

BACKDOOR

Chiara Bergagnini
Riccardo Fontanini
Jennifer Pedron
Marco Tognasca

INDICE



- Definizione
- Classificazioni
  - Volontaria - involontaria
  - Simmetrica – asimmetrica
  - Software – hardware
- Metodi di diffusione
- Conseguenze dell'attacco
- Rilevare, prevenire e difendersi
- Attacco hardware

DEFINIZIONE

- Letteralmente «porta sul retro», «porta di servizio»
- E' un metodo per bypassare la normale autenticazione in un prodotto, un sistema informatico, un crittosistema o un algoritmo
- Permette di accedere in remoto a un computer evitando le consuete procedure di identificazione





CLASSIFICAZIONI

VOLONTARIA - INVOLONTARIA



BACKDOOR AMMINISTRATIVA

- Creata dal gestore di un sistema informatico con le migliori intenzioni
- Permette di accedere al sistema da remoto in modo semplice e veloce
- Generalmente non viene documentata
- Inserita in fase di sviluppo del codice per testare il programma
- Protetta da credenziali facilmente alterabili



BACKDOOR «MALIGNA»

- Backdoor amministrativa scoperta da un hacker e sfruttata come vulnerabilità
- Backdoor appositamente generata da un hacker attraverso malware che vengono installati sul computer delle vittime con l'inganno (phishing, trojan horse, ecc.)

SIMMETRICA - ASIMMETRICA, SOFTWARE - HARDWARE

Backdoor simmetrica: tutti coloro che la trovano possono sfruttarla a loro volta liberamente

Backdoor asimmetrica: può essere utilizzata solo da un attaccante che conosce già l'esistenza di tale vulnerabilità

Backdoor software: inserita segretamente all'interno del software di un ignaro programma di sistema

Backdoor hardware: insita in un componente hardware malevolo

BACKDOOR SOFTWARE - METODI DI INSERIMENTO

- **Aggiungere del codice sorgente**: tipicamente il metodo più diffuso, ma efficace solamente fino a quando il codice sorgente non viene letto e la parte addizionale viene scoperta → repository di GitHub
- **Iniettare codice malevolo in un'applicazione**: l'applicazione infetta continua a funzionare come previsto, ma intanto il codice iniettato viene eseguito in background; normalmente rilevato dagli antivirus → importante controllare la hash signature dell'applicazione
- **Iniettare codice malevolo in un compilatore**: è il compilatore stesso che aggiunge il codice ad ogni programma che lo utilizza; viene eseguita in modo che l'applicazione sembri essere stata compilata correttamente
- **Iniettare codice in un software in esecuzione**: tipicamente coinvolge un XSS, cross-site scripting ; il codice iniettato in esecuzione si propaga così attraverso il sistema, solitamente allo scopo di aprire una connessione di rete.

ALTRI METODI PER GENERARE UNA BACKDOOR

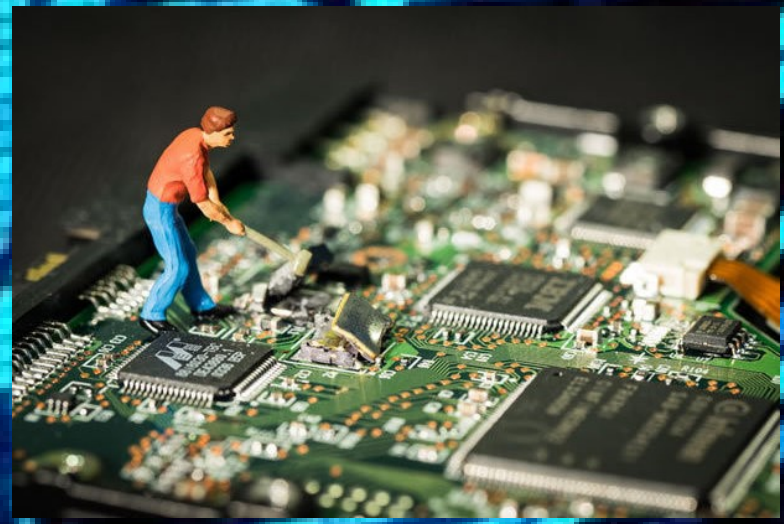
- **Escrow** («depositare in garanzia»): conservare la copia della chiave di crittografia



- **Definire uno standard vulnerabile**: definire standard e impostare parametri con la consapevolezza di possedere i metodi per farli crollare

BACKDOOR HARDWARE

- Codice o microcodice dannoso inserito all'interno di componenti fisici non modificabili (quali alimentatori, elementi circuitali fissi, unità di memoria, ecc.)
- Risulta piuttosto rara e richiede un insieme molto preciso di circostanze per implementarla
- Può coinvolgere la memoria non volatile nei chip (come, per esempio, il BIOS di un PC) o il codice contenuto nel firmware (di un router o di un altro dispositivo di rete) oppure può essere implementata direttamente come trojan hardware nel circuito integrato
- Può essere iniettata al momento della produzione, ossia nel momento in cui l'utente non ha alcun livello di controllo
- In genere ha accesso completo al dispositivo su cui gira
- Si trova ad un livello così basso nell'hardware da essere difficilmente rilevabile
- Non può essere rimossa tramite i metodi convenzionali (software antivirus)

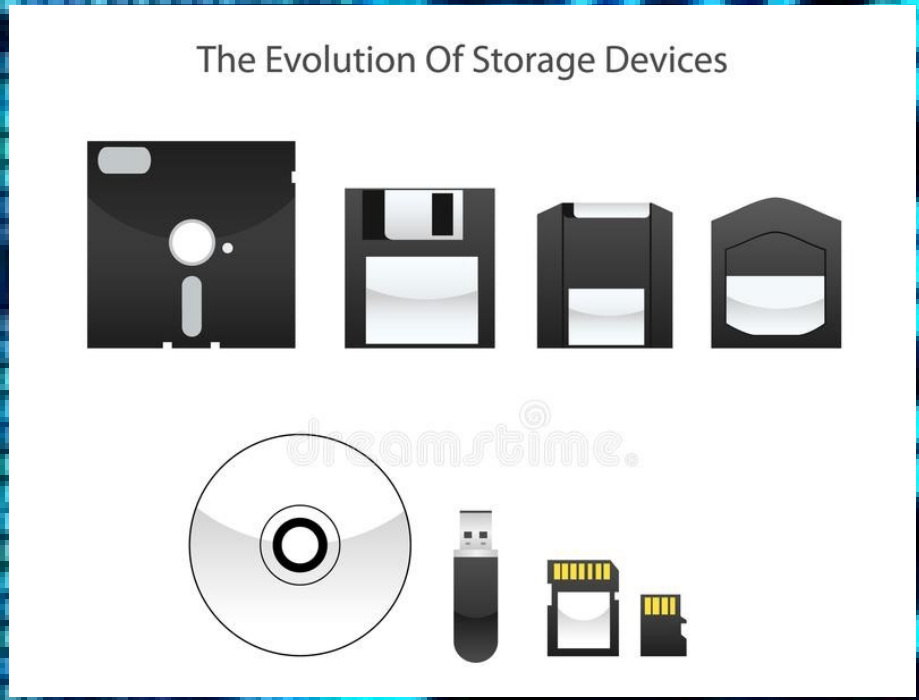




METODI DI DIFFUSIONE

PERIFERICHE RIMOVIBILI

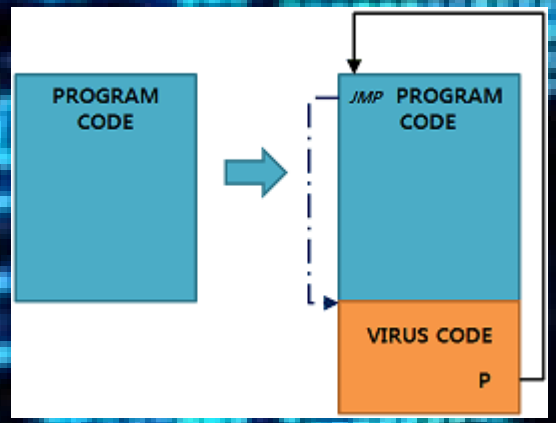
- Floppy
- CD e DVD
- Chiavi USB
- Schede di memoria (Flash, XD, SD etc.)

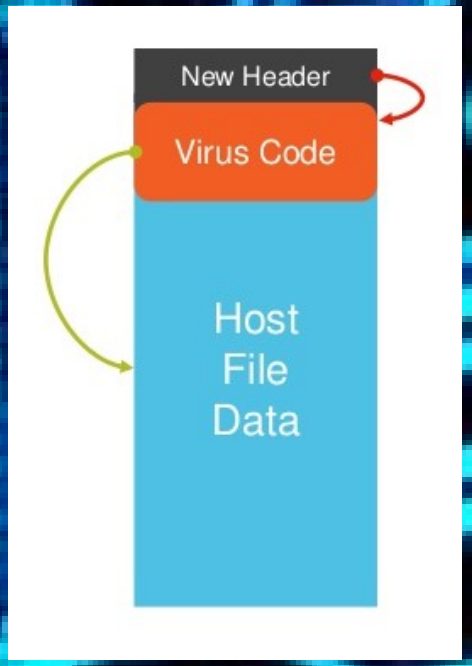


VIRUS CHE INFETTANO ESEGUIBILI, DOCUMENTI E SCRIPT

Virus di tipo

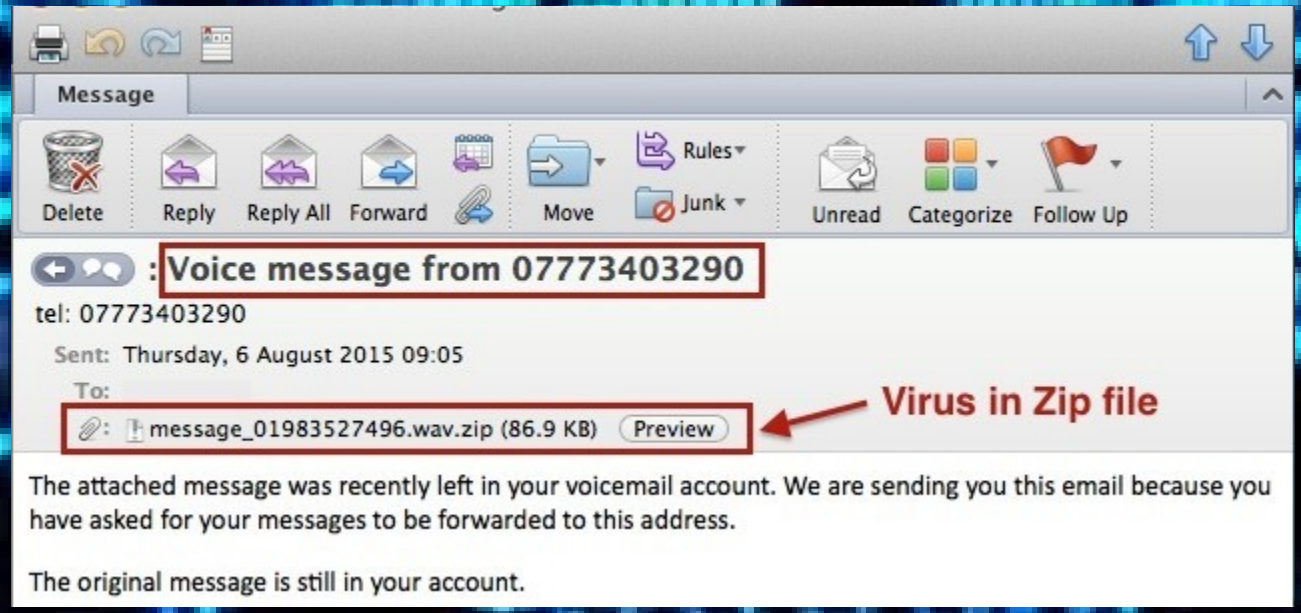
- Appending
- Prepending
- Overwriting
- Macro
- Scripting
- Sourcecode
- etc.



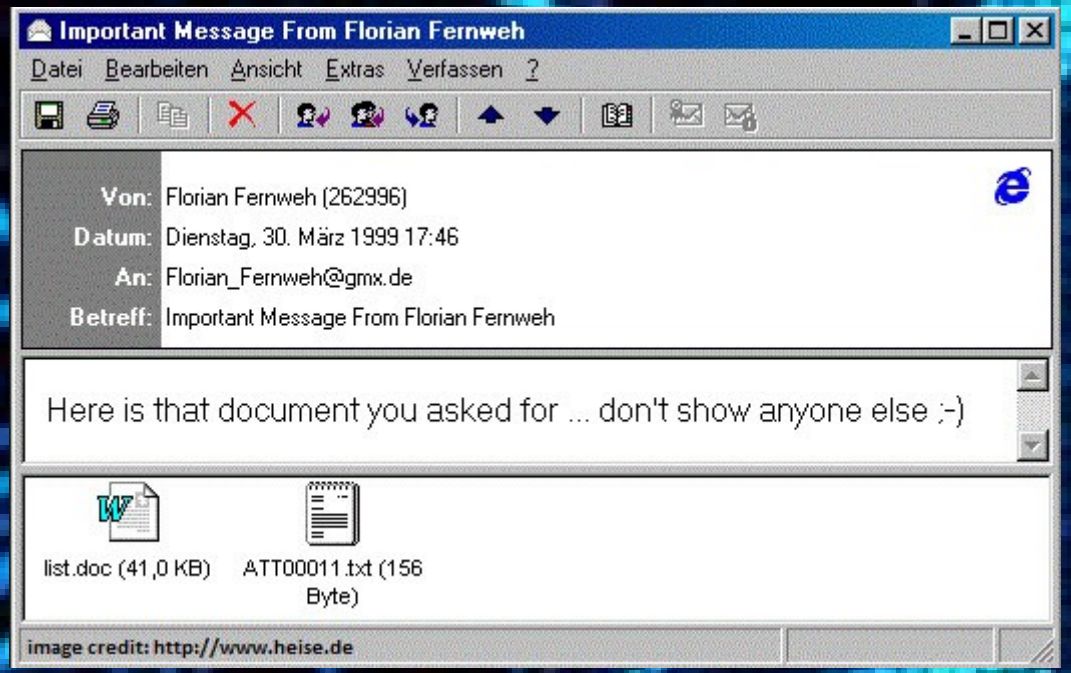


E-MAIL

- Plain-text: tramite gli allegati
- Mail in HTML le cose non sono migliorate
- Le epidemie più pericolose sono state causate da malware che si diffondevano tramite e-mail con un loro motore di posta



DOWNLOAD: MELISSA I_ESEMPIO DI DIFFUSIONE VIA MAIL



- Virus di massa del 1999
- Sfruttò la social engineering: sul «newsgroup alt sex» fu postato un documento word (List.DOC) contenente una lista di 80 siti porno con relativi username e password per accedervi
- Si diffondeva via email utilizzando Outlook spedendosi ai primi 50 indirizzi di posta
- Fatale per molti mail-server: attacco DoS (Denial of Service)
- Nelle versioni successive fu reso più nocivo facendo cancellare al virus file critici per il sistema (Windows).

DIRECTORY CONDIVISE

- I virus possono ricercare sul sistema infetto (se è un server ancor meglio) le directory condivise e infettare i file li presenti o replicarsi al loro interno
- Altri virus possono invece ricercare le directory di default dei programmi peer-to-peer (Kazaa, Gnutella, E-donkey, Fasttrack) e replicarsi con nomi appetibili (crack, liste di password etc).



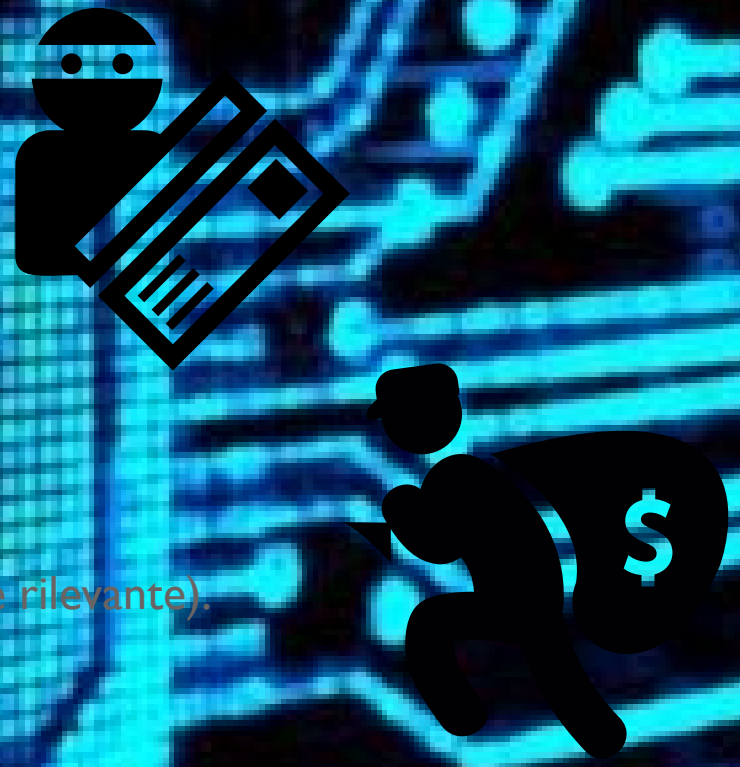




CONSEGUENZE DELL'ATTACCO

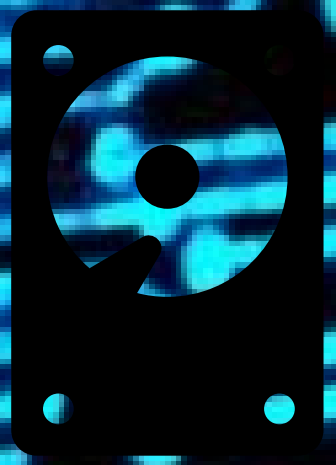
POSSIBILI CONSEGUENZE DI UN "COMPUTER COMPROMESSO"

1. Conseguenze sul tuo computer
   - Difficoltà operative
   - Controllo/furto/danneggiamento di email (incluse liste di indirizzi) e documenti
   - Controllo e possibilità di transazioni finanziarie illecite (a tuo nome)
   - Furto di identità (nuova frontiera negli USA)
2. Uso criminale del tuo computer per altri fini (potrebbe essere penalmente rilevante).



A SECONDA DEL TIPO DI DANNI CAUSATI, I VIRUS POSSONO ESSERE

- **Fastidiosi ma non dannosi**: se comportano solo una diminuzione dello spazio libero sul disco
- **Dannosi**: se provocano problemi alle normali operazioni del computer
- **Molto dannosi**: se causano danni difficilmente recuperabili come la cancellazione di informazioni fondamentali per il sistema





RILEVARE PREVENIRE E DIFENDERSI

COME ACCORGERSENE

Vedi sul monitor:

- Uno schermo blu, oppure figure strane o messaggi incomprensibili, ovvero messaggi di errore di sistema
- Ritardi inusuali nella fase di avvio del computer
- Computer che "va estremamente lento"
- Presenzi di (molti) file corrotti, inaccessibili o mancanti
- Impossibilità di accedere ai dati sul disco o al disco stesso (quindi a tutti i dati)
- Improvvisi (e frequenti) messaggi di memoria insufficiente
- Riavvio spontaneo del computer

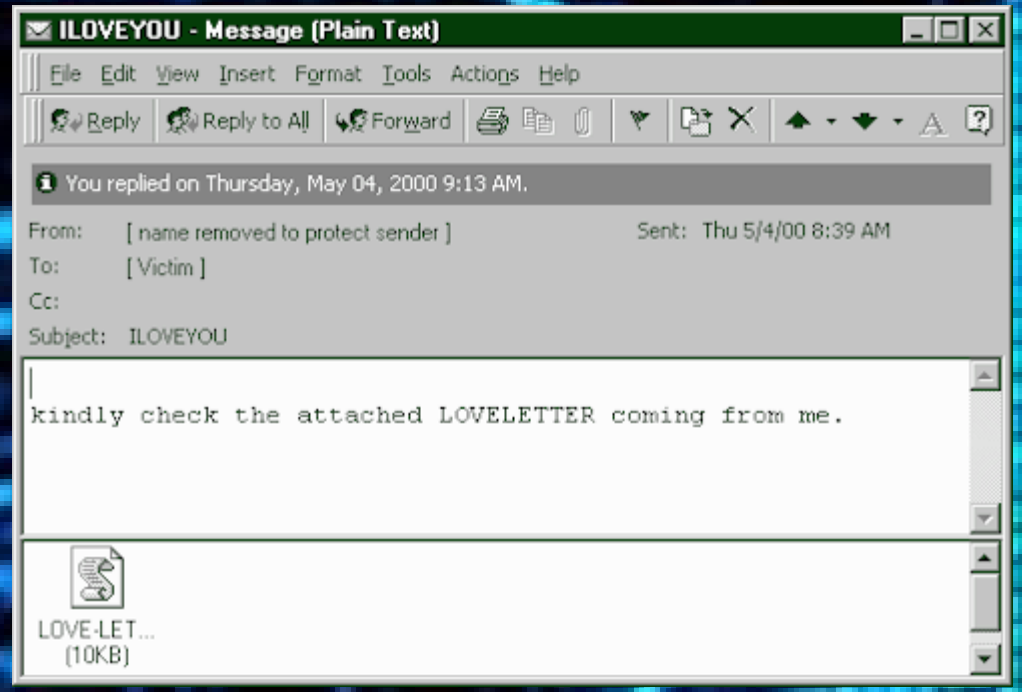
Ma potrebbe anche darsi che non sperimenti alcun sintomo e sei del tutto inconsapevole che il tuo computer è stato compromesso

PREVENIRE



- Antivirus
- Firewall
  - Worm Blaster: effettua l'attacco sulla porta 135, quella utilizzata dal protocollo RPC: se nel sistema è presente un firewall il worm non riuscirà a penetrare nel computer in quanto non riceverà alcuna risposta dalla porta.
- Massima attenzione

PREVENIRE



- Evitare di venire in qualche modo imbrogliati dalle doppie estensioni dei files
  - Loveletter:
    - «kindly check the attached LOVELETTER coming from me.»
    - Allegato: «LOVE-LETTER-FOR-YOU.TXT.vbs.»
  - Consiglio: settare il sistema operativo in modo che visualizzi le estensioni per i tipi di file conosciuti.
- WindowsUpdate

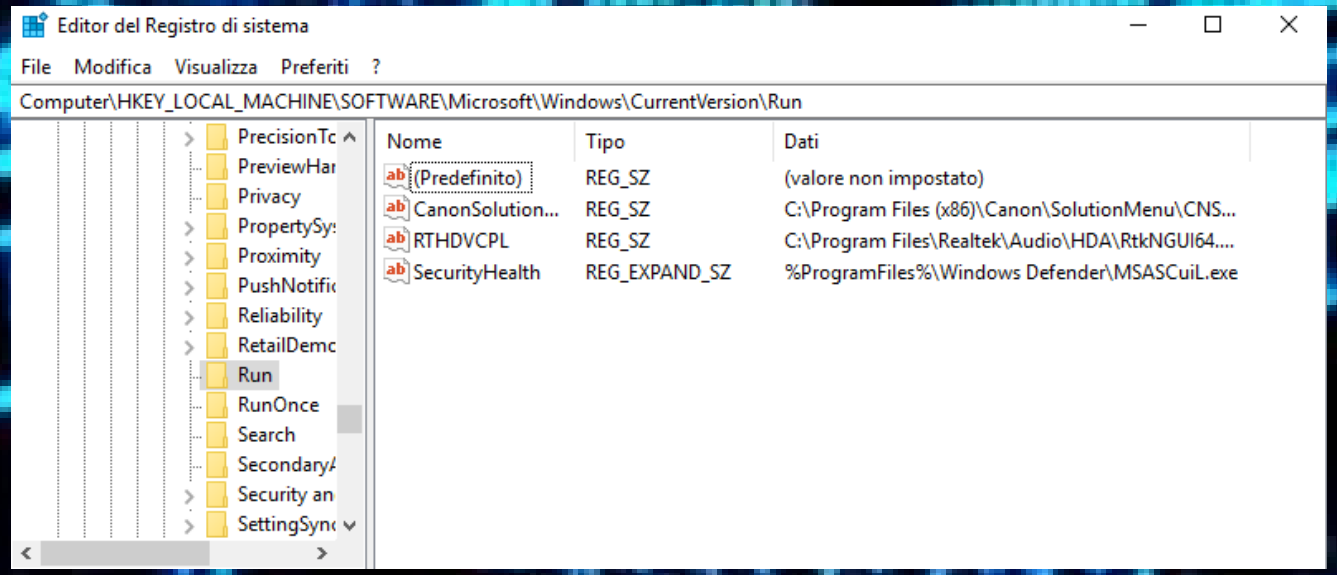
DIFENDERSI

Cosa fare invece quando si sospetta che nel proprio sistema si sia annidato un virus?

- Virus in senso stretto: è bene affidarsi all'antivirus
- Nel caso di altri malware, spesso, è possibile intervenire anche manualmente. Worms, trojans e backdoors non hanno bisogno di un "ospite" ma sono files a sé stanti. Per essere sempre attivi essi devono necessariamente eseguirsi ogni volta che il sistema operativo viene avviato.

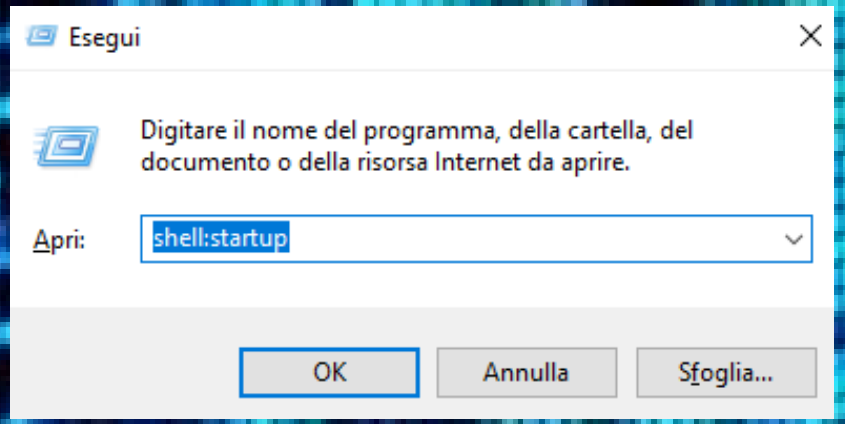
DIFENDERSI - CHIAVI DEL REGISTRO DI SISTEMA

- [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices]
  [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce]
  [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]
  [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce]
  [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]
  [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce]
  [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServices]
- sul pannello di destra verranno visualizzate le applicazioni che vengono eseguite all'avvio del sistema operativo.



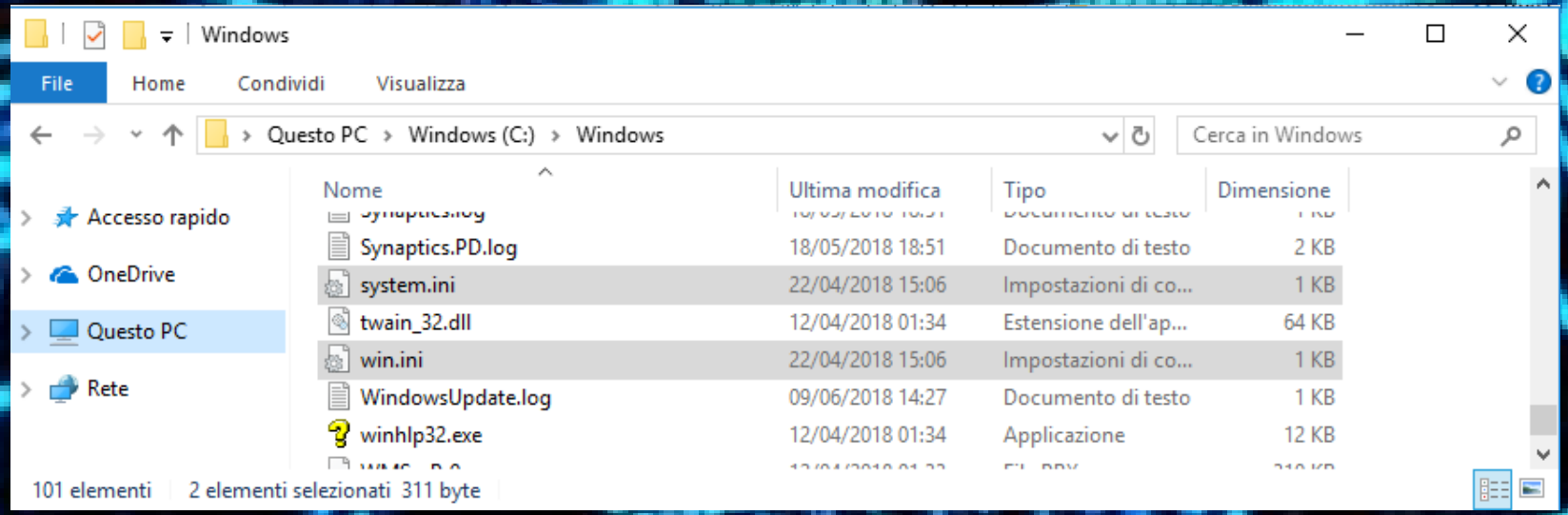
DIFENDERSI - CARTELLA ESECUZIONE AUTOMATICA

- I link (collegamenti) presenti all'interno della cartella Avvio/Start, Programmi, Esecuzione automatica (e quindi i programmi ad essi associati) vengono eseguiti ad ogni avvio del sistema operativo.



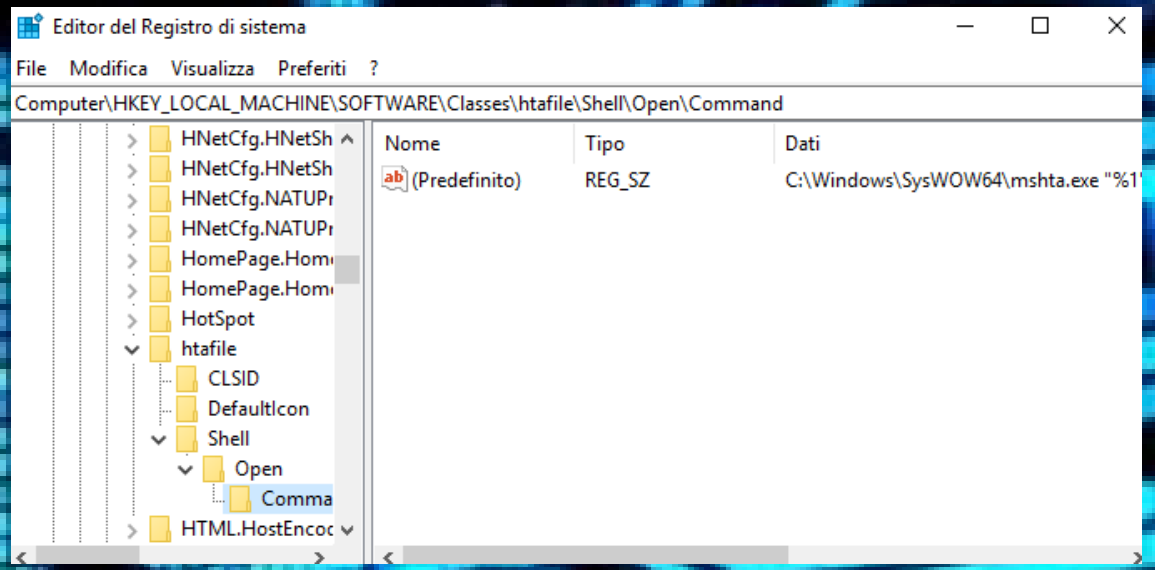
DIFENDERSI - FILES DI SISTEMA

- reperibili nella cartella c:\windows
- system.ini: va controllata la riga shell= contenuta all'interno della sezione [boot]
- win.ini: ad essere visionate devono essere le righe load= o run= eventualmente presenti nella sezione [windows]; in entrambi i casi i programmi specificati dopo le righe riportate vengono eseguiti ogni volta che si avvia il pc.
- Autoruns: http://www.sysinternals.com/files/autoruns.zip



DIFENDERSI - CHIAVI DI REGISTRO

- [HKEY_CLASSES_ROOT\exefile\shell\open\command]
  [HKEY_CLASSES_ROOT\comfile\shell\open\command]
  [HKEY_CLASSES_ROOT\batfile\shell\open\command]
  [HKEY_CLASSES_ROOT\htafile\Shell\Open\Command]
  [HKEY_CLASSES_ROOT\piffile\shell\open\command]
  [HKEY_LOCAL_MACHINE\Software\CLASSES\batfile\shell\open\command]
  [HKEY_LOCAL_MACHINE\Software\CLASSES\comfile\shell\open\command]
  [HKEY_LOCAL_MACHINE\Software\CLASSES\exefile\shell\open\command]
  [HKEY_LOCAL_MACHINE\Software\CLASSES\htafile\Shell\Open\Command]
  [HKEY_LOCAL_MACHINE\Software\CLASSES\piffile\shell\open\command]

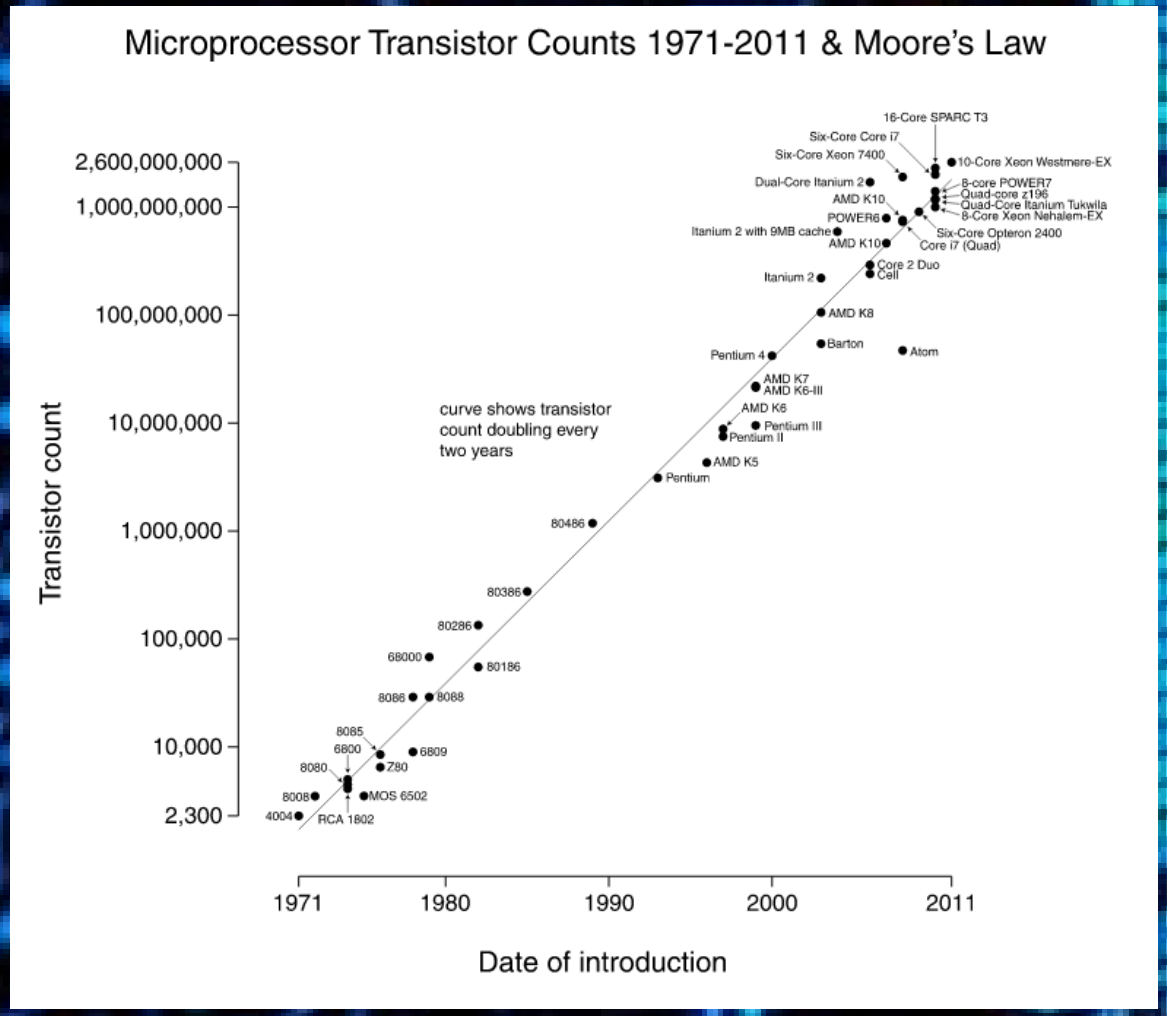


- il valore della stringa predefinita di queste chiavi dovrebbe sempre essere "%1" %*.
- Se una o più tra queste stringhe dovesse risultare modificata in qualcosa come "programma.exe %1" %*, significa che quel programma.exe verrebbe lanciato ogniqualvolta verrebbe eseguito un file con l'estensione relativa alla chiave in cui la stringa è stata modificata



ATTACCO HARDWARE

LEGGE DI MOORE



- Aumento della densità di transistori per unità di superficie

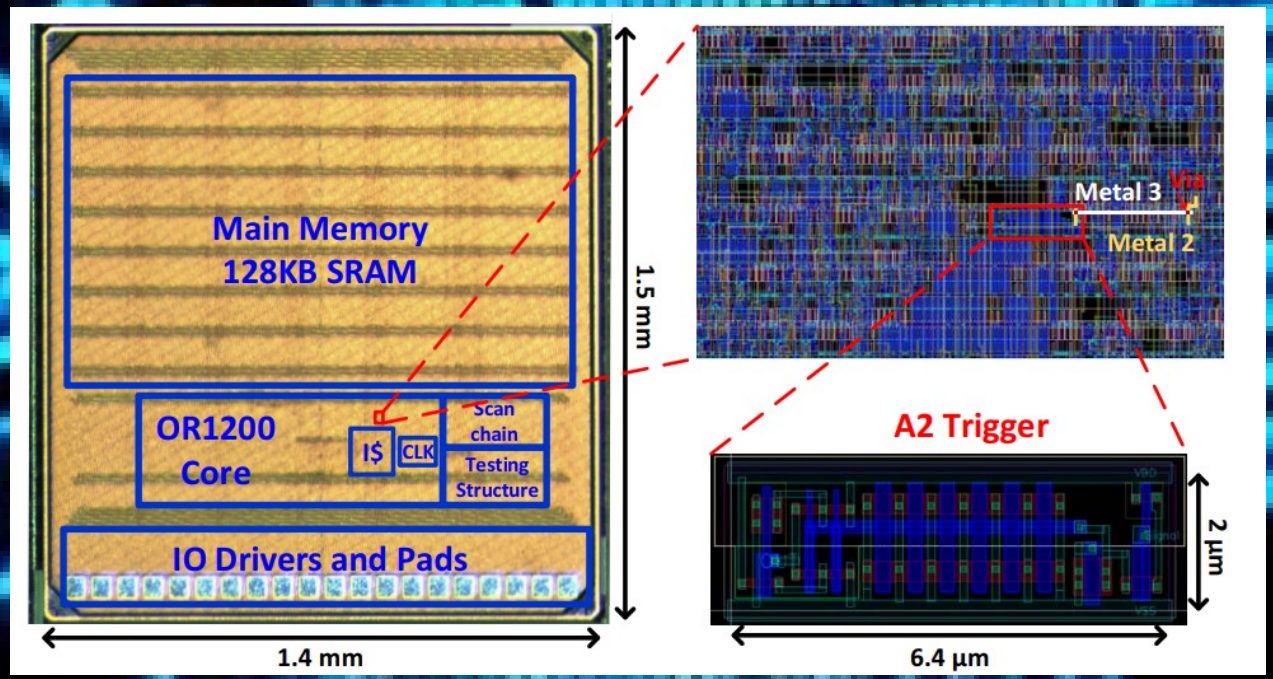
Incremento delle prestazioni

Difficoltà di progettazione e realizzazione

Produzione dei chip affidata ad aziende esterne

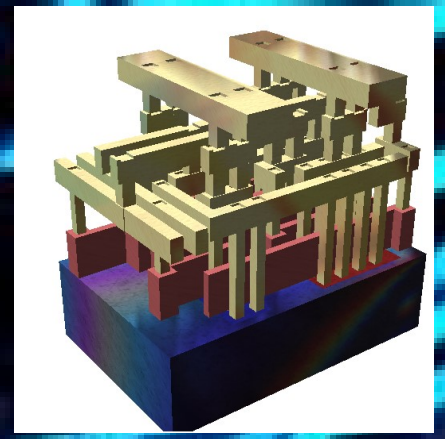
PIATTAFORMA OR 1200

Come esempio vediamo l'implementazione di un attacco hardware inserito su una piattaforma Open Source RISC chiamata OR1200 (comparabile con un ARM 10, usando un processo a 65nm su un area di 2,1 mm^2).



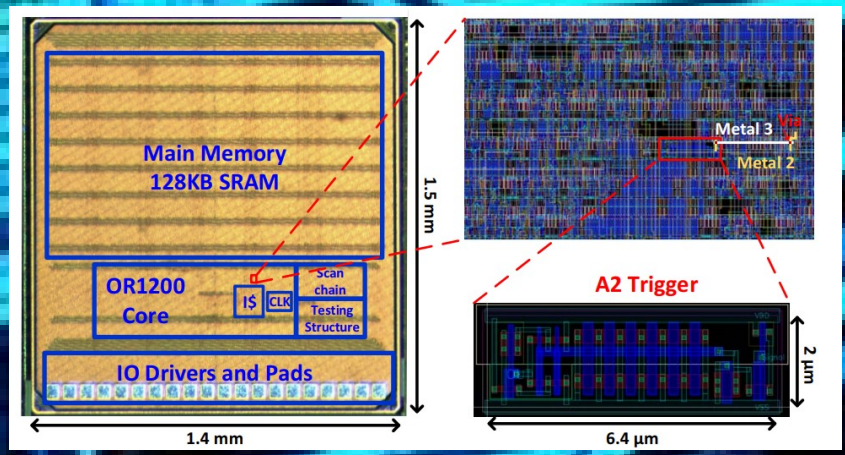
ESEMPIO DI ATTACCO

- Sfruttando gli spazi di progettazione esistenti all'interno del silicio o il design del circuito stesso è possibile inserire un piccolo circuito malevolo
- L'attivazione avviene grazie ad una sequenza inusuale di segnali fisicamente vicini al circuito
- Una volta attivato, il circuito permetterà di imporre l'uscita di un flip-flop ad un valore prescelto
- L' instruction set (IS) stabilisce l'esistenza di un registro Supervision Register (SR) il quale, a seconda del valore del bit contenuto, definisce le modalità di accesso alla macchina
- Modificando tale bit è possibile prendere il controllo dell'intero processore



CARATTERISTICHE DEL CIRCUITO MALEVOLO

- Funzionalità: il circuito dovrà essere in grado identificare la sequenza di attivazione e di resettarsi nel caso questa non sia completa
- Area ridotta: non deve essere visibile
- Potenza ridotta: non deve essere identificabile attraverso un'analisi sulla potenza
- Impatto minimo: non deve variare le costanti di tempo del circuito attaccato
- Compatibilità alle standard cell



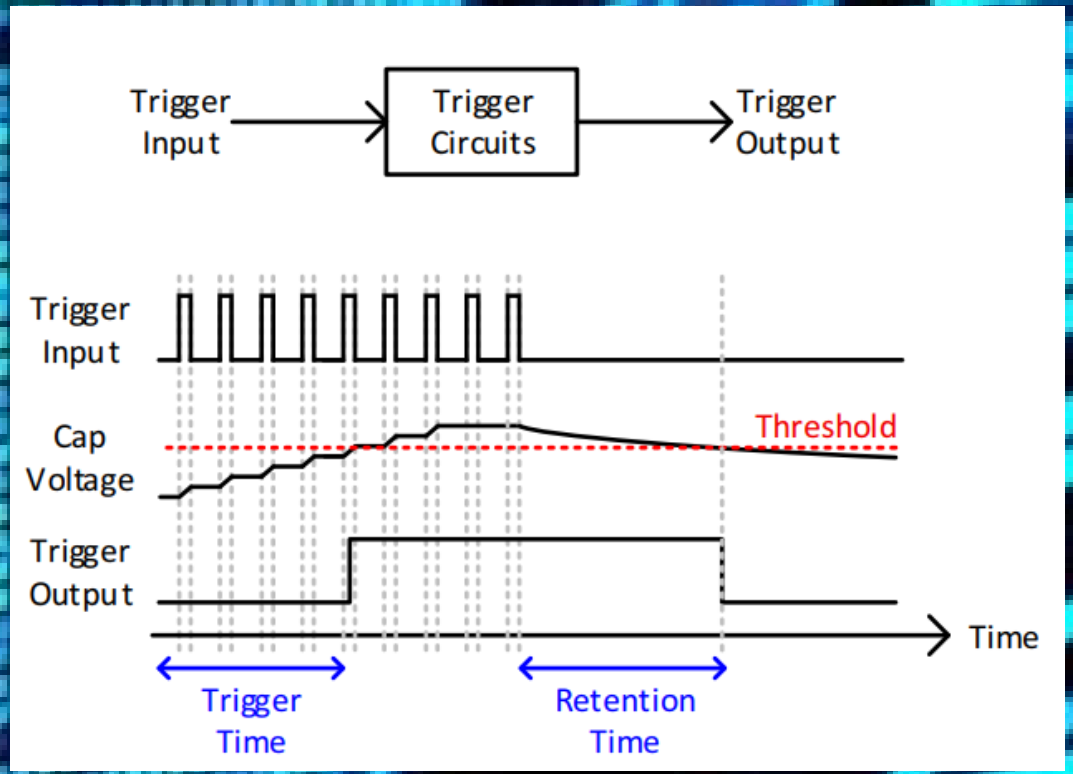
CIRCUITO TRIGGER: L'ACCUMULATORE DI CARICA

L'idea è quella di sfruttare un condensatore come integratore di tensione. Quando il valore di tensione ai suoi capi supera il valore di soglia, allora il circuito di trigger innesca l'attacco.

Problema: corrente di leakage del condensatore

$$i(t) = C\frac{dv(t)}{dt}$$

$$v(t) = \frac{1}{C}\int_{t_0}^{t} i(\tau)d\tau + v(t0)$$

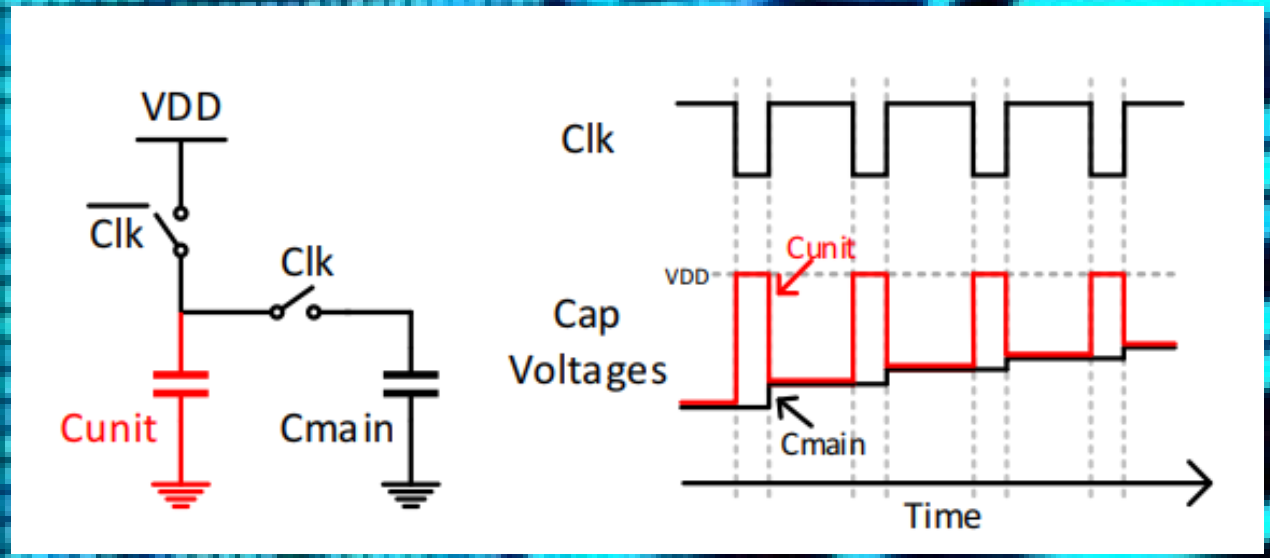


IMPLEMENTAZIONE: CIRCUITO CHARGE PUMP

Sfruttando tale schema, durante il periodo di clock, la carica presente su C_{unit} precedentemente caricata a VDD, viene ripartita tra C_{main} e C_{unit}.

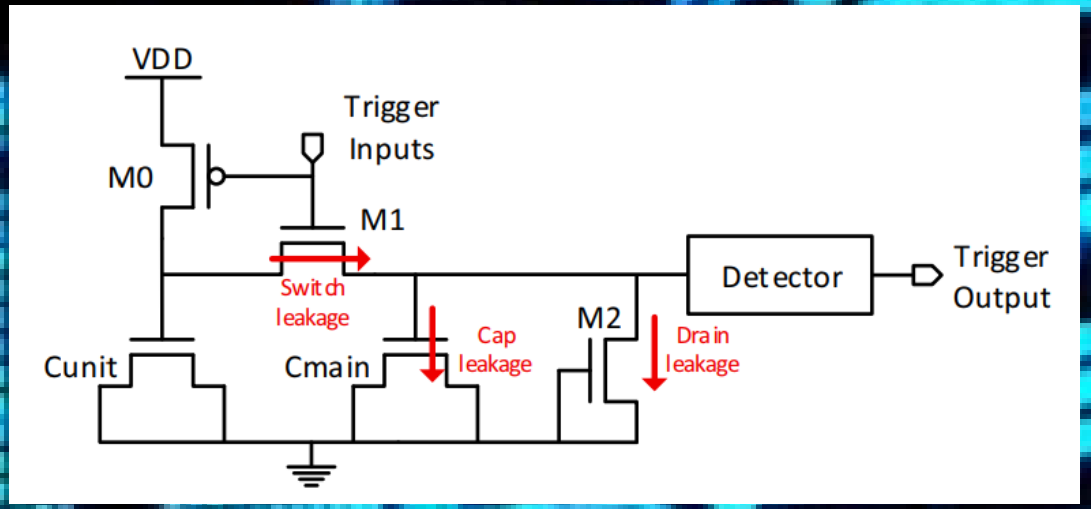
In questo modo il valore della variazione di tensione su C_{main} risulta più stabile rispetto alla corrente di leakage. (Partitore di carica)

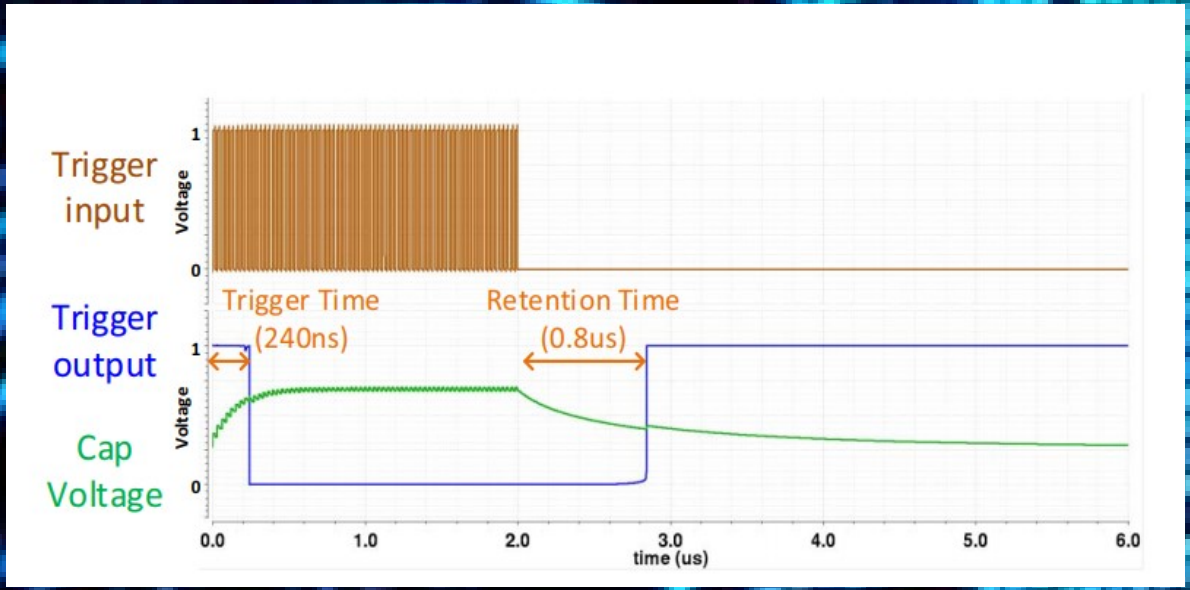
$$\Delta V = \frac{C_{unit} \cdot (V_{DD} - V_0)}{C_{unit} + C_{main}}$$



SCHEMA E SIMULAZIONE

Lo schema implementativo fa uso di condensatori creati grazie alla capacità di gate dei MOS.

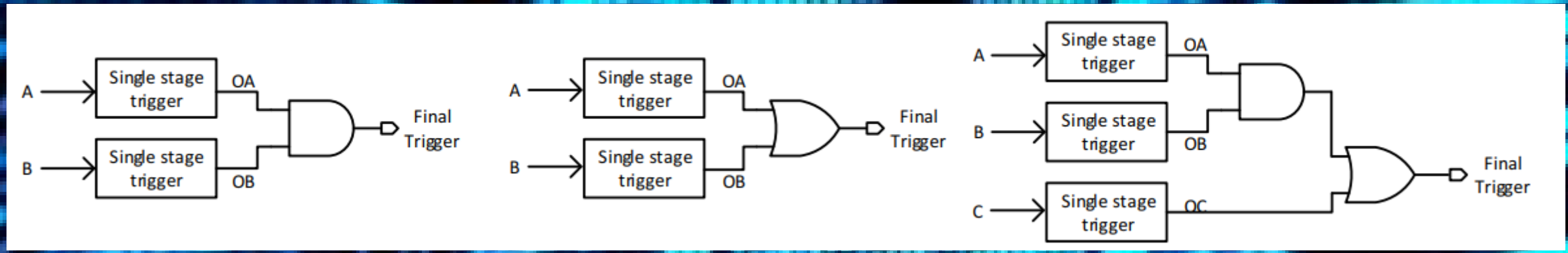




Inoltre per bilanciare e regolarizzare la corrente di leakage è stato introdotto il transistor M2.

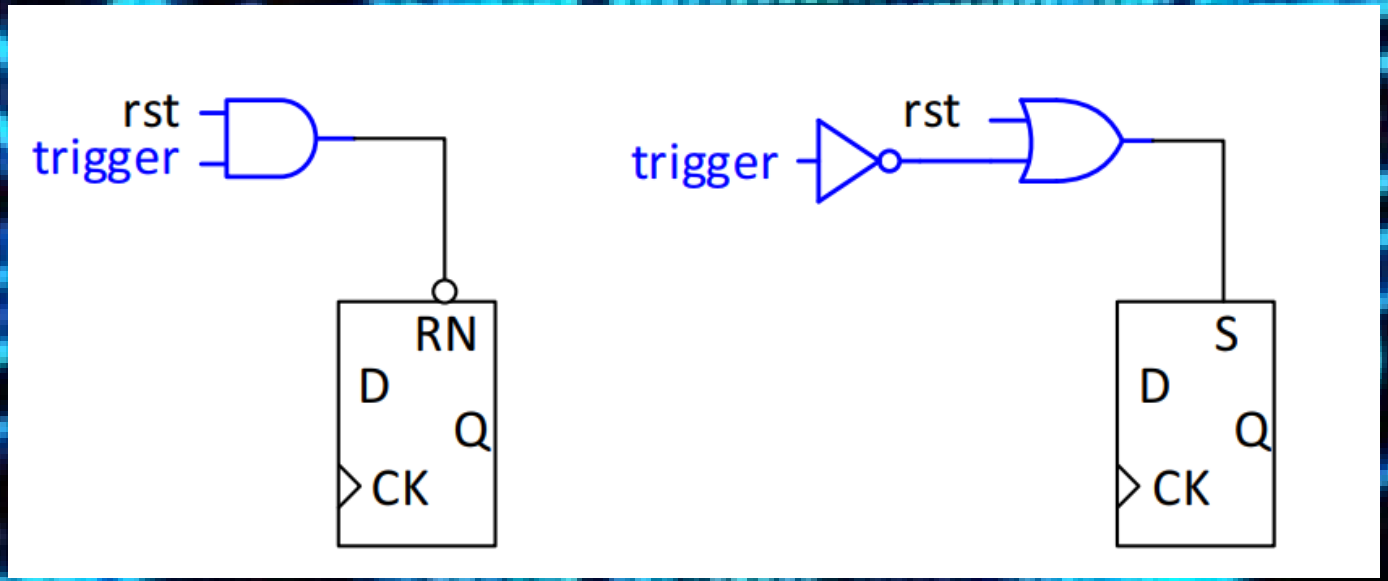
MA QUANTI SEGNALI DI ATTIVAZIONE?

Considerare solamente un segnale di attivazione per effettuare l'attacco potrebbe essere controproducente: possono verificarsi falsi positivi! Quindi combinando più circuiti di sensing con una rete logica è possibile creare serie anche complessa di combinazioni logiche per l'attivazione dell'attacco.



CAPITALIZZARE L'ATTACCO

Il segnale di attivazione dell'attacco quindi può negare il valore di un registro oppure lasciarlo invariato.



SEMPLICITA' DEL CODICE

Il codice per attivare il trigger è semplicissimo e non viene bloccato da un possibile antivirus:

Attivando il flag di DIVISIONE PER ZERO ciclicamente e sfruttandolo come segnale sul quale fare il triggering è possibile sfruttare la vulnerabilità del processore.

```
{r0 is a non-zero register but reads as zero in user mode}
Initialize SR[0]=0                    {initialize to user mode}
while Attack_Success==0 do
   i ← 0
   while i < 500 do
      z ← 1/0
      i ← i + 1
   end while
   if read(special register r0) ≠ 0 then
      Attack_Success ← 1
   end if
end while
```

RISULTATI

- Purtroppo il processo di hacking in fabrication-time è possibile
- L'effetto è devastante: fornisce ad un software non privilegiato, il controllo completo del sistema
- Scoprire l'attacco in fase di test del microprocessore è quasi impossibile
- Proteggersi è molto difficile, la vulnerabilità non viene risolta da patch software

LINK UTILI

- Patch per la risoluzione della vulnerabilità sfruttata dal worm Blaster (KB828741) http://www.microsoft.com/technet/security/bulletin/MS04-012.mspx
- Patch per la risoluzione della vulnerabilità sfruttata dal worm Sasser (KB835732) http://www.microsoft.com/technet/security/bulletin/MS04-011.mspx
- Patch per la risoluzione delle vulnerabilità di Outlook Express http://www.microsoft.com/technet/security/bulletin/MS03-014.mspx (Q330994) http://www.microsoft.com/technet/security/bulletin/MS04-013.mspx (Q837009)
- Osservatorio virus de IlSoftware.it http://www.ilsoftware.it/av.asp
- Tools di rimozione per i worm più diffusi http://www.nod32.it http://www.kaspersky.com/removaltools http://securityresponse.symantec.com/avcenter/tools.list.html

- https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7546493
- https://github.com/openrisc/or1200
- https://openrisc.io/