Secureworks

From Feature to Weapon: Breaking Microsoft Teams and SharePoint integrity

@DrAzureAD

https://linkedin.com/in/nestori

https://aadinternals.com



Dr Nestori Syynimaa

Senior Principal Security Researcher

Secureworks® CTU™

Twitter/Mastodon/BlueSky:

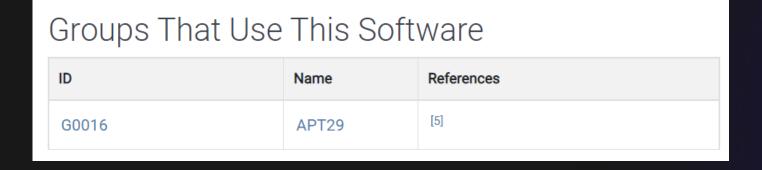
@DrAzureAD @infosec.exchange .bsk.social





AADInternals

- Admin & hacking toolkit for Azure AD & Microsoft 365
- Open source:
 - https://github.com/gerenios/aadinternals
 - https://aadinternals.com/aadinternals
- MITRE ATT&CK
 - https://attack.mitre.org/software/S0677/







by Amith Ramsumair and 36 others









 $\textbf{Olaf Hartong} \ @ olafhartong \cdot 22h$

Replying to @aavdberg and @DrAzureAD

Great advice. This picture of is also epic for memes.

 \bigcirc

2

•

8

Λ,



Ben Owens @BenjaminOwens · 18h

Replying to @aavdberg @nicolonsky and @DrAzureAD

This needs the background removing so @DrAzureAD can be added to security gaps discovered

 \bigcirc 1

ĹŢ

W 1

,Τ,



Ben Owens @BenjaminOwens · 18h

Contents

- SharePoint Migration Options
- What is SPMT
- How does Granular Backup feature work?
- Abusing SPMT API x2
- Demo x2

SharePoint Online Migration options

- Migration Manager
- SharePoint Migration Tool (SPMT)
- Cross-tenant OneDrive migration

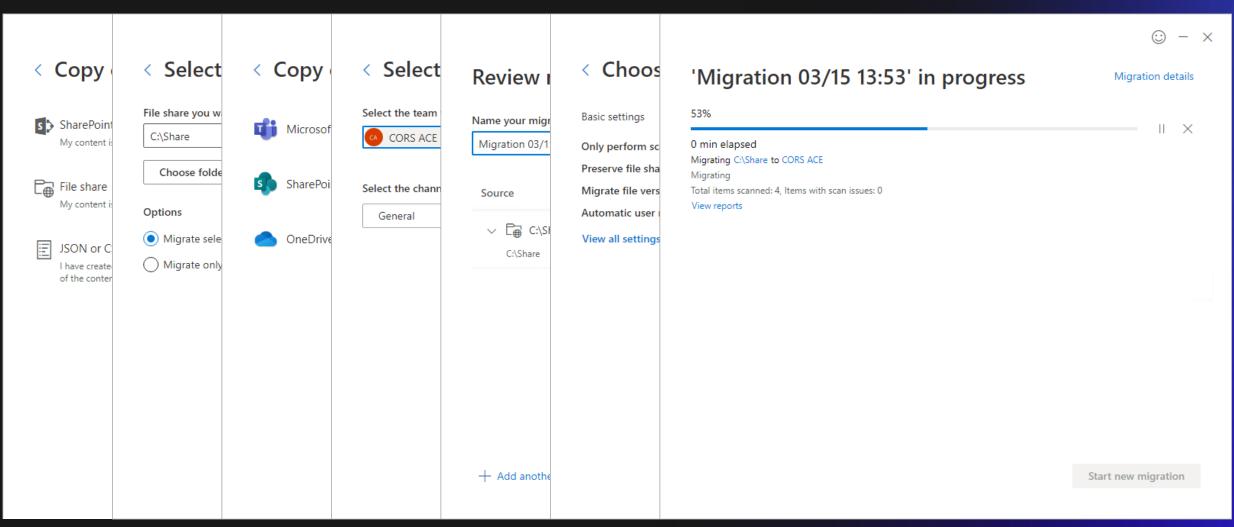
What is SPMT?

- SharePoint Migration Tool (SPMT)
 - a free and easy to use migration solution to help you migrate content from on-premises SharePoint sites to Microsoft 365
- Supports migration to:
 - SharePoint Online, OneDrive, and Teams
- Supports migration from:
 - SharePoint Server 2010, 2013, 2016, and 2019
 - SharePoint Foundation 2010 & 2013
 - Network shares

SPMT process

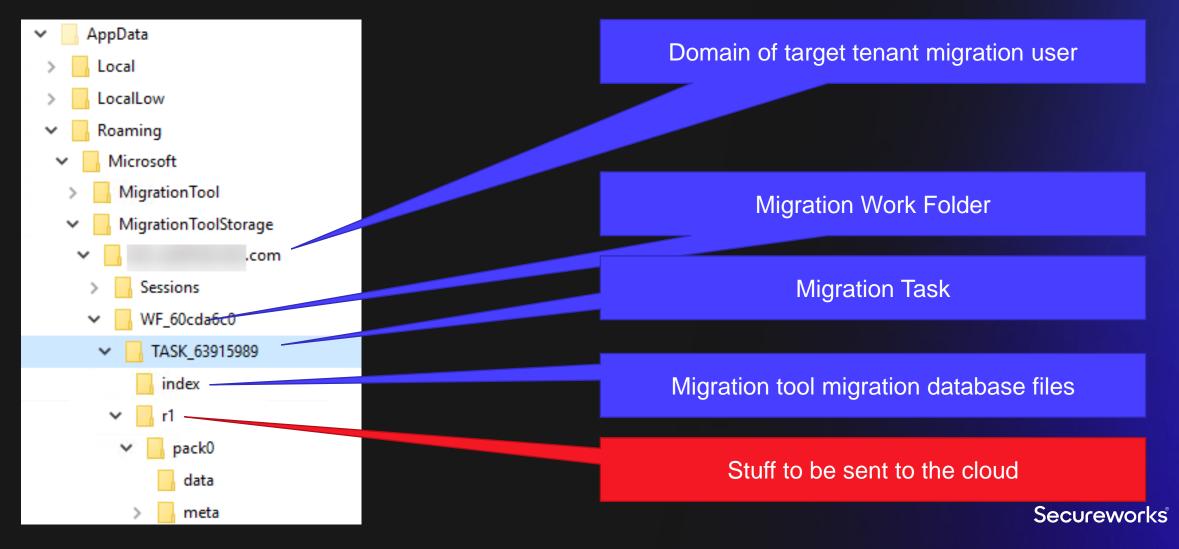
- 1. Install SPMT
- Create migration task
- 3. Monitor and report

Create migration task



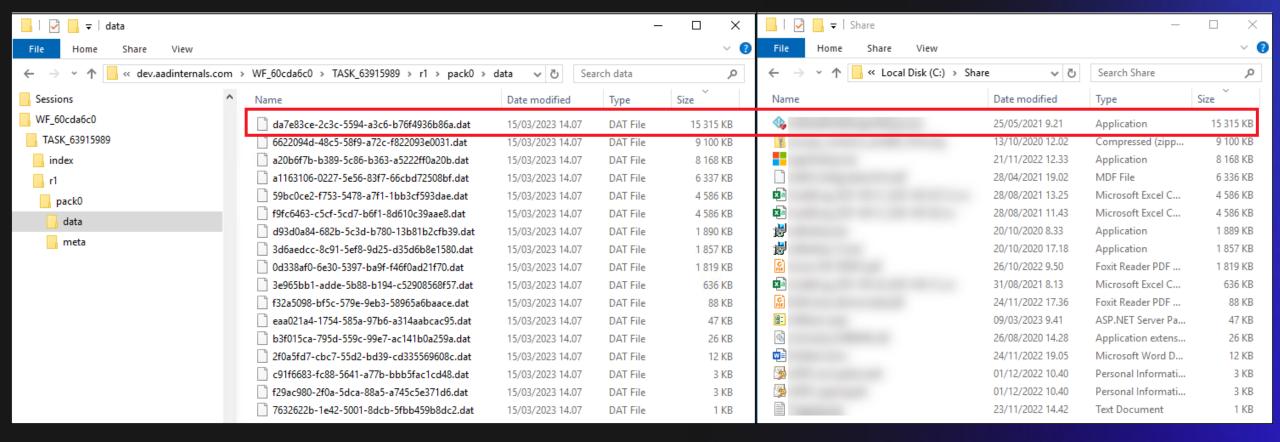
Temporary files

User's AppData\Roaming\Microsoft\MigrationToolStorage



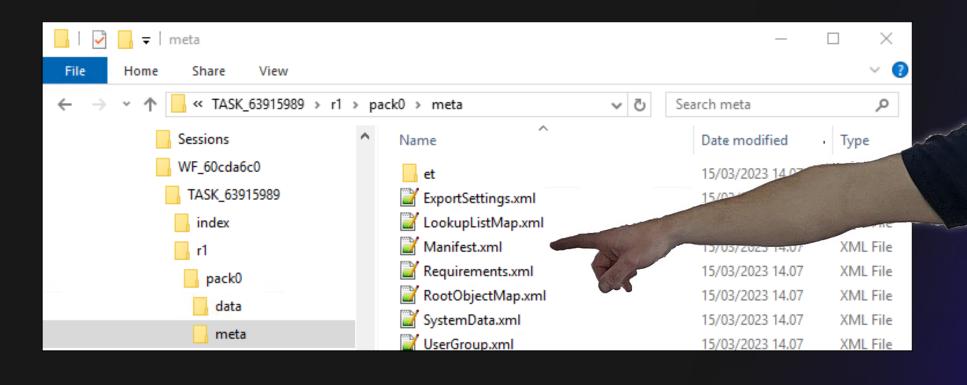
Data

Files are encrypted and renamed to <guid>.dat



Metadata

Files are encrypted



```
?xml version="1.0" encoding="utf-8"?>
<SPObjects xmlns="urn:deployment-manifest-schema">
 <SPObject Id="df34fe4a-5577-4f52-9a52-laa64ce8b92b" ObjectType="SPFolder" ParentId</pre>
   <Folder Id="df34fe4a-5577-4f52-9a52-laa64ce8b92b" Name="admin aadinternals onmic
 </SPObject>
 <SPObject Id="46a4d46c-f9a3-4bb2-80ee-d99e41525f53" ObjectType="SPFolder" ParentId</pre>
   <Folder Id="46a4d46c-f9a3-4bb2-80ee-d99e41525f53" Name="Documents" ParentFolderI
 </SPObject>
 <SPObject Id="acc442c0-d834-4456-b6ec-a755459f491c" ObjectType="SPDocumentLibrary"</pre>
   <DocumentLibrary Id="acc442c0-d834-4456-b6ec-a755459f491c" BaseTemplate="MySiteD"</pre>
  </SPObject>
 <SPObject Id="6ald19a6-ce7d-5d8c-aldf-fea2685034d4" ObjectType="SPFile" ParentId="</pre>
    <File Url="Documents/Tiedosto.txt"
   Id="6a1d19a6-ce7d-5d8c-a1df-fea2685034d4"
   ParentWebId="5ac5b4f2-8830-4b68-8811-276e29e0595d"
   ParentWebUrl="/personal/admin aadinternals onmicrosoft com"
   Name="Tiedosto.txt"
   ListItemIntId="4"
   ListId="acc442c0-d834-4456-b6ec-a755459f491c"
   ParentId="46a4d46c-f9a3-4bb2-80ee-d99e41525f5
   TimeCreated="2022-11-21T11:01:58"
   TimeLastModified="2022-11-23T12:42:30"
   Version="1.0"
   FileValue="0de5973c-83b5-5ffa-9b8a-ae1486b10fe0.dat
   Author="1"
   ModifiedBy="1" -
   MD5Hash="wB9S7yjv9gCsbcgauoCtAg=="
   InitializationVector="YbW1WFmUkZEM7ODugUkJDw=="
     <Properties />
    </File>
 </SPObject>
 <SPObject Id="1894bc18-d81a-573f-bd91-2530089e297e" ObjectType="SPFile" ParentId="</pre>
   <File Url="Documents/BaconIpsum.txt" Id="1894bc18-d81a-573f-bd91-2530089e297e"
     <Properties />
    </File>
 </SPObject>
 <SPObject Id="6ald19a6-ce7d-5d8c-aldf-fea2685034d4" ObjectType="SPListItem"_Parent</pre>
   <ListItem FileUrl="Documents/Tiedosto.txt" DocType="File" ParentFolderId="46a4d4</pre>
     <Fields />
    </ListItem>
 </SPObject>
 <SPObject Id="1894bc18-d81a-573f-bd91-2530089e297e" ObjectType="SPListItem" Parent</pre>
   <ListItem FileUrl="Documents/BaconIpsum.txt" DocType="File" ParentFolderId="46a4"
     <Fields />
    </ListItem>
 </SPObject>
</SPObjects>
```

SPFile object

Timestamps!

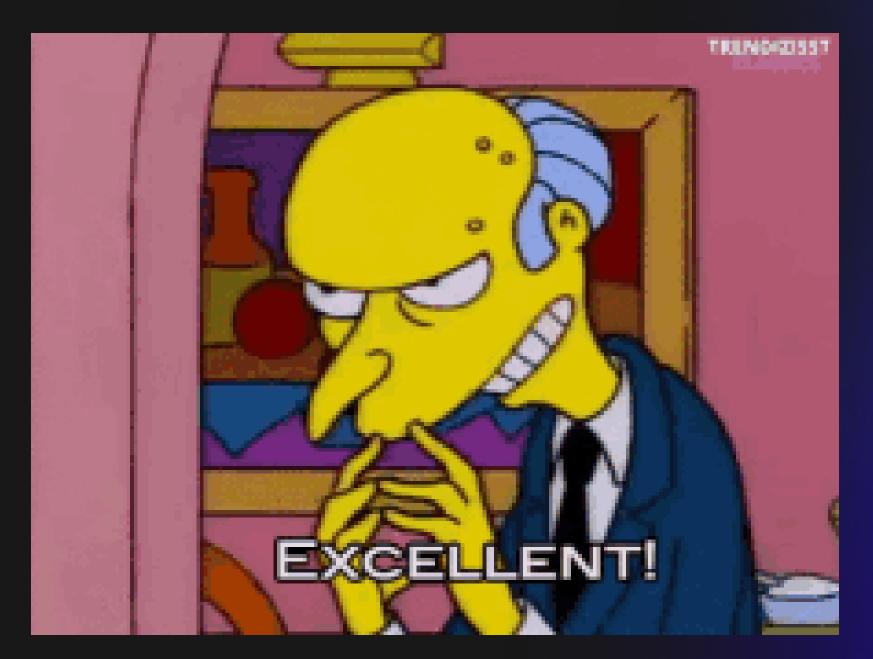
Refers to content file

Author!

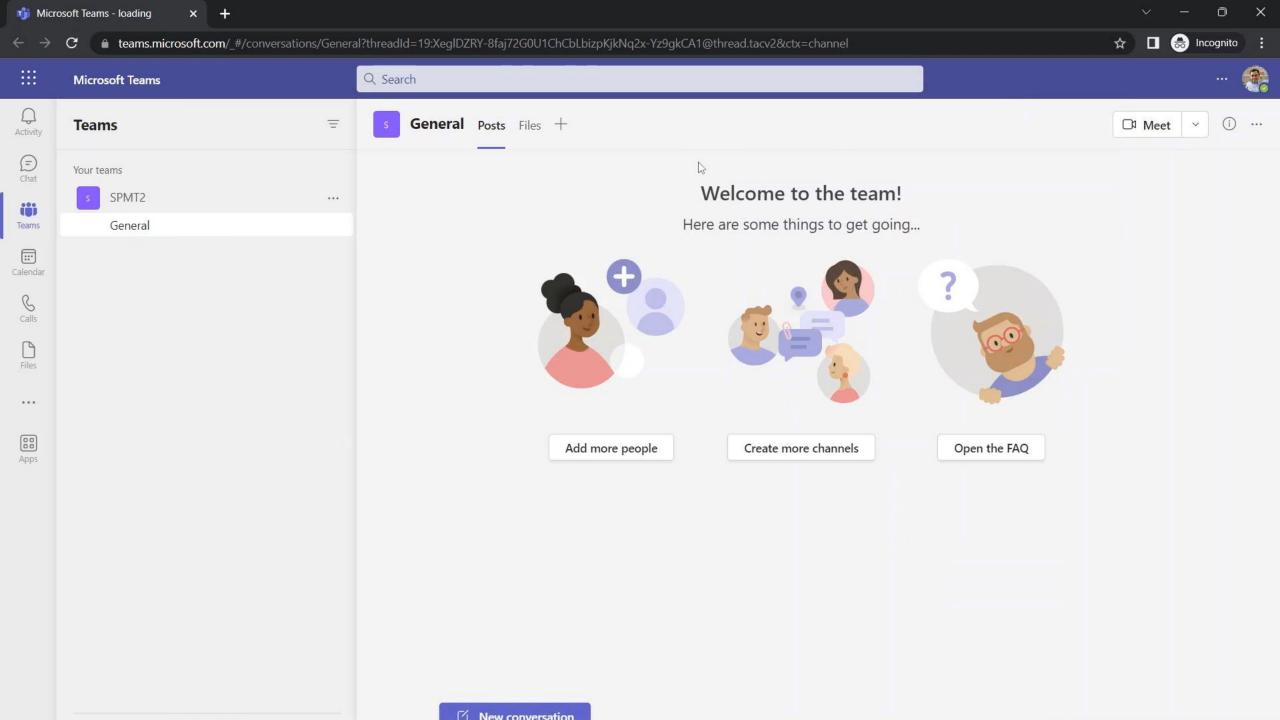
IV for decrypting the file content

Matching SPListItem

Secureworks

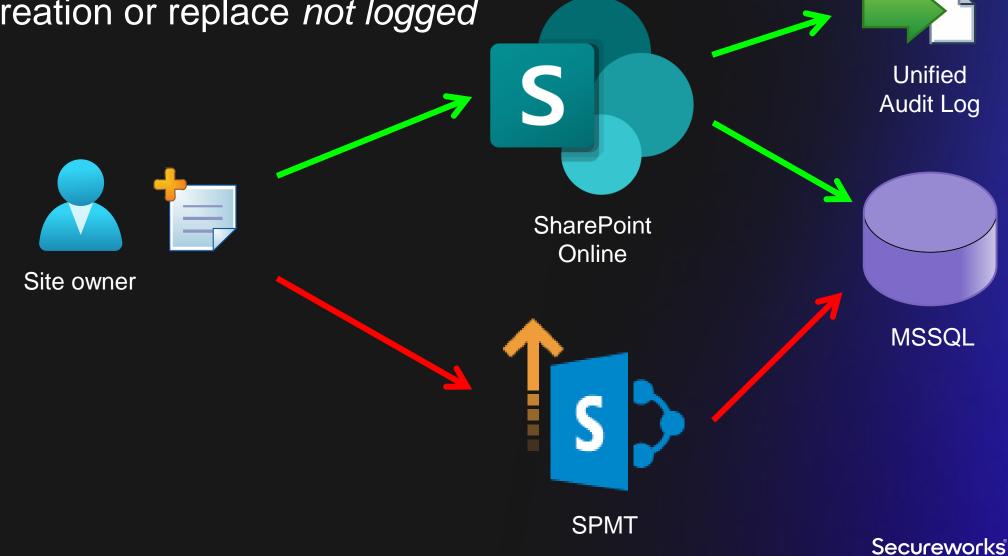


Abusing SPMT: Demo!



SPMT bypasses logging

• File creation or replace not logged



Reported to Microsoft Nov 28 2022

Description

Summary

SharePoint Migration Tool (SPMT) is meant for migrating large amount of files from on-prem file shares to SharePoint, OneDrive, or Teams. By abusing the backend API calls, site owners can spoof and tamper with files.

• Existing file the job, and we expect that a SCA has sufficient knowledge about the migration. For

Observed by

When using the timestamps, and sense for the migration experience.

File creations ar MSRC has investigated this issue and concluded that this does not require immediate Description attention as Migration API overwrites the existing files (clearly documented in SharePoint Online Import Migration API Microsoft Learn). When migrating content 1. Files and the from SharePoint On-premises, customers want to preserve metadata from source files, to keep them on SharePoint Online. Appending versions is not supported and the files will be overwritten. Only SharePoint site collection administrator (SCA) is able to submit

large enterprise customers, a tenant admin is responsible for migration of all content for

an organization. Therefore, preserving the name of the migrator does not make a lot of

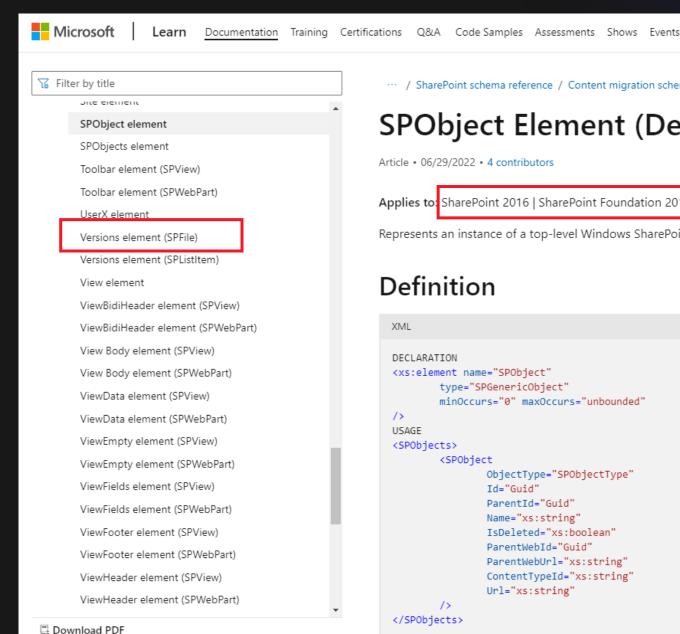
Consequently, site owners (such as a person that creates a Teams site) can create files as any user, including file history (spoofing). Moreover, they can replace existing files using the guid of existing file (tampering with).

When a file is created using SPMT APIs, it is not logged in audit log. When a file is replaced with SPMT APIs, there is a "Deleted file" event performed by "SHAREPOINT\System".

Secureworks

The Next Generation

Google



· · · / SharePoint schema reference / Content migration schemas / DeploymentManifest schema /

SPObject Element (DeploymentManifest)

Article • 06/29/2022 • 4 contributors

Applies to: SharePoint 2016 | SharePoint Foundation 2013 | SharePoint Online | SharePoint Server 2013

Represents an instance of a top-level Windows SharePoint Services 3.0 object (SPGenericObject).

Definition

```
XML
DECLARATION
<xs:element name="SPObject"</pre>
        type="SPGenericObject"
        minOccurs="0" maxOccurs="unbounded"
/>
USAGE
<SPObjects>
        <SP0bject
                 ObjectType="SPObjectType"
                 Id="Guid"
                 ParentId="Guid"
                 Name="xs:string"
                 IsDeleted="xs:boolean"
                 ParentWebId="Guid"
                 ParentWebUrl="xs:string"
                 ContentTypeId="xs:string"
                Url="xs:string"
        />
</SPObjects>
```



CANDIDATEID SITE NUMBER: FN35 REGISTRATION: ra6lon51fe YOUR SCORE: 911

DATE: nestori syynimaa Wednesday, June 10, 2009

NUMBER: 072-630

NG SCORE: 700

T: Pass ONAL RESULTS:

Configure Microsoft Of Needs Developme

Microsoft®

TS: Configuring Microsoft® Windows® SharePoint® Services

NDIDATE: nestori syynimaa

TE: Wednesday, May 13, 2009

AM NUMBER: 070-631 SSING SCORE: 700

SULT: Pass

CTIONAL RESULTS:

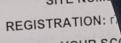
CANDILATE

SITE NUM

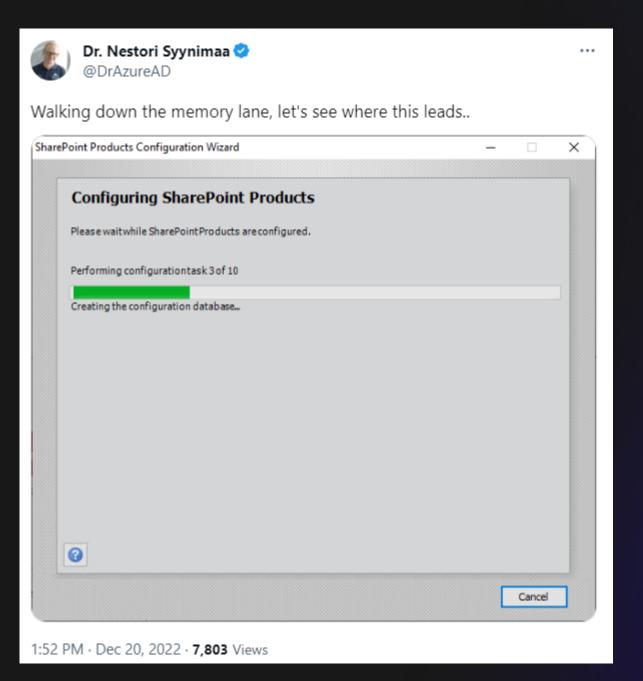
YOUR SCO

Nesten Sypimaa





Deploy Windows SharePoint Services 3.0



On-prem SharePoint backup



Backup and Restore

Central Administration

Application

Management

System Settings

Monitoring

Backup and Restore

Security

Upgrade and Migration

General Application Settings

Apps

Office 365

Configuration Wizards



Farm Backup and Restore

Perform a backup | Restore from a backup | Configure backup settings | View backup and restore history | Check backup and restore job status



Granular Backup

Perform a site collection backup | Export a site or list | Recover data from an unattached content database | Check granular backup job status

Export the contents of a site or a list



Site Or List Export ©

Central Administration

Application Management

System Settings

Monitoring

Backup and Restore

Security

Upgrade and Migration

General Application Settings

Apps

Office 365

Configuration Wizards

Readiness

No export is in progress.

Timer service is running.

Site Collection

Select a site or list to export. First select the site collection that contains the site, then select a site to export. To export a list, select the site collection and site that contain it, and then select the list.

File location:

Specify the destination for the export package.

Export Full Security

Export full security of the site, including author, editors, created by times, and modified by times. This also includes all users in the sites.

Export Versions

Select the version history information to include for files and list items. You can include all versions, the last major version, the current version, or the last major and last minor versions.

Site Collection: http://sharepoint/sites/teamsite1 ▼

Site: No selection -

List: No selection ▼

Filename:

\backups\teamsite.cab

Overwrite existing files
Example: \backup\SharePoint\export.cmp

Export full security

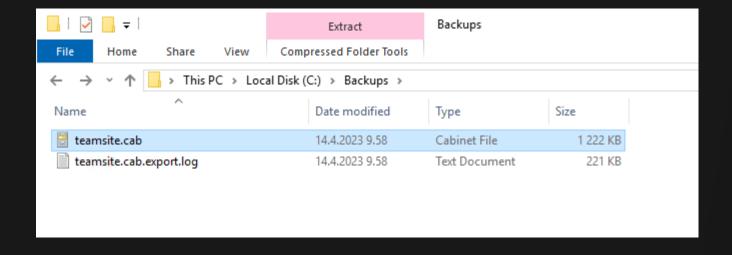
Export versions

All Versions

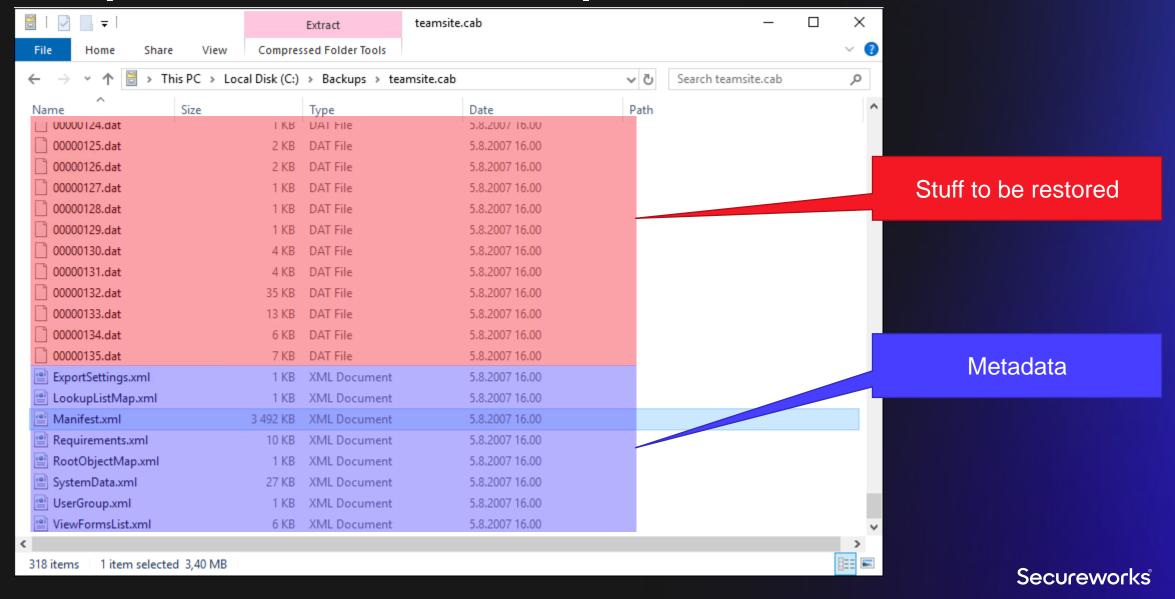
Start Export

Cancel

On-prem SharePoint backup



On-prem SharePoint backup



Same but more

```
<SPObject Id="73e6c285-54af-4628-b4bc-636788a47553" ObjectType="SPFile" ParentId="2feddf69-2280-450d-89b8-d9c4b3de29b1"</pre>
    <File Url="Style Library/Forms/EditForm.aspx"_Id="73e6c285-54af-4628-b4bc-636788a47553" ParentWebId="3a15fe51-d2cb-4
        <WebParts>
            <WebPart Name="1ba6637f-e85c-4f0e-acd2-a99bdb7cf>="DisplayName="" Flags="1048576" Hidden="false" Threaded=
        </WebParts>
    </File>
</SPObject>
<SPObject Id="6b1e3312-0d2c-4ddb-8872-939e1bc8adcb" ObjectType="SPFile" ParentId="2fe112"</pre>
                                                                                                                     de29b1"
    <File Url="Style Library/Forms/repair.aspx" Id="6b1e3312-0d2c-4ddb-8872-939e1bc8a
                                                                                                                     d2cb-4b4
                                                                                                  aspx file!
        <WebParts>
            <WebPart Name="e9727c7b-1ce1-4464-acf3-b1249c83d29c" DisplayName="$Resources.core,kerrink bocuments," Flags="</pre>
        </WebParts>
    </File>
</SPObject>
<SPObject Id="b8590518-372c-48b2-9a59-3da2f62f2ea4" ObjectType="SPFile" ParentId="2feddf69-2280-450d-89b8-d9c4b3de29b1"</pre>
    <File Url="Style Library/Forms/Thumbnails.aspx" Id="b8590518-372c-48b2-9a59-3da2f62f2ea4" ParentWebId="3a15fe51-d2cl
        <WebParts>
            <WebPart Name="965f75bb-8aff-45cb-ab12-53c4c5e65cf9" DisplayName="assetLibTemp" Flags="13" Hidden="true" This</pre>
        </WebParts>
    </File>
</SPObject>
```



Conclusion & hypothesis

- SPMT is using Granular Backup
- Granular Backup allows importing any site content (incl. aspx files)
- Therefore, we can replace design files using SPMT API

Custom script

What custom script can do

Every script that runs in a SharePoint page (whether it's an HTML page in a document library or a JavaScript in a Script Editor Web Part) always runs in the context of the user visiting the page and the SharePoint application. This means:

- Scripts have access to everything the user has access to.
- Scripts can access content across several Microsoft 365 services and even beyond with Microsoft Graph integration.

Custom scripts are prevented by default

Custom Script

Control whether users can run custom script on personal sites and self-service created sites. Note: changes to this setting might take up to 24 hours to take effect.

For more information, see https://go.microsoft.com/fwlink/? LinkId=397546

- Prevent users from running custom script on personal sites
- O Allow users to run custom script on personal sites
- Prevent users from running custom script on self-service created sites
- Allow users to run custom script on self-service created sites

Cross Site Scripting (XSS)??

For security reasons, browsers restrict cross-origin HTTP requests initiated from scripts. For example, xmlhttpRequest and the Fetch API follow the same-origin policy. This means that a web application using those APIs can only request resources from the same origin the application was loaded from unless the response from other origins includes the right CORS headers.

Origin: https://aadinternalsdev.sharepoint.com

Sec-Fetch-Site: same-origin

Sec-Fetch-Mode: cors Sec-Fetch-Dest: empty

Tokens are retrieved using an internal API

To acquire a valid access token, **GraphHttpClient** issues a web request to the /_api/SP.0Auth.Token/Acquire endpoint. This ADI internal use. You should not communicate with it directly in your solutions.

POST https://aadinternalsdev.sharepoint.com/sites/SPMTPOC2/_api/SP.OAuth.Token/Acquire HTTP/1.1

Host: aadinternalsdev.sharepoint.com

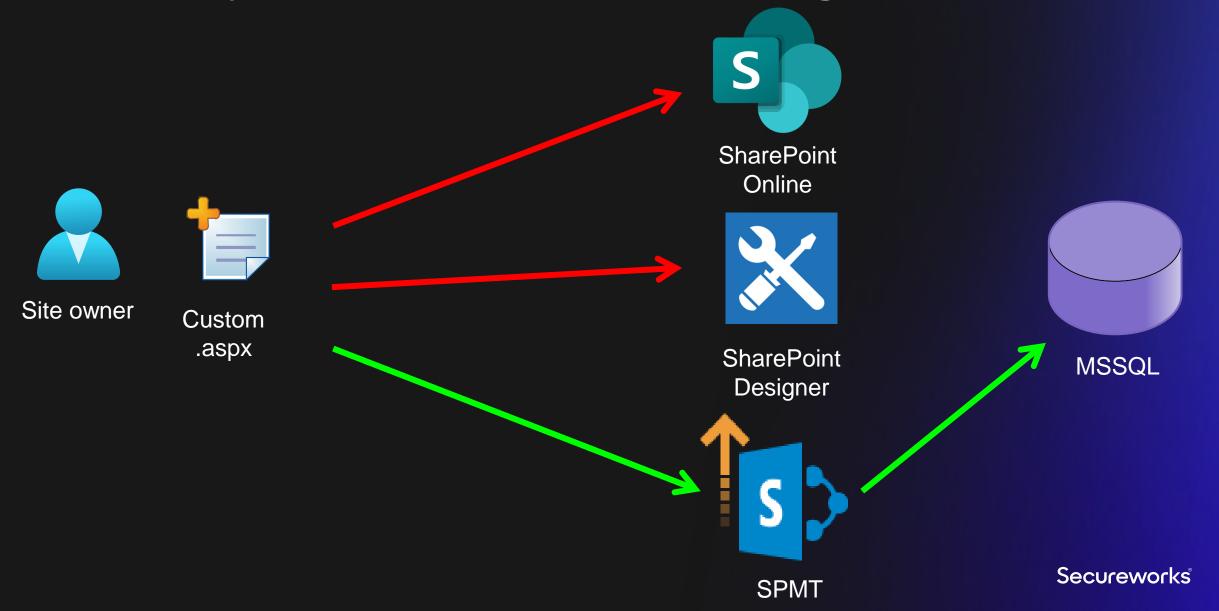
Connection: keep-alive

Content-Lenath: 43

Cookie: SPOIDCRL=//u/PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0idXRmLTgiPz48UlA+VjEyLDBoLmZ8bWVtYmV

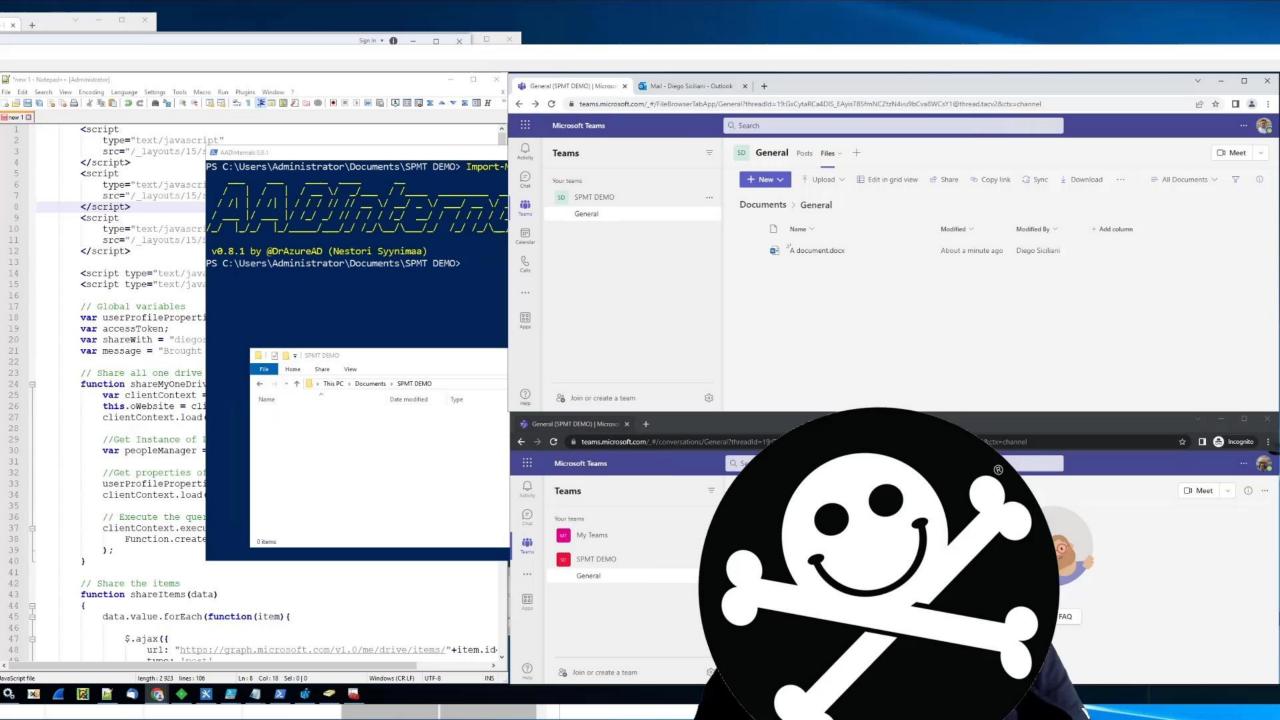
{"resource": "https://graph.microsoft.com"}|

SPMT bypasses custom script settings

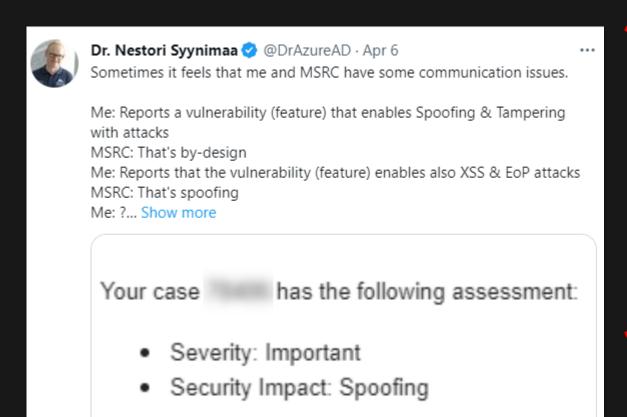




Abusing SPMT 2nd generation: Demo!



Communicating with Microsoft 1/2



Promote

11 20.6K

46

仚

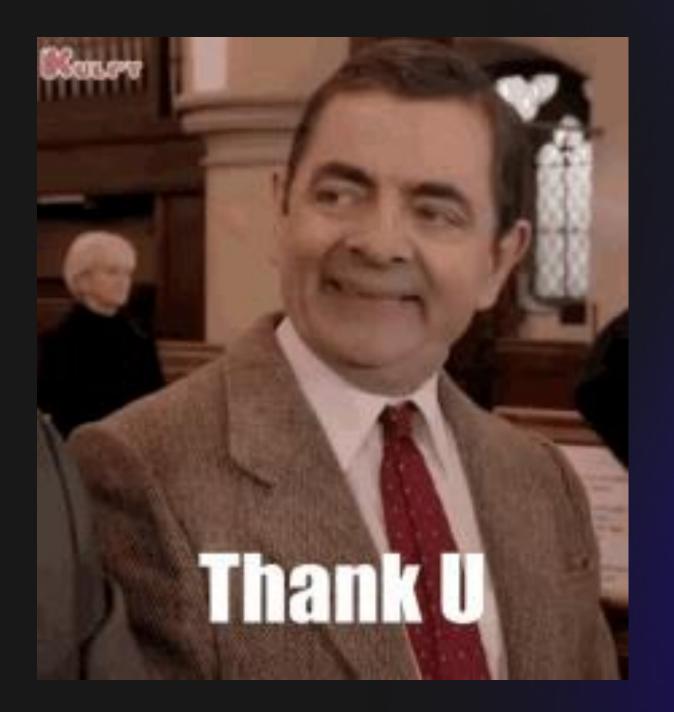
SP.OAuth.Token

```
HTTP/1.1 400 Request

{
    "odata.error": {
        "code": "10001",
        "message": {
             "lang". "en-US",
             "v.rue": "Missing refresh token."
        },
             "error.redirectUrl": "https://aadinter.alsdev.sha
```

Communicating with Microsoft 2/2

- Final fix deployed Aug 10
- Prevents uploading .aspx files when custom script is prevented



Questions?

Secureworks