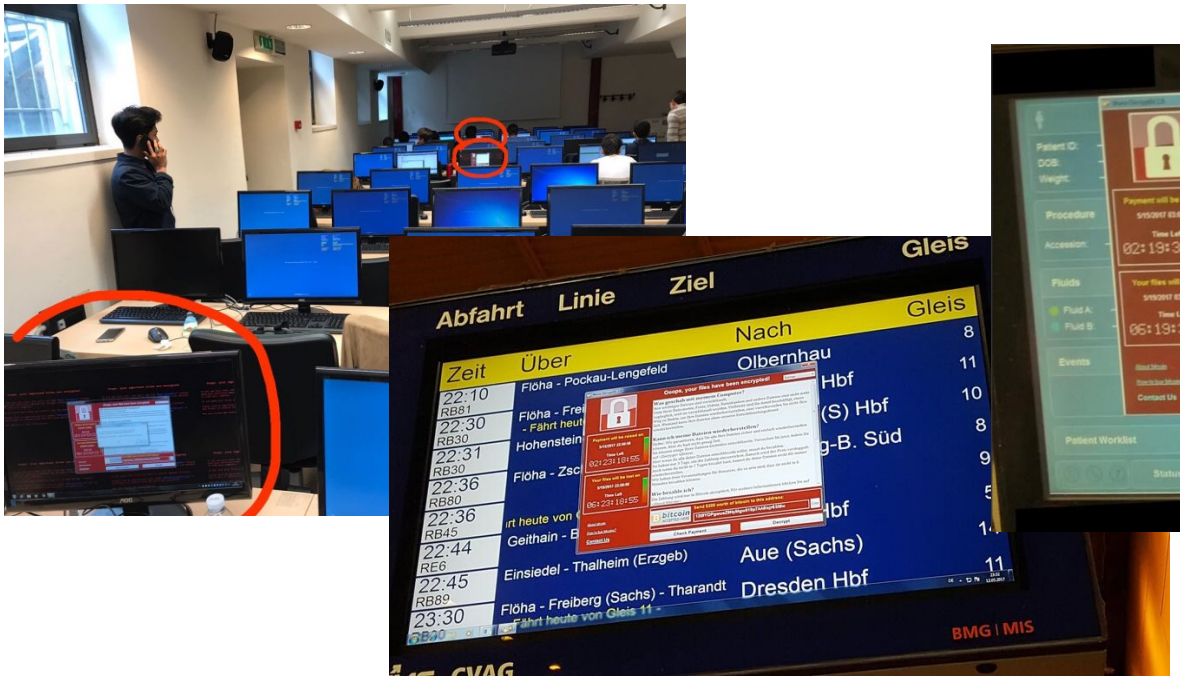
Command & Control

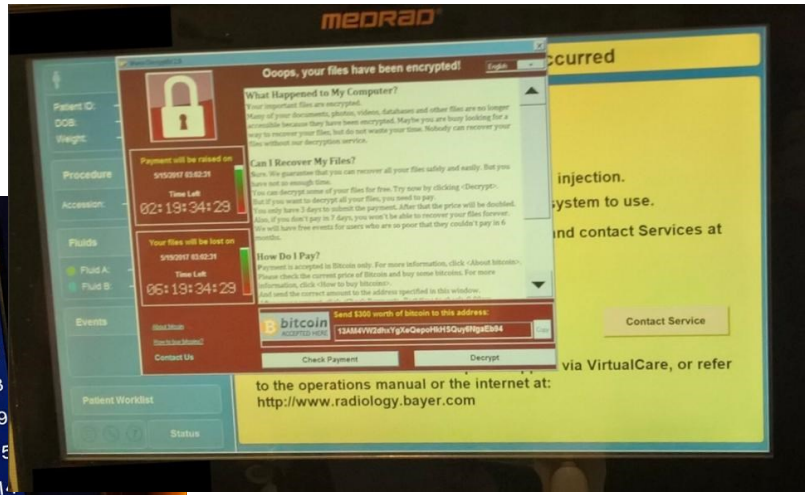
- Malware che espone la macchina infetta al controllo diretto dell'attaccante facendolo diventare un C&C client
- I C&C client ricevono i comandi da C&C server, ovvero computer controllao da un attaccante che viene utilizzato per inviare comandi a sistemi compromessi da malware per
  - Ricevere dati sottratti alle macchine controllate o ad altri per loro tramite
  - Orchestrare una botnet e portare avanti altri attacchi

Dissezione di un malware

- Per capire meglio il funzionamento dei malware è utile vederne un esempio concreto
- L'operazione di decomporre e analizzare un malware si chiama dissezione

Wannacry: A ransomware





Wannacry: Storia

- Outbreak: maggio 2017
  - Fermato in 3 giorni grazie alla scoperta di una kill switch e a una patch d'emergenza di Microsoft
- Ha infettato circa 200.000 macchine in 150 stati
- Danni stimati nell'ordine di 0.1 ~ 1 miliardi di dollari
- Wannacry include anche una componente di C&C
- Usata per stabilire una comunicazione tramite rete TOR con la vittima e fornire istruzioni sul pagamento

Wannacry

- Utilizza 2 vulnerabilità (EternalBlue, DoublePulsar) dei sistemi Windows, trafugate all'NSA nell'Aprile 2017 che le aveva utilizzate per 5 anni
- EternalBlue: permette di effettuare command injection su SAMBA v.1, un software per condivisione file e stampanti a tutt'oggi usato da più di 900.000 sistemi
- DoublePulsar: permette di caricare una libreria (DLL) nel driver SAMBA e mette gli attaccanti in grado di operare in kernel mode e prendere il completo controllo dei sistemi

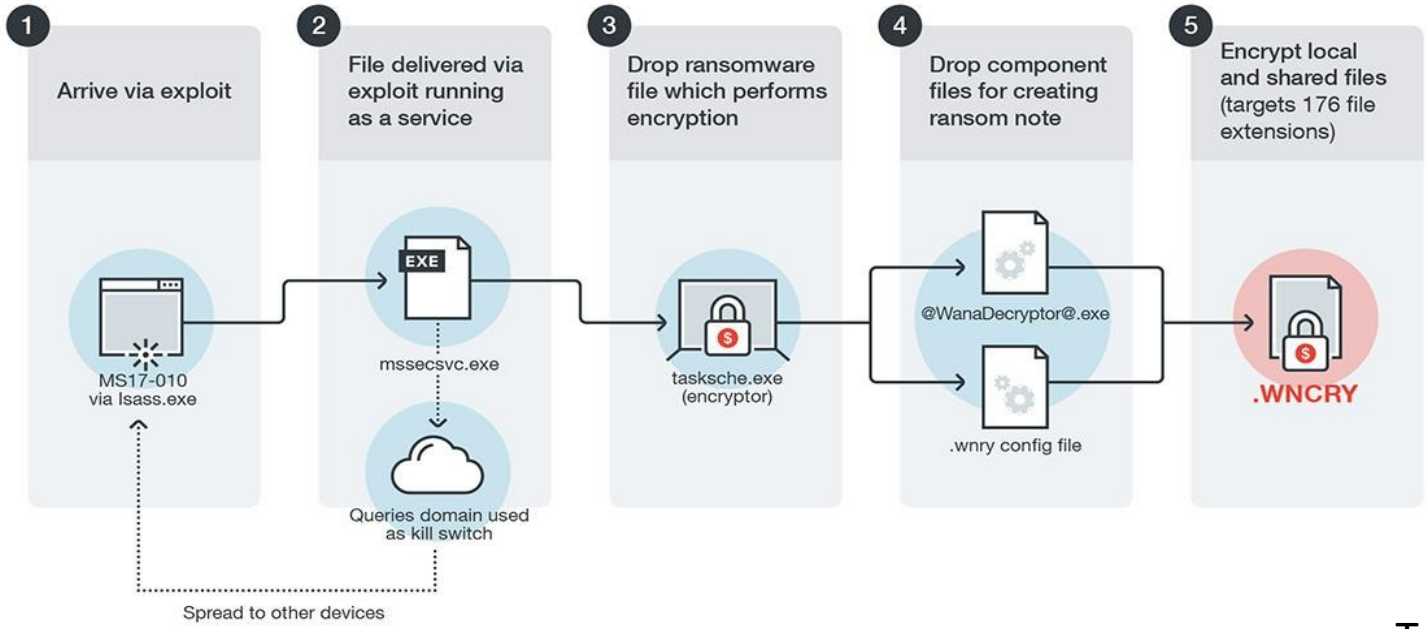
Wannacry

- Carica launcher.dll che si occupa di caricare il primo eseguibile
  - mssecsvc.exe
- L'eseguibile verifica la kill switch (usata per fermare la diffusione incontrollata) cercando di connettersi ad un URL
  - www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
- Infine esegue dropper e infection
  - infection = scan su porta 445 (SAMBA) + deployment

Wannacry: Dropper

- All’inizio dell’esecuzione mssecsvc.exe estrae e lancia il ransomware vero e proprio:
  - tasksche.exe
- Il ransomware estrae da un archivio una serie di file
  - utility e chiave di cifratura
  - istruzioni e dimostrazione (Fino a 10 file possono essere recuperati gratuitamente)

Approfondimento: Workflow



source: Trend Micro

Riferimenti

- http://icact.org/upload/2018/0708/20180708_finalpaper.pdf
- https://securitywithoutborders.org/blog/2019/03/29/exodus.html
- https://github.com/rek7/fireELF

Approfondimento: Malware detection

- Uno dei metodi più diffusi per contrastare la diffusione dei malware è la malware detection. Questo è l'approccio usato tipicamente dagli antivirus, programmi che analizzano il file system della macchina su cui sono in esecuzione alla ricerca di file contenenti malware.
- Tipicamente il riconoscimento avviene tramite confronto delle signature: a ogni malware noto viene associata una firma digitale univoca. L'antivirus calcola la firma per ogni file presente sul sistema e se individua una corrispondenza attiva una procedura di sanitizzazione (dove possibile).
- Questo metodo è molto utilizzato, ma ha serie limitazioni. Prima di tutto richiede che le liste dei malware noti siano sempre aggiornate. Anche quando questo avviene, però, i nuovi malware (0-days attacks) non possono, per definizione, essere riconosciuti fino a quando la loro firma non viene aggiunta alle liste.
- Un'altra seria limitazione deriva dalle tecniche di camuffamento che permettono di modificare la struttura di un malware in modo che la sua firma digitale non corrisponda più a quelle presenti nelle liste.
- Infine, dato che gli antivirus analizzano i file presenti sulla macchina, non possono identificare i malware fileless