ANDORRA DIGITAL

ANC-AD
Agència Nacional de Ciberseguretat d'Andorra

# Informe de Ciberintel·ligència

# SharePoint com a element clau a la taxonomia d'atacs de pesca sofisticats


TLP: WHITE

SETEMBRE 2025

## FITXA DEL DOCUMENT

| Versió | Redactat/Revisat per | Aprovat per | Data aprovació | Data publicació |
|---|---|---|---|---|
| 1.0 | ANC-AD | ANC-AD | 29/09/2025 | 30/09/2025 |

| Registre de canvis | | | |
|---|---|---|---|
| Versió | Pàgines | Data Modificació | Motiu del canvi |
| | | | |

| Propietari del document | ANC-AD |
|---|---|

# ÍNDEX

# 1. METODOLOGIA

Aquest informe aplica els principis de Traffic Light Protocol (TLP). És un esquema creat per fomentar un intercanvi més bo d'informació delicada (però no classificada) en l'àmbit de la seguretat de la informació.

A través d'aquest esquema, d'una manera àgil i senzilla, s'indica fins on pot circular la informació més enllà del receptor immediat, i aquest ha de consultar l'Agència Nacional de Ciberseguretat d'Andorra quan cal distribuir la informació a tercers.

| Codi | Com es fa servir | Com es comparteix |
|---|---|---|
| TLP: RED | S'ha de fer servir **TLP:RED** quan la informació està limitada a persones concretes, i podria tenir impacte en la privacitat, la reputació o les operacions si es fa servir malament. | Els receptors no han de compartir informació designada com a **TLP:RED** amb cap tercer fora de l'àmbit on va ser exposada originalment. |
| TLP: AMBER | S'ha de fer servir **TLP:AMBER** quan la informació ha de ser distribuïda de manera limitada, però suposa un risc per a la privacitat, la reputació o les operacions si és compartida fora de l'organització. | Els receptors poden compartir informació indicada com a **TLP:AMBER** només amb membres de la seva pròpia organització que necessiten conèixer-la, i amb clients, proveïdors o associats que necessiten conèixer-la per protegir-se a si mateixos o evitar danys. L'emissor pot especificar restriccions addicionals per compartir aquesta informació. |
| TLP: GREEN | S'ha de fer servir **TLP:GREEN** quan la informació és útil per a totes les organitzacions que hi participen, com també amb tercers de la comunitat o el sector. | Els receptors poden compartir la informació indicada com a **TLP:GREEN** amb organitzacions afiliades o membres del mateix sector, però mai a través de canals públics. |
| TLP: WHITE | S'ha de fer servir **TLP:WHITE** quan la informació no suposa cap risc de mal ús, conforme a les regles i procediments establerts per a la seva difusió pública. | La informació **TLP:WHITE** pot ser distribuïda sense restriccions, únicament subjecta a controls de copyright. |

## 2. INTRODUCCIÓ

Campanyes de pesca n'hi ha moltes. De fet, és una de les ciberamenaces més freqüents, tant si es concep com a tipologia d'atac, com a vector d'entrada.

Tot i això, si en alguna cosa es diferencien, és en la seva sofisticació. I un dels criteris que poden definir més bé la sofisticació d'una pesca és la seva capacitat per ser reeixida, aconseguir l'objectiu i tenir impacte.

Generalment, tots els consells per poder identificar un cas de pesca fan al·lusió a la manera com es redacten els correus, per tractar d'identificar anomalies en la gramàtica o l'ortografia que permetin identificar un correu il·legítim, o a la intencionalitat, on en to urgent se sol·liciten accions sospitoses, com ara fer pagaments amb mètodes o destinataris inusuals.

Per això, i com que els actors d'amenaça són conscients que la conscienciació sobre aquest tipus d'amenaça ha anat calant tant en entorns corporatius com entre l'usuari d'Internet mitjà, han tingut la necessitat de reinventar-se i buscar noves fórmules (o evolucionar algunes ja existents) perquè els seus atacs acabin tenint èxit.

I és en aquest punt on ha entrat en joc l'ús, i abús, de serveis legítims per camuflar campanyes de pesca després d'accions aparentment normals i quotidianes, i aconseguir no despertar cap mena de sospita.

Com a resultat s'ha identificat un apogeu de campanyes de pesca molt sofisticades i dirigides que fan ús de recursos com ara el SharePoint, el OneDrive o el Dropbox. Eines àmpliament esteses i populars tant en entorns corporatius com personals.

Si s'entén aquest context i a causa del gran impacte que tenen les campanyes de pesca que s'estructuren sobre aquest esquema d'atac, en aquest informe es tractaran les raons que ho expliquen, per què són més difícils de detectar i quines són les lliçons apreses de campanyes analitzades per aconseguir identificar atacs d'aquesta mena.

# 3. PESCA BASADA EN SERVEIS LEGÍTIMS

Els serveis com ara el SharePoint, el Dropbox o el OneDrive han esdevingut eines imprescindibles per a les organitzacions, ja que permeten emmagatzemar, compartir i poder col·laborar en arxius.

I els ciberdelinqüents, per altra banda, s'aprofiten de la confiança que dipositen els usuaris en aquestes plataformes, cosa que els permet jugar amb la carta de fer servir una cosa quotidiana i generalment legítima.

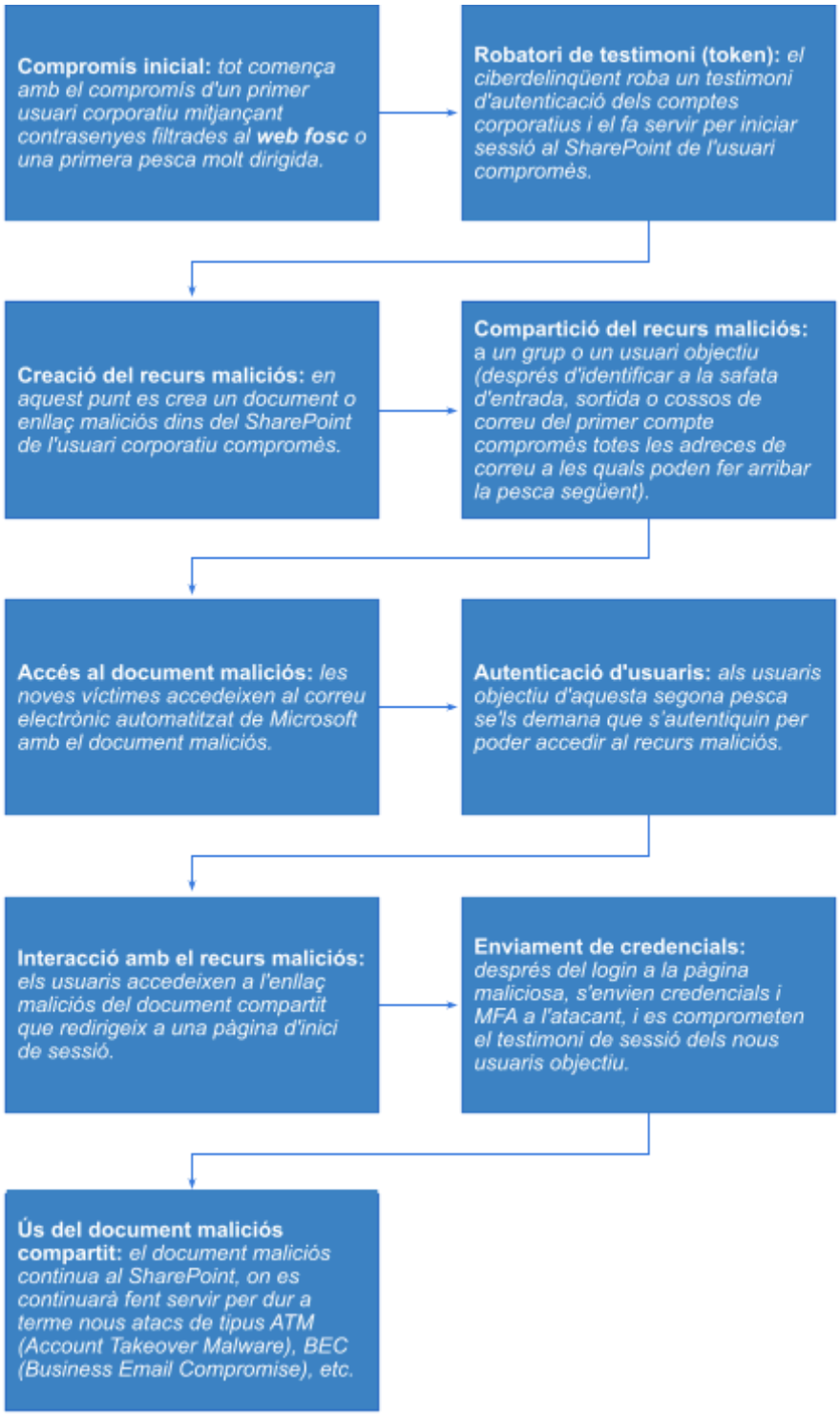
## 3.1. SharePoint, el recurs perfecte per evadir les defenses

El SharePoint és l'eina perfecta per poder fer un bypass d'eines de seguretat i passarel·les de correu electrònic que fa servir habitualment qualsevol organització, i això respon a diverses causes:

- El SharePoint és una eina de Microsoft molt utilitzada i de confiança per a les organitzacions.
- Els dominis o enllaços allotjats a SharePoint no solen aparèixer com a IOC a les BD que solen tenir els sistemes de protecció.
- Els atacants tenen una flexibilitat d'atac molt alta basada en l'agilitat per rotar els dominis i els enllaços que formen part dels seus atacs. En cas que un domini o enllaç sigui denunciat i comenci a identificar-se com a maliciós i, per tant, com a IOC, l'actor d'amenaça en pot fer servir un altre de nou i net de manera ràpida.
- A més de dominis i enllaços, els ciberdelinqüents poden allotjar de manera molt senzilla un altre tipus de recursos, com a contingut maliciós en forma de documents, pàgines d'inici de sessió falses o similars, dins del SharePoint.
- Les pàgines que s'allotgen al SharePoint solen ser dinàmiques, cosa que dificulta el treball a les eines d'anàlisi i detecció, ja que no són capaces de donar-ne un veredicte maliciós.

## 4. TAXONOMIA D'ATAC: MODUS OPERANDI

A l'esquema següent es representa i explica l'atac en detall:



# 5. CAMPANYES DOCUMENTADES

Aquesta metodologia no és nova. De fet, es té constància de l'ús de recursos legítims per dur a terme atacs de pesca, almenys, des del 2019. Però com passa amb tot en el sistema de la ciberdelinqüència, no paren d'evolucionar.

## 5.1 PhishPoint (2018 en endavant)

És un dels primers exemples públics de campanyes de pesca que aprofiten el SharePoint per evadir defenses. El modus operandi és relativament simple però força enginyós.

Comença amb l'enviament d'un correu que diu «algú ha compartit amb tu un document a SharePoint (o una cosa semblant), com ara les típiques notificacions legítimes de Microsoft/SharePoint.

L'enllaç inicial apunta a un document real allotjat a SharePoint (o algun altre recurs legítim). Això permet que s'eludeixin els filtres de seguretat del servei de correu afectat perquè no sembla maliciós en primera instància.

Però en aquest punt és quan comença el veritable compromís: dins del document legítim en qüestió s'hi amaga un enllaç (o diverses redireccions) que, seguidament, portarà l'usuari a una pàgina de pesca. En ella es trobarà amb un formulari d'inici de sessió fals en què, si l'usuari introdueix les seves credencials de l'Office 365, seran robades.

En altres paraules: el primer salt, mitjançant SharePoint, és «legal, cosa que ajuda a eludir moltes defenses basades en la reputació de dominis o enllaços.

L'objectiu típic és obtenir credencials i mètodes d'autenticació complementaris 2FA, tokens o OTP per obtenir accés al *tenant* d'Office 365.

Les raons que expliquen que hagi estat una estratègia d'atac amb tant d'èxit i, per tant, tan recurrent són:

- Fer servir una infraestructura legítima com ara SharePoint, que està molt estesa en entorns corporatius.
- Aparença de col·laboració legítima.
- Gran capacitat per eludir defenses, ja que dificulta als filtres de protecció convencionals distingir aquest tipus de correus maliciosos dels legítims, a causa de l'ús de dominis fiables o, almenys, no informats com a maliciosos.

Cal tenir en compte que «PhishPoint» ha estat una campanya que ha tingut continuïtat, i s'ha adaptat als contextos nous. Però ha marcat sens dubte una generació d'atacs que no depenen únicament d'enllaços maliciosos directes, sinó de l'ús de plataformes que els defensors consideren fiables.

## 5.2 Operacions de robatori de credencials via comptes legítims (2023-2025)

Una evolució natural de PhishPoint ha estat la que ha dut els atacants a aconseguir directament el suport dels comptes legítims compromesos.

En aquests casos, l'atacant aconsegueix comprometre un compte real d'un proveïdor, soci extern o empleat, dins de l'Office 365 o el SharePoint.

Després fa servir aquest compte per compartir documents «infectats» amb els seus contactes. Aquests contactes els identifica revisant tots aquells comptes que puguin aparèixer a la seva agenda, la safata d'entrada, de sortida o, fins i tot en cossos de missatges. I, evidentment, aquests documents porten enllaços que redirigeixen als nous usuaris objectiu pàgines d'inici de sessió falses.

Quan les víctimes fan clic a l'enllaç, se'ls demana que s'autentiquin (suposadament per veure'n el contingut), però estan introduint les credencials en un formulari creat per l'atacant. I sol ser molt eficaç atès que la invitació prové d'un compte conegut o legítim, cosa que comporta no aixecar sospites.

Aquest tipus d'atac ja està integrat a moltes campanyes modernes i complementa enfocaments de pesca més «freds» o convencionals.

## 5.3 ClickFix: atacs HTML + PowerShell + C2 (2025)

A mesura que les defenses milloren (filtres antipesca, detecció basada en URL sospitosos), els atacants han evolucionat cap a tècniques més agressives i barrejades amb execució remota o codi maliciós (*malware*).

La taxonomia en la qual se sustenta ClickFix, o tècniques similars, és:

- Enviar un correu amb un fitxer HTML (o un document amb HTML embegut) que quan l'usuari l'obre, mostra un missatge enganyós com, per exemple, «error en obrir el fitxer, prem aquí per carregar-lo».

- Si l'usuari accepta, se l'indueix a executar una ordre PowerShell o un script local que descarrega programari maliciós des d'un servidor controlat per l'atacant, de vegades aprofitant el SharePoint com a allotjament de la càrrega útil.

- En alguns casos, s'abusa d'API legítimes, i Microsoft Graph s'ha identificat com una de les més habituals, perquè les comunicacions del codi maliciós semblin trànsit «normal» d'Office 365 o SharePoint. I això, en dificulta enormement la detecció.

- El codi maliciós desplegat pot ser de tipus C2, com ara el «Havoc Demon», un dels que ja han estat documentats per la seva alta recurrència i impacte. I així, amb aquest tipus de

codi maliciós (*malware*), l'atacant acaba obtenint accés persistent i control sobre el sistema afectat.

Aquestes campanyes representen un esglaó evolutiu important: ja no es tracta de robar credencials, sinó que l'objectiu subjacent és una infecció persistent o un moviment lateral mitjançant l'ús de la mateixa infraestructura de Microsoft i ocultar comportaments maliciosos.

I això ja mostra una metodologia mitjançant la qual els atacants combinen pesca social amb execució tècnica i persistència.

## 5.4 ToolShell: explotació de vulnerabilitats al back-end de SharePoint (2025)

Mentre que les campanyes de pesca evolucionen a la capa d'interacció amb l'usuari, una evolució paral·lela (i molt més perillosa) ha estat l'explotació directa de vulnerabilitats crítiques a servidors de SharePoint *on premises*. Aquesta línia d'atacs no depèn de la interacció de l'usuari i és més sofisticada.

Una de les operacions d'atac més rellevants identificades durant aquest 2025 ha estat l'explotació activa de CVE-2025-53770 (inclosa la parella, el CVE-2025-53771), que Microsoft anomena part de l'operació «ToolShell». I, si s'aborda de manera cronològica per intentar entendre com va començar a implementar-se i la seva evolució, ens trobaríem davant de les fites clau següents:

- A partir del 7 de juliol del 2025 s'observen els primers intents d'explotació de la vulnerabilitat.
- El 18 de juliol del 2025 es va registrar un salt d'activitat més ampli: desenes de servidors comencen a ser atacats, amb desplegaments de *shells web* (spinstall0.aspx) i extracció de claus de màquina (MachineKey) d'ASP.NET.

### 5.4.1 Anàlisi tècnica de la taxonomia de l'atac

La documentació dels investigadors que han analitzat aquesta operació fa al·lusió directa a les vulnerabilitats que permeten execució de codi remot (RCE) sense autenticació a servidors vulnerables de SharePoint *on-locals*.

El vector d'explotació inclou un POST maliciós a l'*endpoint* /_layouts/15/ToolPane.aspx, i aprofita la manipulació de la capçalera HTTP Referer, juntament amb la desserialització de dades no fiables per executar codi arbitrari.

Després d'obtenir accés, els atacants despleguen un *shell web* (per exemple spinstall0.aspx) a la carpeta TEMPLATE\LAYOUTS. I seguidament, fan servir aquest accés per extreure la ValidationKey i la DecryptionKey del servidor. Per què això és tan important? Perquè aquestes claus els permeten signar càrregues útils malicioses, regenerar sol·licituds signades o, simplement, mantenir persistència. De fet, tenen la capacitat de continuar accedint fins i tot si algú elimina l'intèrpret d'ordres web inicial, perquè ja tenen les claus criptogràfiques per generar càrregues útils legítimes.

És cert que aquí cal parar esment a un detall molt important: no són campanyes orquestrades per qualsevol classe d'actor d'amenaça, no. Fins on s'ha pogut saber i a causa de la seva complexitat, totes les investigacions dutes a terme per Microsoft han permès atribuir aquestes operacions a grups APT avançats, principalment patrocinats per la Xina, com Linen Typhoon, Violet Typhoon i Storm-2603.

### 5.4.2 Informació addicional

Les investigacions dutes a terme sobre ToolShell i campanyes similars, van permetre conèixer que aquestes eren simplement la fase inicial d'operacions més complexes i que buscaven tenir més impacte, i desencadenar en última instància al desplegament de programari de segrest, com es va veure amb «Warlock».

Pel que fa a les vulnerabilitats exposades anteriorment, Microsoft ja va publicar els pedaços pertinents, però també va advertir que els pedaços no resolien el problema per si mateixos en aquells casos en els quals s'hagués arribat a obtenir persistència mitjançant el robatori de claus i, per això, va instar a rotar MachineKeys en tots els casos.

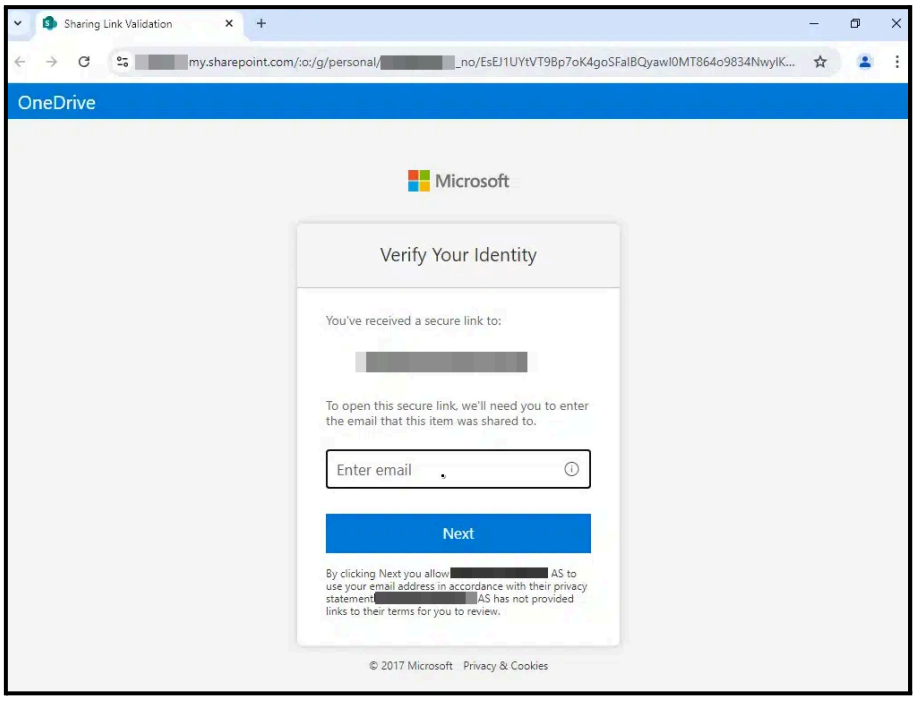
## 6. CAS D'ESTUDI: ANATOMIA DE LA PESCA DEL SHAREPOINT

A continuació, analitzarem i detallarem un cas en el qual uns ciberdelinqüents van obtenir accés a un compte corporatiu i després d'endinsar-se a l'organització van compartir un fitxer maliciós amb diferents contactes corporatius.

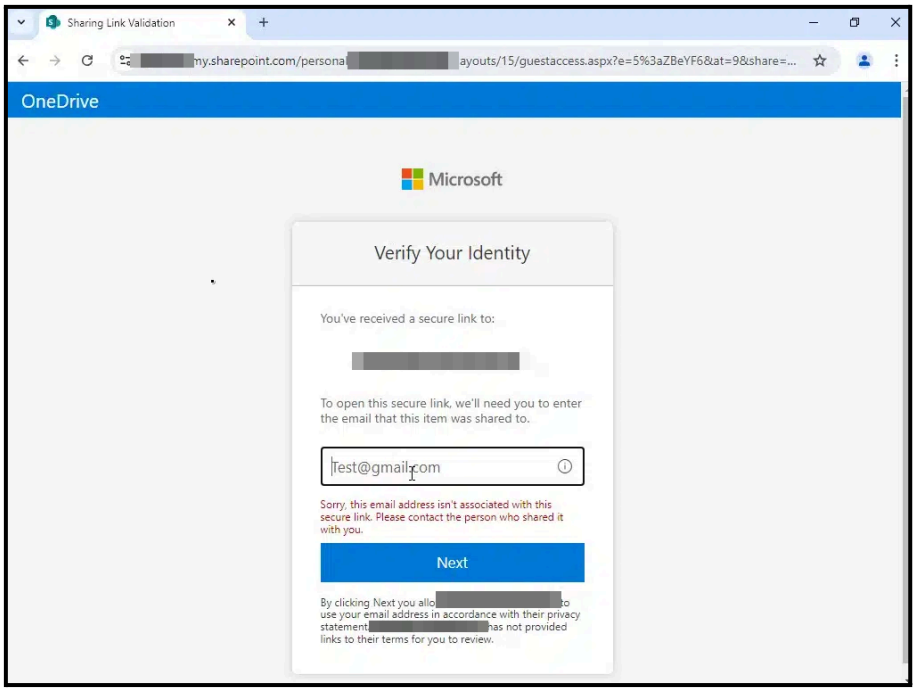
En primer lloc, es va comprometre un compte d'un proveïdor, fet que va permetre que el ciberdelinqüent pogués entrar dins de l'organització i fer-lo servir a favor seu per continuar distribuint l'atac. Després, el ciberdelinqüent va pujar un recurs amb contingut maliciós, més en concret un fitxer de OneNote que incloïa un enllaç maliciós.

D'aquesta manera, el ciberdelinqüent va aprofitar la capacitat de SharePoint i la infraestructura legitima, per poder compartir el fitxer amb tots els contactes corporatius relacionats amb el compte compromès.

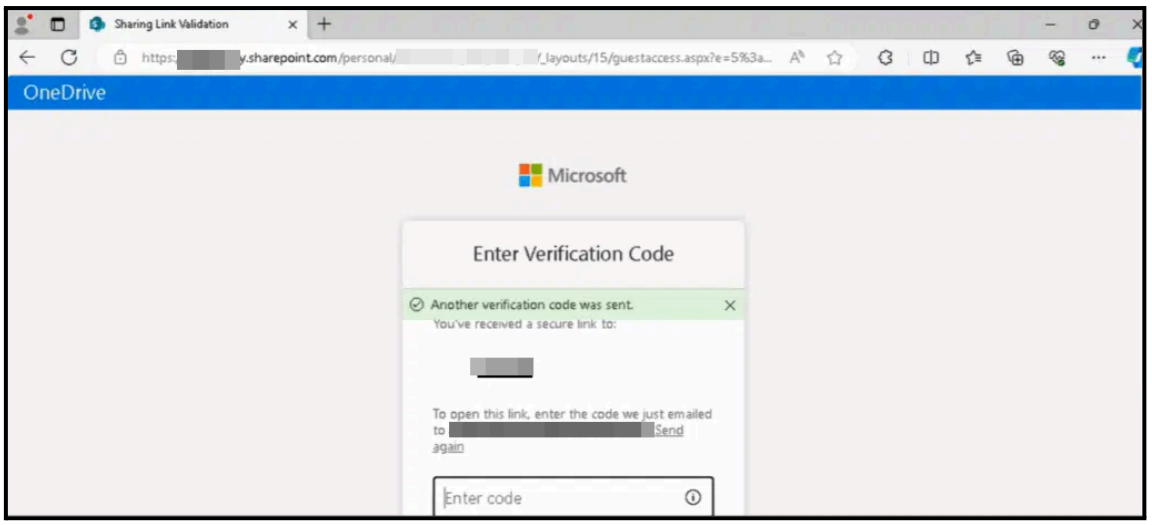
En fer clic al botó «Open», es redirigia a una pàgina d'inici de sessió legítima del mateix SharePoint. Quan els destinataris del correu introduïen les credencials a la pàgina d'inici de sessió, accedien al document maliciós de OneNote, compartit per l'atacant des del primer compte corporatiu que havia aconseguit comprometre.




Però abans, la pàgina d'inici de sessió legitima del mateix SharePoint inclou una fase de validació d'identitat, cosa que fa encara més creïble l'atac. Aquest tipus de fase no es pot evitar mitjançant un compte de prova o un altre compte del mateix domini, només és possible avançar si es proporciona el correu electrònic del destinatari.

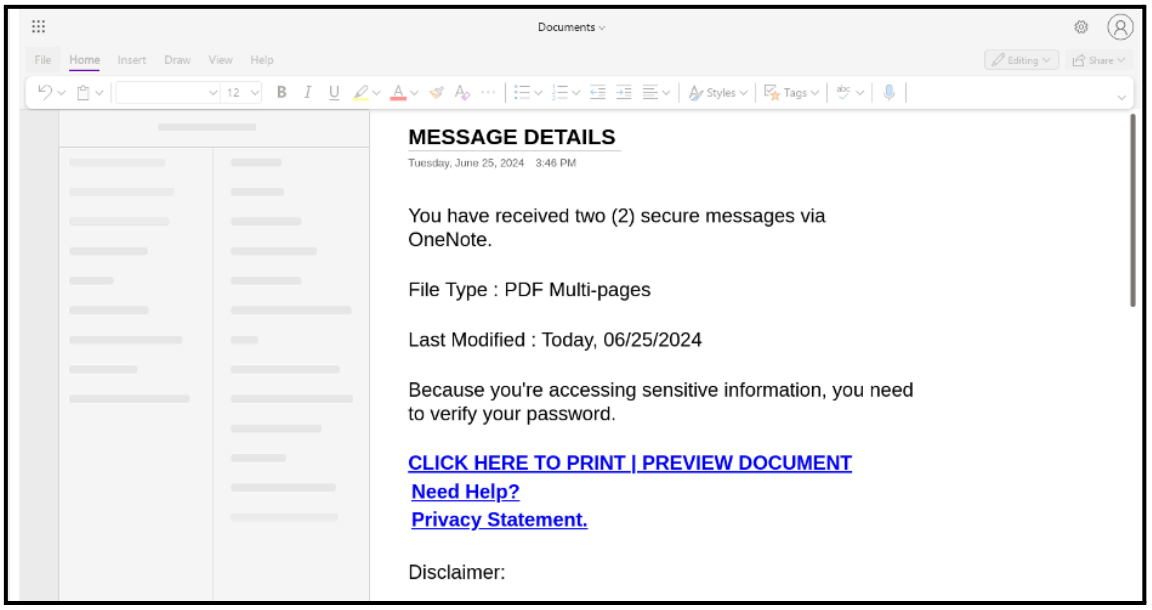



Després que l'usuari introduís correctament el correu electrònic, a la safata d'entrada arribava un codi d'autenticació.




Com es pot apreciar a la imatge, es tracta d'un codi de validació legítim de Microsoft i, novament, veiem com se segueix reforçant la confiança de les víctimes: tot sembla indicar que tant el remitent com el document OneNote són segurs.


Quan el destinatari ja estava dins del document OneNote compartit, veia un enllaç. Si feia clic, el portava a introduir les seves credencials. I, en aquest moment, el ciberdelinqüent les aconseguia.



Segons les motivacions i els objectius que hi hagués després de la campanya de pesca, aquest tipus d'atac podria provocar des del simple robatori de credencials o informació confidencial fins a propagar codi maliciós de tota mena, inclòs programari de segrest.

# 7. RECOMANACIONS D'ATACS DE PESCA DE SHAREPOINT

## 7.1 Recomanacions de prevenció

Per evitar que els ciberdelinqüents puguin comprometre comptes i compartir enllaços maliciosos, les recomanacions que cal seguir són les següents:

- Formació del personal, això és el més important, més important que qualsevol eina que bloqueja tota mena de pesca, i és que formar els empleats perquè puguin reconèixer correus sospitosos fins i tot si provenen de remitents interns és la prevenció més rendible.
- Implementar MFA i revisar accessos OAuth.
- Limitar la compartició externa, controlar permisos dels usuaris i la durada dels URL.
- Fer simulacions de pesca periòdicament per posar a prova els empleats i ajudar-los a millorar en aquest aspecte.
- Aplicar una protecció tecnològica addicional com filtres antipesca, antivirus avançat i solucions específiques per a SharePoint.

## 7.2 Recomanacions de mitigació

Si un usuari està compromès com a víctima d'un atac de pesca, aquestes són les mesures de mitigació que cal prendre:

- Restablir la contrasenya de l'usuari víctima.
- Comprovar si s'ha afegit algun MFA maliciós al compte i, en cas afirmatiu, eliminar-lo.
- Tancar la sessió a tots els dispositius on s'ha allotjat el compte.
- Bloquejar l'URL maliciós inicial del SharePoint i qualsevol domini associat.
- Bloquejar i eliminar els correus electrònics maliciosos i comprovar si hi ha alguna regla maliciosa creada a la safata d'entrada.
- Finalment, fer una anàlisi del dispositiu compromès, per descartar qualsevol signe sospitós.

## 8. CLÀUSULA DE CONFIDENCIALITAT

Aquest document és propietat de l'Agència Nacional de Ciberseguretat d'Andorra. Tota la informació que conté és confidencial, aquesta informació s'actualitzarà regularment per reflectir els possibles canvis dels productes i no podrà ser copiada o revelada a terceres persones sigui totalment o en part, sense consentiment previ exprés de l'Agència Nacional de Ciberseguretat d'Andorra.