Avviso di sicurezza del 19/05/2026

Segnalazione di campagne malevole veicolate tramite documenti condivisi da corrispondenti conosciuti compromessi

Gent. Utenti,
scrivo questo avviso per segnalarvi la recrudescenza di campagne di phishing veicolate tramite documenti malevoli condivisi da contatti conosciuti compromessi.

Questo tipo di attacco arriva da contatti con cui si è collaborato che sono stati compromessi di recente. La mail malevola si presenta solitamente come una richiesta generica di visionare un documento di un progetto in comune. La condivisione malevola spesso è protetta dai sistemi di cifratura legittimi messi a disposizione da Microsoft, come SharePoint e OneDrive. All'interno del documento malevolo è solitamente presente un link che rimanda ad un sito esterno che tenta di carpire le credenziali o registrare un dispositivo malevolo.

Questi attacchi sono particolarmente insidiosi perché sono strutturati in modo da rendere difficile il rilevamento anticipato dell'attacco:

- Il meccanismo di cifratura e protezione che spesso viene aggiunto a questo tipo di condivisioni malevolo rende impossibile l'esame del contenuto da parte di meccanismi automatici di verifica: il contenuto malevolo può essere esaminato ed eventualmente scoperto solo al momento dell'apertura da parte dell'utente; rendendo più pericoloso l'attacco;
- arrivano da contatti da cui spesso si stanno effettivamente aspettando documenti e con cui si hanno contatti più o meno assidui: la reputazione del mittente è quindi fino al momento della compromissione ottima;
- questi attacchi sono graficamente pressoché indistinguibili da uno scambio legittimo.

Occorre estrema prudenza nell'aprire documenti condivisi via mail.

Di seguito vi metto due schermate che possono essere utili per riconoscere questi due insidiosi attacchi.

Se avete dubbi su una mail sospetta, inoltratela a **sicurezza@unimi.it.**
Se avete il dubbio di essere caduto in una campagna malevola, cambiate la pasword accedendo a https://auth.unimi.it/password e scriveteci a **sicurezza@unimi.it** o aprite un ticket su SPOC.

Per qualunque richiesta di informazioni su questi argomenti, scrivete a **sicurezza@unimi.it.**

Grazie per l'attenzione, i più cordiali saluti.

Massimo Marchi
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

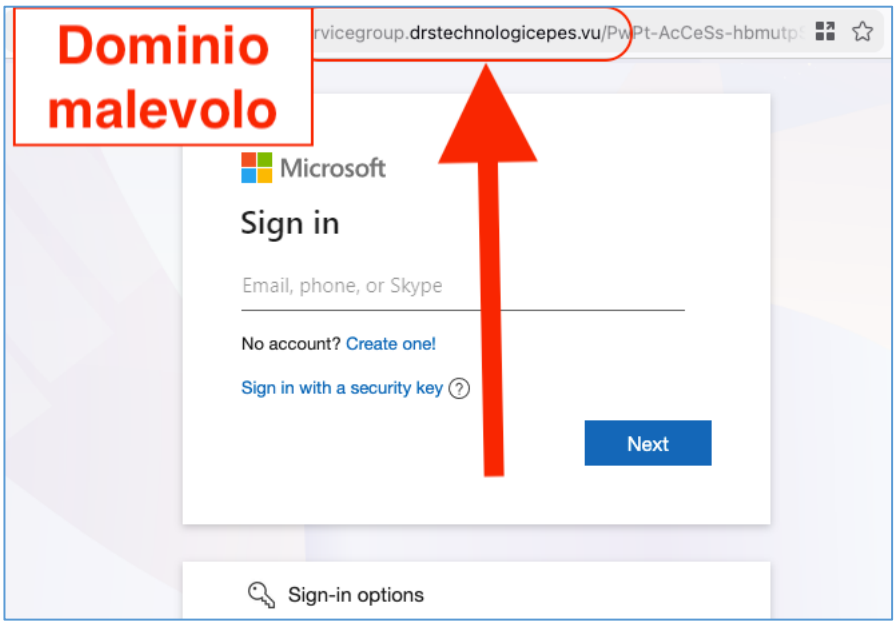
Gli attacchi nel dettaglio

Il furto dell'account in queto tipo di attacchi può avvenire in due modi:

Attacco tipo "Uomo-nel-mezzo" (Man-in-the-middle)

l'attaccante cerca di indurre la vittima ad inserire le vostre credenziali in un sito malevolo che mima l'autenticazione Microsoft. in questo caso l'unico momento in cui potete accorgervi che qualcosa non va come atteso è al momento dell'inserimento della password.

Il form dove inserire le credenziali è spesso indistinguibile da form legittimo di Microsoft. Per rilevare il tentativo di furto occorre prestare attenzione all'indirizzo mostrato nel browser **che deve appartenere al dominio "microsoftonline.com"**. Di seguito un esempio che mostra dove occorre prestare attenzione per rilevare il tentativo di furto:

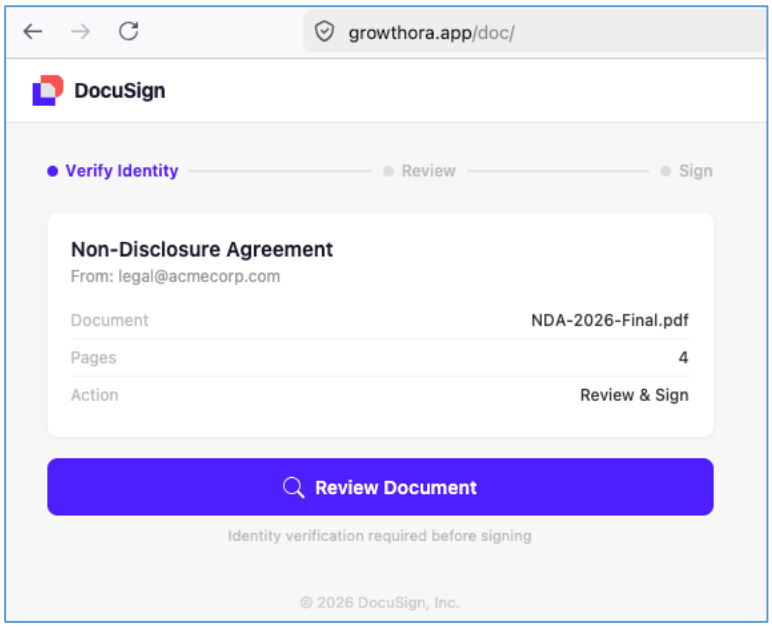


Attacco basato sulla registrazione di un dispositivo malevolo

Ancora più insidioso è l'**attacco basato sulla registrazione di un dispositivo malevolo.** In questo caso, l'attaccante cerca di convincervi a collegare un dispositivo malevolo al vostro account.

L'attacco è particolarmente insidioso perché tutta la procedura si svolge usando sistemi legittimi Microsoft. Non è semplice accorgersi della trappola. All'inizio viene comunicato che è necessario autenticarsi per accedere ad un documento condiviso ma in realtà quella che viene celata è la procedura per loggare un dispositivo al proprio account, attraverso l'inserimento di un codice alfanumerico. Se si procede fino alla fine, l'attaccante ottiene un dispositivo connesso al vostro account sotto il suo controllo.

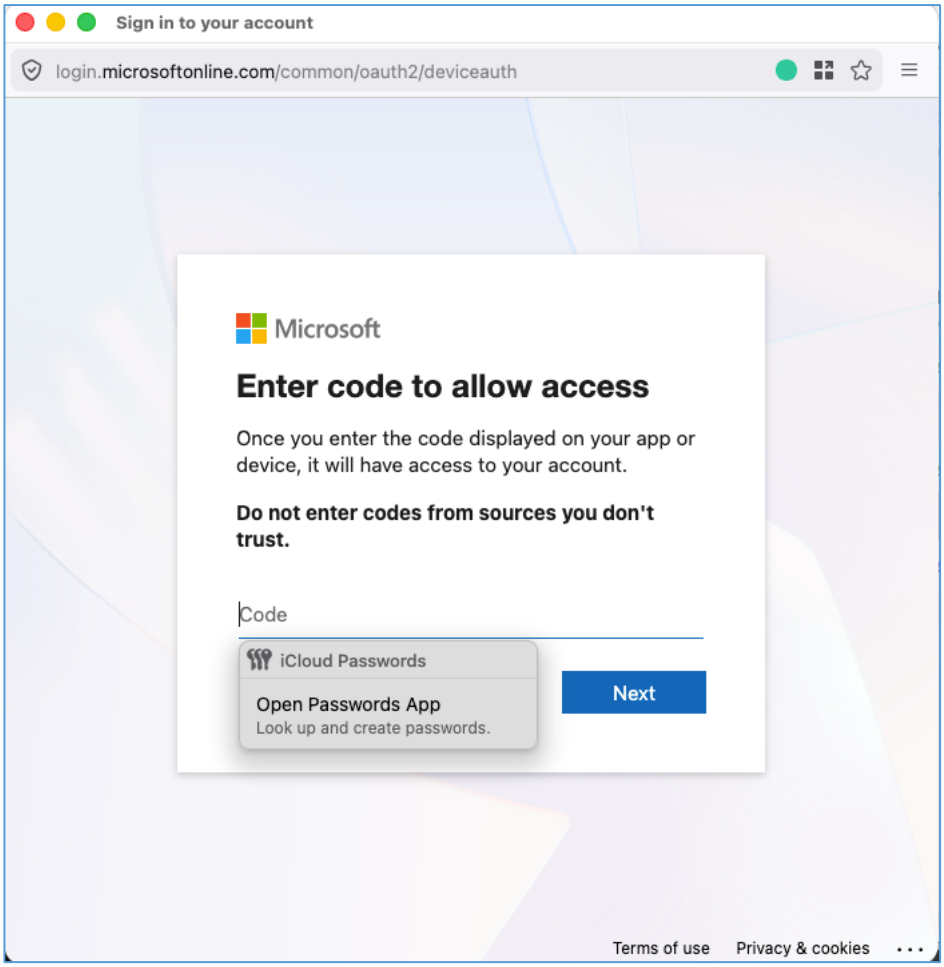
Di seguito è riportata una tipica sequenza di inizio del processo di registrazione. All'inizio viene mostrata una schermata che comunica a necessità di sbloccare un documento:



Di seguito viene presentato un codice che va inserito in seguito; **prestate la massima diffidenza se vi viene proposto un codice simile**:

Il pulsante *COPY* copia il codice negli appunti del vostro dispositivo e attiva il successivo pulsante *Sign in with Microsoft* che condice alla procedura di registrazione del dispositivo malevolo.

La procedura prosegue sull'infrastruttura legittima Microsoft; non ci sono altri indicatori che possono segnalare l'attacco. L'obbiettivo di tutto il processo è registrare il dispositivo dell'attaccante:



Dopo aver inserito il codice alfanumerico precedente si prosegue con l'autenticazione a due fattori legittima Microsoft.

Se si cade in questi due tipi di attacco, è necessario cambiare immediatamente la password usando il servizio di cambio password di Ateneo:

https://auth.unimi.it/password

e darne rapida comunicazione al nostro ufficio scrivendo a **sicurezza@unimi.it** o aprendo un ticket su SPOC.