

ESERCIZIO S5_L5 CAMPAGNA_PHISHING

Descrizione:

In questo progetto viene simulata una campagna di phishing etico a scopo didattico, realizzata con l'ausilio della piattaforma GoPhish. L'obiettivo della campagna è riprodurre un attacco mirato, impersonando un tecnico affiliato al supporto di Microsoft365.

Obiettivo della campagna

L'obiettivo simulato è ottenere l'accesso a credenziali aziendali (email e password) da parte di dipendenti ignari, sfruttando un contesto urgente e plausibile: l'aggiornamento del sistema di di Microsoft365.

Tecnica di Ingegneria Sociale

La simulazione ha, in un contesto reale, l'obiettivo di:

1. Individuare su LinkedIn il responsabile IT reale di varie aziende strutturate.
2. Esplorazione della rete dei suoi collegamenti e del sito aziendale per identificare le email ed i contatti di potenziali dipendenti con ruoli nei reparti meno formati in ambito security.
3. Creazione di un pretesto credibile, in cui il mittente dichiara di:
 - Lavorare in collaborazione con il reparto IT aziendale.
 - Avere ricevuto istruzioni da parte del responsabile IT per rivolgersi direttamente ai vari destinatari.
4. Invio di un'email fittizia in cui si chiede di effettuare l'accesso a un nuovo portale per aggiornamento credenziali, minacciando in caso contrario la sospensione dei servizi Microsoft e la cancellazione della casella email.

Email inviata

L'email è firmata da un tecnico fittizio, Marco Rizzi, operante per conto del supporto Microsoft365. Il dominio mittente è stato registrato appositamente per lo scopo (auth365-sync.it) e configurato con Cloudflare Tunnel per renderlo pubblicamente accessibile.

Landing Page

È stata realizzata una pagina HTML custom, ispirata al portale Microsoft365 ma priva di riferimenti ufficiali, caricata come landing page su GoPhish. La pagina raccoglie email e password tramite form **POST**, in un ambiente sicuro e ad uso esclusivamente didattico.

Tecnologie utilizzate

- [✓] Gophish per gestione campagna e raccolta dati
- [✓] Cloudflare Tunnel per esporre il server locale
- [✓] Dominio personalizzato auth365-sync.it
- [✓] Ricognizione OSINT su LinkedIn per simulare targeting reale
- [✓] Server SMTP fornito dal docente (mail12.dominiofaiDATE.com)

Contesto etico e formativo

Tutti gli elementi della campagna sono stati realizzati in ambienti controllati e con finalità formativa, come parte del programma di consapevolezza alla sicurezza informatica (security awareness). Nessuna attività è stata rivolta a soggetti reali esterni o inconsapevoli.

TESTO DELL'EMAIL DI PHISHING

Gentile dipendente,

Mi chiamo Marco Rizzi e collaboro con il team tecnico Microsoft365. In queste settimane stiamo implementando un aggiornamento progressivo delle credenziali e dell'interfaccia di accesso per alcune aziende, tra cui la vostra.

In collaborazione con il vostro responsabile IT ("*nome ottenuto tramite LinkedIn*"), ci è stato comunicato che avremmo potuto rivolgerci direttamente a voi per formalizzare il funzionamento del nuovo portale d'accesso iniziale.

Il suo account risulta ancora non allineato con la nuova interfaccia, per cui la invitiamo a completare l'accesso entro oggi alle 17:00 tramite il portale dedicato:

👉 Verifica l'accesso ora: {{.URL}}

⚠ In caso di mancato aggiornamento, l'accesso ai servizi Microsoft365 (Teams, Outlook, SharePoint) sarà sospeso e tutte le email al suo interno saranno cancellate in automatico dal sistema.

Grazie per la collaborazione.

Marco Rizzi
Supporto Tecnico Microsoft365
m.rizzi@ms365-syncsupport.it
Operante in collaborazione con il vostro reparto IT

ANALISI DELLO SCENARIO

Perché lo scenario è credibile

- Microsoft Teams è uno strumento largamente utilizzato in contesti aziendali e accademici, e gli utenti sono abituati a ricevere notifiche di aggiornamenti.
- Il linguaggio formale, l'urgenza apparente e il riferimento a una "nuova interfaccia" rendono l'email verosimile.
- Il mittente ha un nome plausibile ("IT Support - Microsoft365") e un dominio apparentemente coerente (ma falso).

Campanelli d'allarme evidenti

1. **URL sospetto e non ufficiale**
Il link presente nell'email non è un dominio Microsoft ufficiale. L'uso di "secure" e "update" è una tecnica comune per mascherare link malevoli.
2. **Senso di urgenza e minaccia velata**
Frase come "entro le ore 17:00 di oggi" e "le email al suo interno saranno cancellate" inducono la vittima a cliccare impulsivamente senza riflettere.
3. **Email di mittente non verificabile**
L'indirizzo email non è un dominio aziendale riconosciuto.

Varianti per simulazione avanzata (opzionali)

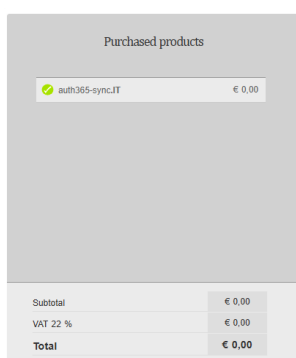
- Inserire un allegato PDF con il link mascherato come "manuale d'uso della nuova interfaccia".
- Includere nel corpo email il logo di Microsoft Teams (per aumentare la credibilità visiva).
- Simulare anche una pagina di login finta graficamente simile al portale Microsoft (per esercizio, non per uso reale).

PROCESSO CREAZIONE SERVER PHISHING

1. Registrazione dominio

- Nome scelto: `auth365-sync.it`, simile a Microsoft365 per aumentarne la credibilità.

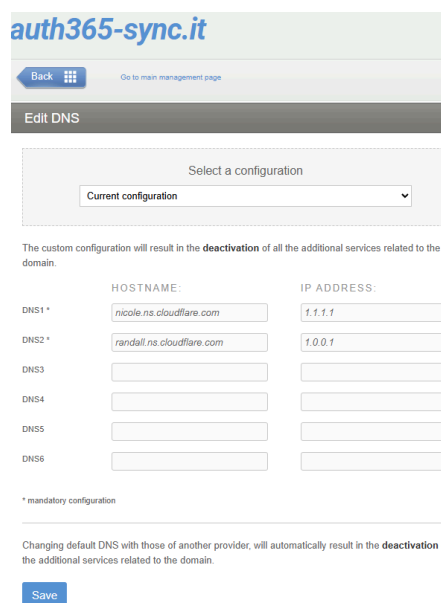
Iniziamo acquistando un dominio con nome simile alla truffa che andremo ad effettuare:



2. Configurazione DNS via Cloudflare

- Collegamento dominio a Cloudflare
- Aggiunta record CNAME `login` puntato al tunnel generato

Configuriamo poi i server DNS per far gestire il servizio da Cloudflare:



auth365-sync.it

Back Go to main management page

Edit DNS

Select a configuration

Current configuration

The custom configuration will result in the **deactivation** of all the additional services related to the domain.

	HOSTNAME:	IP ADDRESS:
DNS1 *	nicole.ns.cloudflare.com	1.1.1.1
DNS2 *	randall.ns.cloudflare.com	1.0.0.1
DNS3		
DNS4		
DNS5		
DNS6		

* mandatory configuration

Changing default DNS with those of another provider, will automatically result in the **deactivation** of the additional services related to the domain.

Save

****3. Installazione Cloudflare Tunnel su Kali****

- Clonazione repository da GitHub
- Comando di registrazione e ottenimento ID

Scarichiamo cloudflare su kali tramite github ed installiamolo:

```
(kali㉿kali)-[~]
$ wget https://github.com/cloudflare/cloudflared/releases/latest/download/cloudflared-linux-amd64.deb
sudo dpkg -i cloudflared-linux-amd64.deb

--2025-08-01 07:17:25-- https://github.com/cloudflare/cloudflared/releases/latest/download/c
Resolving github.com (github.com) ... 140.82.121.3
Connecting to github.com (github.com)|140.82.121.3|:443 ... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://github.com/cloudflare/cloudflared/releases/download/2025.7.0/cloudflared-l
--2025-08-01 07:17:25-- https://github.com/cloudflare/cloudflared/releases/download/2025.7.0
Reusing existing connection to github.com:443.
HTTP request sent, awaiting response... 302 Found
Location: https://release-assets.githubusercontent.com/github-production-release-asset/106867
-ab1947aa7ab06sktid=398a6654-997b-47e9-b12b-9515b896b4de6skt=2025-08-01T10%3A51%3A00Z&sk=202
29tIiwia2V5Ijoia2V5MSIsImV4cCI6MTc1NDA0NzM0NSwibmJmIjoxNzU0MDQ3MDQ1LCJwYXRoIjoicmVsZWZzZWZzc2
eam%2Foctet-stream
--2025-08-01 07:17:25-- https://release-assets.githubusercontent.com/github-production-relea
-5711-43a1-aedd-ab1947aa7ab06sktid=398a6654-997b-47e9-b12b-9515b896b4de6skt=2025-08-01T10%3A5
NlcmNvbnRlbnQuY29tIiwia2V5Ijoia2V5MSIsImV4cCI6MTc1NDA0NzM0NSwibmJmIjoxNzU0MDQ3MDQ1LCJwYXRoIjo
ion%2Foctet-stream
Resolving release-assets.githubusercontent.com (release-assets.githubusercontent.com) ... 185.
Connecting to release-assets.githubusercontent.com (release-assets.githubusercontent.com)|185
HTTP request sent, awaiting response... 200 OK
Length: 20166246 (19M) [application/octet-stream]
Saving to: 'cloudflared-linux-amd64.deb'

cloudflared-linux-amd64.deb 100%[=====
2025-08-01 07:17:29 (5.03 MB/s) - 'cloudflared-linux-amd64.deb' saved [20166246/20166246]

Selecting previously unselected package cloudflared.
(Reading database ... 441934 files and directories currently installed.)
Preparing to unpack cloudflared-linux-amd64.deb ...
Unpacking cloudflared (2025.7.0) ...
Setting up cloudflared (2025.7.0) ...
Processing triggers for man-db (2.13.1-1) ...
Processing triggers for kali-menu (2025.3.0) ...
```

****4. Configurazione file `config.yml`****

- Impostazione hostname, tunnel ID, credenziali

****5. Avvio del tunnel e test accessibilità da remoto****

Logghiamo il seguente comando:

```
(kali㉿kali)-[~]
$ cloudflared tunnel login
A browser window should have opened at the following URL:

https://dash.cloudflare.com/argotunnel?aud=6callback=https%3A%2F%2Flogin.cloudflareaccess.org%2F_PKGMGTUaP4Pj-SITloM5n04UB2qDw6fQ4ILHmS05R0%3D

If the browser failed to open, please visit the URL above directly in your browser.
2025-08-01T11:44:05Z INF You have successfully logged in.
If you wish to copy your credentials to a server, they have been saved to:
/home/kali/.cloudflared/cert.pem
```

Riceveremo dunque le credenziali e l'ID che ci servirà per la registrazione tramite il portale.

```
(kali㉿kali)-[~]  
$ cloudflared tunnel create gophish-tunnel  
Tunnel credentials written to /home/kali/.cloudflared/75cdf9f1-0855-4428-9fae-b704a41dd8d0.json. cloudflared chose th  
Created tunnel gophish-tunnel with id 75cdf9f1-0855-4428-9fae-b704a41dd8d0
```

Una volta attivato il servizio Cloudflare premiamo su "Add Record" all'interno del menù di gestione del DNS:

DNS

Records

Configure DNS records and review [proxy status](#) of your hostnames.

[DNS documentation](#)

Recommended steps to complete zone set-up

[Hide](#)

- ✓ Add an A, AAAA, or CNAME record for **www** so that **www.auth365-sync.it** will resolve.
- ✓ Add an A, AAAA, or CNAME record for your **root domain** so that **auth365-sync.it** will resolve.
- ✓ Add an MX record for your **root domain** so that mail can reach **@auth365-sync.it** addresses or [set up restrictive SPF, DKIM, and DMARC records](#) to prevent email spoofing. [New Alert](#)

DNS management for auth365-sync.it

Review, add, and edit DNS records. Edits will go into effect once saved.

DNS Setup: Full ⓘ [Import and Export](#) [Dashboard Display Settings](#)

Search DNS Records

[Add filter](#)

Q

[Search](#)

[Add record](#)

<input type="checkbox"/>	Type ⓘ	Name ⓘ	Content ⓘ	Proxy status ⓘ	TTL ⓘ	Actions
--------------------------	--------	--------	-----------	----------------	-------	---------

No DNS records. Add a DNS record individually or import a BIND file above.

Aggiungiamo un CNAME login assieme al target ricevuto tramite l'installazione del servizio su kali

DNS management for auth365-sync.it

Review, add, and edit DNS records. Edits will go into effect once saved.

DNS Setup: Full ⓘ [Import and Export](#) [Dashboard Display Settings](#)

Search DNS Records

[Add filter](#)

Q

[Search](#)

[Add record](#)

login.auth365-sync.it is an alias of 75cdf9f1-0855-4428-9fae-b704a41dd8d0.cfargotunnel.com and has its traffic proxied through Cloudflare.

Type	Name (required)	Target (required)	Proxy status	TTL
CNAME	login	b704a41dd8d0.cfargotunnel.com	<input checked="" type="checkbox"/> Proxied	Auto
	Use @ for root	E.g. www.example.com		

Autorizziamo il dominio che abbiamo collegato in precedenza:

Authorize Cloudflare Tunnel

Cloudflare Tunnel wishes to serve as an origin on one of your zones.

Please select the zone you want to add a Tunnel to.

Search across all accounts...

Name	Status	Account	Plan	Plan Status
auth365-sync.it	✓ Active	X4fbpw39ri@vwkins.c...	Free	Active

Authorize Tunnel for auth365-sync.it ✕

To finish configuring Tunnel for your zone, click Authorize below.

Success

Cloudflared has installed a certificate allowing your origin to create a Tunnel on this zone.

You may now close this window and start your Cloudflare Tunnel!

Configuriamo i parametri di cloudflare tramite il file config.yml:

```
(kali㉿kali)-[~/cloudflared]
$ nano ~/.cloudflared/config.yml
```

Settiamo i vari dettagli qui sotto:

```
File Actions Edit View Help
GNU nano 8.4
tunnel: 75cdf9f1-0855-4428-9fae-b704a41dd8d0
credentials-file: /home/kali/.cloudflared/75cdf9f1-0855-4428-9fae-b704a41dd8d0.json


ingress:
- hostname: login.auth365-sync.it
  service: http://localhost:3333
- service: http_status:404
```

E startiamo avviando infine il servizio:

```
(kali@kali)~/.cloudflared
$ cloudflared tunnel run gophish-tunnel
2025-08-01T12:45:32Z INF Starting tunnel tunnelID=75cdf9f1-0855-4428-9fae-b704a41dd8d0
2025-08-01T12:45:32Z INF Version 2025.7.0 (Checksum 51e3909335fd7ba2ed5c696b0a6fb7d4a74f6a15bf36615cea0fccba620cfb3f)
2025-08-01T12:45:32Z INF GOOS: linux, GOVersion: go1.24.4, GoArch: amd64
2025-08-01T12:45:32Z INF Settings: map[cred-file:/home/kali/.cloudflared/75cdf9f1-0855-4428-9fae-b704a41dd8d0.json credentials-file:/home/kali/.cloudflared/75cdf9f1-0855-4428-9fae-b704a41dd8d0.json]
2025-08-01T12:45:32Z INF cloudflared will not automatically update if installed by a package manager.
2025-08-01T12:45:32Z INF Generated Connector ID: 6af233f0-92ce-4e8d-a46f-a3f4202637ab
2025-08-01T12:45:32Z INF Initial protocol quic
2025-08-01T12:45:32Z INF ICMP proxy will use 10.0.2.15 as source for IPv4
2025-08-01T12:45:32Z INF ICMP proxy will use fd00::31c3:9720:f247:8462 in zone eth0 as source for IPv6
2025-08-01T12:45:32Z INF ICMP proxy will use 10.0.2.15 as source for IPv4
2025-08-01T12:45:32Z INF ICMP proxy will use fd00::31c3:9720:f247:8462 in zone eth0 as source for IPv6
2025-08-01T12:45:32Z INF Starting metrics server on 127.0.0.1:20242/metrics
2025-08-01T12:45:32Z INF Tunnel connection curve preferences: [X25519MLKEM768 CurveP256] connIndex=0 event=0 ip=198.41.192.227
2025/08/01 08:45:32 failed to sufficiently increase receive buffer size (was: 208 kiB, wanted: 7168 kiB, got: 416 kiB). See https://github.com/quic-go/quic-go/wiki/UDP-Buffer-Sizes for details.
2025-08-01T12:45:32Z INF Registered tunnel connection connIndex=0 connection=10f05628-0c8d-42c9-b016-8cd2e96cd00d event=0 ip=198.41.192.227 location=mxp02 protocol=quic
2025-08-01T12:45:32Z INF Tunnel connection curve preferences: [X25519MLKEM768 CurveP256] connIndex=1 event=0 ip=198.41.200.33
2025-08-01T12:45:32Z INF Registered tunnel connection connIndex=1 connection=fe54c8fa-341d-4034-b0f9-662d0fbd8b11 event=0 ip=198.41.200.33 location=fco01 protocol=quic
2025-08-01T12:45:32Z INF Tunnel connection curve preferences: [X25519MLKEM768 CurveP256] connIndex=2 event=0 ip=198.41.200.63
2025-08-01T12:45:32Z INF Registered tunnel connection connIndex=2 connection=9638dc93-f7b0-44ef-87bf-0ad12a1d2b14 event=0 ip=198.41.200.63 location=fco01 protocol=quic
2025-08-01T12:45:32Z INF Tunnel connection curve preferences: [X25519MLKEM768 CurveP256] connIndex=3 event=0 ip=198.41.192.27
2025-08-01T12:45:32Z INF Registered tunnel connection connIndex=3 connection=f484c69-5288-4362-bfef-dced016bb56a event=0 ip=198.41.192.27 location=mxp01 protocol=quic
```

Apriamo dunque l'homepage del servizio gophis e logghiamo:

login.auth365-sync.it/login?next=%2F



This connection is not secure. Logins entered here could be compromised. [Learn More](#)

Manage Passwords

in

Sign in

Nella sezione sending profiles configuriamo i parametri SMTP presi in prestito dal docente Paolo Rampino:

New Sending Profile

✕

Name:

SMTP DominioFaiDaTe

Interface Type:

SMTP

SMTP From: ⓘ

test@paolorampino.it

Host:

mail12.dominiofaiDate.com:465

Username:

test@paolorampino.it

Password:

●●●●●●●●●●●●●●●●

☒ Ignore Certificate Errors ⓘ

Email Headers:

X-Custom-Header

{{.URL}}-gophish

+ Add Custom Header

Show

10

 entries

Search:

Header ▲	Value ▼
No data available in table	

Showing 0 to 0 of 0 entries

Previous

Next

 Send Test Email

Cancel

Save Profile

Creiamo poi una fake Webpage che andrà aperta dalle nostre vittime:

New Landing Page

Name:

[Import Site](#)

HTML

```
<button type="submit">Accedi</button>
</form>
<div class="info">
  Accesso riservato ai dipendenti aziendali autorizzati.
</div>
</div>
</body>
</html>
```

☒ Capture Submitted Data

☒ Capture Passwords

Warning: Credentials are currently **not encrypted**. This means that captured passwords are stored in the database as cleartext. Be careful with this!

Redirect to:

[Cancel](#) [Save Page](#)

Lanciamo dunque la campagna phishing:

New Campaign

Name:

Email Template:

Landing Page:

URL:

Launch Date: August 1st


Send Emails By (Optional)

Sending Profile: SMTP Don

Groups: test

Test Email

[Campaign](#)

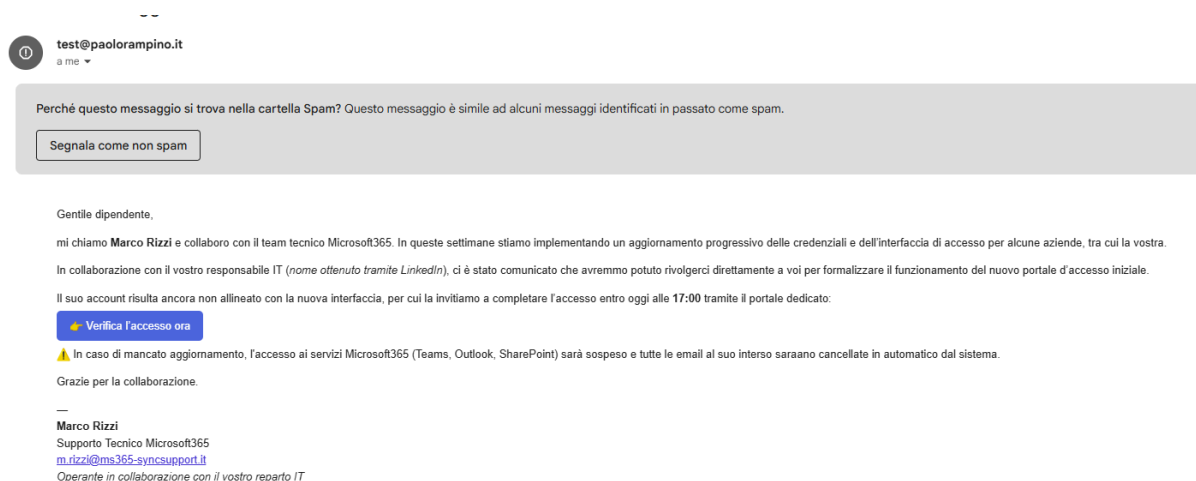


Campaign Scheduled!

This campaign has been scheduled for launch!

[OK](#)

Di seguito possiamo visionare quello che appare una volta ricevuta ed aperta l'email:



Una volta cliccato sul link l'utente verrà rediretto al sito clone e, se inserirà le credenziali, ogni dato fornito verrà mandato alla piattaforma Gophish dell'attaccante.

The image shows a mockup of a login form titled 'Accedi a Microsoft 365'. It features two input fields: 'Nome utente:' and 'Password:'. Below the password field is a blue button labeled 'Accedi'. The form is centered on a light grey background.

CONCLUSIONI:

La simulazione della campagna phishing condotta in questo progetto ha rappresentato un'esperienza pratica estremamente formativa, permettendo di approfondire sia gli aspetti tecnici che quelli psicologici legati alla sicurezza informatica.

Dal punto di vista tecnico, la configurazione di **GoPhish**, l'utilizzo di un **dominio personalizzato** tramite Cloudflare Tunnel e l'integrazione con un server **SMTP funzionante** hanno reso possibile la realizzazione di un'infrastruttura di attacco realistica e completamente funzionante, seppur confinata in un contesto didattico e controllato.

In particolare, la fase di **creazione della landing page** ha mostrato quanto sia semplice – per un utente con conoscenze tecniche di base – replicare l'aspetto di portali web ufficiali, confermando la necessità di una formazione continua per gli utenti aziendali al fine di riconoscere le minacce.

Questa attività ha permesso di consolidare nozioni fondamentali legate a:

- Tecniche di **social engineering**
- Sicurezza delle infrastrutture web
- Attacchi **spear phishing** personalizzati
- Configurazioni di rete e DNS
- Simulazione e misurazione del rischio umano

Infine, il progetto dimostra quanto sia importante integrare l'aspetto umano nella cybersecurity. Nessuna tecnologia, per quanto avanzata, può sostituire un personale consapevole e formato: è proprio qui che simulazioni come questa assumono il massimo valore educativo.