4 ore con il Malware

prof. Luigi Coppolino

04/04/2024

Di cosa parleremo

- Cosa è un malware
- Tipologie di malware
- A caccia di malware: gli antivirus
- Analisi del malware con laboratori
  - statica e dinamica

Di cosa avrete bisogno

- Per i laboratori:
  - Un computer, un tablet o un cellulare
  - Se avete un computer vi conviene aprire questo link https://github.com/colui77/seminario
- Per seguire il corso:
  - Pazienza e caffè

L'ATTUALITÀ ATTRAVERSO LE CARTE

Nucleare: l'Aiea condanna l'Iran

I SITI NUCLEARI IRANIANI

27/11/2009
di Alfonso Desiderio

L'Agenzia Internazionale per l'Energia Atomica ha approvato una risoluzione di condanna nei

Novembre 2009

ESTERI

Il premier israeliano spinge per una risoluzione pïï¿½ dura da parte dell'Onu
"Teheran lavora seriamente in segreto per dotarsi di armi non convenzionali"

Nucleare Iran, l'allarme di Olmert
"Piano militare, ne siamo certi"

BERLINO – "Abbiamo la certezza che l'Iran ha in corso un programma segreto per costruire armi nucleari". Lo ha detto il premier israeliano Ehud Olmert parlando a Berlino nel corso di una conferenza stampa congiunta con la cancelliera tedesca Angela Merkel. Per scongiurare questa possibilitï¿½, ha aggiunto, "nessuna opzione deve

la 'Giornata nazionale dell'energia atomica' il presidente Ahmadinejad
naugurato il primo impianto per la produzione di combustibile centrali

an, ancora una sfida sul nucleare
uovo impianto per arricchire uranio

unciato l'avvio di centrifughe supermoderne. "Sono settemila quelle in funzione"
recedenza da Teheran cauta apertura al dialogo offerto dal '5+1'. Timori dall'occidente

Il presidente iraniano Ahmadinejad

TEHERAN – L'Iran ï¿½ riuscito ad ottenere nuovi progressi nella tecnologia nucleare nonostante "le pressioni, la propaganda e le minacce militari del nemico". Lo ha detto oggi il presidente Mahmud Ahmadinejad. Che ha inaugurato ad Isfahan, nella 'Giornata nazionale dell'energia atomica', il primo impianto per la produzione di combustibile per alimentare centrali nucleari.

Ahmadinejad ha sottolineato le due principali novitï¿½ annunciate oggi: la produzione per la prima volta di combustibile nucleare pronto per essere immesso nei reattori e la produzione di due nuovi tipi di centrifughe "capaci di fornire uranio arricchito ad un ritmo

Aprile 2009

Focus

SCIENZA AMBIENTE CULTURA COMPORTAMENTO TECNOLOGIA FOCUS LIVE FOCUS SCONTI ABBONATI ALLA RIVISTA

Scienze Iran: allarme virus nei pc della centrale nucleare

Infettati i pc della centrale nucleare.

AI_Intro.mp4

Attacco hacker mondiale: virus "Wan chied

Ooops, your files have been encrypted!

Cyberspies penetrate electrical grid: report

Consiglia | Consiglia questo elemento prima di tutti i tuoi amici.

MOTHERBOARD | By Kim Zetter | Mar 25 2019, 2:00pm
TECH BY VICE

Hackers Hijacked ASUS Software

U.S. Power G

Attacco hacker mondiale: virus "Wannacry" chiede il riscatto, ospedali britannici in tilt. "Usato codice Nsa"

Un "ransomware" lanciato su centomila siste
Pagamenti in corso, rischio truffa. Colpita an

di TIZIANO TONIUTTI

Symantec. | Connect

Enter keywords to search...

COMMUNITY: Security | Blogs | Security Response

Login or Register to participate

Symantec Intelligence Quarterly Report: Targeted Attacks on Critical Infrastructures

Updated: 14 Feb 2011 | Translations available: 日本語

Téo Adams SYMANTEC EMPLOYEE

+1
1 Vote

Symantec. | Official Blog

There's been lots of discussion lately on targeted attacks which are, as the name implies, cyberattacks directed at specific individuals, organizations, corporations, or sectors. These targeted attacks, particularly on critical infrastructure, are the focus of our Symantec Intelligence Quarterly Report: October – December 2010.

SUBSCRIBE

ABBONATI A Rep: | Lo leggo dopo | 12 maggio 2017

OGGI SU Rep:

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT

ABBONATI *Tra i bersagli anche la società britannica pubblic*

560 mila

nuovi malware al giorno

> 1 Miliardo in circolazione

560 mila

nuovi malware al giorno

> 1 Miliardo in circolazione

MALICIOUS + SOFTWARE

560 mila

nuovi malware al giorno

> 1 Miliardo in circolazione

MALWARE

560 mila

Cos’è un malware?
Malware è un termine generico che indica software dannosi progettati per compromettere o sfruttare qualsiasi tipo di dispositivo, servizio o rete programmabile. [McAfee]

MALWARE

560 mila

nuovi malware al giorno

> 1 Miliardo in circolazione

Trojan
il 58% del
malware

11,5 miliardi di
dollari/anno
per
ransomware

9 casi su 10
hanno inizio
con phishiing

56 il

nu

> 1

MALWARE PIÙ DIFFUSI

VIRUS

Produce sempre più **copie di sé** con cui infetta file o aree del disco. Richiede almeno un'interazione dell'utente.

https://cyberdivision.net/

Trojan
il 58% del
malware

11,5 miliardi di
dollari/anno
per
ransomware

9 casi su 10
hanno inizio
con phishiing

5G ... il nu...

> 1

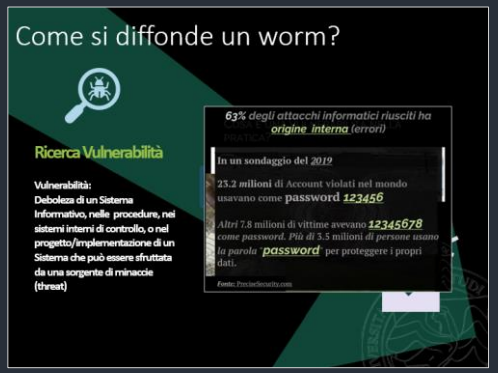
MALWARE PIÙ DIFFUSI

VIRUS

Produce sempre più **copie di sé** con cui infetta file o aree del disco. Richiede almeno un'interazione dell'utente.

WORM

Malware **auto-replicante** che sfrutta la rete per propagarsi. Si diffonde senza interazioni dell'utente.



https://cyberdivision.net/

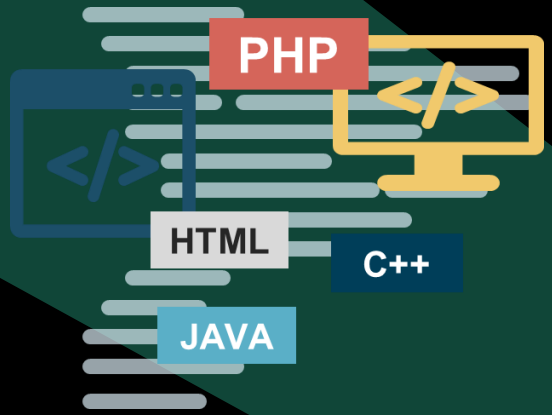
Trojan il 58% del malware

11,5 miliardi di dollari/anno per ransomware

9 casi su 10 hanno inizio con phishiing

Come si diffonde un worm?

Ricerca Vulnerabilità



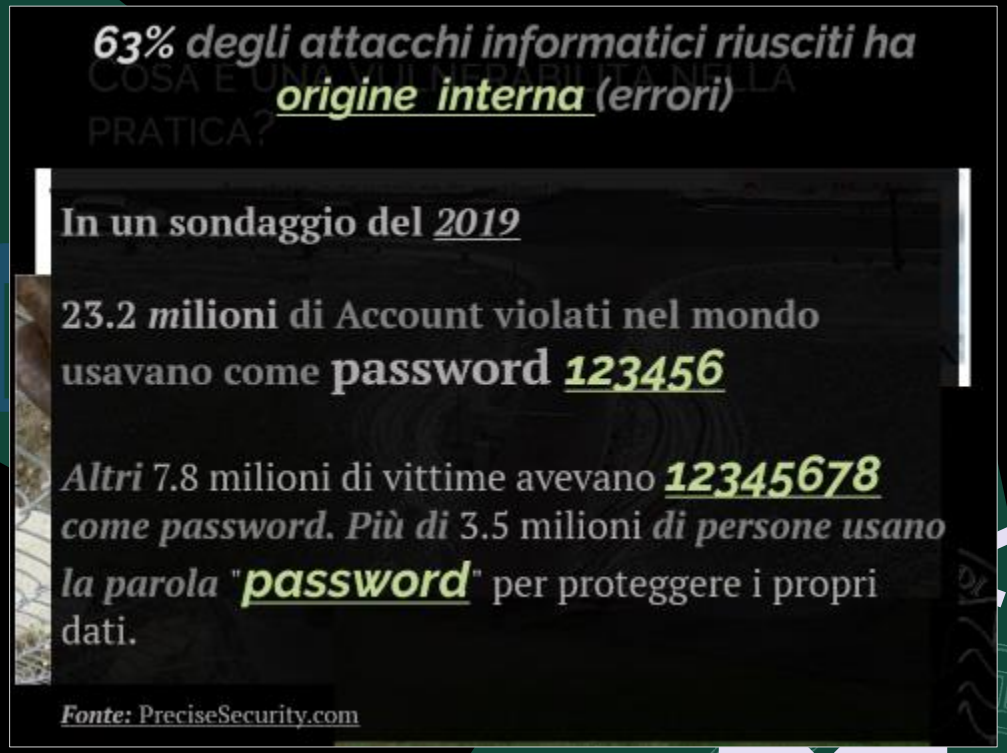
Selezione Exploit

Attacco

Come si diffonde un worm?

Ricerca Vulnerabilità

Vulnerabilità:
Deboleza di un Sistema Informativo, nelle procedure, nei sistemi interni di controllo, o nel progetto/implementazione di un Sistema che può essere sfruttata da una sorgente di minaccie (threat)



63% degli attacchi informatici riusciti ha origine interna (errori)

COSA È UNA VULNERABILITÀ NELLA PRATICA?

In un sondaggio del *2019*

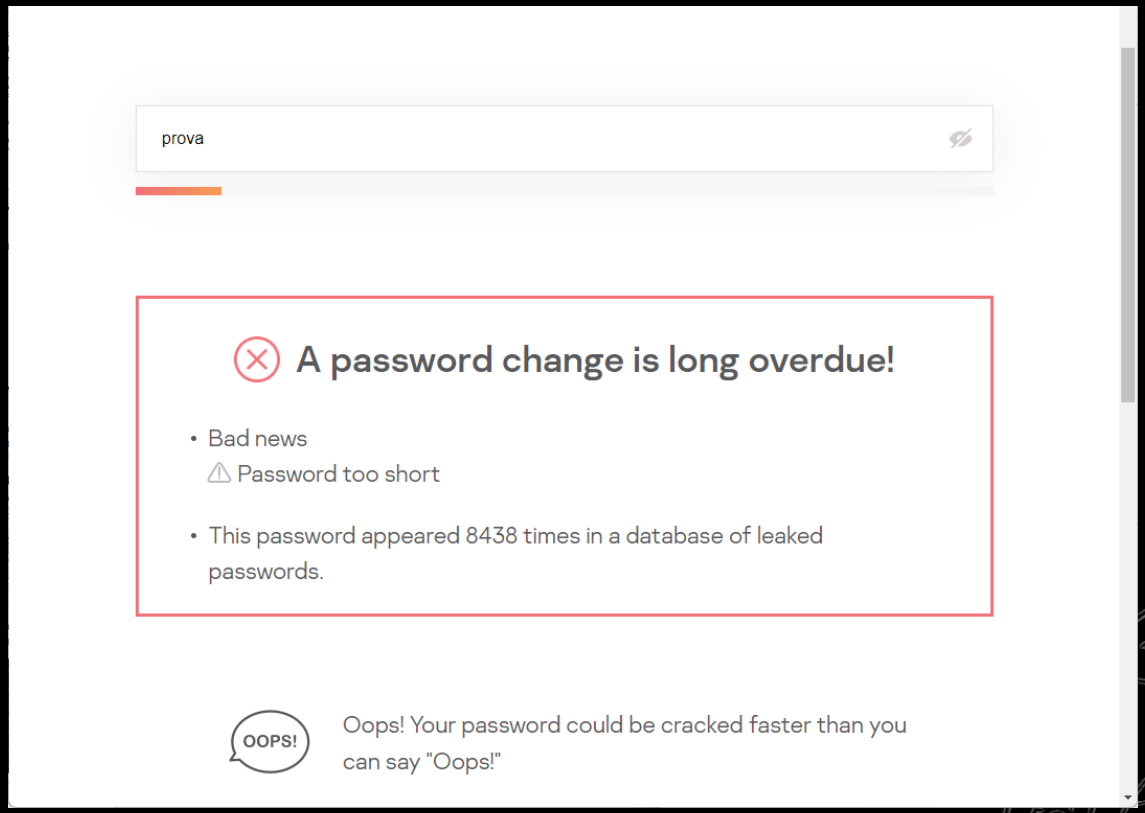
23.2 *m*ilioni di Account violati nel mondo usavano come password *123456*

Altri 7.8 milioni di vittime avevano ***12345678*** ***come password. Più di*** 3.5 milioni ***di persone usano la parola*** "***password***" per proteggere i propri dati.

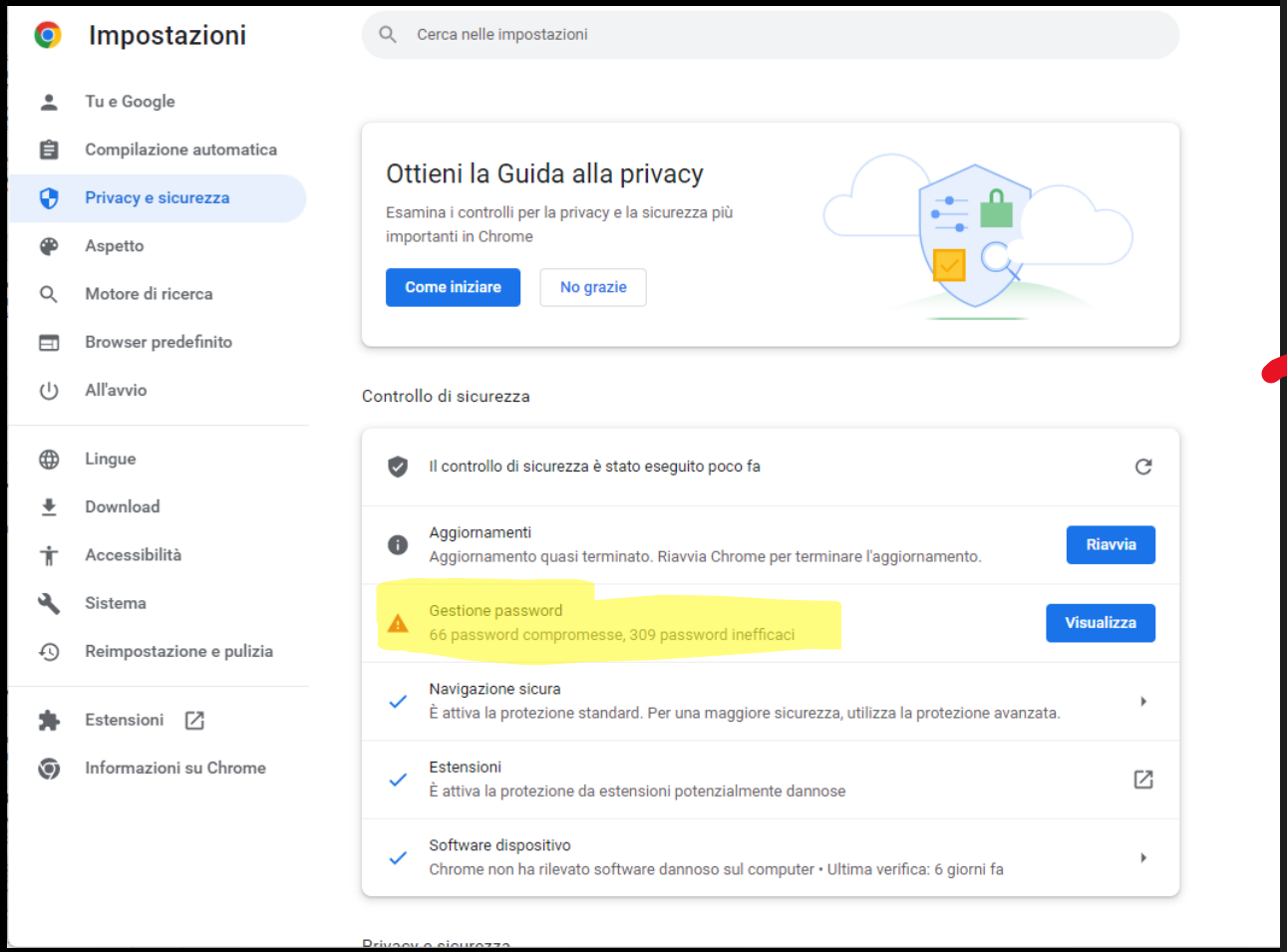
Fonte: PreciseSecurity.com

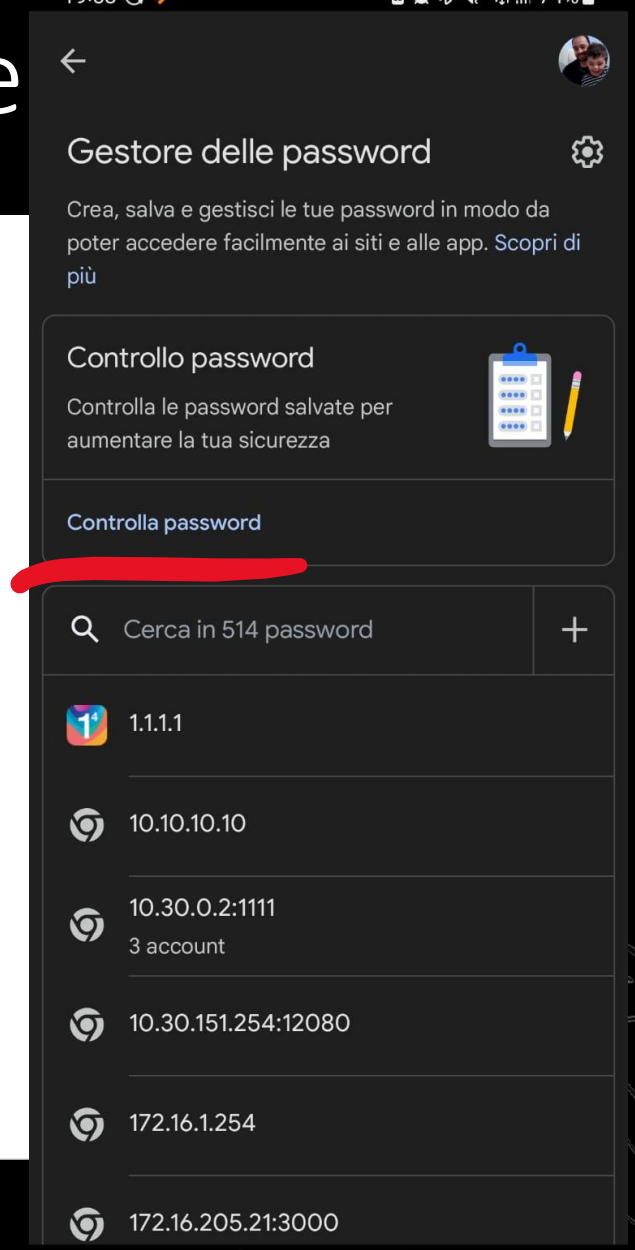
Kaspersky Password Checker

https://password.kaspersky.com/

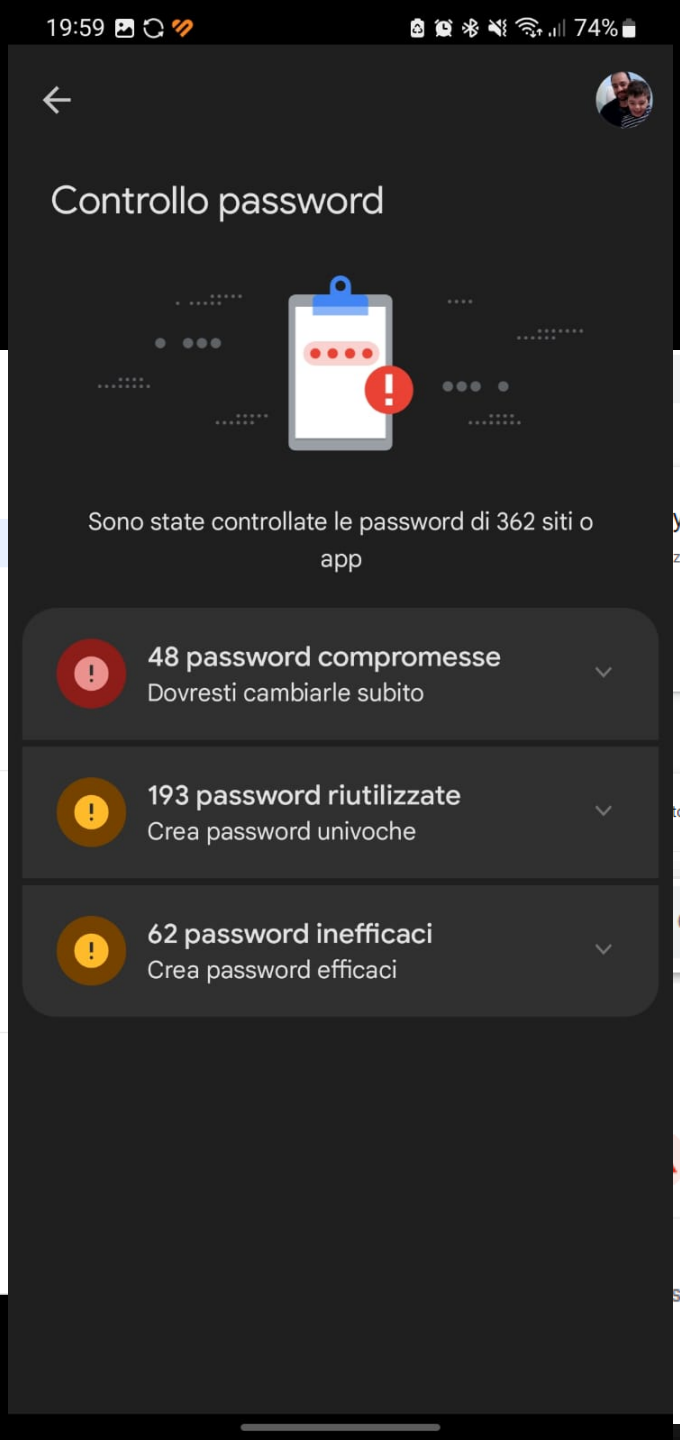


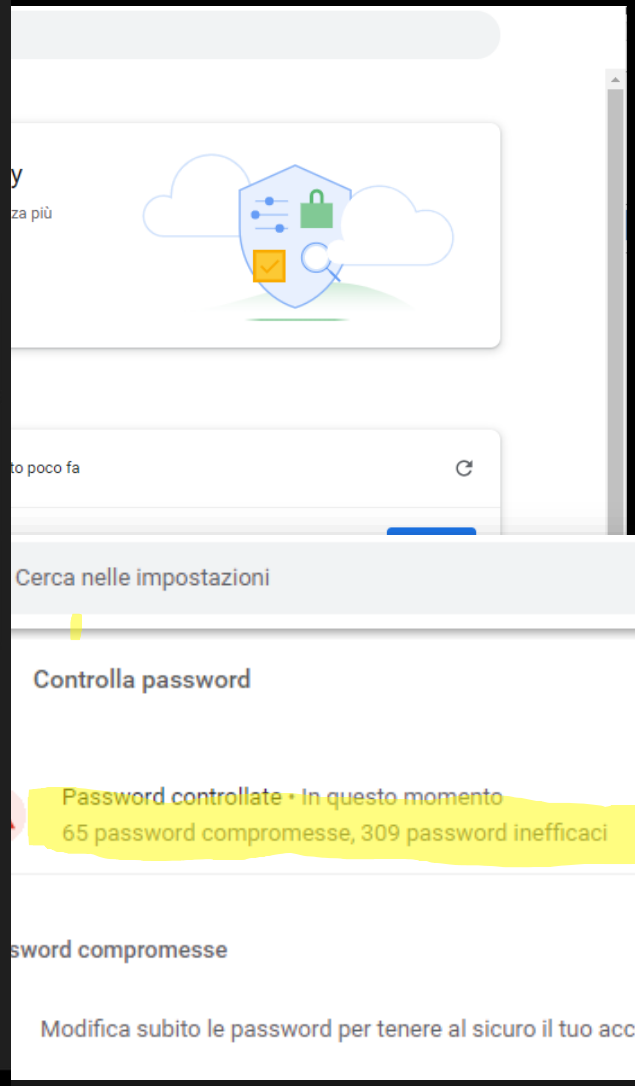
Chrome Security Checke





urity Checker





Pwned Passwords

- https://haveibeenpwned.com/Passwords

Anno 2016…
MIRAI blocca il mondo

Un DDoS volumetrico… basato sulla quantità di traffico generato

145,000 dispositivi coinvolti … basato su IoT

Il volume massimo generato fino ad allora: 400 Gbps

Il volume di MIRAI 1Tbps

How does malware turn IoT devices into bots or zombies?

In general, email phishing is a demonstrably effective way of infecting the computer - the victim is tricked into either clicking a link that points to a malicious website, or downloading infected attachment. Many times the malicious code is written in such a way that common antivirus software is not able to detect it.

In the case of Mirai, the user doesn't need to do much beyond leaving the default username and password on a newly installed device unchanged.

Giorno 05/02/2023

Massiccio attacco hacker in Italia e nel mondo. Migliaia i server bloccati. L'Agenzia per la cybersicurezza: "Aggiornarli subito"

a cura di Redazione Cronaca nazionale

Oltre ai sistemi colpiti, ricorda l'Agenzia, "ne restano molti ancora esposti". La strategia è quella di bloccare il computer e chiedere un riscatto. La Francia il Paese più colpito, ma tutta l'Europa e il Nordamerica sono nel mirino. Domani vertice a Palazzo Chigi

05 FEBBRAIO 2023 AGGIORNATO 06 FEBBRAIO 2023 ALLE 09:09

2 MINUTI DI LETTURA

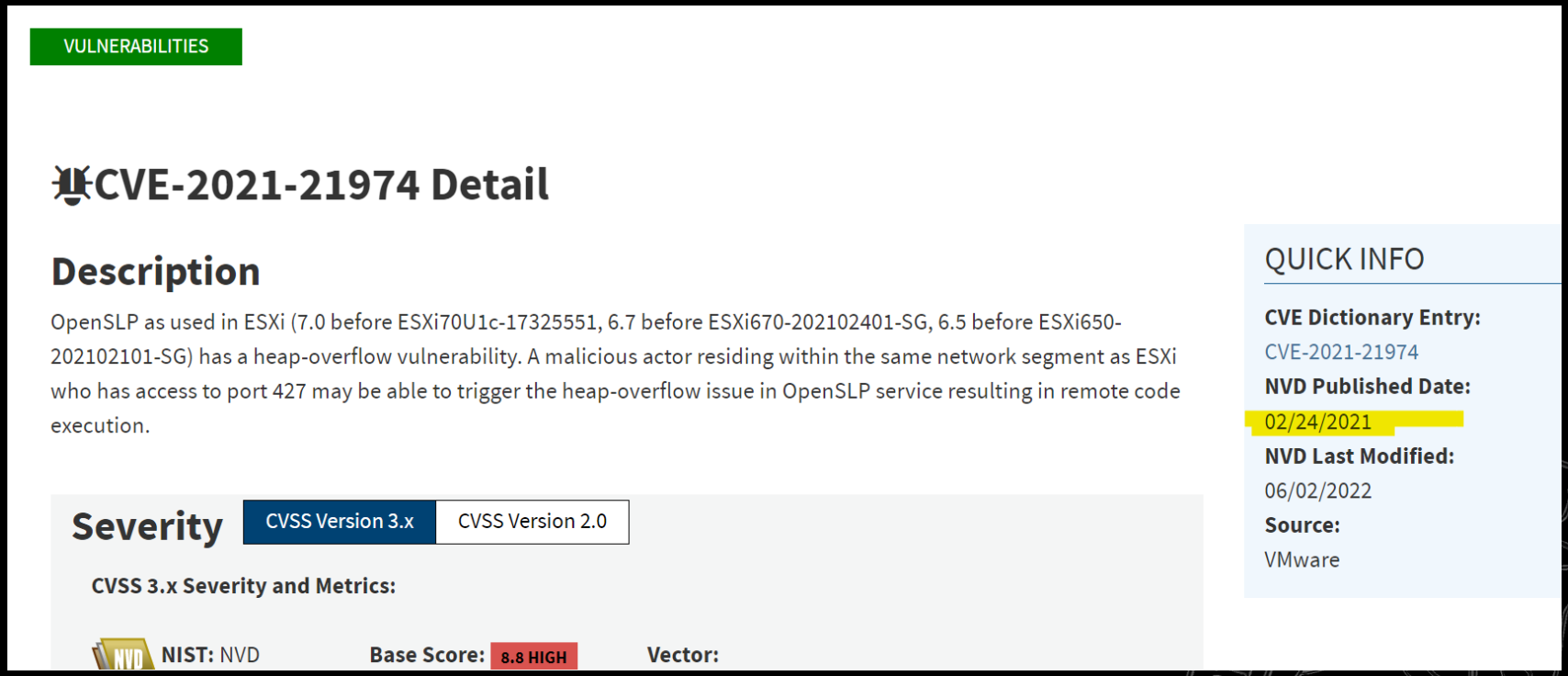
Ma non solo email…05/02/2023

Attacco RANSOMWARE

Vulnerabilità sfruttata: CVE-2021-21974

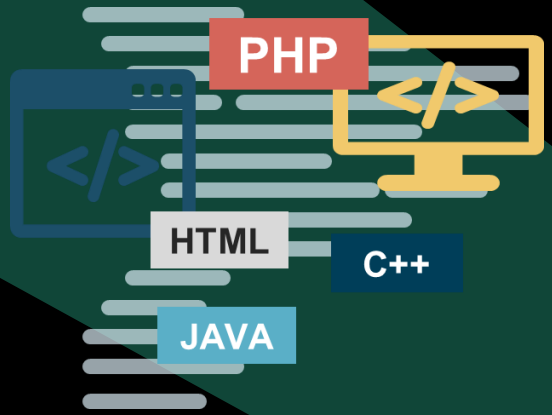
Cosa è un CVE?

https://nvd.nist.gov/vuln/detail/CVE-2021-21974



Come si diffonde un worm?

Ricerca Vulnerabilità



Selezione Exploit

Exploit:
Una applicazione che sfrutta una vulnerabilità

Attacco

Come si diffonde un worm?

Ricerca V

Durante la fase di attacco

- Accesso Iniziale: è già avvenuta, malware su vittima
- Persistenza: far in modo che se il sistema viene riavviato il malware sia automaticamente lanciato in esecuzione
- Recupero di funzionalità: download o preparazione di altre parti del virus
- Priviledge escalation: aumentare i privilegi sulla macchina vittima
- Movimento laterale: raggiunge altri sistemi
- [Command and Control]: riceve ed esegue comandi
- Impact: mette in atto il suo scopo
- [Data exfiltration]: invia dati raccolti localmente

Attacco

L'exploit viene lanciato e se ha successo riesce a trasferirsi sul Sistema vittima

56 il

nu

> 1

MALWARE PIÙ DIFFUSI

VIRUS

Produce sempre più **copie di sé** con cui infetta file o aree del disco. Richiede almeno un'interazione dell'utente.

WORM

Malware **auto-replicante** che sfrutta la rete per propagarsi. Si diffonde senza interazioni dell'utente.

https://cyberdivision.net/

Trojan
il 58% del
malware

11,5 miliardi di
dollari/anno
per
ransomware

9 casi su 10
hanno inizio
con phishiing

5G ... il

nu...

> 1

MALWARE PIÙ DIFFUSI

VIRUS

Produce sempre più **copie di sé** con cui infetta file o aree del disco. Richiede almeno un'interazione dell'utente.

TROJAN

Malware **mascherato** da software/file utile, che nasconde virus o elementi dannosi.

WORM

Malware au... la rete per... senza intera...

https://cyberdivision.net/

Trojan
il 58% del
malware

11,5 miliardi di
dollari/anno
per
ransomware

9 casi su 10
hanno inizio
con phishiing

BREAKING NEWS

LIVE

AVETE UN TROJAN SUI VOSTRI CELLULARI

56 il

nu

> 1

MALWARE PIÙ DIFFUSI

VIRUS

Produce sempre più **copie di sé** con cui infetta file o aree del disco. Richiede almeno un'interazione dell'utente.

TROJAN

Malware **mascherato** da software/file utile, che nasconde virus o elementi dannosi.

WORM

Malware **auto-replicante** che sfrutta la rete per propagarsi. Si diffonde senza interazioni dell'utente.

https://cyberdivision.net/

Trojan
il 58% del
malware

11,5 miliardi di
dollari/anno
per
ransomware

9 casi su 10
hanno inizio
con phishiing

I RANSOMWARE

- Il ransomware è un tipo di malware che blocca l'accesso al sistema o ai file dell'utente e richiede un pagamento (riscatto=ransom) per ripristinare l'accesso
  - Il ransomware può causare interruzioni gravi delle attività con conseguenti danni finanziari

Trends and statistics

Estorsione a due livelli

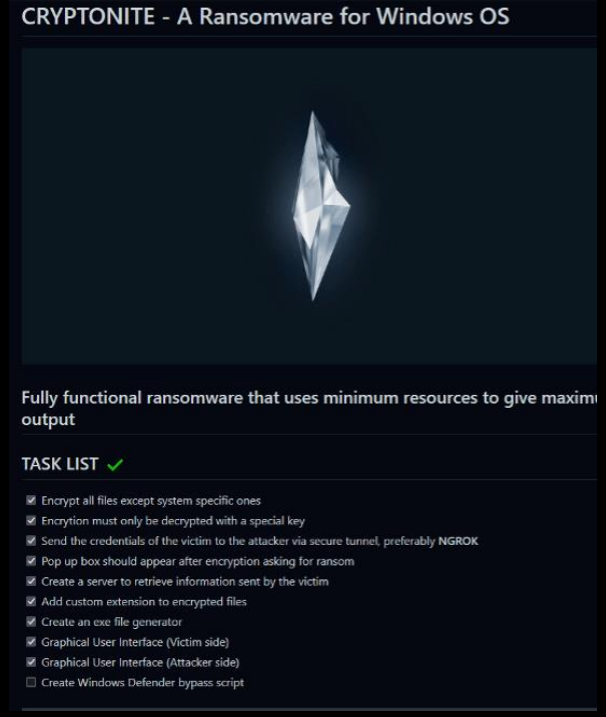
Ransomware-as-a-service

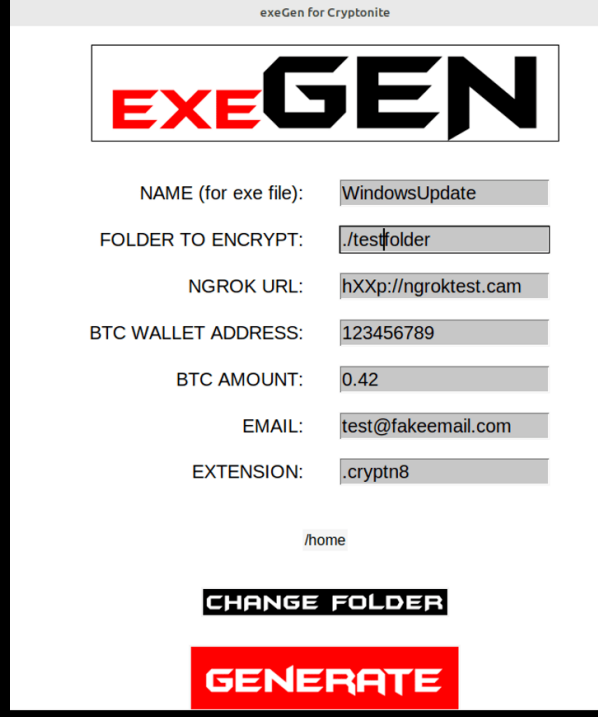
Cloud-aware ransomware

intermittent encryption

R-a-a-S

- Il ransomware SunTzu
  - venduto a 10.000 dollari una tantum
- Diversi gruppi attivi:
  - RainMaker labs, GandCrab, Sodinokibi, Jokeroo
- La piattaforma Cryptonite
  - Rilasciata open-source
  - Dotata di interfaccia grafica





56 il

nu

MALWARE PIÙ DIFFUSI

VIRUS

Produce sempre più **copie di sé** con cui infetta file o aree del disco. Richiede almeno un'interazione dell'utente.

TROJAN

Malware **mascherato** da software/file utile, che nasconde virus o elementi dannosi.

sfrutta
ffonde

WARE

esso ad aree del proprio computer, che
nte e criptate. Per ottenere nuovamente
chiesto il pagamento di un **riscatto**.

https://cyberdivision.net/

Trojan
il 58% del
malware

11,5 miliardi di
dollari/anno
per
ransomware

5 casi su 10
hanno inizio
con phishiing


BREAKING
NEWS
LIVE
AVETE UNA
BACKDOOR SUI
VOSTRI CELLULARI

WhatsApp: un bug consentiva di assumere il controllo dell'app dalla videochiamata

10 Ottobre 2018 21

WIRED BACKCHANNEL BUSINESS CULTURE GEAR IDEAS SCIENCE SECURITY

LILY HAY NEWMAN SECURI

How Hac

All it took to compr

WHATSAPP, SCOPERTO UN GRAVE BUG DI SICUREZZA SUBITO

WhatsApp | Provato | Guide | Articoli | Notizie | Immagini

Di **Alessio Marino** | 27 Settembre 2022, Ore 14:43

Whatsapp ha annunciato la scoperta di une vulnerabilità critica che fortunatamente è stata corretta nella versione più recente dell'app ma che

https://www.whatsapp.com/security/advisories/2022/

AGGIORNARE *SEMPRE* TUTTO QUANTO E' AGGIORNABILE

560

nuovi

> 1 Mili

Infiltrating the Google Play Store

Analysts at Dr. Web antivirus report that adware apps and data-stealing Trojans were among the most prominent Android threats in May 2022.

At the top of the report are spyware apps that can steal information from other apps' notifications, primarily to snatch one-time 2FA passcodes (OTP) and take over accounts.

Among the many threats that managed to infiltrate the Google Play Store, the following five are still available:

- **PIP Pic Camera Photo Editor** – 1 million downloads, malware masquerading as image-editing software, but which steals the Facebook account credentials of its users.
- **Wild & Exotic Animal Wallpaper** – 500,000 downloads, an adware trojan that replaces its icon and name to 'SIM Tool Kit' and adds itself to the battery-saving exceptions list.
- **ZodiHoroscope** – Fortune Finder – 500,000 downloads, malware that steal Facebook account credentials by tricking users into entering them, supposedly to disable in-app ads.
- **PIP Camera 2022** – 50,000 downloads, camera effects app that is also a Facebook account hijacker.
- **Magnifier Flashlight** – 10,000 downloads, adware app that serves videos and static banner ads.

Trojan
il 58% del
malware

11,5 miliardi di
dollari/anno
per
ransomware

9 casi su 10
hanno inizio
con phishiing

CURIOSITA’

ecco le nostre foto dell’estate

PAURA

Non hai pagato e stai per essere bloccato

EMPATIA

Amico FB: ho trovato questo video divertente, guardalo anche tu

AVIDITA’

Hai vinto un buono Amazon…

PHISHING

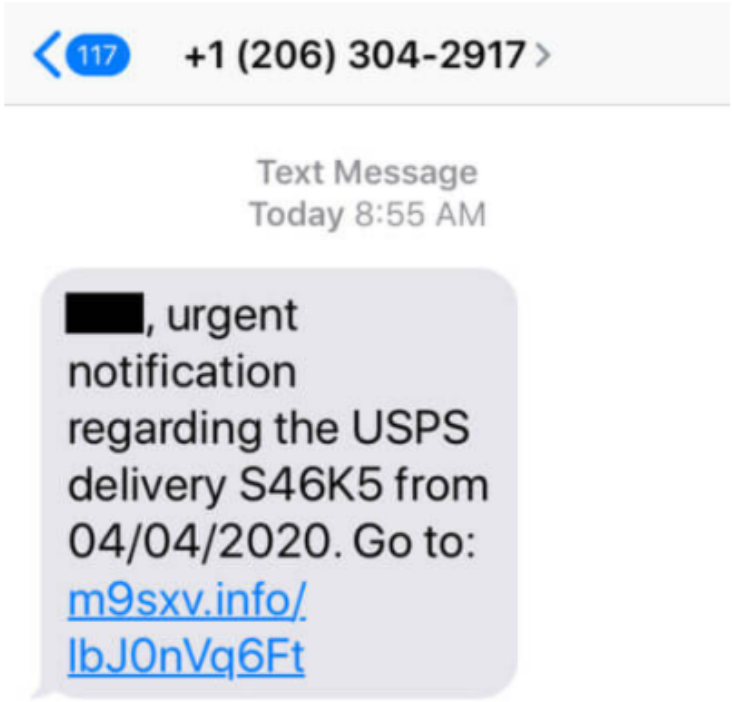
https://github.com/topics/facebook-phishing

SMISHING

A new SMS-based phishing ("smishing") campaign is using the United States Postal Service (USPS) as a disguise to target mobile users.

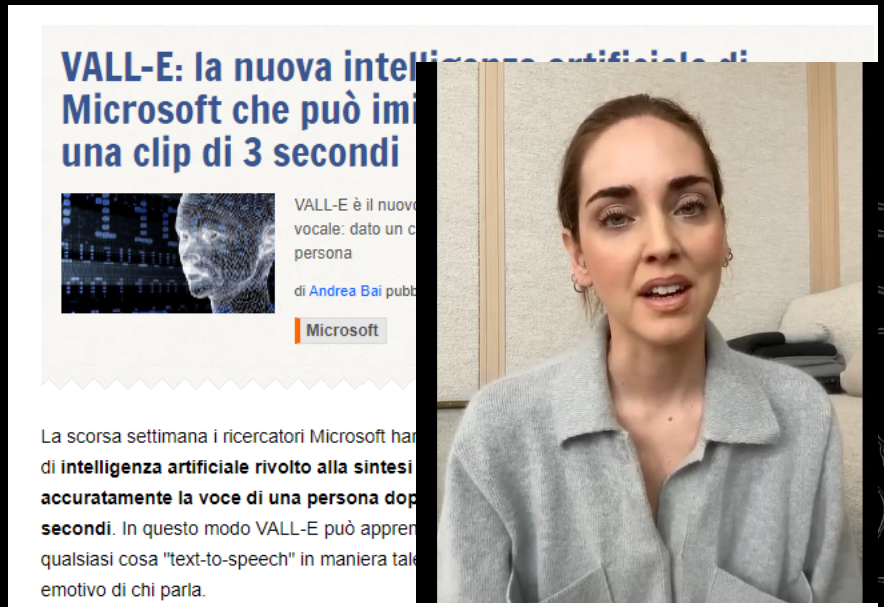
On September 15, SlickRockWeb CEO Eric JN Eliason tweeted out two examples of the operation.

Both attack SMS messages claimed to contain important information about a USPS package. Using that lure, they attempted to trick the recipient into clicking on a link containing the domain "m9sxv[.]info."



An example of the smishing campaign masquerading as the USPS. (Source: Twitter)

https://valle-demo.github.io/



VALL-E: la nuova intel… Microsoft che può imi… una clip di 3 secondi

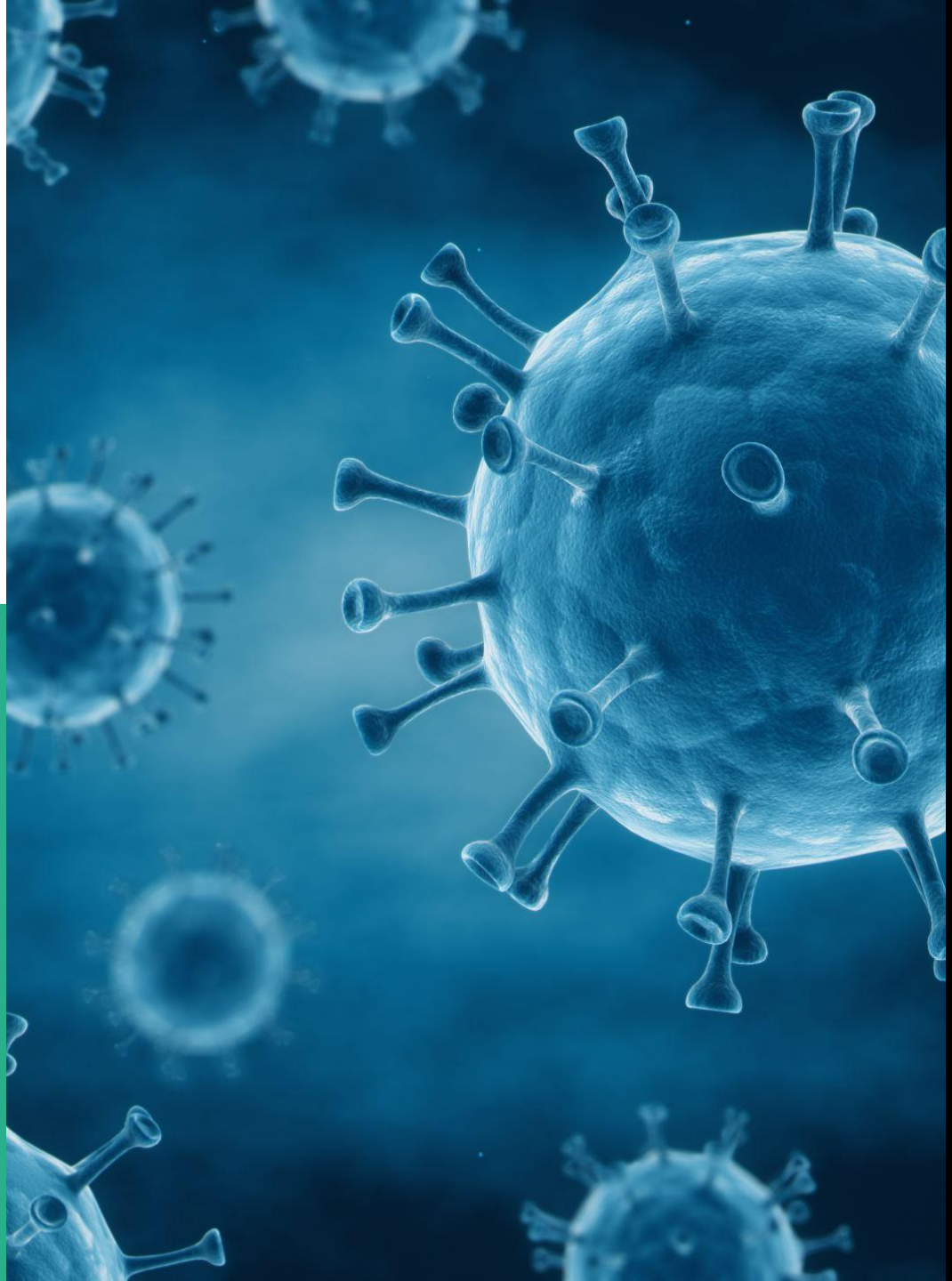
VALL-E è il nuov… vocale: dato un c… persona

di Andrea Bai pubb…

Microsoft

La scorsa settimana i ricercatori Microsoft har… di **intelligenza artificiale rivolto alla sintesi … accuratamente la voce di una persona dop… secondi**. In questo modo VALL-E può appren… qualsiasi cosa "text-to-speech" in maniera tale… emotivo di chi parla.

E se lo combinassimo con una AI generativa come AI?



A caccia di malware…

Come funziona un antivirus?

Come è fatto un file eseguibile windows?

- Tutti i file eseguibili sono binari (fatti di 0 e 1)
  - Alcune sequenze binarie corrispondono a delle lettere (codice ASCII)
  - Altre non sono visualizzabili come testo
- Ogni file ha un header e un corpo
  - L'header consente di capire come intepretare il file

PE View

00004550 ⇔ PE

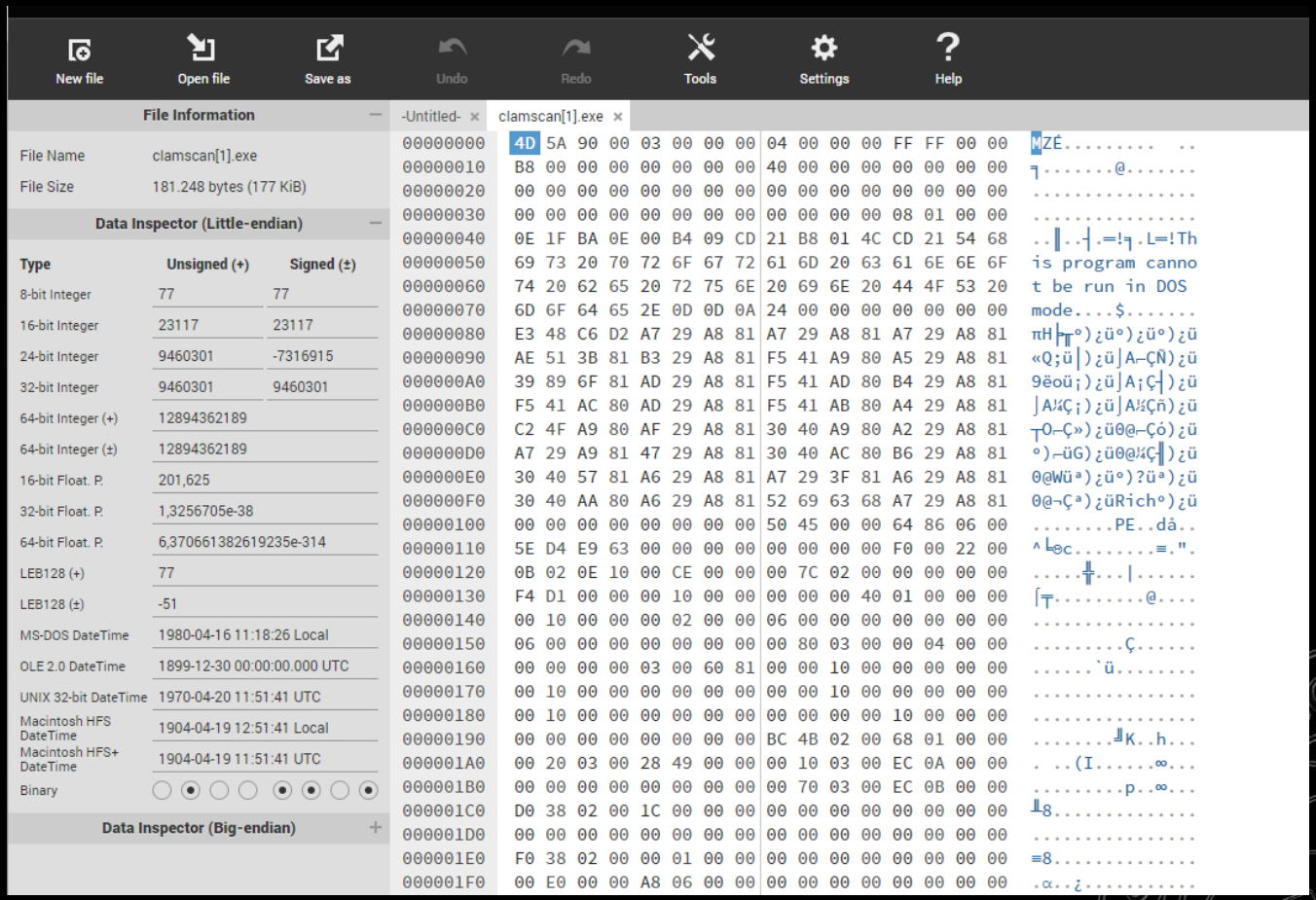
DOS header
DOS stub
PE Header/IMAGE NT header

https://hexed.it/

https://github.com/colui77/seminario/blob/c03e4d7a0cd0703a35db01d6274bd4fc73aa0ad3/clamscan.exe?raw=true

Esercizio: analizziamo un file eseguibile

Proviamo a navigare il file



Firma o signature

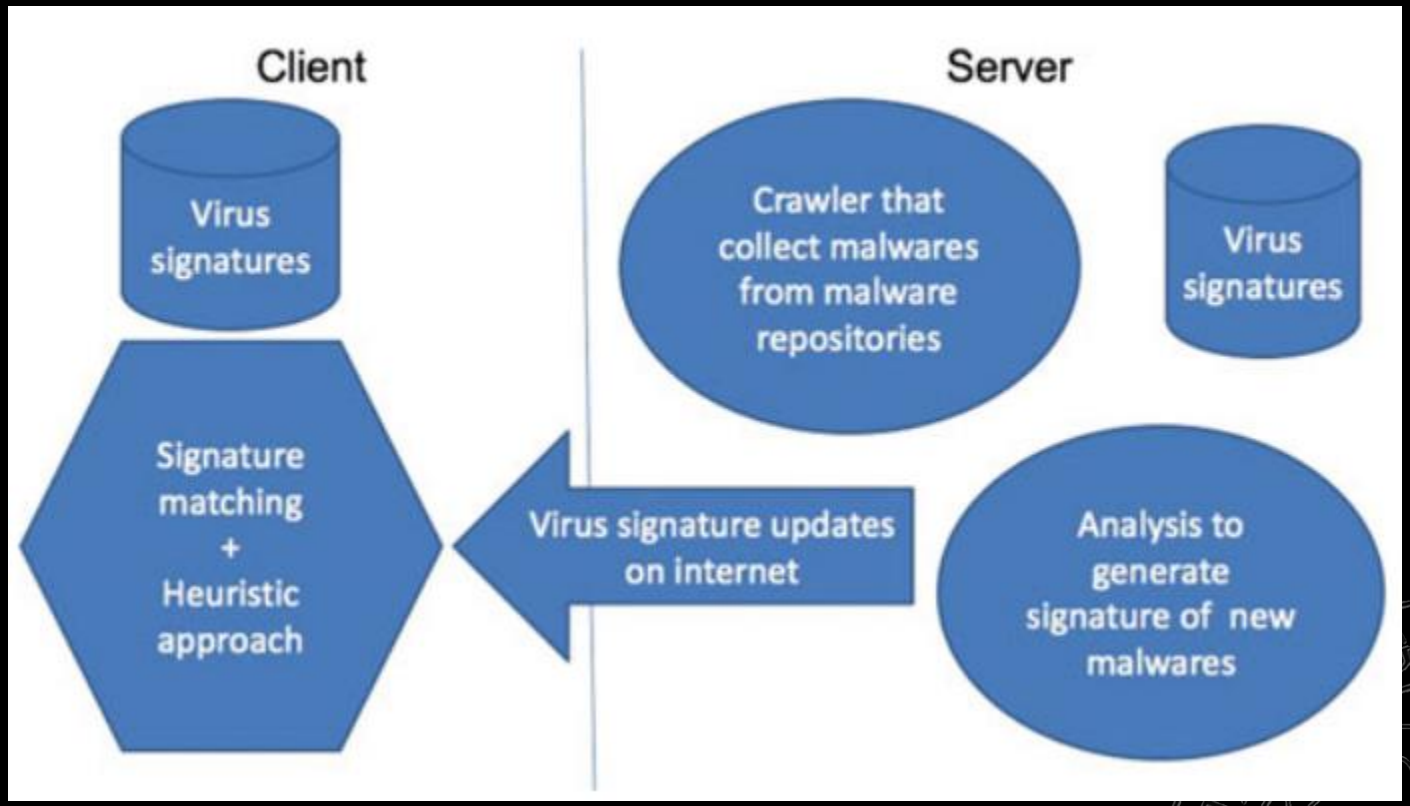
una sequenza univoca utile a poter identificare il Malware

Esempi di firme per:

klez.E/Worm
33be732d4000bd08104000e89eeafff80bd08104000be7d2d400
0e849eafffff6a00e8350000064756d6d792e6578650065 3a5c776
96e646f77735c53795374656d33325c644c6c63616368655c6464
642e65786500ff254c404000ff25544040a,

Worm/MyP-arty
aa328cf24554d90b07c407eca9a4cf02a4d5a90000332c8b26904
ffffb840f97f370080040e1fba0e00b409cd1b8014c001f027c54
686973c363616e042568d54562e2c876b0ffbf0420444f53

Ricerca per firma



I Falsi positivi

		Classificazione dell'AV	
		Goodware	**Malware**
File originale	**Goodware**	True Negative (TN)	**False Positive (FP)**
	Malware	**False Negative (FN)**	True Positive (TP)

Una partita a scacchi

Encrypted Malware

- Il malware si compone di due parti: modulo di cifratura/decifratura e corpo del malware cifrato
- Quando avviene l'infezione il malware decifra il suo corpo e lo manda in esecuzione
- Se deve propagarsi ricifra il corpo con una nuova chiave

Malware Polimorfico

- Il malware usa un motore mutazionale che gli consente di modificare il suo codice senza alterare le sue funzionalità

Le due tecniche possono essere mischiate

Come si ottiene il polimorfismo?

- Un semplice esempio (in C anziché assembly per semplicità)

```
int a = 5;
printf("a vale %d\n", a);
```

```
int b = 4;
printf("a vale");
int a = b+1;
printf(" %d\n",a);
```

I Moderni Antivirus

Ricerca per pattern anziché firme fisse

Esempio: ricerca di "ciao mondo"

Supponiamo di cercare la stringa "ciao mondo" (https://codebeautify.org/string-hex-converter)

```
ciao mondo => 6369616f206d6f6e646f
```

Possibili pattern sono:

```
6369616f??6d6f6e646f  corrisponde anche a
                      ciao-mondo ciao_mondo

6369616f*6d6f6e646f   corrisponde anche a
                      ciao-_mond ciao…mondo
```

Ricerca per euristiche

Euristiche

Statiche: si decompila un programma sospetto ottenendo il suo codice sorgente. Il codice viene quindi confrontato con virus noti e presenti nel database euristico. In caso di similarità oltre una certa soglia il codice viene contrassegnato come possibile minaccia.

Dinamiche: si cerca di identificare alcuni comportamenti sospetti (modifica ad altri file, auto-replicazione, tentative di persistenza). Spesso l'analisi è operata eseguendo il sospetto in ambiente protetto così da superare le sue difese (es. decodifica del corpo, tecniche di anti-debugging e anti-reversing)

Pro: consentono di identificare virus sconosciuti

Contro: molti falsi positivi

Tecniche di evasione

Usate dal Malware per riconoscere di essere in esecuzione in un ambiente controllato (di analisi)

Circa il 98% del malware usa almeno una tecnica di evasione

Oltre il 32% usa 6 o più tecniche

Il ransomware **CERBER** ne usa 28

Alcune tecniche comuni

Interazioni con l'utente (movimenti del mouse, scrolling di documenti, …)

Caratteristiche del Sistema (programmi installati, specifiche hw, reboot del Sistema, …)

Caratteristiche di una sandboxes (file tipici, nomi dei volume, ..)

Tecniche basate sul tempo (attivazione dopo un certo tempo)

Obfuscation (cambiare il nome delle funzioni, cifratura di informazioni rilevanti)

https://evasions.checkpoint.com/

Modern era Malware Analysis

- Hiding
  - VM based viruses
  - Using Neural Networks
  - Using WebAssembly

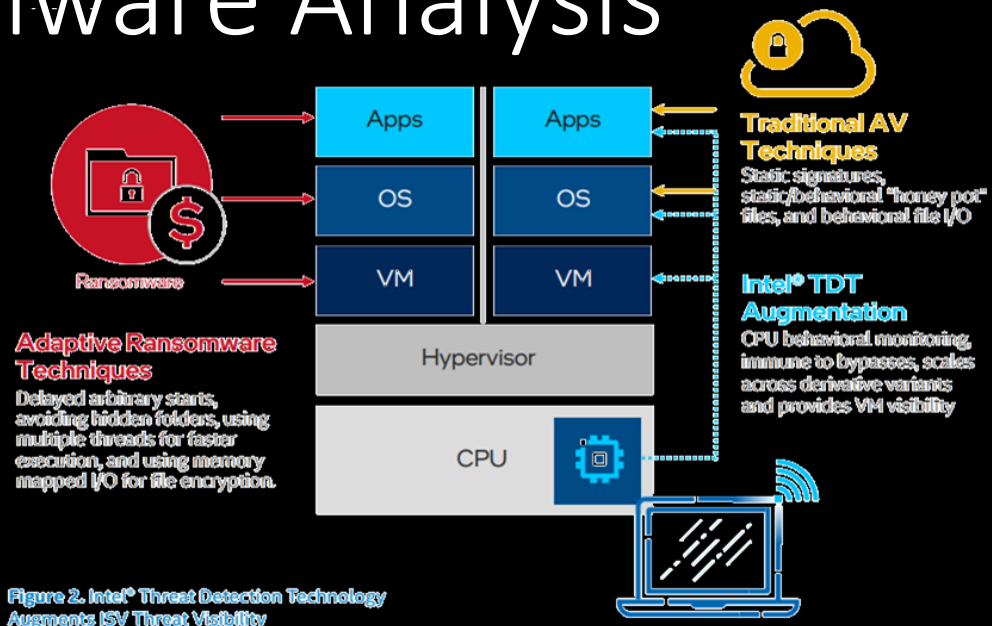


Figure 2. Intel® Threat Detection Technology Augments ISV Threat Visibility

- Hunting
  - AI/ML based
    - Pattern matching: known patterns in memory
    - Random Forest Classifier or KNN:
      - resource usage/system calls
      - string extraction
      - Entropy calculation (Shannon entropy of memory blocks)
  - CPU Support:
    - Intel Threat Detection Technology (TDT)
      - Offloads Memory Scanning and ML workloads from CPU to GPU
      - Provides CPU telemetry as a feature form ML algorithms

Casi di Studio

Clam AV

- Clam AV is a multiplatform open source AV
- Primary detection patterns:
  - MD5 hashes of known malicious binaries
  - MD5 hashes of PE sections (parts of an executable)
  - Hexadecimal signatures
  - Whitelist database of known good files
- Additional techniques
  - Logical signatures (combinations of signatures throughout logical operators)
  - Icon signatures
  - PE metadata strings
  - Container metadata

YARA rules

- YARA (http://virustotal.github.io/yara/) is a tools helping to describe malware families based on text or binary patterns
  - Each description is a rule
- Used at: Symantec, Kaspersky, McAfee, Trend Micro, ...
- YARA comes with a file scanner and a python library (yara-python extension)
- YARA-CI can be used for continuous test of YARA rules in a git-hub repository

Introduzione Malware Analysis

Il processo di analisi

Static analysis

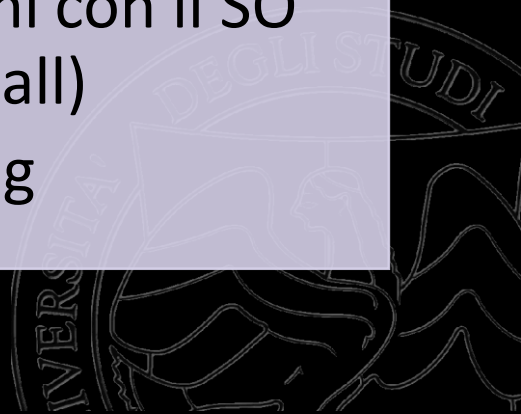
Codice non eseguito

- Documentazione
- **Stringhe, simboli, hooks, librerie, riferimenti**
- Codice Sorgente
- **Disassembly e assembly code**

Dynamic analysis

Codice eseguito

- Interazioni con l'ambiente (file system, network, registry, …)
- Interazioni con il SO (system call)
- debugging



Tecniche di analisi statica

Analisi delle stringhe

Analisi hash e altre informazioni dell'eseguibile

Analisi dell'entropia

Analisi delle stringhe

- Analizzare le stringhe può rilevare informazioni interessanti
- Esempi di stringhe interessanti:
  - bitcoin
  - locked
  - crypt/decrypt
  - mutex
  - chiavi di registro usate per la persistenza come ad esempio HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
- In alcuni casi le stringhe possono essere cifrate, prima di analizzarle si può provare a decifrarle con dei tools specific
  - FireEye Labs Obfuscated String Solver (FLOSS)

Esercizio: analisi delle stringhe

Programma di analisi:
https://www.boxentriq.com/code-breaking/text-extractor

file di test:
https://github.com/colui77/seminario/blob/ba937b1e4733bba37dcd6171e5333b79fb82fee5/test1_malware?raw=true

Esercizio: analisi con VirusTotal

Programma di analisi:
https://www.virustotal.com/gui/home/upload

file di test:
https://github.com/colui77/seminario/blob/ba937b1e4733bba37dcd6171e5333b79fb82fee5/test1_malware?raw=true

Ripetiamo l'analisi con il virus originale

Programma di analisi:
https://www.virustotal.com/gui/home/upload

file di test:
https://github.com/colui77/seminario/blob/main/test2_malware?raw=true

Analisi dinamica

- Effettueremo un'analisi dinamica automatizzata
  - Esecuzione del codice in una sandbox
    - Una sandbox è un ambiente di esecuzione isolato dal computer reale all'interno del quale possiamo eseguire il malware e monitorare sia il suo comportamento sia le sue interazioni con il resto del mondo
  - Useremo come sandbox hybrid-alanlysis

https://www.hybrid-analysis.com/

https://github.com/colui77/seminario/blob/main/test_seminario_malware?raw=true

In conclusione

- Abbiamo imparato cosa è un malware e quali sono i comportamenti tipici di un malware
- Abbiamo visto quali sono i principali tipi di malware e come si diffondono
- Abbiamo visto come funzionano gli antivirus e come i malware cercano di non farsi rivelare
- Abbiamo visto come effettuare l'analisi statica di un malware
- Abbiamo visto come effettuare un'analisi dinamica automatica di un malware
- NON SIAMO DIVENTATI IMMUNI DAI MALWARE!!! FATE ATTENZIONE!!!

Approfondimenti e contatti

Prof. Luigi Coppolino

luigi.coppolino@uniparthenope.it

DIPARTIMENTO INGEGNERIA, UNIVERSITA' DEGLI STUDI DI NAPOLI PARTHENOPE

https://ingegneria.uniparthenope.it/

Coordinatore del corso di studi Ingegneria e Scienze Informatiche per la Cybersecurity

sicurezzainformatica.uniparthenope.it

Clam AV

- Clam AV is a multiplatform open source AV
- Primary detection patterns:
  - MD5 hashes of known malicious binaries
  - MD5 hashes of PE sections (parts of an executable)
  - Hexadecimal signatures
  - Whitelist database of known good files
- Additional techniques
  - Logical signatures (combinations of signatures throughout logical operators)
  - Icon signatures
  - PE metadata strings
  - Container metadata

Installing Clam AV

- Ubuntu

```
$ sudo apt install clamav clamav-daemon –y
```

- Starting/Stopping

```
$ sudo systemctl start/stop clamav-freshclam
```

- Download fresh rules (after stopping)

```
$ sudo freshclam
```

Analyzing CLAM AV signatures

- In Linux systems typically under

  `/var/lib/clamav`

- Signatures stored in **main.cvd** and **daily.cvd** (alternately they may have .cld extensions)
  - main.cvd file primary base of signatures
  - daily.cvd incremental daily updates
- sigtool : tools provided with clamAV source to unpack the signature files:
  - `sigtool -u /var/lib/clamav/main.cvd`
  - The resulting files are archives of signatures

Signature structure

- A signature is in the form:

```
SigName:Target:Offset:HexadecimalSignature
```

  - **SigName** field is a unique, descriptive name for your signature

    Typical format for ClamAV signature names in the official signature databases:

    ```
    {platform}.{category}.{name}-{signature id}-{revision}
    ```

  - **Target** parameter can be any of

0 = Any file type
1 = Windows PE
2 = OLE (e.g. Office, VBA)
3 = Normalized HTML
4 = E-mail file (e.g. RFC822 message, TNEF)
5 = Image files (e.g. jpeg, png)
6 = ELF
7 = Normalized ASCII file
8 = Unused
9 = Mach-O binaries (new in v0.96)

ASCII rules

- Assuming to search for files containing “hello world” string we can create a signature as follows

```
TestHelloWorld:0:*:68656c6c6f20776f726c64
```

- **68656c6c6f20776f726c64** is the hexadecimal for “Hello world”
  - We can use the sigtool to obtain it as follows

```
$ sigtool --hex-dump
hello world
68656c6c6f20776f726c640a
```

Using wildcards

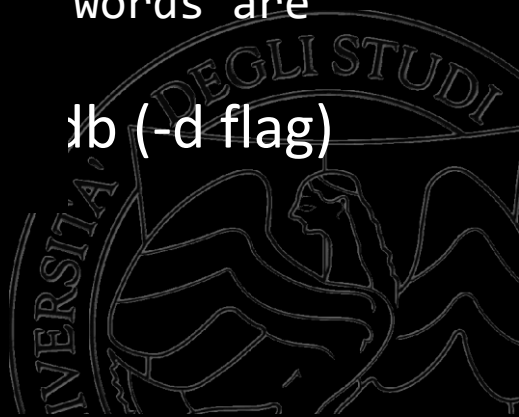
- It is possible to use wildcards
  - **??** -> any byte value (00 to FF)
    - 68656c6c6f**??**776f726c64
    - “hello” , “world” separated by any character
  - ***** -> any value
    - 68656c6c6f*****776f726c64
    - “hello” , “world” separated by any number of characters
- It is possible to define an offset or an interval for the offset
  - TestHelloWorldOffset45:0:**45**:68656c6c6f20776f726c64
  - TestHelloWorldBetween200And250:0:**200,50**:68656c6c6f20776f726c64

Creating a new signatures db

- Signatures included in a `.ndb` file
- Example
  - add the `TestHelloWorldAnyDistance:0:*:68656c6c6f*776f726c64` signature to the `clam_helloworld.ndb` file
  - cre d
    cor
    “ for ‘hello’
    a words are
    t
  - No db (-d flag)

```
osboxes@osboxes:~$ clamscan -d clam_helloworld.ndb text.txt
/home/osboxes/text.txt: TestHelloWorldAnyDistance.UNOFFICIAL FOUND

----------- SCAN SUMMARY -----------
Known viruses: 1
Engine version: 0.103.6
Scanned directories: 0
Scanned files: 1
Infected files: 1
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
Time: 0.009 sec (0 m 0 s)
Start Date: 2022:07:03 12:28:07
End Date:   2022:07:03 12:28:07
osboxes@osboxes:~$
```



Binary signatures

- Let's consider the following snippet from an MS Office malware

Offset	Instruction	Byte codes
00000000	xor ecx,ecx	33c9
00000002	mov cx,0x147	66b94701
00000006	xor byte [edx+ecx],0xe9	80340ae9
0000000A	loop 0xfffffffc	e2fa
0000000C	jmp 0xc	eb0a

- The related rule will be

```
ShellcodeXOR:0:*:33c966b9470180340ae9e2faeb0a
```

Parametric signatures

- If we want a signature which is independent from some parameters, we can use the wildcards
- As an example for the previous code we can use the template

```
xor ecx, ecx
mov cx, ??
xor byte [edx+ecx], ??
loop ??
jmp ??
```

- And thus the signature

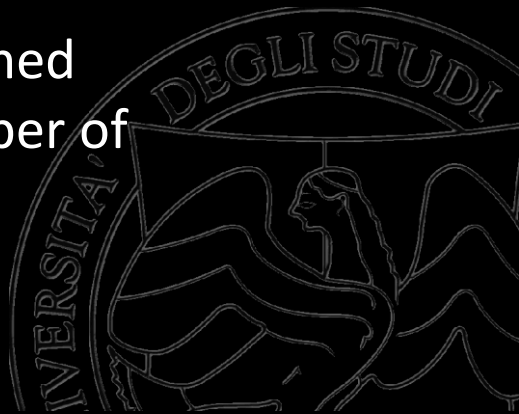
```
shellcode_xor:0:*:33c966b9???80340a??e2??eb
```

Logical Signatures

- Introduced with ClamAV v0.96
- Rules are triggered when multiple conditions apply

```
SigName;Target;Expression;Sig0;Sig1;..;SigN
```

  - `SigName` and `Target` as before
  - `Expression` is a logical expression using 0 to N as operands, each representing the corresponding Signature (0 for Sig0, 1 for Sig1, …)
  - Using `&` and `|` , signatures 0 …N can be combined
  - =, <, and > operators, used to control the number of occurrences of each signature



Logical Signature examples

- Searching for “hello” and “world” no matter their relative order

```
HelloWorldLogic;Target:0;0&1;68656c6c6f;776f726c64
```

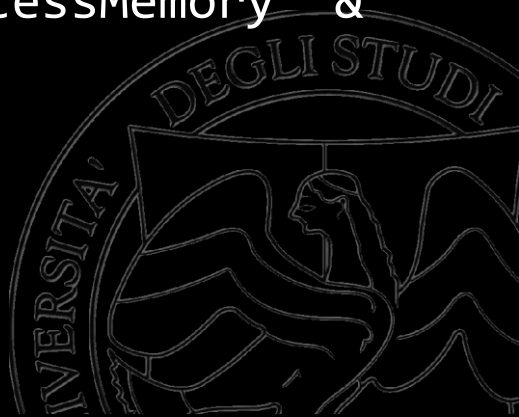
- Searching for “hello” at least two time and three “world”

```
HelloWorldLogic;Target:0;(0>2)&(1=3);68656c6c6f;776f726c64
```

A realistic example 1/2

- Malware that uses code injection to execute within another process
- Detection criteria
  - `WriteProcessMemory` and `CreateRemoteThread` strings: API functions used to perform the injection
  - `SeDebugPrivilege` string: debug system priviledge system privilege, that a process must enable before calling either of the above API functions
  - A string such as `iexplore.exe` or `explorer.exe`: The name of the target process
- Detection logic:

```
(“iexplore” | “explorer.exe”) & (“WriteProcessMemory” & “CreateRemoteThread” & “SeDebugPrivilege”)
```



A realistic example 2/2

- The final logical signature

```
ProcessInjector;Target:1;(0|1)&(2&3&4);696578706c6f72652e657865;\
6578706c6f7265722e657865;\
536544656275675072697696c656765; \
43726561746552656d6f746546872656164; \
57726974655072f636573734d656d6f7279
```

  - We are assuming no-packeter used

YARA rules

- YARA (http://virustotal.github.io/yara/) is a tools helping to describe malware families based on text or binary patterns
  - Each description is a rule

- Used at: Symantec, Kaspersky, McAfee, Trend Micro, …
- YARA comes with a file scanner and a python library (yara-python extension)
- YARA-CI can be used for continuous test of YARA rules in a git-hub repository

YARA rules

Rule description (YARA keywords not accepted):
alphanumeric but first character not a digit

stores additional information
about the rule.

Strings to look for
Can be
-text
-hex (raw bytes)
-regular expressions

```
rule silent_banker
{
  meta:
      description = "This is just an example“
      threat_level = 3
      in_the_wild = true
  strings:
      $a = {6A 40 68 00 30 00 00 6A 14 8D 91}
      $b = {8D 4D B0 2B C1 83 C0 27 99 6A 4E 59 F7 F9}
      $c = "UVODFRYSIHLNWPEJXQZAKCBGMT" ascii wide nocase
  condition:
      $a or $b or $c
}
```

Modifiers:

```
$a=”mlwstr” fullword
$a=”mlwstr” wide
$a=”mlwstr” wide ascii
a=”mlwstr” nocase
```

the rule result is true if…

```
uint16(0) == 0x5A4D
(filesize<5MB)
2 of ($a,$b,$c)
$a and not $b
(#a > 0) and (#b == 3)
```

Sample string patterns

- ASCII string ‘WriteProcessMemory’

$a={57 72 69 74 65 50 72 6f 63 65 73 73 4d 65 6d 6f 72 79 0a}

- Possible variants

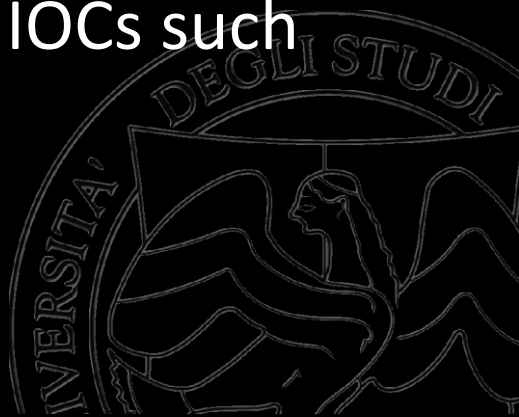
$a={57 72 69 74 65 50 72 6f ?? ?5 73 73 4d 65 6d 6f 72 79 0a} -> wildcard

$a={57 72 69 [2-5] 50 72 6f 63 65 73 73 4d 65 6d 6f 72 79 0a} -> offset intervals

$a={57 72 (01 02 | 03 04) 6f 63 65 73 73 4d 65 6d 6f 72 79 0a} -> alternatives

Useful strings

- **Mutexes** – used by malware to check if a device has already been compromised Rare and unusual user agents – Identified when malware communicates with its C2 infrastructure.
- **Registry keys** –created by malware as a persistence mechanism.
- **Encrypted config strings** – Malware will often encrypt its config which contains useful IOCs such as IP addresses and domains.



Using parts of the PE file

- Possible by adding the syntax ‘import pe’ to the start of a YARA rule
  - pe.**imports**(“winhttp.dll”, “WinHttpConnect”)
  - pe.**machine** == pe.MACHINE_AMD64
  - pe.**version_info**[“CompanyName”] contains AmAZon.cOm
  - pe.**imphash**() == “0E18F33408BE6E4CB217F0266066C51C”
  - pe.**section**[0].name == “code”

YARA in practice

- $ yara rule.yara malicious.exe
- YARA-CI
  - Reduce false positives: Compares a rule against a db of 1 million know files
  - Reduce false negatives: in the meta section it is possible to include the hash of files that must be detected as malware…YARA-CI downloads the files from VirusTotal and checks whether they trigger or not the detection

```
rule Agent_BTZ_Proxy_DLL_1 {
   meta:
      description = "Detects Agent-BTZ Proxy DLL - activeds.dll"
      license = "https://creativecommons.org/licenses/by-nc/4.0/"
      author = "Florian Roth"
      reference = "http://www.intezer.com/new-variants-of-agent-btz-comrat-found/"
      date = "2017-08-07"
      hash1 = "9c163c3f2bd5c5181147c6f4cf2571160197de98f496d16b38c7dc46b5dc1426"
      hash2 = "628d316a983383ed716e3f827720915683a8876b54677878a7d2db376d117a24"
   strings:
      $s1 = "Software\\Microsoft\\Windows\\CurrentVersion\\Explorer\\Modules" fullword wide
   condition:
      ( uint16(0) == 0x5a4d and filesize < 300KB and all of them and pe.exports("Entry") )
}
```

YARA and ClamAV

- ClamAV version 0.99 and above can process YARA rules
- ClamAV virus database file names ending with ".yar" or ".yara" are parsed as yara rule files
- ClamAV definitions can be translated in YARA rules
  - https://github.com/sec51/clamav-yara