Analisi tecnica di un attacco Adversary-in-the-Middle (AiTM) finalizzato al bypass dei meccanismi di autenticazione multifattore (MFA)

1. Tipologia di attacco analizzata: Adversary-in-the-Middle (AiTM)

Lo scenario oggetto della presente relazione analizza un **attacco di phishing di tipo Adversary-in-the-Middle (AiTM)**, una tecnica avanzata che consente all'attaccante di **intercettare in tempo reale il flusso di autenticazione dell'utente** e ottenere un accesso non autorizzato a servizi protetti da **autenticazione multifattore (MFA)**.

L'attacco si basa sull'utilizzo di un **proxy controllato dall'attaccante**, che si interpone tra il browser dell'utente e il servizio legittimo. Durante il processo di autenticazione, il proxy intercetta e inoltra:

- le credenziali di accesso (username e password);
- le richieste di autenticazione MFA;
- **i token di sessione o i cookie di autenticazione** restituiti dal servizio target.

In questo modo, l'attaccante non compromette direttamente il meccanismo MFA, ma **sfrutta il flusso di autenticazione legittimo dell'utente**, ottenendo una sessione autenticata valida e riutilizzabile senza ulteriori challenge MFA.

2. Obiettivo tecnico dell'attacco

L'obiettivo dell'attacco AiTM analizzato è **la compromissione degli account degli utenti target** attraverso l'acquisizione delle credenziali di accesso e della **sessione autenticata**, al fine di ottenere un accesso non autorizzato ai servizi aziendali protetti da MFA.

In particolare, l'attacco è finalizzato a:

- **ottenere username e password** inseriti dall'utente durante il processo di autenticazione;
- **intercettare e riutilizzare i token di sessione** o i cookie di autenticazione validi;
- **bypassare i controlli MFA** sfruttando il flusso di autenticazione legittimo;
- **accedere ai servizi aziendali** senza ulteriori richieste di autenticazione forte.

La compromissione della sessione consente all'attaccante di **operare immediatamente sui sistemi target**, mantenendo l'accesso fino alla scadenza o revoca dei token di sessione.

Un ulteriore obiettivo dell'attacco è rappresentato dal **riutilizzo delle credenziali**. In presenza di pratiche di password reuse, le credenziali sottratte possono consentire l'accesso ad altri account o piattaforme aziendali, ampliando l'ambito della compromissione.

3. Descrizione dello scenario di attacco e raccolta delle informazioni

Lo scenario analizzato prevede come target **dipendenti di un'organizzazione che si avvale di un fornitore esterno per la gestione delle trasferte aziendali**.
Prima dell'invio della comunicazione di phishing, l'attaccante ha condotto una fase preliminare di **raccolta delle informazioni (Open Source Intelligence – OSINT)**, rivolta **sia all'organizzazione target sia al fornitore di servizi di viaggio,** con l'obiettivo di identificare gli utenti e di costruire un contesto operativo coerente e credibile.

L'attività di raccolta delle informazioni ha incluso:

- ricerche mirate tramite motori di ricerca;
- utilizzo di strumenti di correlazione e analisi OSINT;
- analisi dei profili pubblicamente accessibili sui social network professionali e personali;
- analisi di comunicazioni e contenuti riconducibili al fornitore di servizi di viaggio.

Attraverso tali attività sono state raccolte informazioni quali:

- nome e cognome degli utenti;
- indirizzi email aziendali, generalmente strutturati secondo pattern standard (es. nome.cognome@azienda.it o nome.cognome@azienda.com);
- ruolo professionale e contesto lavorativo;
- riferimenti a viaggi, trasferte o collaborazioni professionali;
- informazioni sui fornitori esterni utilizzati dall'organizzazione target.

Parallelamente, l'attaccante può condurre attività di raccolta informazioni anche **nei confronti del fornitore di servizi di viaggio**, al fine di replicarne fedelmente modalità operative e comunicative.
Tali attività possono includere:

- analisi dei siti web istituzionali, portali clienti e aree di supporto;
- consultazione di documentazione pubblica, FAQ e materiali commerciali;
- raccolta di informazioni su template email, firme automatiche e disclaimer;
- **interazioni dirette con il fornitore**, ad esempio fingendosi un potenziale cliente interessato:
    - all'acquisto di un viaggio personale;
    - alla valutazione del servizio per una **azienda fittizia**.

Queste interazioni consentono all'attaccante di osservare direttamente:

- il formato e lo stile delle comunicazioni email;
- la terminologia utilizzata;
- la struttura dei messaggi automatici;
- le modalità di presentazione dei link e delle aree riservate.

Le informazioni raccolte vengono utilizzate per **popolare una base dati di utenti target** e per **replicare con elevata precisione i modelli comunicativi del fornitore legittimo**, riducendo la probabilità di rilevazione da parte delle vittime.

Questa fase preliminare risulta determinante per l'efficacia dell'attacco, in quanto consente di **allineare il contenuto della comunicazione malevola alle aspettative operative degli utenti**, aumentando il tasso di successo dell'interazione con il link di phishing.

4. Email di phishing utilizzata nello scenario

Nello scenario analizzato, l'attacco AiTM viene innescato tramite l'invio di una **email di phishing costruita per simulare una comunicazione legittima proveniente dal fornitore di servizi di gestione viaggi aziendali**.

L'email si presenta come una notifica automatica di conferma prenotazione e contiene informazioni coerenti con il contesto operativo dell'utente target, tra cui:

- riferimento a una prenotazione di viaggio;
- indicazione del passeggero;

- dettagli del volo (tratta, data, orario);
- invito ad accedere a un'area riservata per la consultazione o la gestione della prenotazione.

Dal punto di vista strutturale, la comunicazione è progettata per replicare:

- il layout tipico delle email transazionali;
- un tono formale e informativo;
- una firma riconducibile a un servizio di booking;
- l'assenza di allegati, riducendo la probabilità di blocco da parte dei sistemi di sicurezza email.

L'elemento centrale dell'email è rappresentato dal **link di accesso all'area riservata**, che indirizza l'utente verso una piattaforma controllata dall'attaccante.
Tale piattaforma è progettata per **replicare l'interfaccia del servizio legittimo** e per agire come **proxy AiTM**, intercettando il traffico tra l'utente e il servizio reale.

Una volta cliccato il link, l'utente viene indotto a inserire le proprie credenziali di accesso.
Durante questa fase, il proxy AiTM:

- intercetta le credenziali inserite;
- inoltra la richiesta di autenticazione al servizio legittimo;
- intercetta il flusso MFA;
- acquisisce i token di sessione restituiti al termine dell'autenticazione.

L'email rappresenta pertanto **il vettore di accesso iniziale (Initial Access)** dell'attacco, consentendo l'avvio della catena di compromissione descritta nei paragrafi precedenti.

4.1 Email di phishing – Contenuto dell'artefatto

Di seguito è riportato il contenuto dell'email di phishing utilizzata nello scenario descritto.
L'email rappresenta l'artefatto impiegato come vettore di accesso iniziale nell'attacco AiTM.

Oggetto: Conferma prenotazione volo – AZ 2189 | Roma → Berlino – 21 Febbraio

Mittente: Atlas Travel Desk
Indirizzo email: booking@altascorporatetravel-services.com

Gentile Nome Cognome,

la informiamo che è stata confermata la prenotazione a suo nome, effettuata tramite il servizio di gestione trasferte aziendali.

Di seguito i dettagli del volo:

• Passeggero: Nome Cognome
• Volo: AZ 2189
• Tratta: Roma (FCO) → Berlino (BER)
• Data: 21/02
• Orario di partenza: 09:10

Se il viaggio rientra nelle sue attività programmate, non è richiesta alcuna azione.

Per consultare lo stato della prenotazione o verificare i dettagli del viaggio, è possibile accedere alla piattaforma di prenotazione tramite l'area riservata.

👉 Accedi all'area riservata

All'interno dell'area riservata sarà possibile:

visualizzare l'itinerario completo

verificare il centro di costo associato

consultare eventuali servizi inclusi

richiedere modifiche o annullamenti, se previsti

Cordiali saluti,

Atlas Travel Desk
booking@altascorporatetravel-services.com

Messaggio generato automaticamente dal sistema di gestione trasferte.

5. Analisi tecnica dell'email di phishing

L'email di phishing analizzata presenta una struttura e un contenuto progettati per **favorire l'interazione immediata dell'utente**, pur in assenza di richieste esplicitamente urgenti o allarmistiche.
Dal punto di vista tecnico-operativo, è possibile individuare sia **elementi che rafforzano la credibilità del messaggio**, sia **indicatori che possono suggerire una possibile natura malevola della comunicazione**.

Elementi di credibilità

L'email include diversi elementi che ne aumentano la verosimiglianza:

- **Oggetto coerente e contestualizzato**, contenente riferimenti specifici a un volo, a una tratta e a una data;
- **Scenario plausibile di trasferta aziendale**, coerente con il contesto lavorativo dell'utente target;
- **Assenza di toni allarmistici**, che contribuisce a ridurre la percezione di una minaccia immediata;
- **Tono formale e informativo**, tipico delle comunicazioni automatiche;
- **Assenza di allegati**, riducendo il rischio di blocco da parte dei sistemi di sicurezza email;
- **Presenza di una firma e di un disclaimer**, che rafforzano l'apparenza di messaggio generato automaticamente.

Sebbene l'email non contenga richieste urgenti esplicite, **la presenza di una prenotazione non effettuata direttamente dall'utente** può indurlo ad **agire nell'immediato per comprenderne l'origine**, favorendo l'interazione con il link proposto.

Un ulteriore elemento che rafforza la credibilità del messaggio è rappresentato dalla **somiglianza tra il dominio del mittente e quello del fornitore legittimo**.
Ad esempio:

- Indirizzo email phishing: booking@altascorporatetravel-services.com
- Indirizzo email legittimo: booking@atlascorporatetravel.com

La differenza, limitata a una porzione del dominio, può risultare difficilmente individuabile in una valutazione superficiale, soprattutto in contesti operativi caratterizzati da un elevato volume di comunicazioni email.

Indicatori di sospetto

Nonostante il livello di realismo, l'email presenta alcuni indicatori che, se analizzati attentamente, possono suggerire una possibile natura malevola:

- **Dominio del mittente simile ma non identico** a quello del fornitore ufficiale;
- **Invito ad accedere a un'area riservata tramite link**, anziché tramite portali abitualmente utilizzati;
- **Assenza di riferimenti univoci** quali codici prenotazione interni o identificativi aziendali;
- **Link non contestualizzato**, la cui destinazione effettiva non è verificabile senza un'analisi preventiva;
- **Richiesta implicita di autenticazione**, che comporta l'inserimento delle credenziali aziendali su una piattaforma esterna.

Questi indicatori, se correttamente riconosciuti, possono consentire di **identificare anomalie nel flusso di comunicazione** e interrompere la catena di attacco prima della compromissione.

6. Impatto tecnico della compromissione

Nel caso in cui l'utente interagisca con l'email di phishing e completi il processo di autenticazione sulla piattaforma controllata dall'attaccante, l'attacco AiTM consente la **compromissione simultanea delle credenziali di accesso e della sessione autenticata**.

Dal punto di vista tecnico, l'impatto dell'attacco include:

- **Acquisizione delle credenziali di accesso** (username e password) inserite dall'utente;
- **Intercettazione dei token di sessione o dei cookie di autenticazione** rilasciati dal servizio legittimo al termine del processo MFA;
- **Bypass dei controlli MFA**, mediante riutilizzo della sessione autenticata senza necessità di ulteriori challenge;
- **Accesso non autorizzato ai servizi target** fino alla scadenza o revoca dei token di sessione.

La disponibilità di una sessione autenticata valida consente all'attaccante di **operare sui servizi compromessi con gli stessi privilegi dell'utente**, senza generare eventi di

autenticazione anomali facilmente rilevabili.

In presenza di **riutilizzo delle credenziali**, l'impatto può estendersi ulteriormente, consentendo:

- accesso ad altri servizi aziendali che utilizzano le stesse credenziali;
- compromissione di account federati o integrati tramite Single Sign-On (SSO);
- ampliamento della superficie di attacco verso ulteriori applicazioni o sistemi interni.

Nel caso in cui la piattaforma di prenotazione viaggi sia **integrata o federata con l'infrastruttura dell'organizzazione target**, la compromissione iniziale può propagarsi ad altri servizi senza richiedere ulteriori autenticazioni, aumentando l'estensione tecnica dell'attacco.

7. Considerazioni tecniche finali

Lo scenario analizzato evidenzia come un attacco di phishing di tipo **Adversary-in-the-Middle (AiTM)**, supportato da un'attività preliminare strutturata di raccolta delle informazioni, consenta di **aggirare i meccanismi di autenticazione multifattore (MFA)** senza sfruttare vulnerabilità tecniche nei sistemi target.

L'efficacia dell'attacco deriva dalla combinazione di:

- un contesto operativo coerente e plausibile;
- una comunicazione email allineata ai modelli utilizzati dal fornitore legittimo;
- l'intercettazione del flusso di autenticazione dell'utente tramite proxy AiTM;
- la compromissione della sessione autenticata anziché del solo fattore di autenticazione.

L'analisi dimostra che la **presenza dell'MFA, se non accompagnata da ulteriori controlli sulla sessione e sull'integrità del flusso di accesso**, non è sufficiente a prevenire questo tipo di attacco.

Lo scenario descritto rappresenta un esempio realistico di compromissione basata sul **sfruttamento del comportamento dell'utente e del contesto applicativo**, evidenziando come le tecniche di phishing evolute possano mantenere un'elevata efficacia anche in ambienti con misure di autenticazione avanzate.