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

MVP
Microsoft®
Most Valuable
Professional

MICROSOFT
MOST VALUABLE
Security
Researcher
ESTD. 2022
VOLUME

Secureworks®

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/



Groups That Use This Software

ID	Name	References
G0016	APT29	[5]

Liked

by Amith Ramsumair and 36 others

Andre van den Berg - #WIMVP 🇳🇱 🐱👤 @aavdberg · Sep 22

Good tip by @DrAzureAD about preventing MFA bypass by identity provider #IdentySummit



5 22 131

Olaf Hartong @olafhartong · 22h

Replying to @aavdberg and @DrAzureAD

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

2 8

Ben Owens @BenjaminOwens · 18h

Replying to @aavdberg @nicolonsky and @DrAzureAD

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

1 1

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

https://learn.microsoft.com/en-us/sharepointmigration/migrate-to-sharepoint-online

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

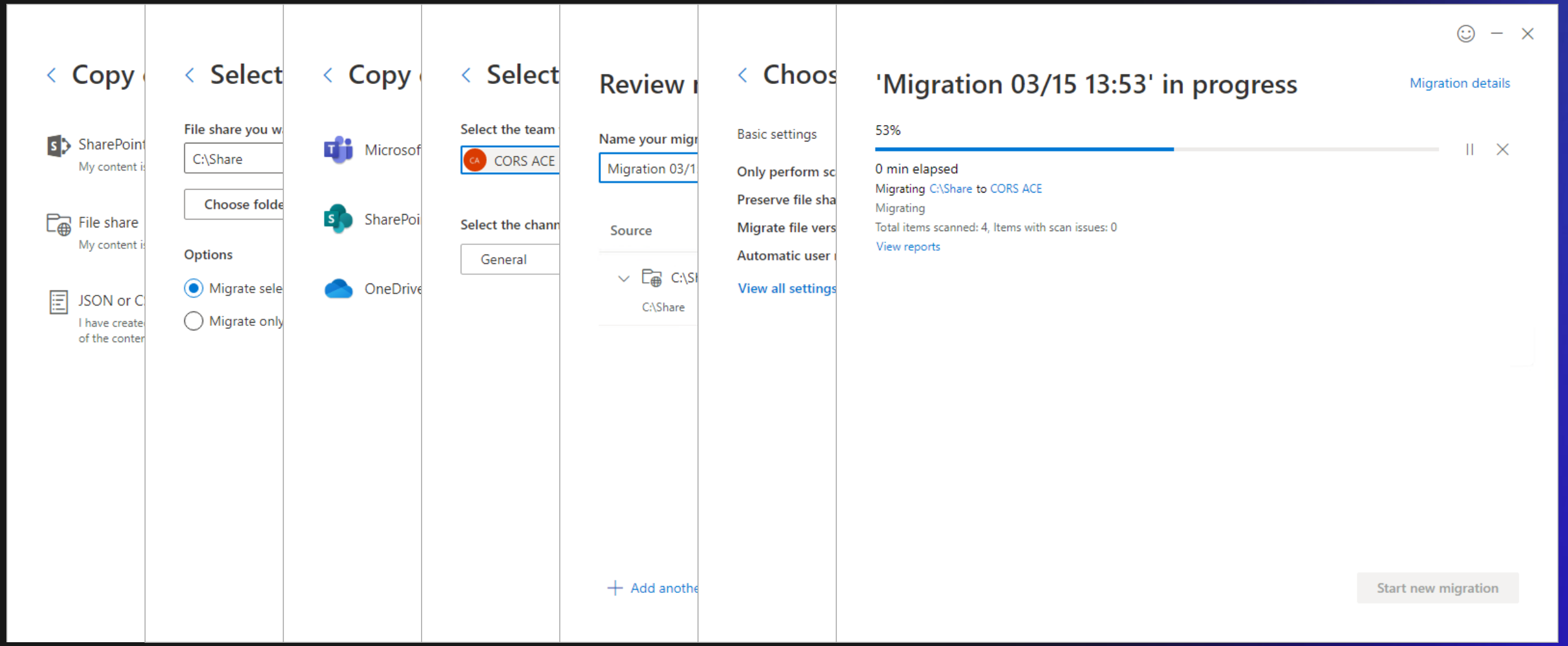
https://learn.microsoft.com/en-us/sharepointmigration/introducing-the-sharepoint-migration-tool

SPMT process

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

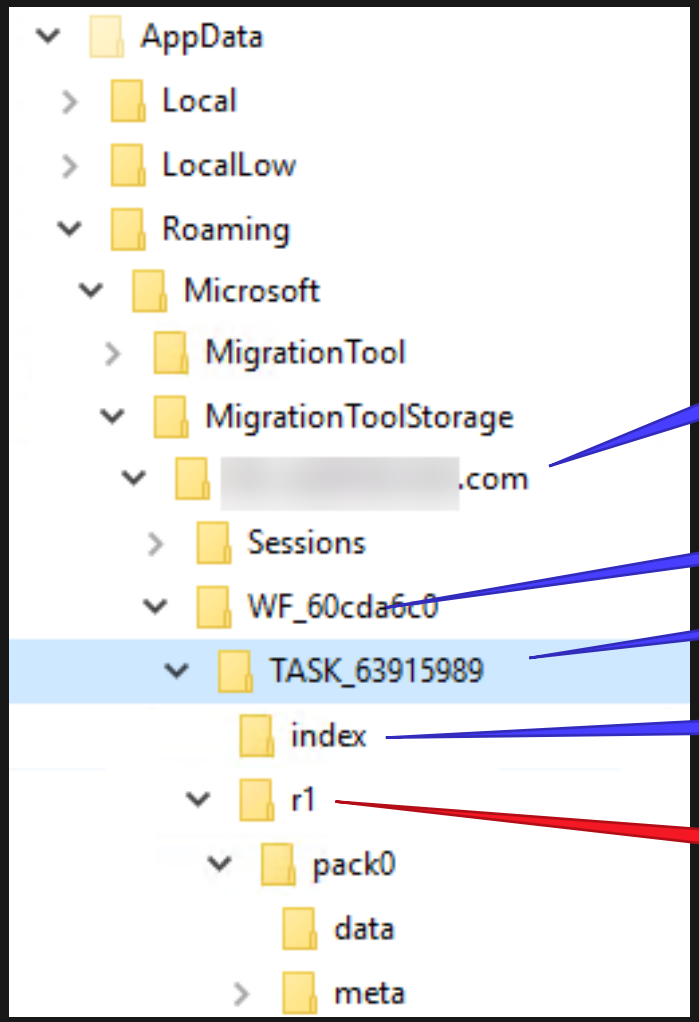
https://learn.microsoft.com/en-us/sharepointmigration/introducing-the-sharepoint-migration-tool

Create migration task



Temporary files

- User's `AppData\Roaming\Microsoft\MigrationToolStorage`



Domain of target tenant migration user

Migration Work Folder

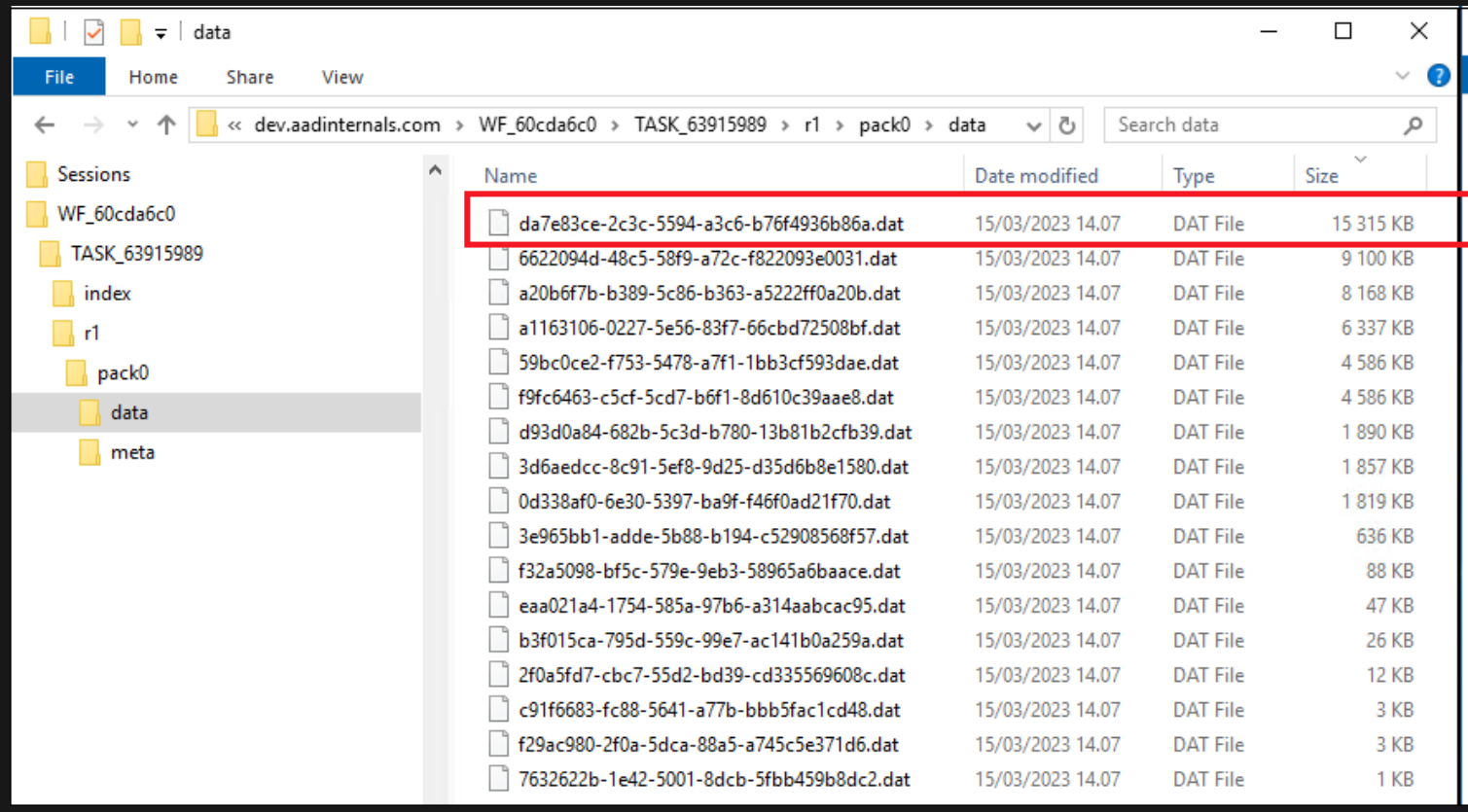
Migration Task

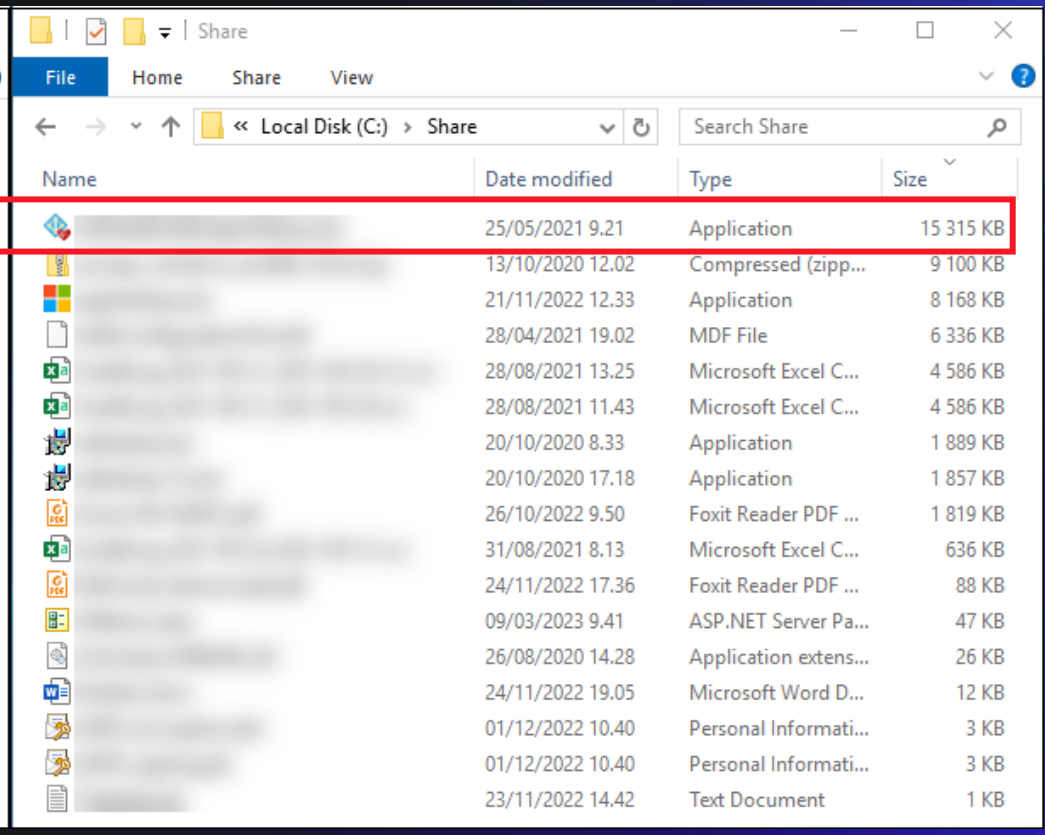
Migration tool migration database files

Stuff to be sent to the cloud

Data

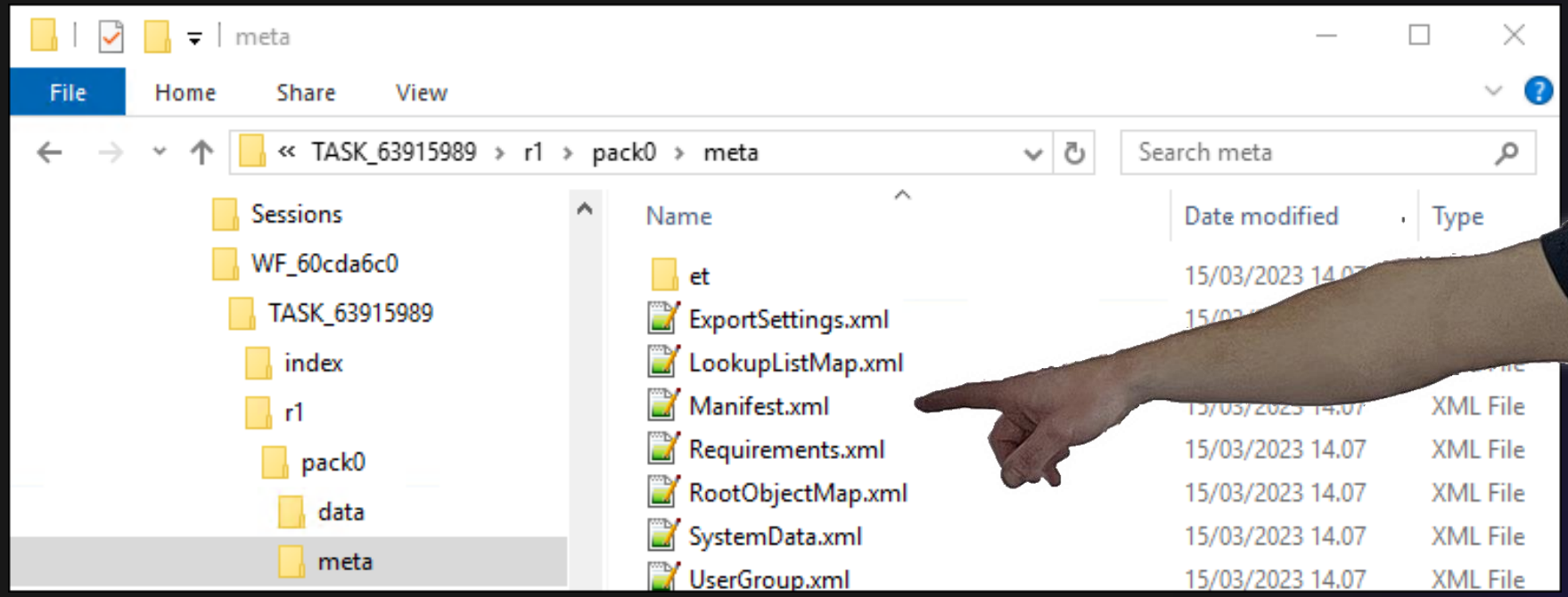
- Files are encrypted and renamed to `<guid>.dat`





Metadata

- Files are encrypted







SPFile object

Timestamps!

Refers to content file

Author!

IV for decrypting the file content

Matching SPListItem

Secureworks



Secureworks

Abusing SPMT: Demo!

Microsoft Teams - loading

teams.microsoft.com/_#/conversations/General?threadId=19:XeglDZRY-8faj72G0U1ChCbLbizpKjkNq2x-Yz9gkCA1@thread.tacv2&ctx=channel

Incognito

Microsoft Teams

Search

Activity
Chat
Teams
Calendar
Calls
Files
Apps

Teams

Your teams

SPMT2

General

General Posts Files

Meet

Welcome to the team!

Here are some things to get going...







Add more people

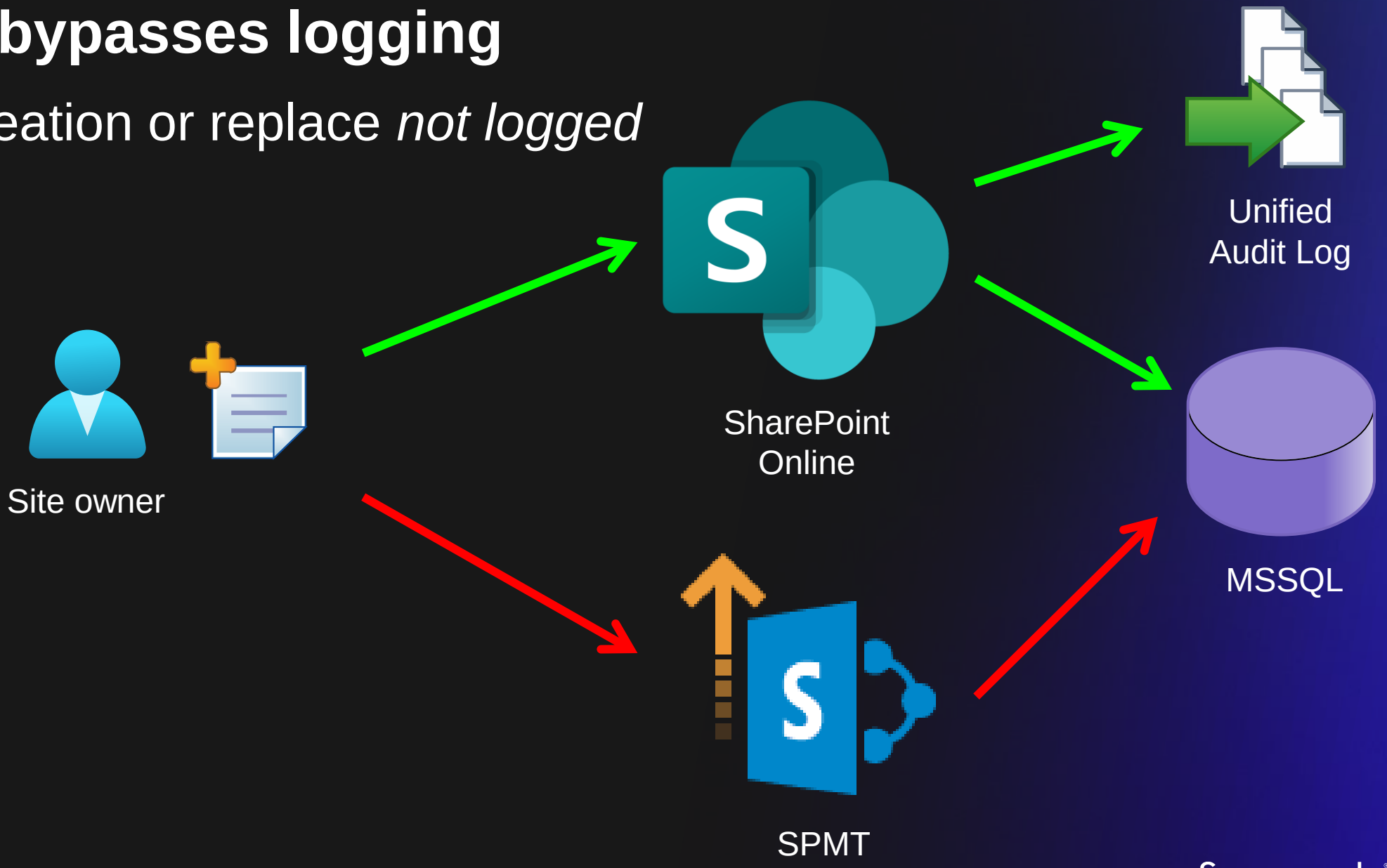
Create more channels

Open the FAQ

New conversation

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.

File creations ar

Descriptio

SPMT migratio

1. Files and th
2. A job is sta

Expected be

- Migrated fi
- Existing file
- File creatio

Observed b

When using the
timestamps, an

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".

MSRC has investigated this issue and concluded that this does not require immediate attention as Migration API overwrites the existing files (clearly documented in SharePoint Online Import Migration API | Microsoft Learn). When migrating content 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 the job, and we expect that a SCA has sufficient knowledge about the migration. For 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 sense for the migration experience.

Secureworks

The Next Generation

Secureworks®

Google ❤

Microsoft | Learn Documentation Training Certifications Q&A Code Samples Assessments Shows Events

Filter by title

- SPObject element
- SPObjects element
- Toolbar element (SPView)
- Toolbar element (SPWebPart)
- UserX element
- Versions element (SPFile)
- Versions element (SPListItem)
- View element
- ViewBidiHeader element (SPView)
- ViewBidiHeader element (SPWebPart)
- View Body element (SPView)
- View Body element (SPWebPart)
- ViewData element (SPView)
- ViewData element (SPWebPart)
- ViewEmpty element (SPView)
- ViewEmpty element (SPWebPart)
- ViewFields element (SPView)
- ViewFields element (SPWebPart)
- ViewFooter element (SPView)
- ViewFooter element (SPWebPart)
- ViewHeader element (SPView)
- ViewHeader element (SPWebPart)

Download PDF

··· / 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**).

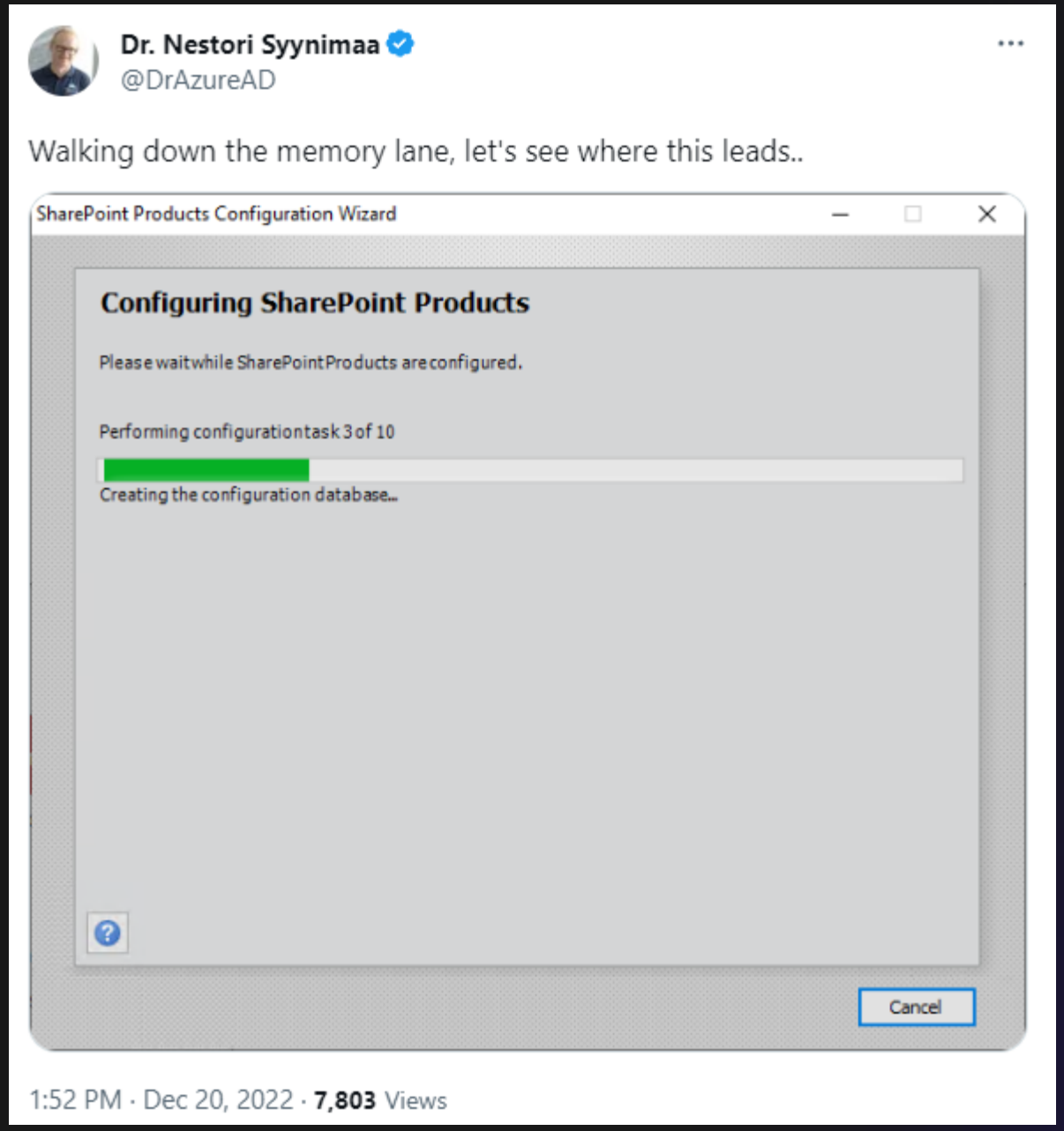
Definition

XML

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

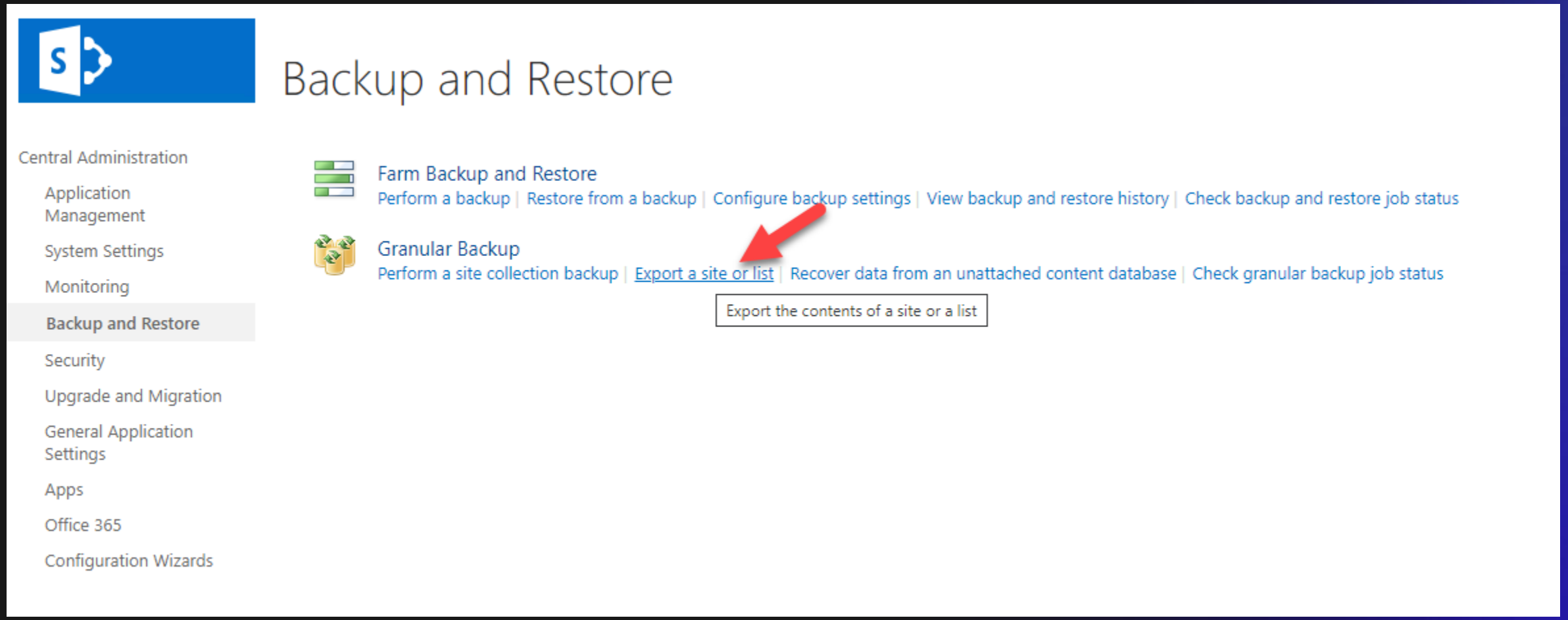
Secureworks


Microsoft®
TS: Configuring Microsoft® Office SharePoint® Server 2007
CANDIDATE ID
SITE NUMBER: FN35
REGISTRATION: ra6lon51fe
YOUR SCORE: 911
DATE: nestori syynimaa
Wednesday, June 10, 2009
NUMBER: 072-630
NG SCORE: 700
LT: Pass
ONAL RESULTS:
Strong
Configure Microsoft Off
Needs Development
Manage Search
Needs Developme
Configure Conte
Needs Develop
Configure Bu
Needs Deve
Manage F
Needs D
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:
Deploy Windows SharePoint Services 3.0
Strong
SITE NUM
REGISTRATION:
YOUR SC
Nestori
Syynimaa
CLOUD IDENTIT
SUMMIT '22



Secureworks®

On-prem SharePoint backup





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.

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

Site: No selection

List: No selection

File location:

Specify the destination for the export package.

Filename:

\backups\teamsite.cab

Overwrite existing files

Example: \\backup\SharePoint\export.cmp

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 full security

Export Versions

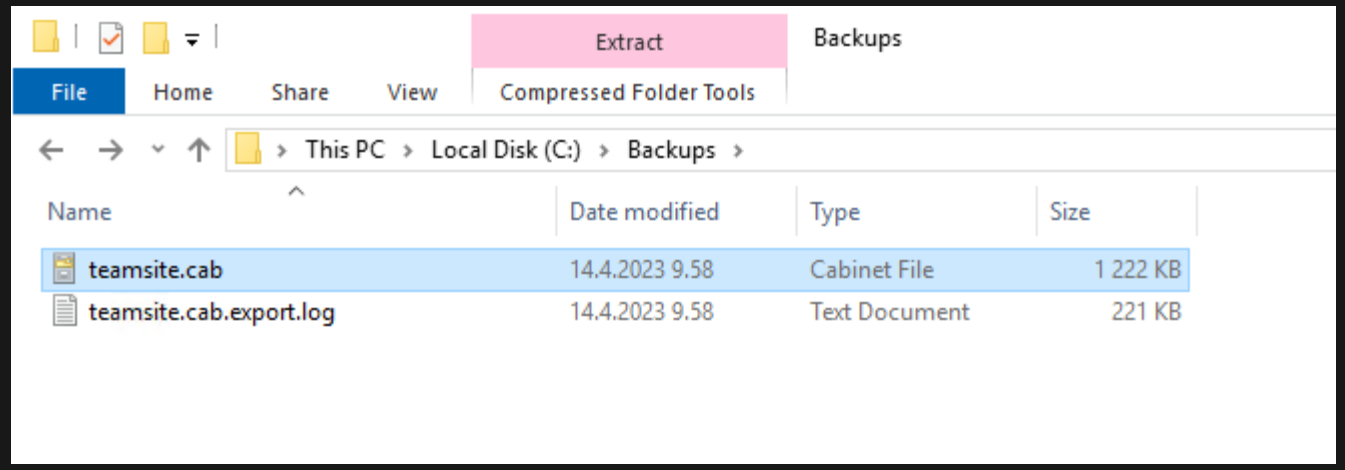
Select the version history information to include for files and list items. You can include all versions, the last major version, the current version, or the last major and last minor versions.

Export versions

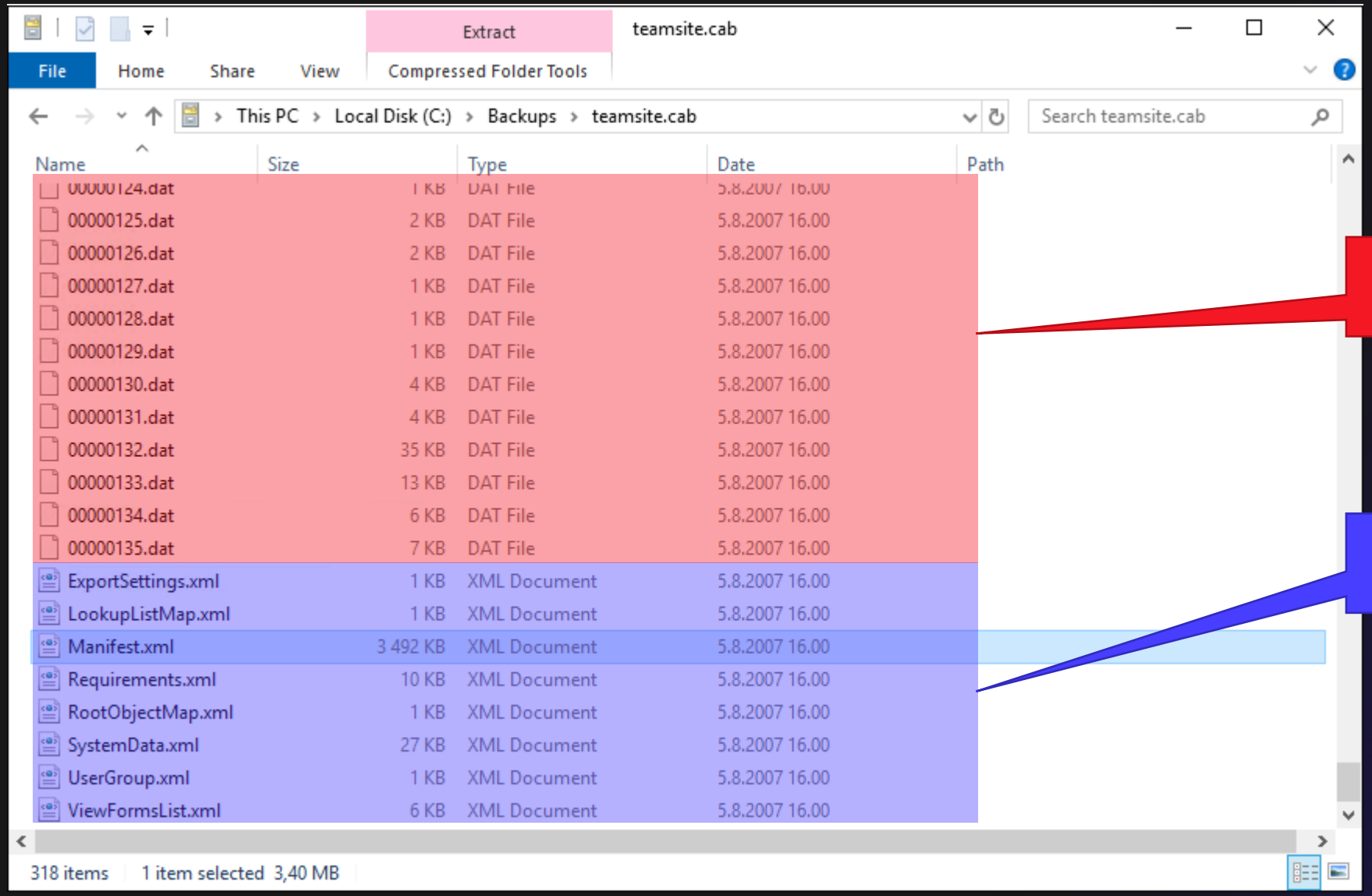
All Versions

Start Export | Cancel

On-prem SharePoint backup



On-prem SharePoint backup



Stuff to be restored

Metadata

Secureworks

Metadata: Manifest.xml

- Same but more




```
<SPObject Id="73e6c285-54af-4628-b4bc-636788a47553" ObjectType="SPFile" ParentId="2feddf69-2280-450d-89b8-d9c4b3de29b1"
    <File Url="Style Library/Forms/EditForm.aspx" Id="73e6c285-54af-4628-b4bc-636788a47553" ParentWebId="3a15fe51-d2cb-4
        <WebParts>
            <WebPart Name="1ba6637f-e85c-4f0e-acd2-a99bdb7cf94c" DisplayName="" Flags="1048576" Hidden="false" Threaded=
        </WebParts>
    </File>
</SPObject>
<SPObject Id="6b1e3312-0d2c-4ddb-8872-939e1bc8adcb" ObjectType="SPFile" ParentId="2fe
    <File Url="Style Library/Forms/repair.aspx" Id="6b1e3312-0d2c-4ddb-8872-939e1bc8a
        <WebParts>
            <WebPart Name="e9727c7b-1ce1-4464-acf3-b1249c83d29c" DisplayName="$Resources:core,Relink_Documents;" Flags="
        </WebParts>
    </File>
</SPObject>
<SPObject Id="b8590518-372c-48b2-9a59-3da2f62f2ea4" ObjectType="SPFile" ParentId="2feddf69-2280-450d-89b8-d9c4b3de29b1"
    <File Url="Style Library/Forms/Thumbnails.aspx" Id="b8590518-372c-48b2-9a59-3da2f62f2ea4" ParentWebId="3a15fe51-d2cb
        <WebParts>
            <WebPart Name="965f75bb-8aff-45cb-ab12-53c4c5e65cf9" DisplayName="assetLibTemp" Flags="13" Hidden="true" Thr
        </WebParts>
    </File>
</SPObject>
```

https://learn.microsoft.com/en-us/sharepoint/dev/schema/spobject-element-deploymentmanifest



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

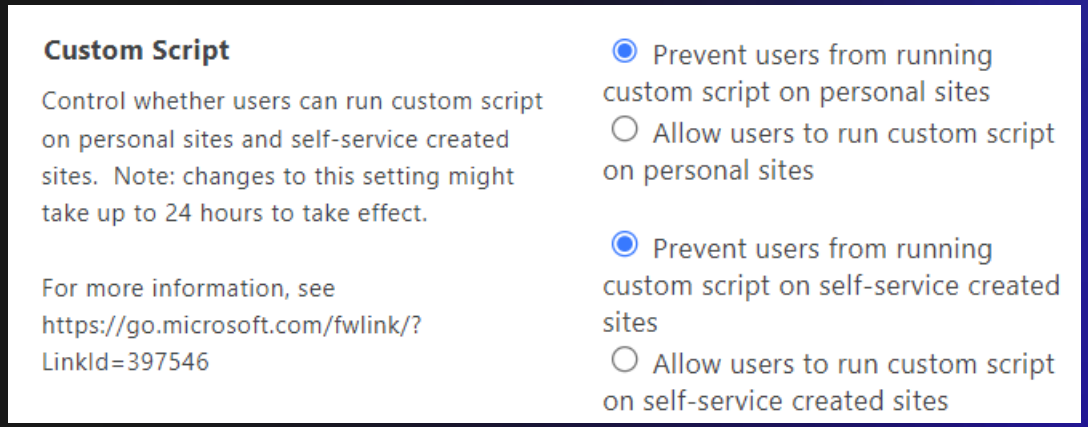
Custom script

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



https://learn.microsoft.com/en-us/sharepoint/allow-or-prevent-custom-script

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.OAuth.Token/Acquire` endpoint. This API is for internal use. You should not communicate with it directly in your solutions.

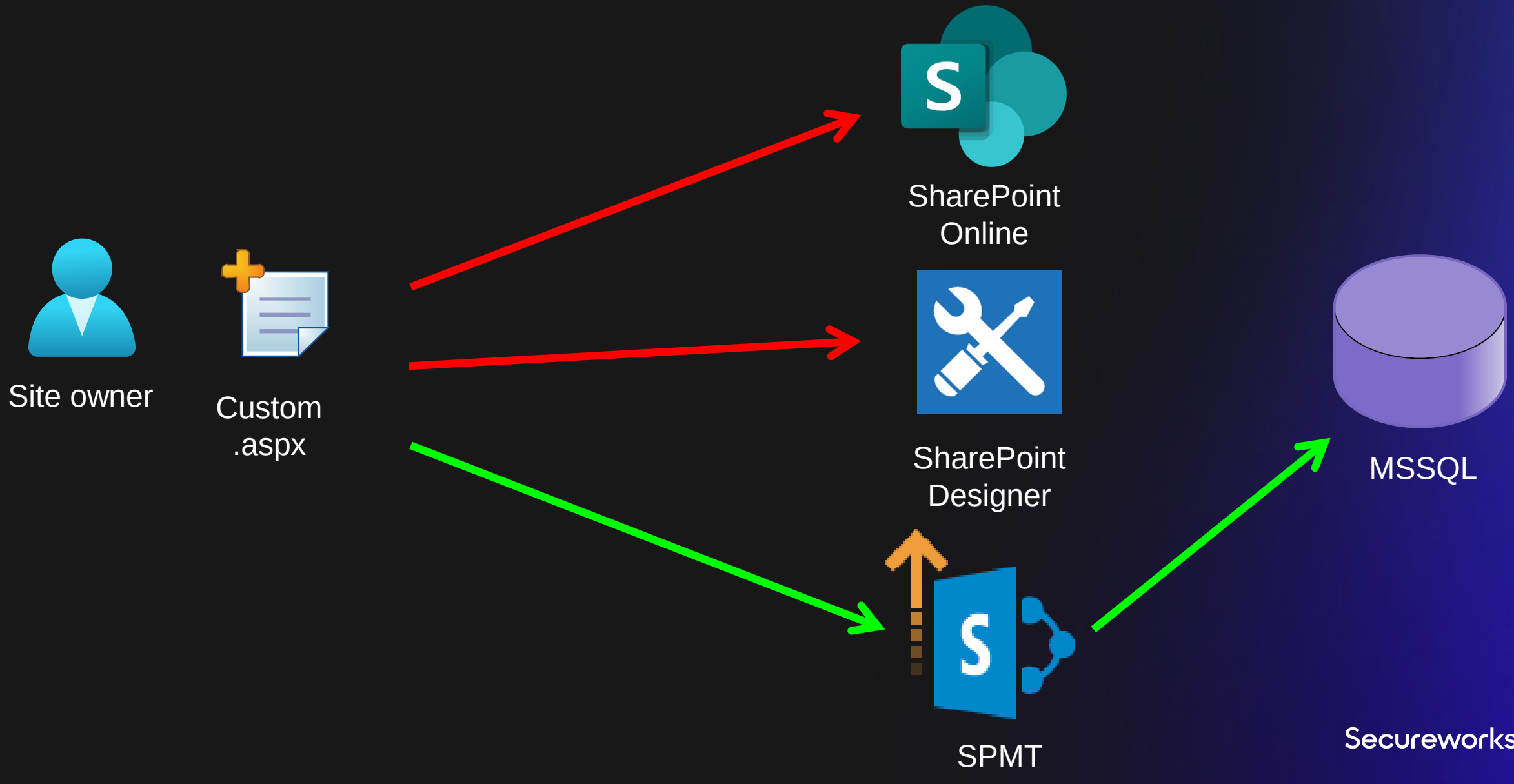
```
POST https://aadinternalsdev.sharepoint.com/sites/SPMTPOC2/_api/SP.OAuth.Token/Acquire HTTP/1.1
Host: aadinternalsdev.sharepoint.com
Connection: keep-alive
Content-Length: 43
Cookie: SPOIDCRL=//u/PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0idXRmLTgiPz48U1A+VjEyLDBoLmZ8bWVtYmV
{"resource": "https://graph.microsoft.com"}
```



https://github.com/SharePoint/sp-dev-docs/blob/main/docs/spfx/overview-graphhttpclient.md

Se

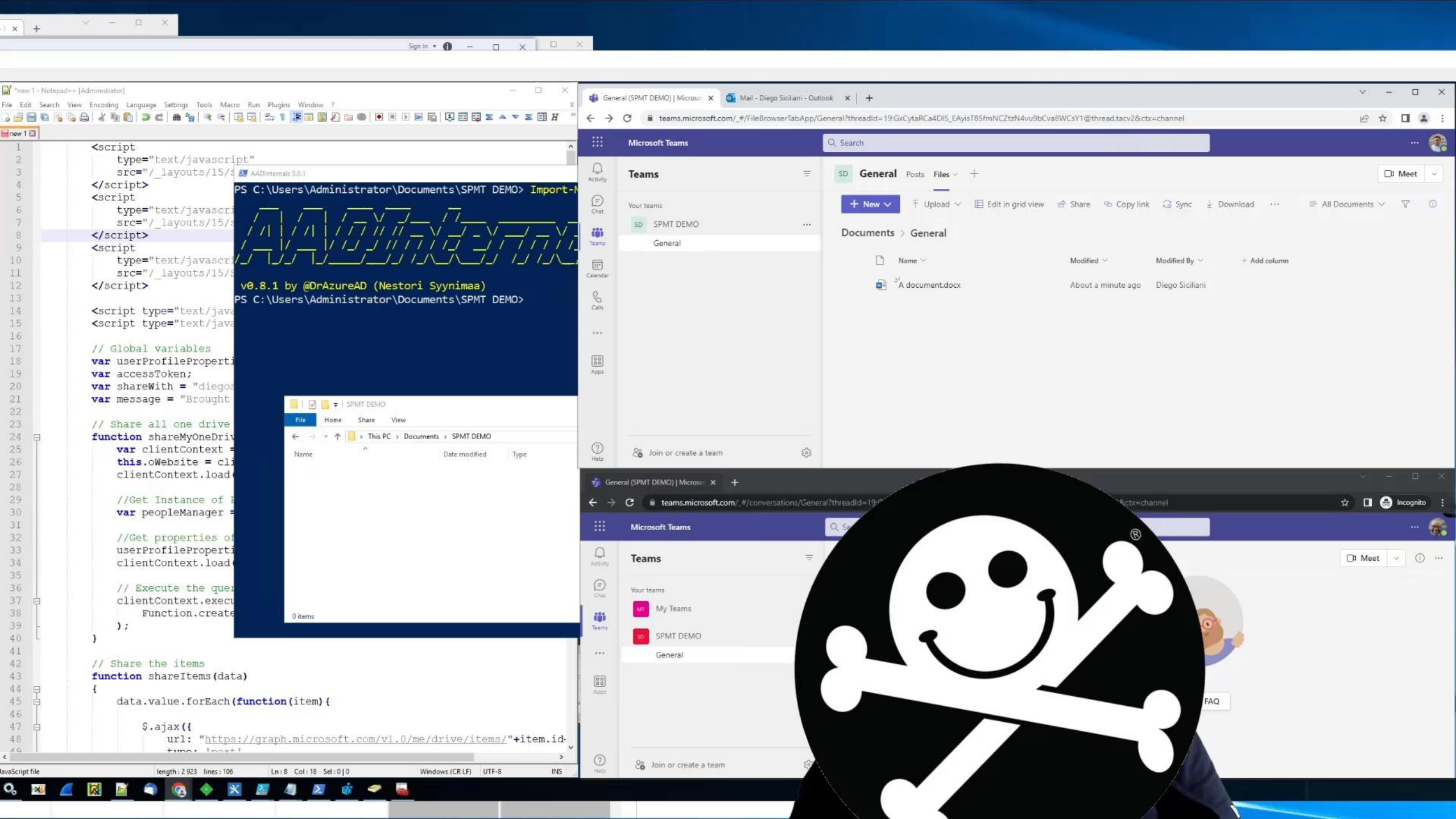
SPMT bypasses custom script settings



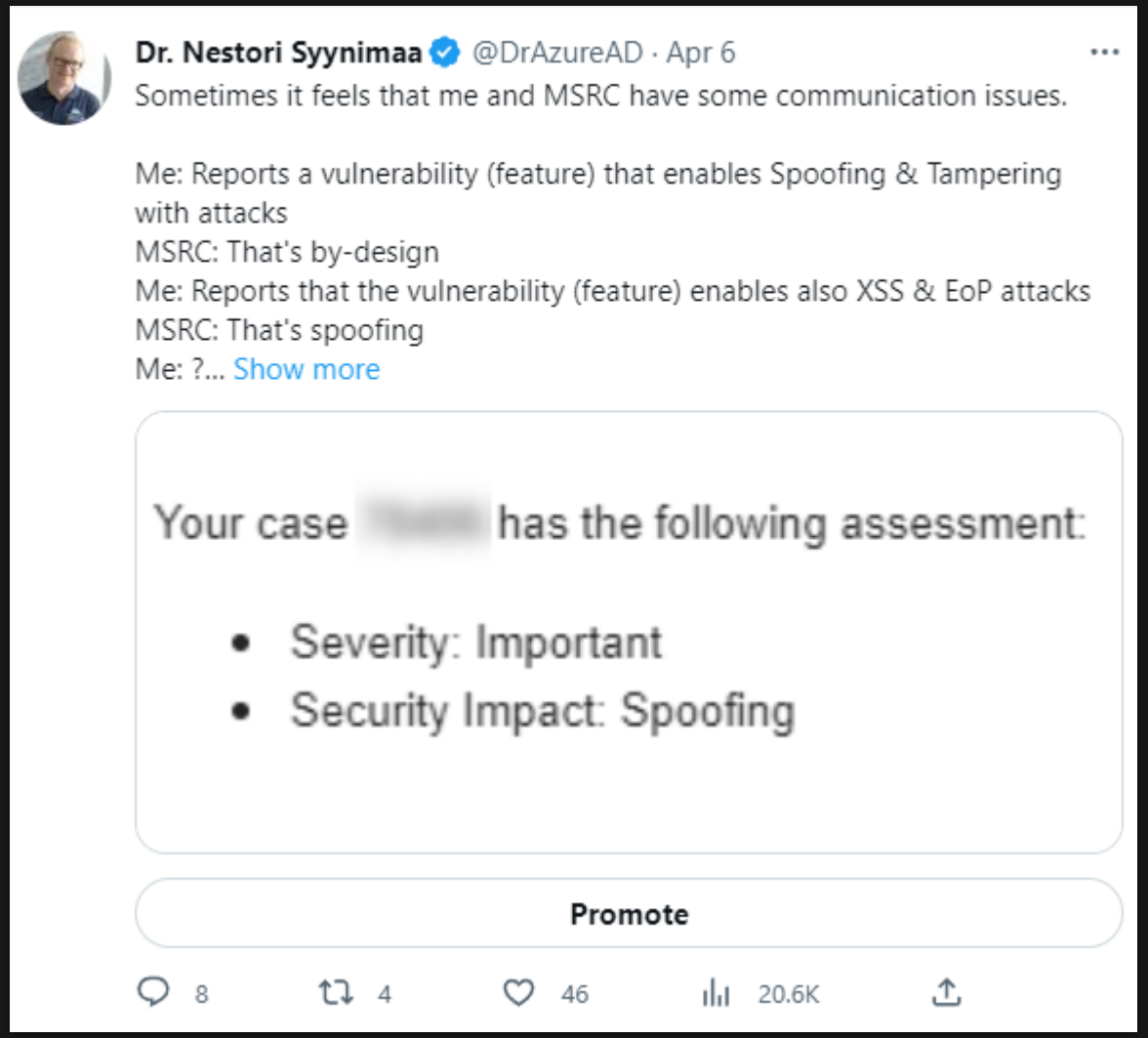
Secureworks®


TRENDIZISST

Abusing SPMT 2nd generation: Demo!


PS C:\Users\Administrator\Documents\SPMT DEMO> Import-
v0.8.1 by @DrAzureAD (Nestori Syynimaa)
PS C:\Users\Administrator\Documents\SPMT DEMO>
Microsoft Teams
Teams
SPMT DEMO
General
Documents > General
A document.docx
About a minute ago
Diego Siciliani
Join or create a team
My Teams
FAQ

Communicating with Microsoft



Dr. Nestori Syynimaa @DrAzureAD · Apr 6

Sometimes it feels that me and MSRC have some communication issues.

Me: Reports a vulnerability (feature) that enables Spoofing & Tampering with attacks
MSRC: That's by-design
Me: Reports that the vulnerability (feature) enables also XSS & EoP attacks
MSRC: That's spoofing
Me: ?... Show more

Your case [redacted] has the following assessment:

- Severity: Important
- Security Impact: Spoofing

Promote

8 4 46 20.6K

- SP.OAuth.Token

```
HTTP/1.1 400 Bad Request

{
    "odata.error": {
        "code": "10001",
        "message": {
            "lang": "en-US",
            "value": "Missing refresh token."
        },
        "error.redirectUrl": "https://aadinternalsdev.sha
    }
}
```

Secureworks



Secureworks

Questions?

Secureworks®

Secureworks®