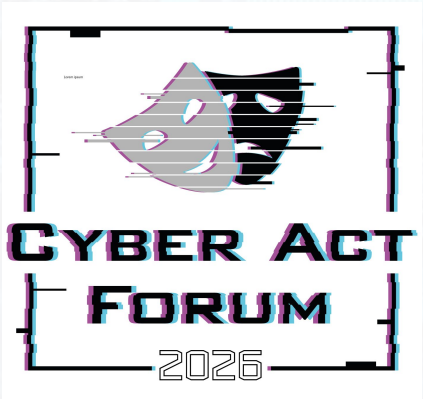
Dall'OTP al Cookie Theft: anatomia di un MFA Bypass

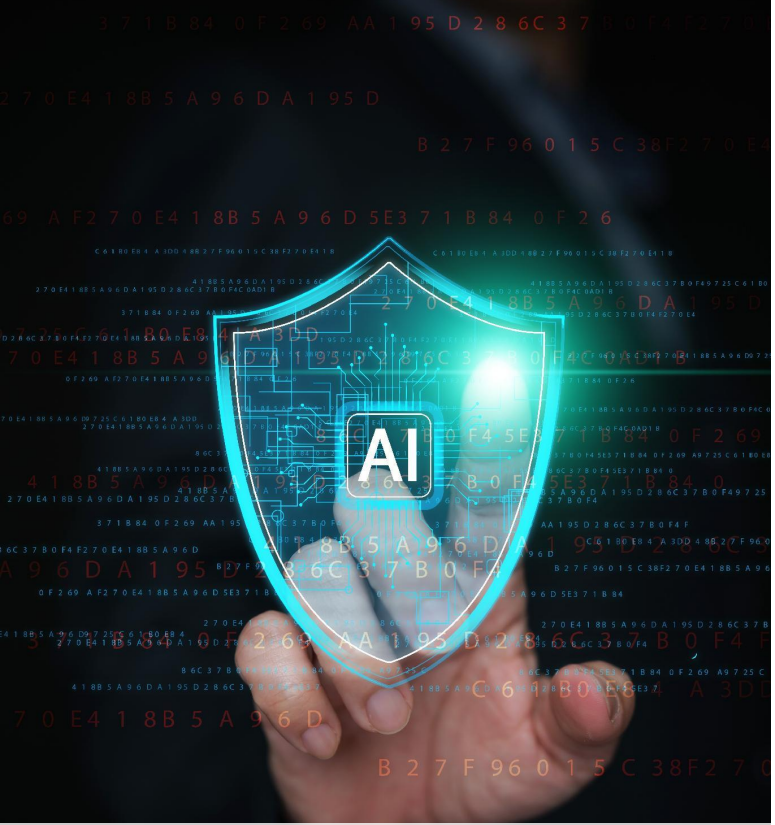
Joele Milazzo
Security Administrator



Chi siamo

La business unit **WeSecure's** è nata dalla sinergia tra l'esperienza di **WeTech's** nella progettazione e implementazione di soluzioni di cybersecurity e l'esperienza di **NIS Group** nella fornitura di servizi gestiti e specializzati nello stesso campo. L'obiettivo della B.U. è **proteggere le aziende dalle minacce cibernetiche** sempre più complesse in un panorama digitale in continua evoluzione. Grazie a un team di esperti altamente qualificati e a una vasta gamma di soluzioni ad hoc offriamo numerosi **servizi di sicurezza IT** che coprono l'intero ambito della cybersecurity.





WE secure's

Cybersecurity a 360°

La divisione dedicata alla **sicurezza informatica** : soluzioni personalizzate, scalabili e completamente integrate, tailor-made, per proteggere aziende pubbliche e private da ogni minaccia.

LE TRE UNIT OPERATIVE

COU

Cybersecurity Operations Unit

Sicurezza quotidiana: monitoraggio, reazione rapida e consulenza normativa.

SIU

Security Infrastructure Unit

Progettazione e realizzazione di infrastrutture IT sicure, robuste e scalabili.

CYSAT

Awareness & Training

Formazione e sensibilizzazione per aziende e per le scuole.

Cos'è l'MFA

Autenticazione Multi-Fattore

Tre categorie di fattori:

Knowledge >> qualcosa che sai (Password, PIN)

Possession >> qualcosa che hai (Token, Smartphone, SmartCard)

Inherence >> qualcosa che sei (impronta, volto)

L'MFA richiede la combinazione di almeno 2 fattori di categorie diverse



Cos'è l'MFA

2FA vs. MFA

2FA = esattamente 2 fattori

MFA = 2 o più fattori di diverse categorie

Ma attenzione, "due password" non è 2FA poiché appartengono alla stessa categoria!

Spesso questi termini vengono confusi. È importante chiarire che la forza non sta nel numero di fattori ma nella loro eterogeneità.



Flusso standard

Utente inserisce le credenziali
Username + password

Verifica del primo fattore
Controllo password (knowledge)

Richiesta secondo fattore
OTP, push notification, token

Verifica del secondo fattore
Controllo possession / inherence

Sessione autentica
Emissione cookie / token di sessione



Una nuova prospettiva

Perché l’attaccante punta meno alla password?

- Le password si rubano «facilmente», ma l’MFA le ha rese meno preziose

- Da qui un nuovo bersaglio: tutto ciò che viene dopo l’autenticazione

- Molte tecniche fanno leva sull’ingegneria sociale



Una nuova prospettiva

Perché l’attaccante punta meno alla password?

- Le password si rubano «facilmente», ma l’MFA le ha rese meno preziose

- Da qui un nuovo bersaglio: tutto ciò che viene dopo l’autenticazione

- Molte tecniche fanno leva sull’ingegneria sociale



Una nuova prospettiva

Perché l’attaccante punta meno alla password?

- Le password si rubano «facilmente», ma l’MFA le ha rese meno preziose

- Da qui un nuovo bersaglio: t
  dopo l’autenticazione

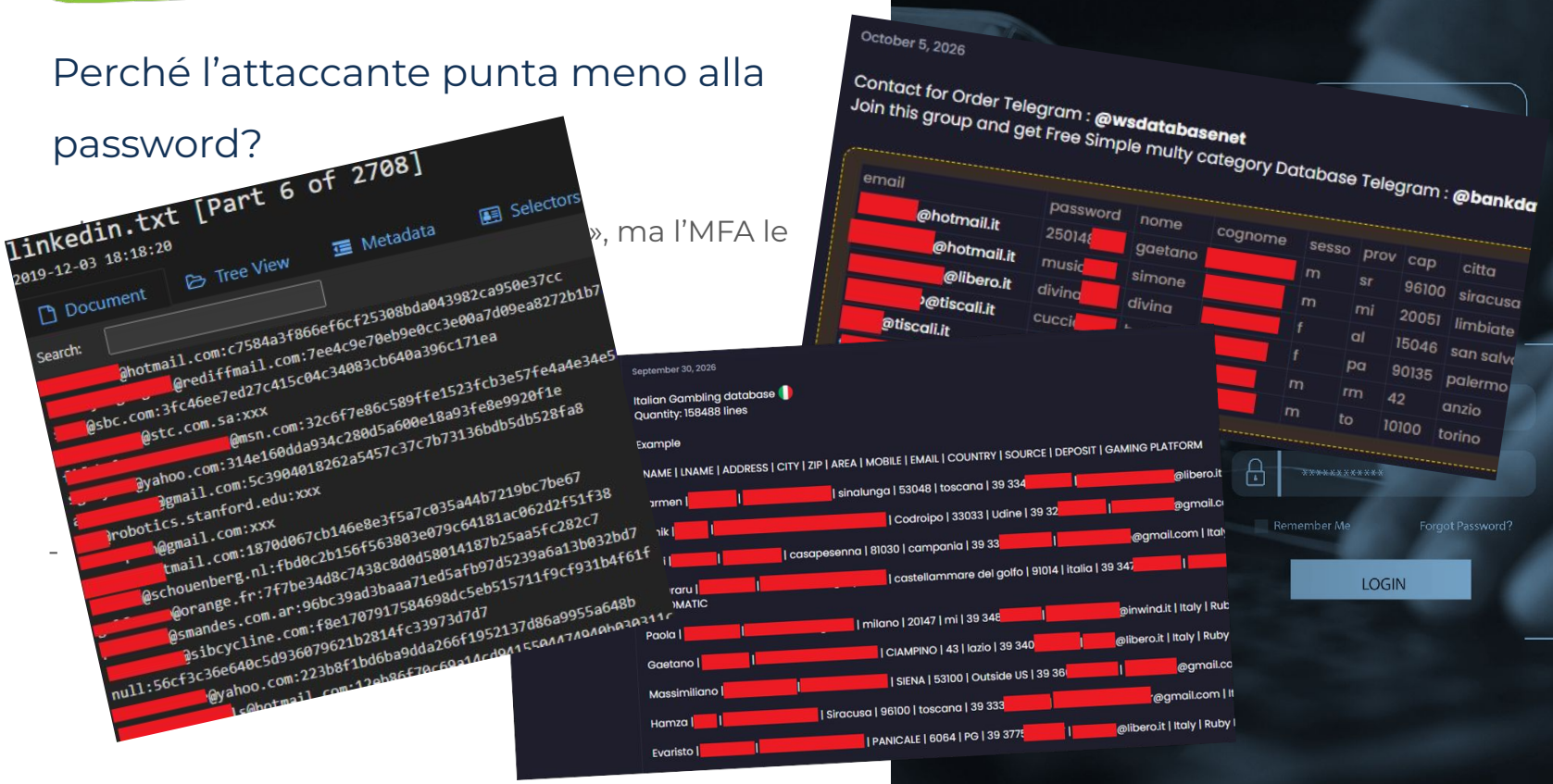
- Molte tecniche fanno leva su



Una nuova prospettiva

Perché l’attaccante punta meno alla password?

- », ma l’MFA le



MFA fatigue

Detta anche Push Bombing

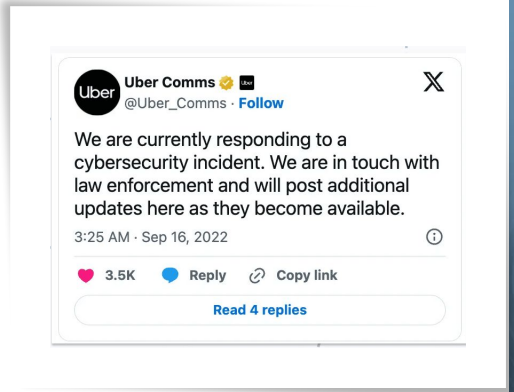
- L’attaccante ha già la password
- Invia decide di richieste consecutive
- La vittima approva per fastidio o distrazione

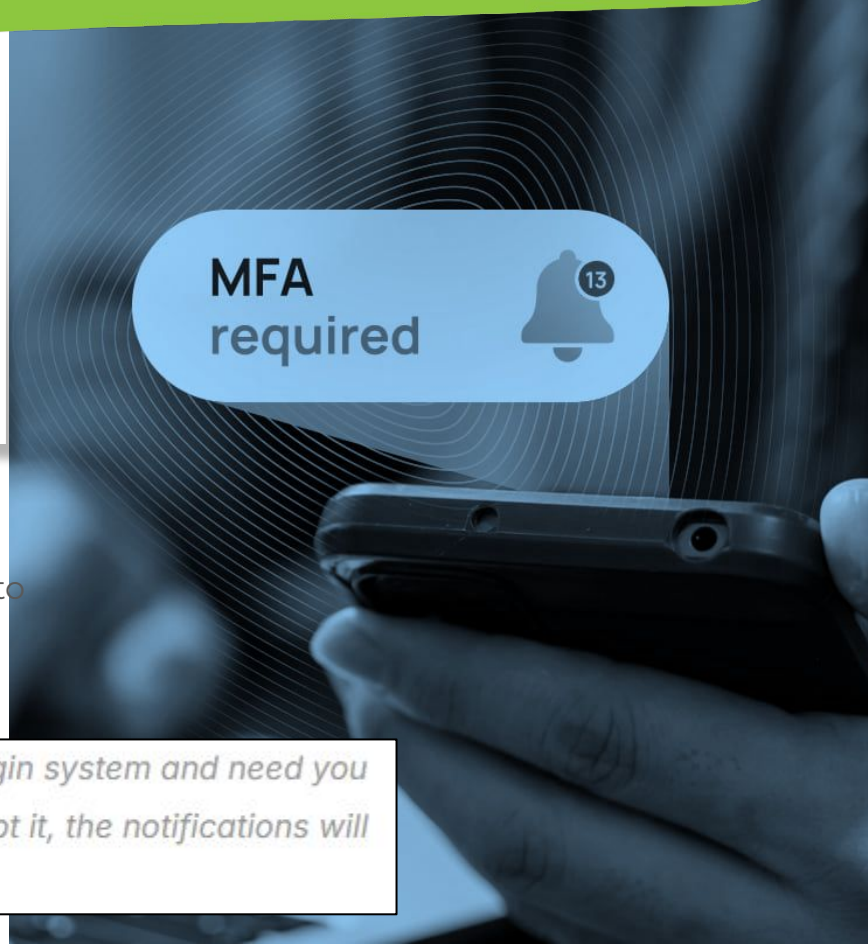
Nessun exploit. Solo ingegneria sociale



MFA fatigue

L'utente attaccato aveva accesso alla rete interna di Uber tramite VPN ed MFA tramite Duo Security





- L'attaccante ha iniziato a inviare notifiche all'utente tentando continuamente di fare login
- L'utente ha ricevuto eccessive notifiche che gli hanno bloccato il dispositivo
- Introduzione dell'ingegneria sociale > Messaggio WhatsApp

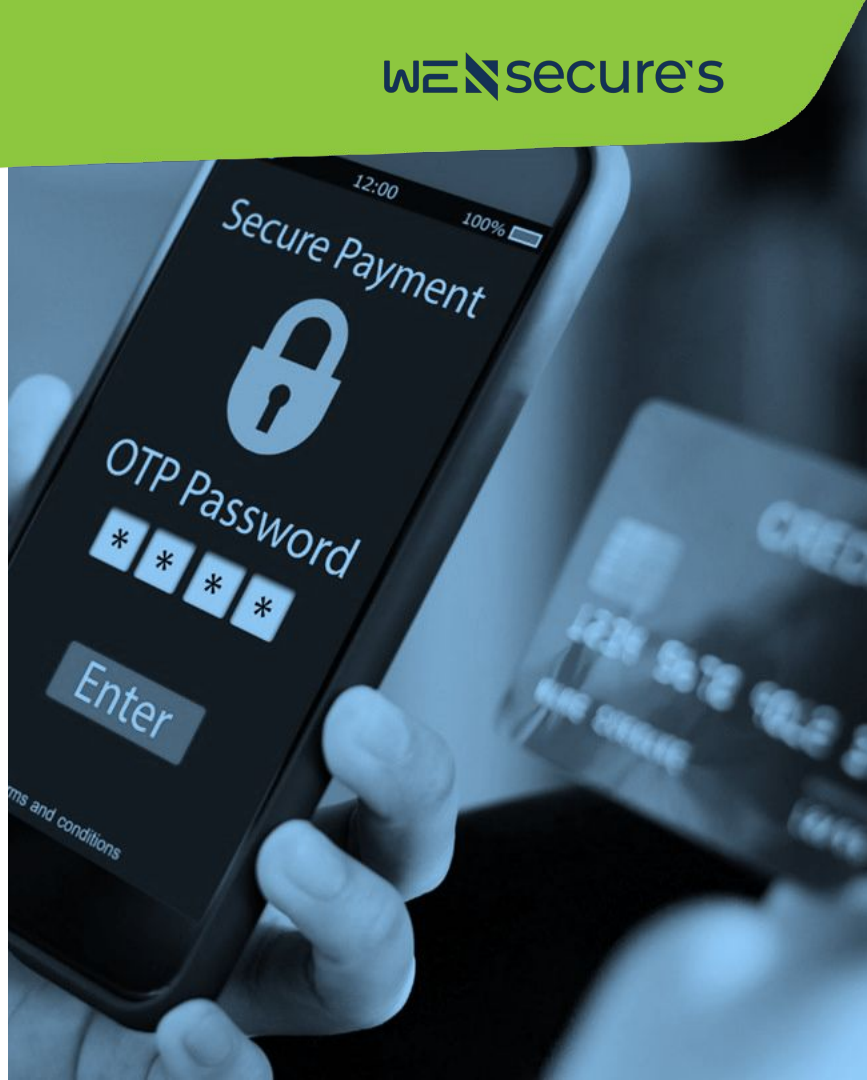
"Hi, this is Uber IT support. We're experiencing a bug with the login system and need you to accept the MFA notification so it can be reset. Once you accept it, the notifications will stop."

OTP Phishing

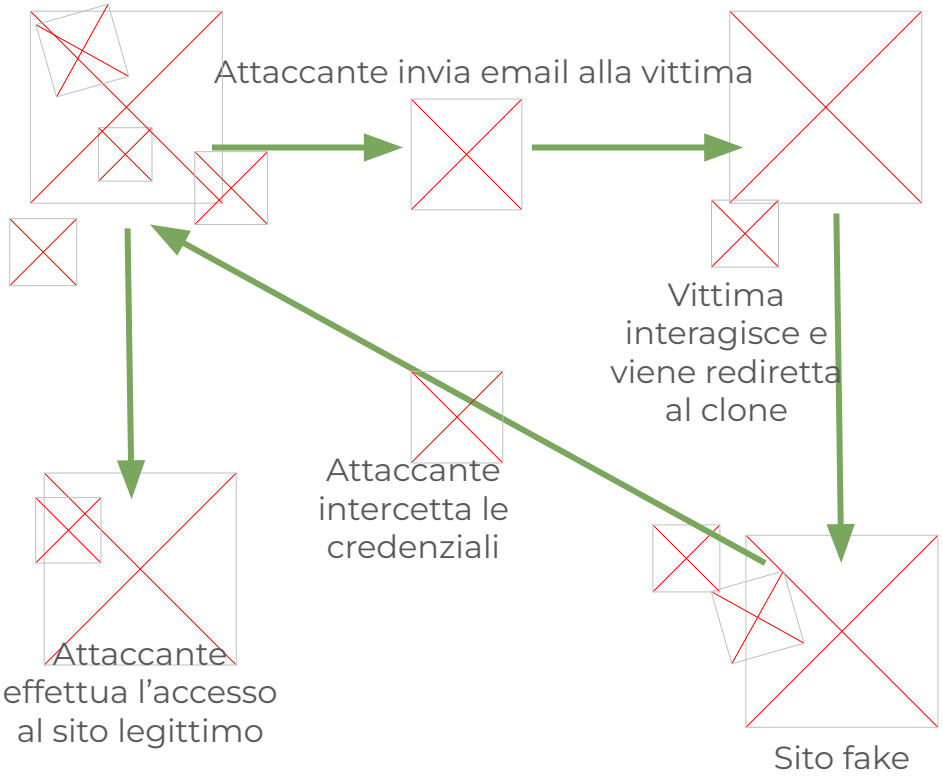
Real-time relay

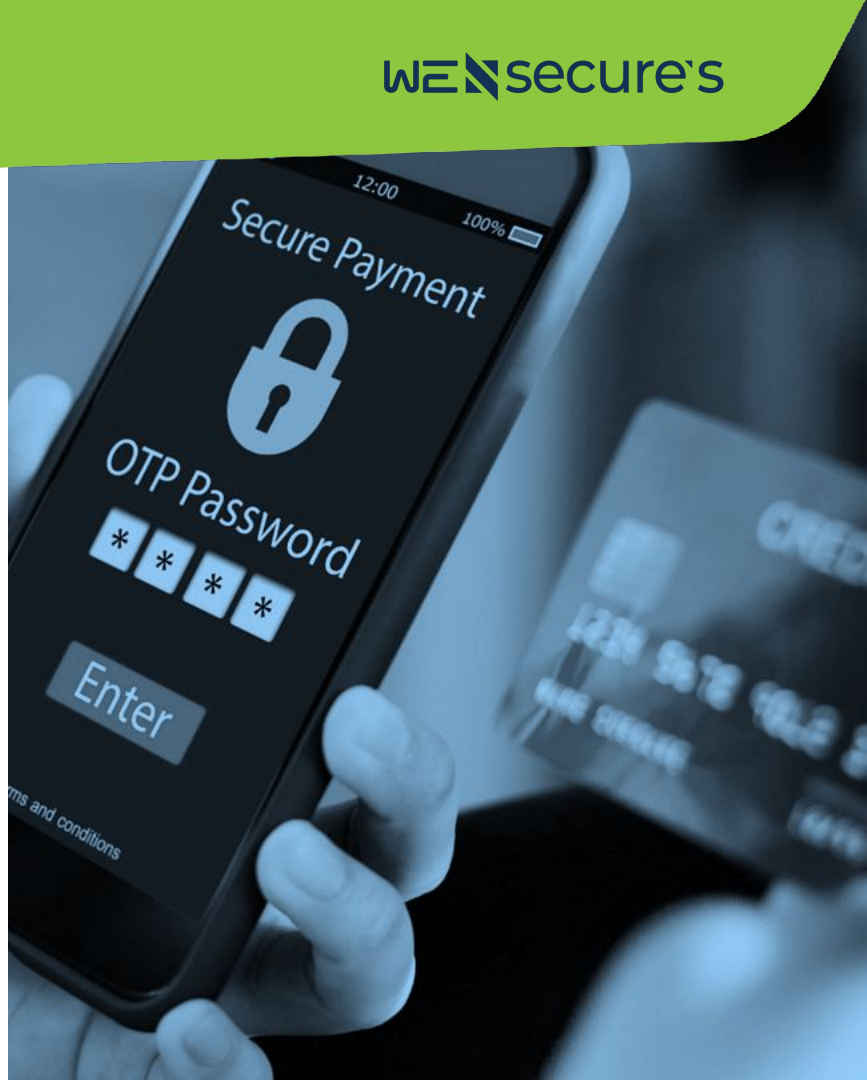
- Sito clone dell'originale che raccoglie pwd + OTP
- Inoltro dei dati al sito legittimo
- La sessione viene aperta dall'attaccante

Rapida sincronizzazione in una finestra temporale stretta



OTP Phishing



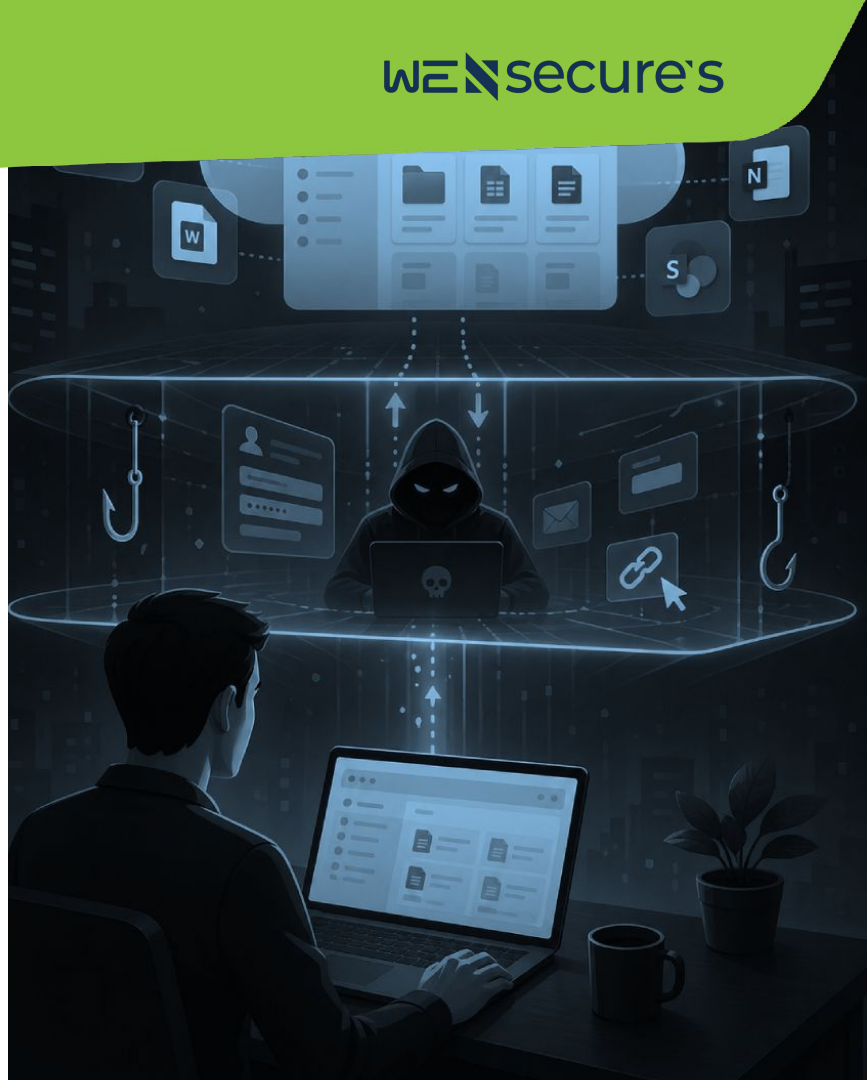


AITM

Adversary-In-The-Middle

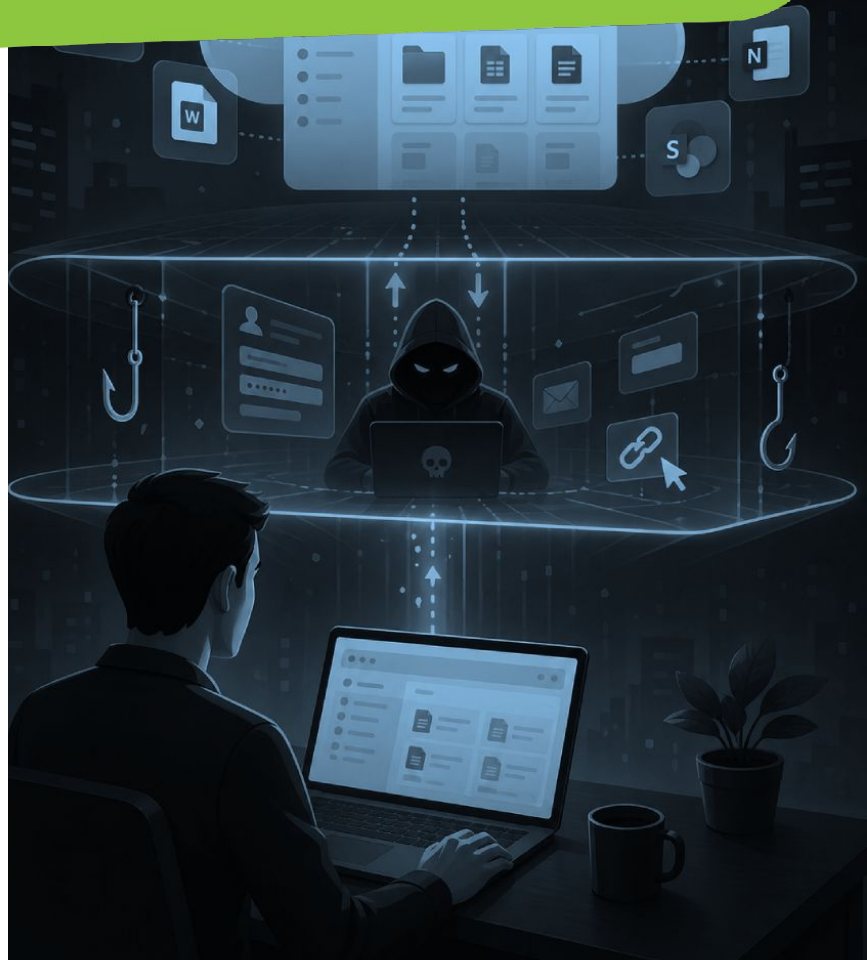
- Un reverse proxy si posiziona tra la vittima e il sito legittimo
- Intercetta credenziali, OTP e cookie di sessione
- L’attaccante eredita la sessione già autenticata

Nessuna limite alla finestra temporale dal momento che il proxy lavora autonomamente



AITM


Sito fake
Username
Password
MFA
Attaccante ottiene credenziali e cookie di sessione
Accesso al sito legittimo
Cookie di sessione



AITM

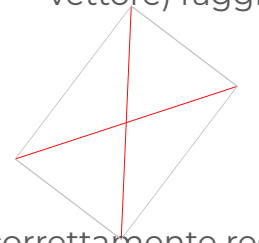


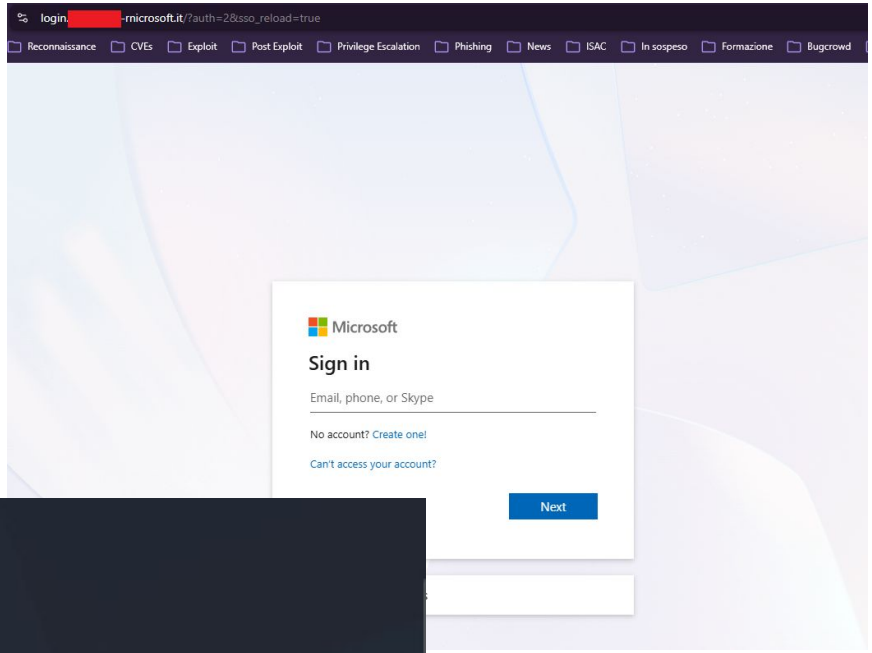
Lista della spesa:

- VPS
- Dominio
- Certificato
- Record DNS configurati
- Evilginx configurato:
    - Dominio
    - IP pubblico
    - Phishlet
    - Lure

AITM

L'utente (previa mail di phishing o altro vettore) raggiunge la destinazione





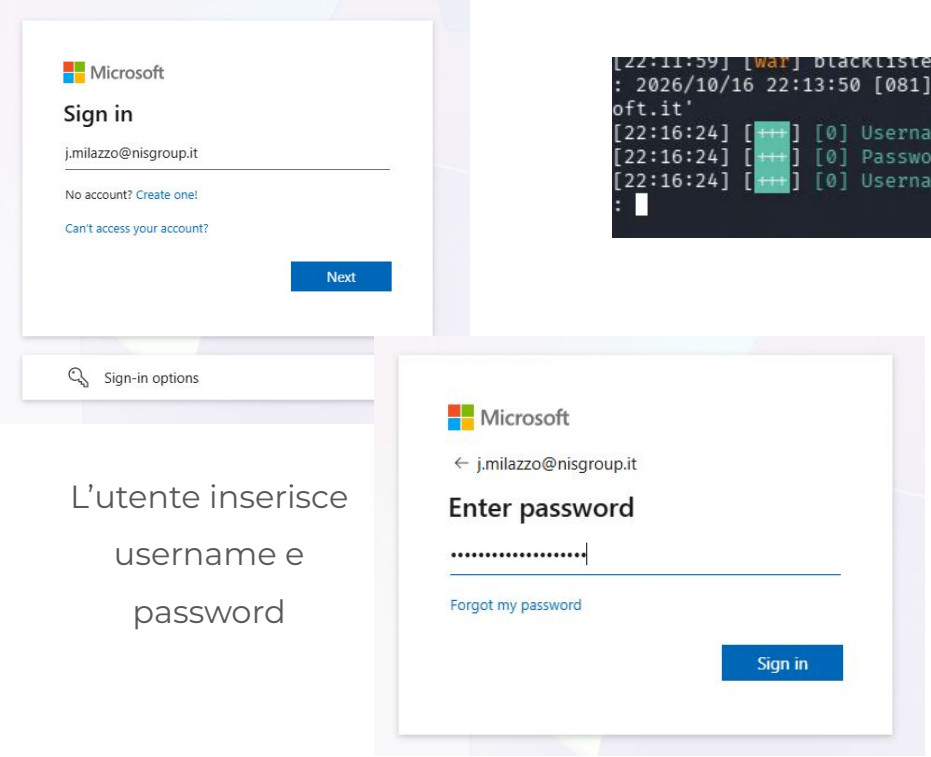
La chiamata è correttamente registrata da Evilginx

```
: lures create m365
[22:04:45] [inf] created lure with ID: 0
: lures edit 0 redirect_url https://office.com
[22:05:00] [inf] redirect_url = 'https://office.com'
: lures get-url 0

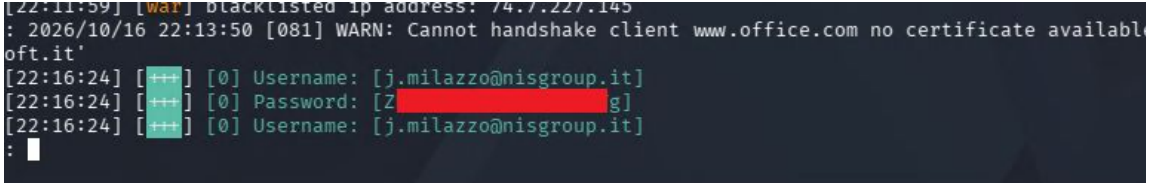
https://login.[redacted]-rnicrosoft.it/iBrHIqJa

[22:05:25] [imp] [0] [m365] new visitor has arrived: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, lik
e Gecko) Chrome/155.0.0.0 Safari/537.36 ([redacted])
[22:05:25] [inf] [0] [m365] landing URL: https://login.[redacted]-rnicrosoft.it/iBrHIqJa
```

AITM

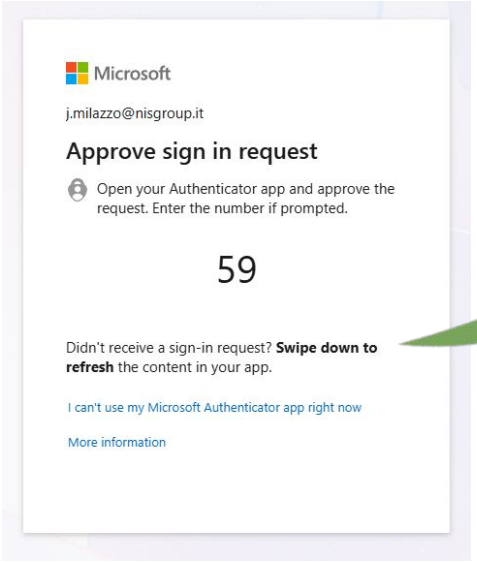


L'utente inserisce username e password

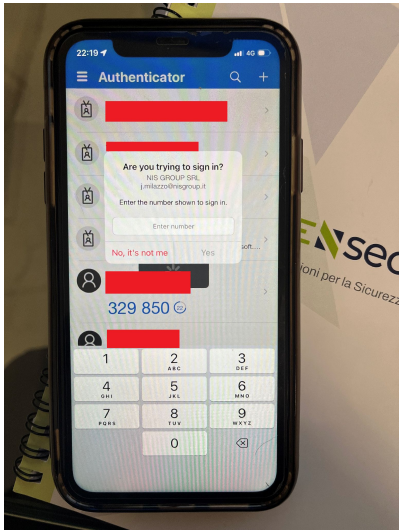


I dati vengono intercettati e mostrati in chiaro all'attaccante

AITM



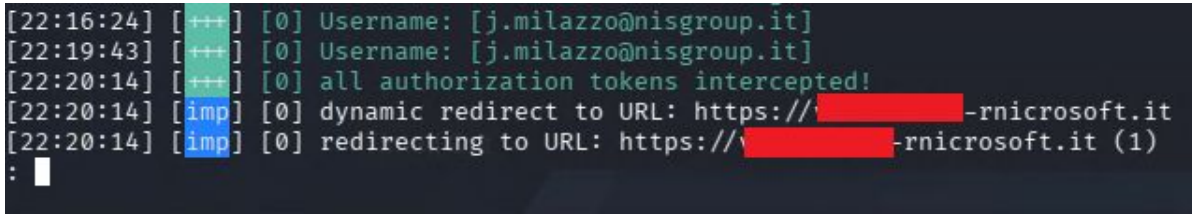
Il secondo fattore fa il suo lavoro, un numero deve essere inserito in Authenticator



Un pop-up si apre in Authenticator per validare la login



.. Ancora una conferma e ..



Token di sessione intercettato. Redirect ed accesso

Protezione

Non tutta l'MFA è vulnerabile allo stesso modo:

- **FIDO2/WebAuthn**: durante la registrazione il dispositivo genera una coppia di chiavi crittografiche (pubblica e privata) legata in modo specifico a quel sito. La chiave privata non lascia mai il dispositivo
- **Binding crittografico**: il browser invia al dispositivo anche il dominio esatto della richiesta, e la firma include quel dominio. Se il dominio non corrisponde a quello registrato il dispositivo si rifiuta di firmare



Protezione

Non tutta l’MFA è vulnerabile allo stesso modo:

- **Token binding**: il cookie viene legato crittograficamente al client che lo ha ricevuto. Copiato altrove, il binding non corrisponde e il server lo rifiuta.
- **Conditional access**: ad ogni richiesta il sistema valuta segnali come IP, paese e dispositivo. Se il contesto cambia rispetto all'originale blocca l'accesso o richiede una nuova autenticazione.



Aewareness Training

Questi attacchi fanno leva sull'**ingegneria sociale**, non su falle tecniche, ma lasciano sempre segnali: un URL leggermente diverso, una richiesta MFA mai sollecitata, troppe notifiche push in pochi secondi.

Riconoscerli, prima di premere "approva", può fare la differenza..



WE secure's

