

# Approfondimento Cybersecurity

---

## PHISHING E RANSOMWARE

A cura di:

- Davide Flagiello  
A13002377

## Introduzione

---

# PHISHING E RANSOMWARE

«Gli attacchi di **phishing** utilizzano e-mail fraudolente, SMS, telefonate o siti Web per indurre le persone a condividere dati sensibili, scaricare malware o esporsi in altro modo al crimine informatico».

In un tipico attacco di phishing, l'attaccante si finge di essere qualcuno di cui la vittima si fida. Invia un messaggio che invita la vittima a pagare, aprire un allegato o fare click su un collegamento che porta ad un sito facsimile di banche o simili per rubare dati sensibili o far scaricare file malevoli.

Il **phishing** è popolare tra i criminali informatici ed è molto efficace. Secondo il report Cost of a Data Breach di **IBM**, il phishing è il vettore di violazione dei dati più comune, e rappresenta il 16% di tutte le violazioni. [Fonte](#)

«Con la parola **ransomware** viene indicata una classe di malware che rende inaccessibili i dati dei computer infettati e chiede il pagamento di un riscatto, in inglese ransom, per ripristinarli.»

Tecnicamente sono trojan crittografici e hanno come unico scopo l'estorsione di denaro, attraverso un sequestro di file, che mediante la cifratura li rende inutilizzabili.

Usualmente i ransomware sono diffusi attraverso il phishing.

# Simulazione attacco phishing

---

In questo caso per simulare l'attacco phishing ho utilizzato il servizio mail di libero.it. Nella realtà dei fatti l'email degli attaccanti sono fasulle ed hanno nomi molto simili alle vere email di una banca o organizzazioni a cui facciamo affidamento così da non destare sospetti nella vittima.


---

## Sospensione conto corrente

**BL** Banca della Campania L. Vanvitelli <davidets23@libero.it>  
A userest12345@libero.it

INDIETRO



 1 allegato ► Scarica Salva in Drive

In allegato le cause che hanno portato alla sospensioni del suo conto corrente

[Accedi](#)

Gli oggetti dell'email e la descrizione sono in genere fatte per allarmare l'utente e indurlo, in questo caso, a entrare nel sito per immettere i dati del proprio account. Inoltre in allegato ho inserito un semplice programma che simula un ransomware per crittare i file del malcapitato e chiedere un riscatto.

Generalmente ad un attacco phishing si accompagna un attacco di **email spoofing** così da nascondere la vera email(falsa) e utilizzare una di vere associazioni o siti.

# Fasi dell'attacco phishing

Generalmente le fasi di un attacco phishing sono:

- Pianificazione
- Creazione dell'email
- Invio dell'email
- Raccolta delle credenziali

In questo ho scritto un semplice codice in python per inviare l'email all'utente «vittima» contenente l'allegato per l'attacco ransomware e il collegamento al sito truffa.

```
# Dati dell'email
spoofed_sender_email = 'davidets23@libero.it' # Indirizzo email di libero
spoofed_sender_name = 'Banca della Campania "L.Vanvitelli"' # Nome falsificato
receiver_email = 'usertest12345@libero.it'
subject = 'Sospensione conto corrente'
body = 'In allegato le cause che hanno portato alla sospensioni del suo conto corrente'
link_text = 'Accedi!'
link_url = 'http://localhost/login_system'
attachment_path = r'conto_corrente.pdf.exe' # Percorso dell'allegato

# Chiede la password
password = getpass.getpass(prompt='Inserisci la password per l'email: ')

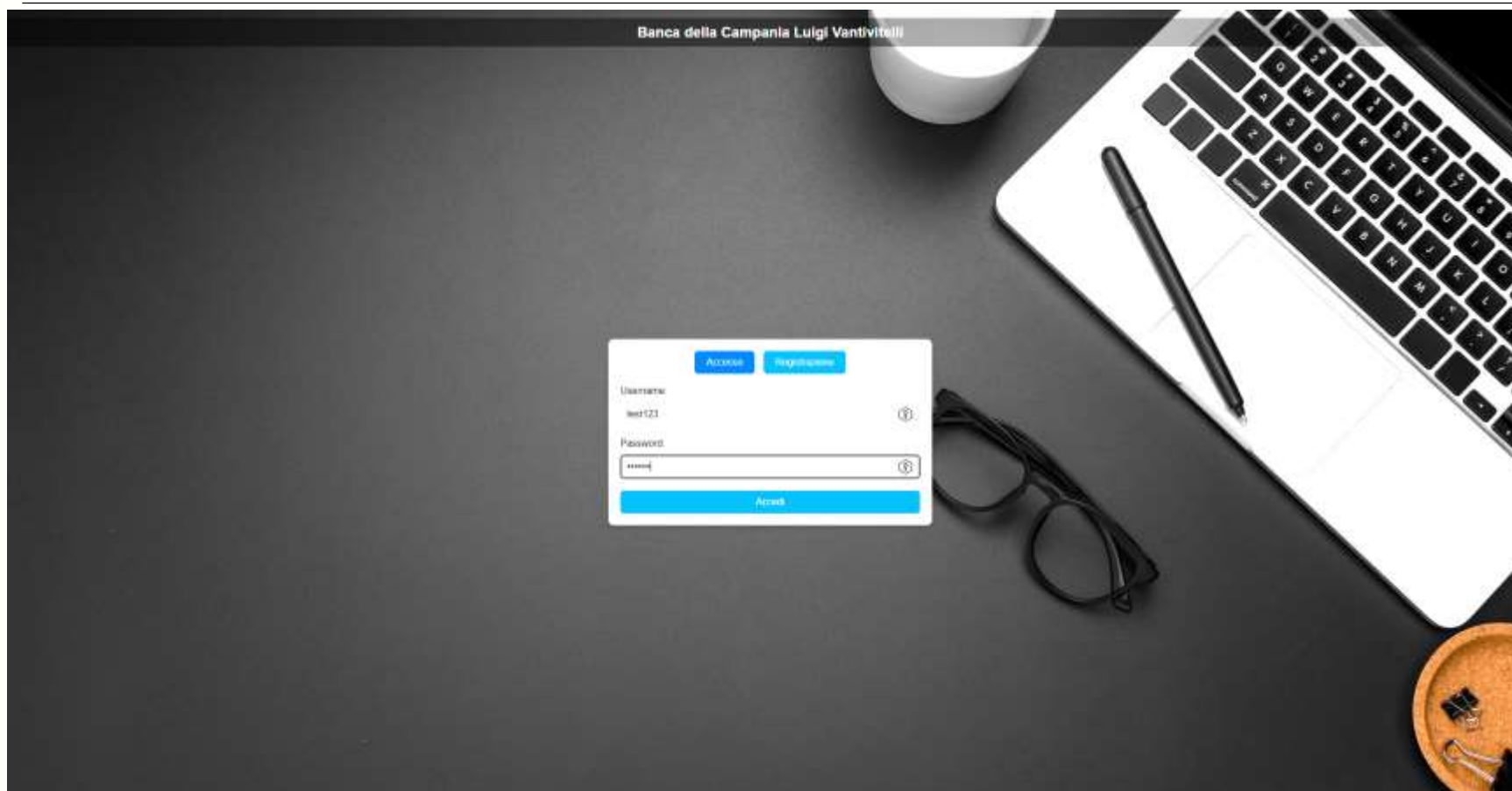
# Invio email
send_email(spoofed_sender_email, spoofed_sender_name, receiver_email, subject, body, password, link_text, link_url, attachment_path)
```

Parte del codice per i  
dati da inserire

```
PS C:\universita\terzo anno\cybersecurity approfondimento> python phishing.py
Inserisci la password per l'email:
Inizio invio email...
Allegato Conto_corrente.pdf.exe aggiunto con successo
Connessione al server SMTP...
Connessione TLS avviata.
Login effettuato con successo
Email inviata con successo a usertest12345@libero.it
```

Esecuzione del codice

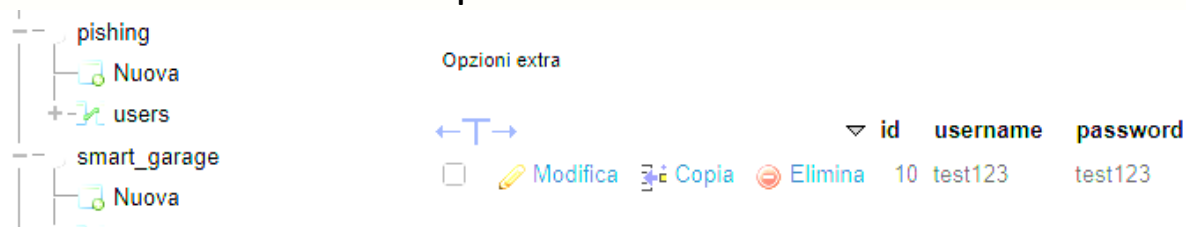
# Fasi dell'attacco phishing



Il **link** porta ad un ipotetico sistema di login di un sito facsimile di un ipotetica «banca della campania Luigi Vanvitelli». In questo caso la vittima, ignara che si tratti di un sito fake, tenterà di loggare con i propri dati ma quest'ultimi saranno invece salvati in un database dell'attaccante e usati poi per scopi malevoli. L'utente verrà poi reindirizzato al sito ufficiale(dipartimento di ingegneria in questo caso) così da far pensare che si sia trattato di un errore di connessione e non destare sospetti.

# Fasi dell'attacco phishing

## Database che salva i dati personali



id	username	password
10	test123	test123

Reindirizzamento al sito del dipartimento di ingegneria quando si immettono i dati e si clicca «Accedi»

```
13 if ($stmt->execute()) {
14     // Reindirizza a un sito dopo il login riuscito
15     header("Location: https://www.ingegneria.unicampania.it");
16     exit();
17 } else {
18     echo "Errore: " . $stmt->error;
19 }
```

# Fasi dell'attacco ransomware

---

Le fasi di un attacco ransomware prevedono:

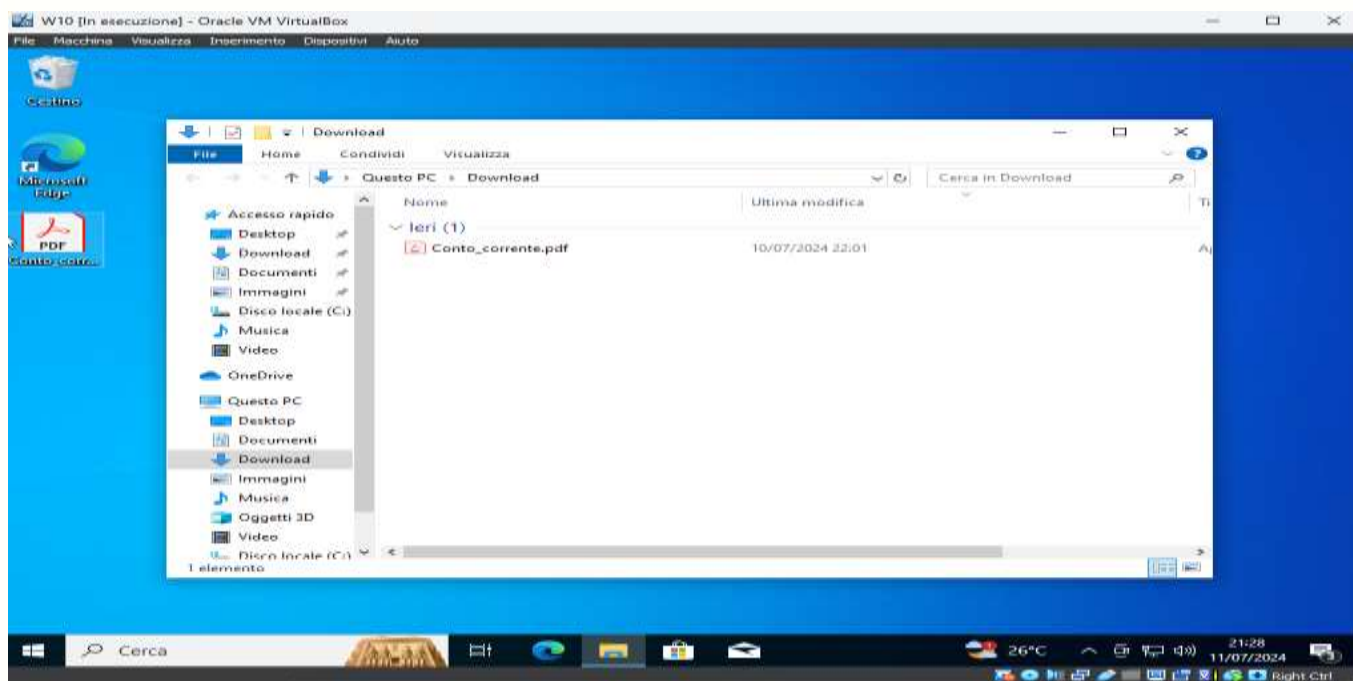
- Infezione iniziale
- Esecuzione del payload
- Crittografia dei file
- Richiesta di riscatto

L'infezione iniziale e' iniziata con la fase di phishing. Dopodiche l'esecuzione del payload viene eseguita dall'utente quando apre il file.

Questo tipo di attacco puo' causare gravi danni come perdita di dati, interruzioni di attivita' aziendali, danni alla reputazione e costi di riscatto e ripristino.

# Fasi dell'attacco ransomware

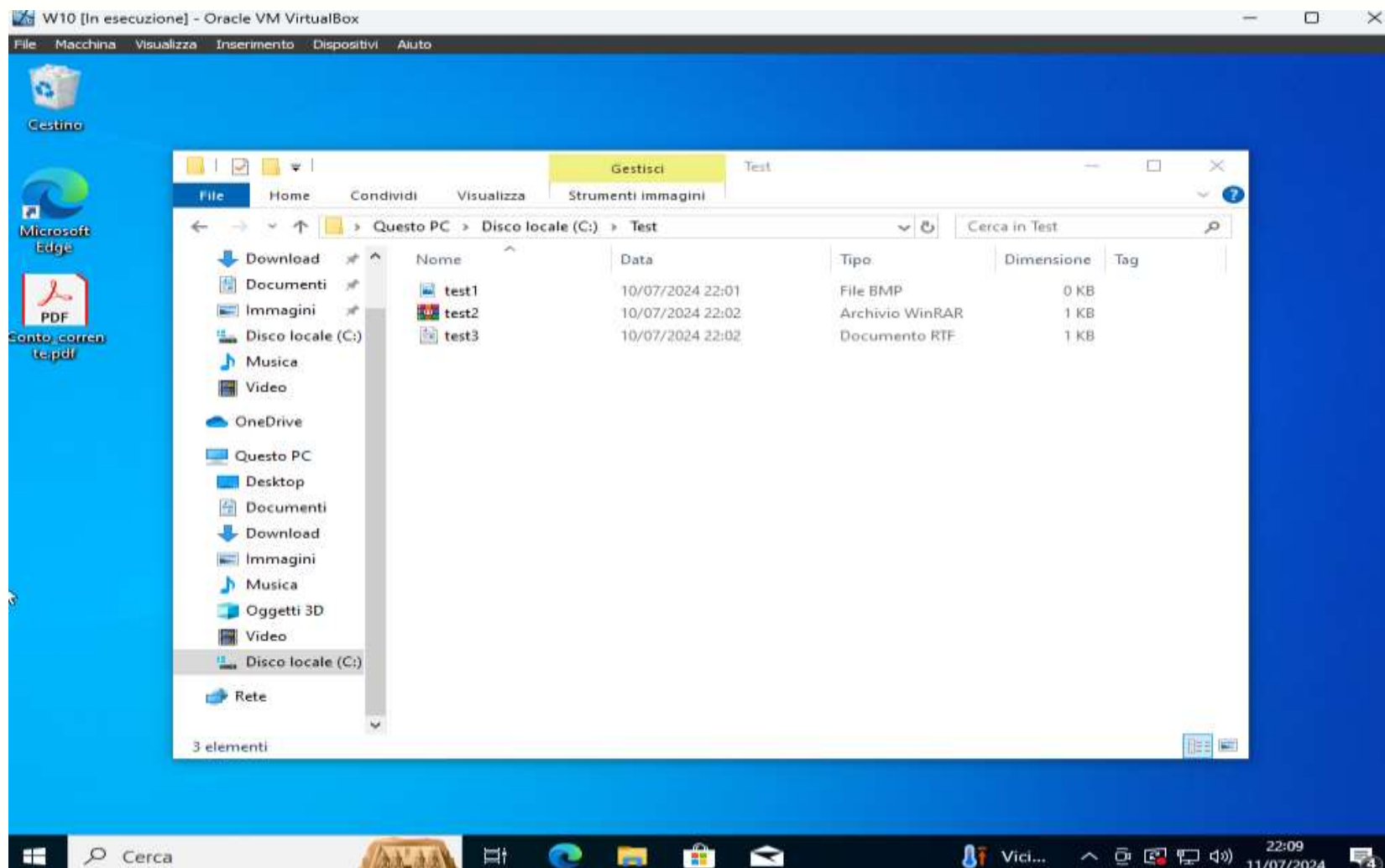
Per quanto riguarda il ransomware, invece, l'allegato contiene un codice python mascherato come un semplice documento pdf.



L'obiettivo è quello di far scaricare il file all'utente e farlo aprire. Il file una volta aperto aprirà un file pdf vuoto e nel frattempo esegue il codice in background facendo in modo di criptare la directory «C:\test» della VM. Inoltre crea un semplice .txt per le istruzioni di riscatto.

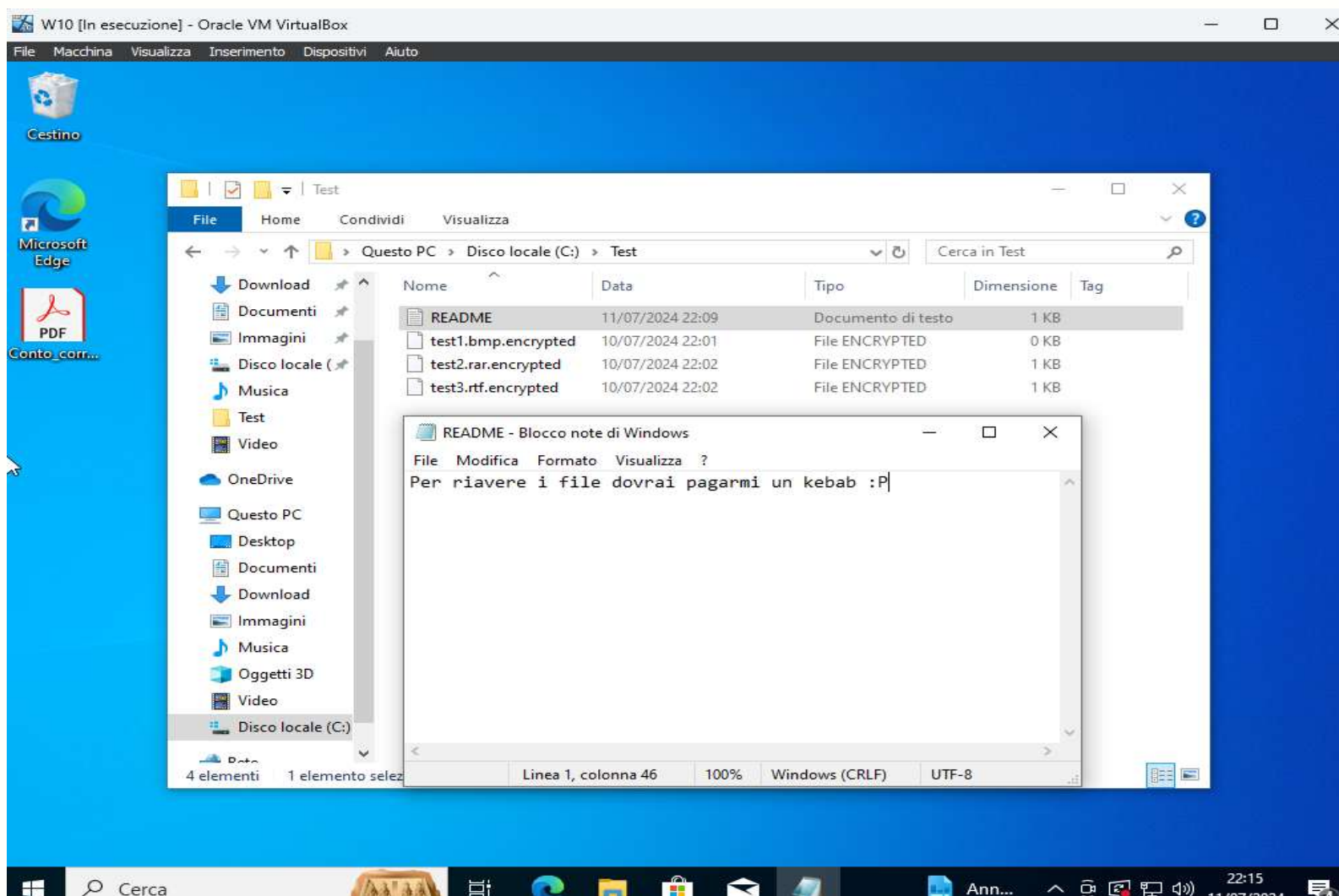


# Fasi dell'attacco ransomware



Prima dell'apertura del file «Conto\_corrente.pdf»

# Fasi dell'attacco ransomware



Dopo l'apertura del file

## Fasi dell'attacco ransomware

---

In questo caso ho «sfruttato» il fatto che normalmente windows nasconde l'estensione dei file agli utenti e difatti ho rinominato il file «conto\_corrente.pdf» e modificato l'icona mettendo quella del pdf. In realta' pero' il file e' un eseguibile.

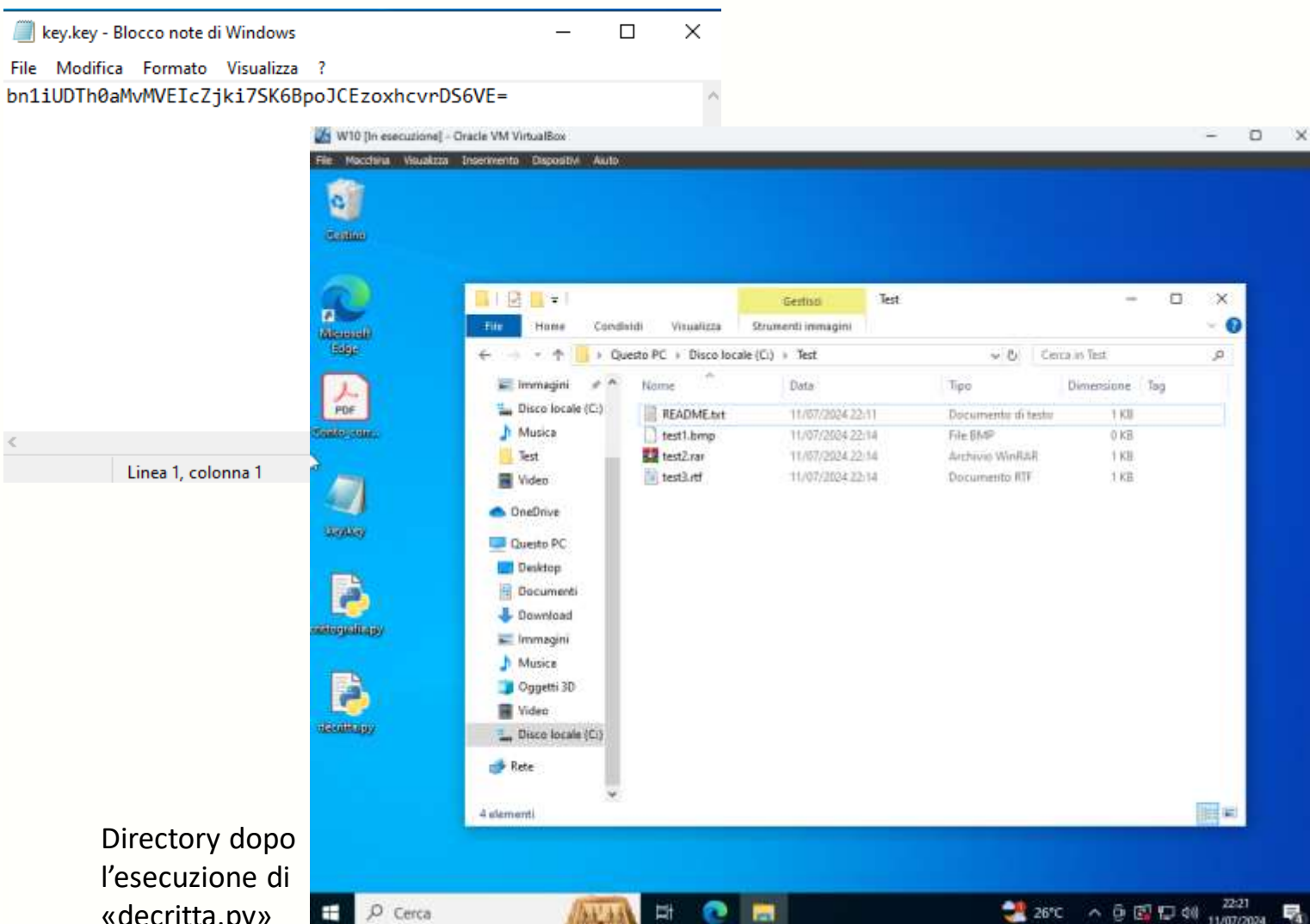
Ad alti livelli questa tecnica e' chiamata **steganografia**. «Nel campo della cybersecurity, la **steganografia** è uno strumento spesso utilizzato da criminali informatici, che possono nascondere malware o ransomware all'interno di file apparentemente innocui, al fine di attaccare un bersaglio». Per esempio, potrebbero nascondere dati, occultare uno strumento dannoso o inviare istruzioni per server di comando e controllo.

Questo codice non e' un vero e proprio ransomware poiche non utilizza una chiave per crittare ma si limita a cambiare l'estensione dei file rendendoli cosi inutilizzabili. Un vero ransomware utilizza delle chiavi per far si che solo con quest'ultime sia possibile recuperare i file.



Il file critta.py fa proprio questo, critta i file utilizzando una chiave che salva in un file .txt. Poi sara' decritta.py che attraverso la chiave salvata riesce a decrittare i file. In questo caso ho utilizzato una crittografia simmetrica.

# Fasi dell'attacco ransomware



## Prevenzione e difesa

---

### **Prevenzione attacco phishing**

1. Controllare sempre il link e il mittente della mail prima di cliccare qualunque indirizzo, ancora meglio non cliccare sul link, ma copiarlo invece nella barra dove si inserisce l'indirizzo del browser.
2. Prima di cliccare su un qualunque link, bisogna verificare che l'indirizzo mostrato è davvero lo stesso indirizzo Internet al quale il link condurrà. Un controllo che può essere effettuato in modo semplice, passando il mouse sopra il link stesso.
3. Usare solo connessioni sicure, in particolar modo quando si accede a siti sensibili. Controllare che la connessione sia HTTPS e verificare il nome del dominio all'apertura di una pagina. Questi fattori sono importanti soprattutto quando si usano siti che contengono informazioni sensibili, come pagine per l'online banking, i negozi online, i social media e via scorrendo.
4. Non condividere mai i propri dati sensibili con una terza parte. Le compagnie ufficiali non chiedono mai informazioni del genere via email.
5. Implementazione di soluzioni di sicurezza email e autenticazione a due fattori (2FA)

### **Prevenzione attacco ransomware**

1. La miglior protezione è la prevenzione. Il primo passo da fare è aggiornare sempre sia il nostro antivirus che il sistema operativo.
2. Vitale è anche il backup dei dati, cioè copie funzionanti e recenti dei propri file. In questo modo, se il ransomware dovesse infettare il sistema, una copia dei dati rimarrebbe protetta, dandoci l'opportunità di ripristinarli all'occorrenza. Altrettanto importante è la protezione del backup, che deve essere isolato e non accessibile da un qualsiasi utente collegato in rete. Abbiamo casi di backup non protetto sul quale il Ransomware è riuscito ad accedere ed a criptare i dati. A quel punto la vittima si trova alla mercé dell'attaccante.
3. Se si viene attaccati, le buone pratiche dicono che non bisogna mai pagare il riscatto.

# Conclusione

---

Il test effettuato e' stato eseguito con l'utilizzo di una macchina virtuale con windows 10 installato e un altro sistema con cui inviare l'email. Il sito facsimile e' stato realizzato con xampp utilizzando php, html e css. L'invio dell'email e il file per simulare un ransomware sono stati invece scritti in python. La steganografia del file pdf invece l'ho simulata con l'utilizzo di winrar attraverso questa [guida](#).

[Link](#) alla repository di github.

Tutti i riferimenti sono presi da:

- Wikipedia
- IBM
- Cisco
- Python documentation
- Cybersecurity 360