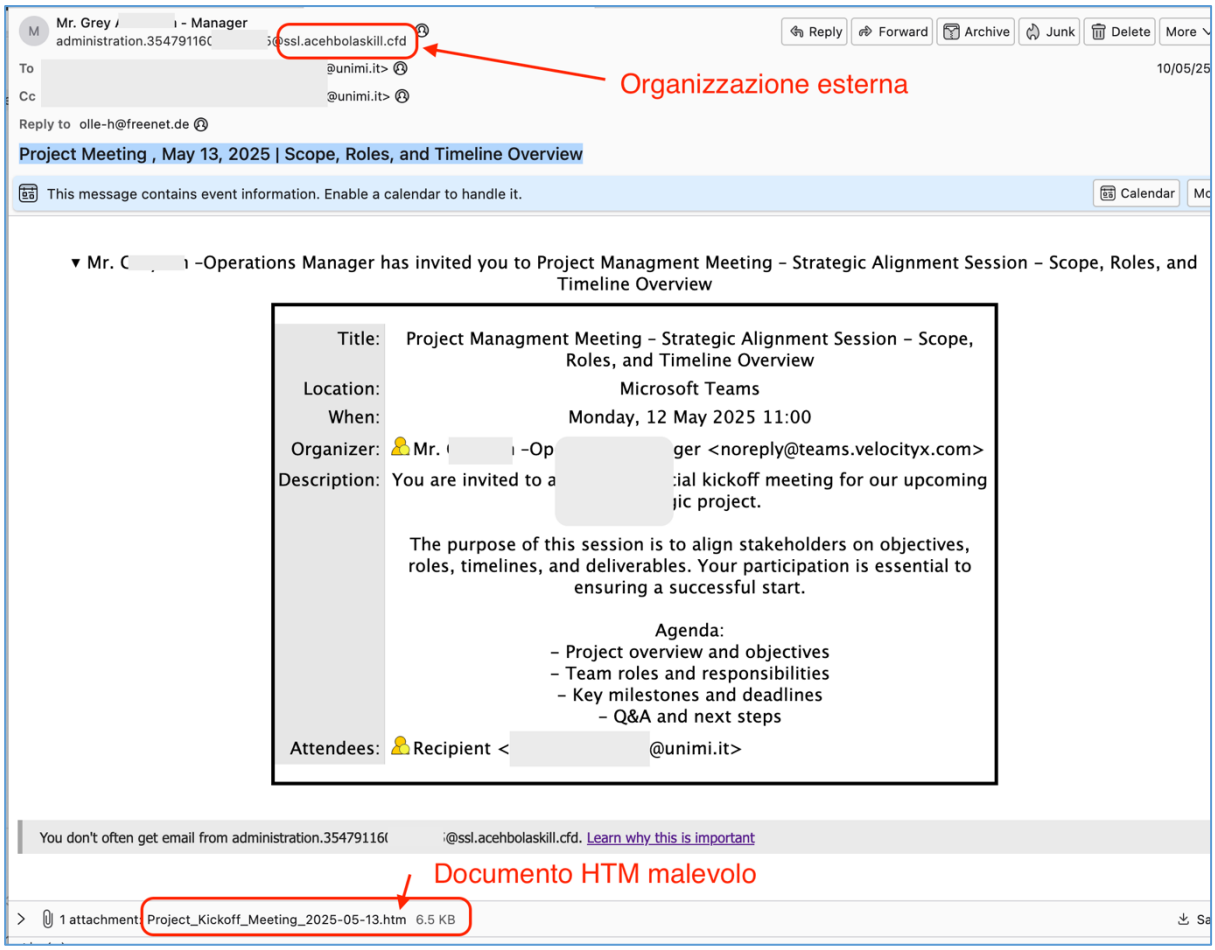
Avviso di sicurezza del 12/05/2025

Segnalazione di campagna malevola che sfrutta inviti Microsoft Teams

Riportiamo in questo bollettino i dettagli di una campagna malevola di phishing che ha interessato l'Ateneo e che sfrutta inviti a meeting Teams.
La mail si presenta come un invito ad un meeting Teams, all'interno della mail è allegato un documento malevolo HTM contenente codice malevolo che ha lo scopo di rubare le credenziali di Ateneo. Qualora aveste inserito le credenziali in tale form occorre contattare immediatamente **sicurezza@unimi.it**.

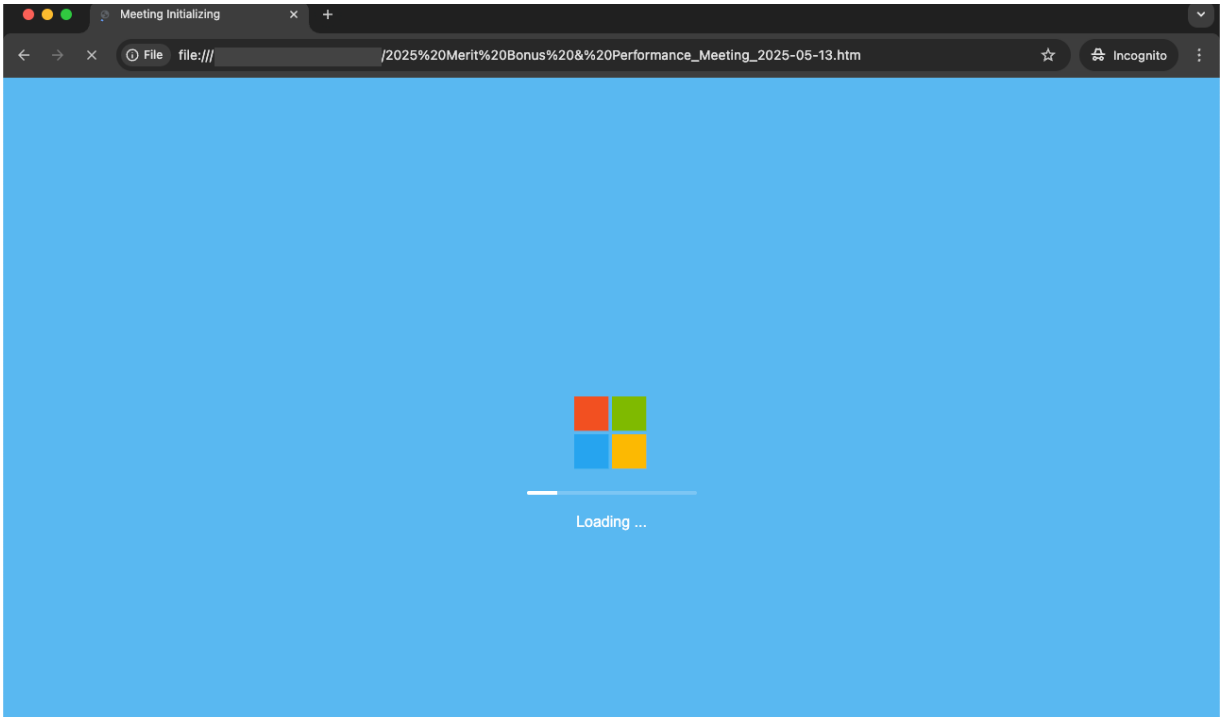
L'attacco in dettaglio

Di seguito riportiamo l'esempio di una di queste mail:



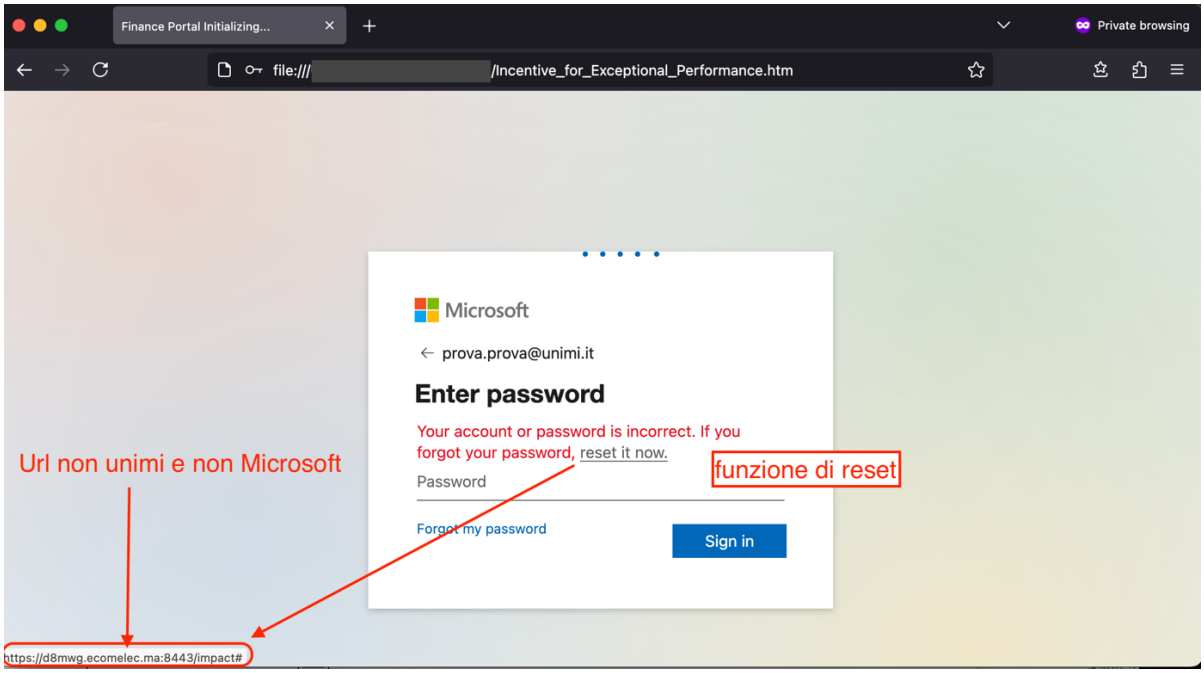
La mail si presenta come proveniente da un indirizzo mail di un dominio esterno all'Ateneo, nel presente caso:

e propone un meeting Teams di varia motivazione.
Alla mail è allegato un documento HTM contenete del codice malevolo che simula un'autenticazione Microsoft:



Per comunicare con il server malevolo, la simulazione usa delle porte di comunicazione non standard, es:

Se il browser è abilitato a tale tipo di traffico non standard, si giunge ad una schermata di autenticazione del tutto simile ad una autenticazione Microsoft:



In alcuni casi è possibile riconoscere il *form* come malevolo esaminando il link di reset della password: esso non punta né ad un portale di Ateneo, né ad un sito riconducibile a Microsoft.

Se malauguratamente si inserisce la password di Ateneo occorre:

- Cambiare immediatamente la password di Ateneo attraverso il servizio di portale di Ateneo:

  https://auth.unimi.it/'password

- Dare immediatamente comunicazione all'ufficio **sicurezza@unimi.it**, indicando il momento di inserimento della password e del successivo cambio password.

Per ulteriori informazioni potete contattare l'Ufficio CERT scrivendo a **sicurezza@unimi.it.**

Sperando di essere stati utili,
i più cordiali saluti

Massimo Marchi
Responsabile Ufficio CERT e Gestione Incidenti
Settore Cybersecurity - Direzione ICT
Università degli Studi di Milano
Via Giuseppe Colombo n. 46 - 20133 Milano
Info: https://work.unimi.it/servizi/security_gdpr/118546.htm