



# CLOUD IDENTITY SUMMIT '20

Identity Security Track

## AADInternals: Building the ultimate Azure AD hacking tool

Dr. Nestori Syynimaa

Community Event by



BONN

sponsored by



# About the speaker



- Dr. Nestori Syynimaa
  - CIO @ Cities surrounding Tampere
  - Lecturer @ University of Jyväskylä
  - Owner @ Gerenios Ltd
- MCITP, MCSA, MCT, MS Certified Expert
- Author of AADInternals
- [www.linkedin.com/in/nestori](http://www.linkedin.com/in/nestori)
- <http://o365blog.com>

# Contents

- Introduction to AADInternals
- Why did I do it?
- How the cloud works?
- Examples:
  - Get-AADIntServiceLocations
  - Set-AADIntUserPassword
  - Get-AADIntOneDriveFiles
  - Invoke-AADIntUserEnumerationAsGuest
  - Invoke-AADPhishing

# Introduction to AADInternals



# AADInternals

- PowerShell module (33778 lines of code)
- Admin & hacking toolkit for Azure AD & Office 365
- Open source:
  - <https://github.com/gerenios/aadinternals>
  - <https://o365blog.com/aadinternals/>
- Easy to install & use:

```
PS C:\> Install-Module AADInternals
PS C:\> Import-Module AADInternals
```



```
v0.4.4 by @NestoriSyynimaa - Cloud Identity Summit 2020 edition
```

# Why did I do it?



gerenios



# Why did I do it?

- I have a dev background (since 1980's)
- MCT since 2014 - keen to know how things work under-the-hood
- I wanted to:
  - Make people aware of information security (issues)
  - Share my knowledge with the community in an easy-to-use form -> PowerShell module



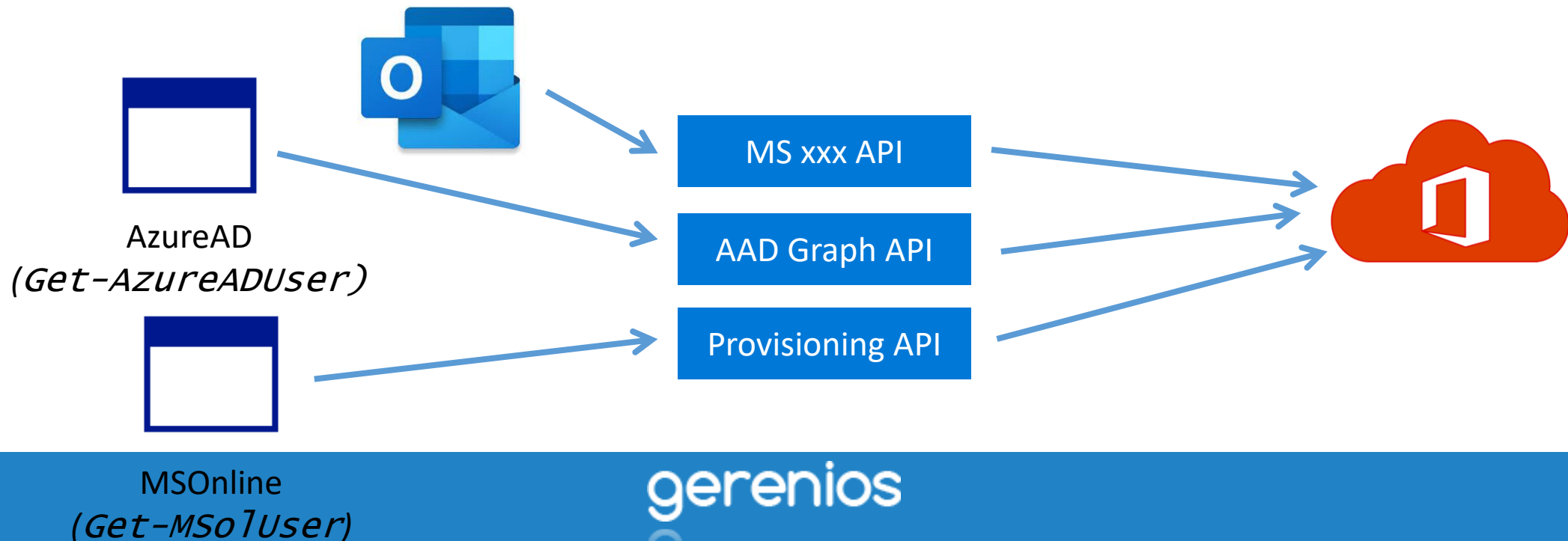
# How the cloud works?





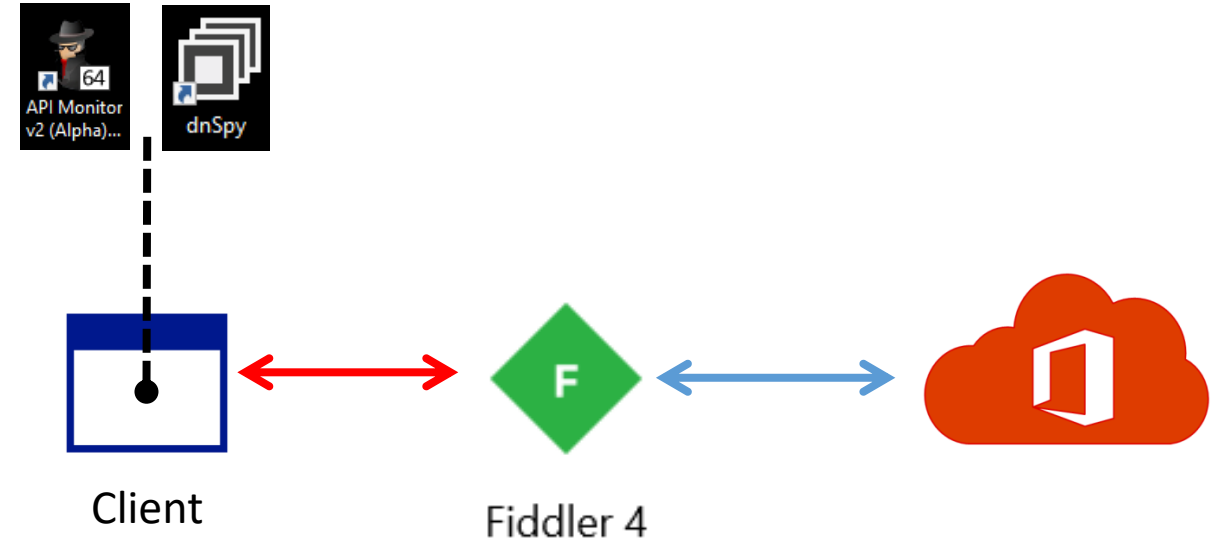
# How the cloud works?

- Everything is in the cloud: cloud does/knows what clients tell
- Communication via HTTP REST APIs
- OAuth authentication (=Access Tokens)



# How I do research

- Man-in-the-middle (MITM)
  - Fiddler or Burp
  - Allows intercepting http(s) traffic
- Reverse-engineer
  - Rohitab API Monitor
  - dnSpy
- Read documentation 😊



# Some API endpoints

"Thing"	API	Address
MSOnline module	Provisioning API	https://provisioningapi.microsoftonline.com/provisioningwebservice.svc
AzureAD module	<a href="#">Azure AD Graph</a>	https://graph.windows.net/<tenant>/<command>
Azure AD Connect	Sync provisioning service	https://adminwebservice.microsoftonline.com/provisioningservice.svc
	<a href="#">Microsoft Graph</a>	https://graph.microsoft.com/<version>
Teams		https://api.spaces.skype.com https://substrate.office.com/search/api/v1/ https://presence.teams.microsoft.com/v1/

# Examples



# Get-AADIntServiceLocations

- Get-MsolCompanyInformation
  - Gets company wide settings from Azure AD
  - Content-Type: application/soap+xml
  - Only a subset of returned information is shown

```
DisplayName           : Black Hat
PreferredLanguage     : en
Street                :
City                  :
State                 :
PostalCode            :
Country               :
CountryLetterCode     : US
TelephoneNumber       : 8006427676
MarketingNotificationEmails : {}
TechnicalNotificationEmails : {admin@blackhat.myo365.site}
SelfServePasswordResetEnabled : True
UsersPermissionToCreateGroupsEnabled : True
UsersPermissionToCreateLOBAppsEnabled : True
UsersPermissionToReadOtherUsersEnabled : True
UsersPermissionToUserConsentToAppEnabled : True
DirectorySynchronizationEnabled : True
DirSyncServiceAccount : Sync_SERVER_2980bcb19aa3@M365x403056.onmicrosoft.com
LastDirSyncTime       : 28.5.2020 7.08.53
LastPasswordSyncTime  : 28.5.2020 7.12.06
PasswordSynchronizationEnabled : True
```

```
<b:ReturnValue xmlns:c="http://schemas.microsoft.com/2004/07/Microsoft.Online.Administration">
  <c:AllowAdHocSubscriptions>true</c:AllowAdHocSubscriptions>
  <c:AllowEmailVerifiedUsers>true</c:AllowEmailVerifiedUsers>
  <c:AuthorizedServiceInstances xmlns:d="http://schemas.microsoft.com/2003/10/Serialization"
  <c:AuthorizedServices/>
  <c:City i:nil="true"/>
  <c:CompanyDeletionStartTime i:nil="true"/>
  <c:CompanyTags xmlns:d="http://schemas.microsoft.com/2003/10/Serialization/Arrays"
  <c:CompanyType>CompanyTenant</c:CompanyType>
  <c:CompassEnabled i:nil="true"/>
  <c:Country i:nil="true"/>
  <c:CountryLetterCode>US</c:CountryLetterCode>
  <c:DapEnabled i:nil="true"/>
  <c:DefaultUsageLocation i:nil="true"/>
  <c:DirSyncAnchorAttribute>mS-DS-ConsistencyGuid</c:DirSyncAnchorAttribute>
  <c:DirSyncApplicationType>1651564e-7ce4-4d99-88be-0a65050d8dc3</c:DirSyncApplicationTy
  <c:DirSyncClientMachineName>SERVER</c:DirSyncClientMachineName>
  <c:DirSyncClientVersion>1.5.30.0</c:DirSyncClientVersion>
  <c:DirSyncServiceAccount>Sync_SERVER_2980bcb19aa3@M365x403056.onmicrosoft.com</c:DirSy
  <c:DirectorySynchronizationEnabled>true</c:DirectorySynchronizationEnabled>
  <c:DirectorySynchronizationStatus>Enabled</c:DirectorySynchronizationStatus>
  <c:DisplayName>Black Hat</c:DisplayName>
  <c:InitialDomain>M365x403056.onmicrosoft.com</c:InitialDomain>
  <c>LastDirSyncTime>2020-05-28T09:39:08Z</c>LastDirSyncTime>
  <c>LastPasswordSyncTime>2020-05-28T09:12:52Z</c>LastPasswordSyncTime>
  <c:MarketingNotificationEmails xmlns:d="http://schemas.microsoft.com/2003/10/Serializa
  <c:MultipleDataLocationsForServicesEnabled i:nil="true"/>
  <c:ObjectId>c0295e5e-58f1-4388-a0d8-535753398c5a</c:ObjectId>
  <c>PasswordSynchronizationEnabled>true</c>PasswordSynchronizationEnabled>
  <c:PortalSettings>
  <c:PostalCode i:nil="true"/>
  <c:PreferredLanguage>en</c:PreferredLanguage>
  <c:ReleaseTrack>FirstRelease</c:ReleaseTrack>
  <c:ReplicationScope>NA</c:ReplicationScope>
  <c:RmsViralSignUpEnabled>true</c:RmsViralSignUpEnabled>
  <c:SecurityComplianceNotificationEmails xmlns:d="http://schemas.microsoft.com/2003/10/
  <c:SecurityComplianceNotificationPhones xmlns:d="http://schemas.microsoft.com/2003/10/
  <c:SelfServePasswordResetEnabled>true</c:SelfServePasswordResetEnabled>
  <c:ServiceInformation>
  <c:ServiceInstanceInformation>
  <c:State i:nil="true"/>
  <c:Street i:nil="true"/>
  <c:SubscriptionProvisioningLimited>false</c:SubscriptionProvisioningLimited>
  <c:TechnicalNotificationEmails xmlns:d="http://schemas.microsoft.com/2003/10/Serialization/Arrays"
  <c:TelephoneNumber>8006427676</c:TelephoneNumber>
  <c:UIExtensibilityUri i:nil="true" xmlns:d="http://schemas.microsoft.com/2003/10/Serialization/Arrays"/>
  <c:UsersPermissionToCreateGroupsEnabled>true</c:UsersPermissionToCreateGroupsEnabled>
  <c:UsersPermissionToCreateLOBAppsEnabled>true</c:UsersPermissionToCreateLOBAppsEnabled>
  <c:UsersPermissionToReadOtherUsersEnabled>true</c:UsersPermissionToReadOtherUsersEnabled>
  <c:UsersPermissionToUserConsentToAppEnabled>true</c:UsersPermissionToUserConsentToAppEnabled>
  <c:WhenCreated>2019-07-14T07:03:20Z</c:WhenCreated>
</b:ReturnValue>
```

```
<c:ServiceInstanceInformation>
  <c:ServiceInstanceInformation>
    <c:GeographicLocation>
      <c:Country>US</c:Country>
      <c:Region>NA</c:Region>
      <c:State i:nil="true"/>
    </c:GeographicLocation>
    <c:ServiceInstance>Windows/SDF</c:ServiceInstance>
    <c:ServiceInstanceEndpoints i:nil="true"/>
  </c:ServiceInstanceInformation>
  <c:ServiceInstanceInformation>
    <c:GeographicLocation>
      <c:Country>US</c:Country>
      <c:Region>NA</c:Region>
      <c:State i:nil="true"/>
    </c:GeographicLocation>
    <c:ServiceInstance>SCO/PROD_AMSUA0502_03</c:ServiceInstance>
    <c:ServiceInstanceEndpoints i:nil="true"/>
  </c:ServiceInstanceInformation>
  <c:ServiceInstanceInformation>
    <c:GeographicLocation>
      <c:Country>US</c:Country>
      <c:Region>NA</c:Region>
      <c:State i:nil="true"/>
    </c:GeographicLocation>
    <c:ServiceInstance>MultiFactorService/NA001</c:ServiceInstance>
    <c:ServiceInstanceEndpoints i:nil="true"/>
  </c:ServiceInstanceInformation>
```



# Set-AADIntUserPassword

- Azure AD Connect (if configured) synchronises password hashes from Active Directory to Azure AD
- Content-Type: application/soap+msbin1 ☹️
- WCF Binary Message Inspector by Will Fuqua!

Headers | TextView | SyntaxView | WebForms | HexView | WCF Binary | Auth | Cookies | **Raw** | JSON | XML

POST <https://adminwebservice.microsoftonline.com/provisioningservice.svc> HTTP/1.1  
Content-Type: application/soap+xml  
x-ms-aadmsods-apiaction: GetCompanyConfiguration  
x-ms-aadmsods-appid: 1651564e-7ce4-4d99-88be-0a65050d8dc3  
client-request-id: e6feb2a0-5509-458f-8c22-b73139607732  
x-ms-aadmsods-clientversion: 8.0  
x-ms-aadmsods-dirsyncbuildnumber: 1.5.30.0  
x-ms-aadmsods-fimbuildnumber: 1.5.30.0  
x-ms-aadmsods-tenantid: c0295e5e-58f1-4388-a0d8-535753398c5a  
x-ms-aadmsods-machineid: 0cf2774f-a188-4bd3-b4b3-3a690374325d  
x-ms-aadmsods-provisioningsessiondesc: Connector-7a88170a-d27a-487d-868c-46cd4ae1421f  
Host: adminwebservice.microsoftonline.com  
Content-Length: 3090  
Expect: 100-continue  
Accept-Encoding: gzip, deflate

V0  
[]S0  
[]aV0D  
[]fhttp://schemas.microsoft.com/  
ApplicationId[]6http://schemas.mic  
BearerToken[]6http://schemas.micro  
ClientVersion[]6http://schemas.mic  
IssueDateTime[]6http://schemas.mic  
LanguageId[]6http://schemas.micros  
TrackingId[]6http://schemas.micros  
[]Chttps://adminwebservice.micro

Headers	TextView	SyntaxView	WebForms	HexView	WCF Binary	Auth	Cookies	Raw	JSON	XML
00000000	50 4F 53 54 20 68 74 74 70 73 3A 2F 2F 61 64 6D 69 6E 77 65 62 73 65 72 76 69 63 65 2E 6D									
0000001E	69 63 72 6F 73 6F 66 74 6F 6E 6C 69 6E 65 2E 63 6F 6D 2F 70 72 6F 76 69 73 69 6F 6E 69 6E									
0000003C	67 73 65 72 76 69 63 65 2E 73 76 63 20 48 54 54 50 2F 31 2E 31 0D 0A 43 6F 6E 74 65 6E 74									
0000005A	2D 54 79 70 65 3A 20 61 70 70 6C 69 63 61 74 69 6F 6E 2F 73 6F 61 70 2B 6D 73 62 69 6E 31									
00000078	0D 0A 78 2D 6D 73 2D 61 61 64 6D 73 6F 64 73 2D 61 70 69 61 63 74 69 6F 6E 3A 20 47 65 74									
00000096	43 6F 6D 70 61 6E 79 43 6F 6E 66 69 67 75 72 61 74 69 6F 6E 0D 0A 78 2D 6D 73 2D 61 61 64									
000000B4	6D 73 6F 64 73 2D 61 70 70 69 64 3A 20 31 36 35 31 35 36 34 65 2D 37 63 65 34 2D 34 64 39									
000000D2	39 2D 38 38 62 65 2D 30 61 36 35 30 35 30 64 38 64 63 33 0D 0A 63 6C 69 65 6E 74 2D 72 65									
000000F0	71 75 65 73 74 2D 69 64 3A 20 65 36 66 65 62 32 61 30 2D 35 35 30 39 2D 34 35 38 66 2D 38									
0000010E	63 32 32 2D 62 37 33 31 33 39 36 30 37 37 33 32 0D 0A 78 2D 6D 73 2D 61 61 64 6D 73 6F 64									
0000012C	73 2D 63 6C 69 65 6E 74 76 65 72 73 69 6F 6E 3A 20 38 2E 30 0D 0A 78 2D 6D 73 2D 61 61 64									
0000014A	6D 73 6F 64 73 2D 64 69 72 73 79 6E 63 62 75 69 6C 64 6E 75 6D 62 65 72 3A 20 31 2E 35 2E									
00000168	33 30 2E 30 0D 0A 78 2D 6D 73 2D 61 61 64 6D 73 6F 64 73 2D 66 69 6D 62 75 69 6C 64 6E 75									
00000186	6D 62 65 72 3A 20 31 2E 35 2E 33 30 2E 30 0D 0A 78 2D 6D 73 2D 61 61 64 6D 73 6F 64 73 2D									
000001A4	74 65 6E 61 6E 74 69 64 3A 20 63 30 32 39 35 65 35 65 2D 35 38 66 31 2D 34 33 38 38 2D 61									
000001C2	30 64 38 2D 35 33 35 37 35 33 33 39 38 63 35 61 0D 0A 78 2D 6D 73 2D 61 61 64 6D 73 6F 64									
000001E0	73 2D 6D 61 63 68 69 6E 65 69 64 3A 20 30 63 66 32 37 34 66 2D 61 31 38 38 2D 34 62 64									
000001F8	33 2D 62 34 62 33 2D 33 61 36 39 30 33 37 34 33 32 35 64 0D 0A 78 2D 6D 73 2D 61 61 64 6D									
00000216	73 6F 64 73 2D 70 72 6F 76 69 73 69 6F 6E 69 6E 67 73 65 73 73 69 6F 6E 64 65 73 63 3A 20									
00000234	43 6F 6E 6E 65 63 74 6F 72 2D 37 61 38 38 31 37 30 61 2D 64 32 37 61 2D 34 38 37 64 2D 38									
00000252	36 38 63 2D 34 36 63 64 34 61 65 31 34 32 31 66 0D 0A 48 6F 73 74 3A 20 61 64 6D 69 6E 77									
00000270	65 62 73 65 72 76 69 63 65 2E 6D 69 63 72 6F 73 6F 66 74 6F 6E 6C 69 6E 65 2E 63 6F 6D 0D									
00000288	0A 43 6F 6E 74 65 6E 74 2D 4C 65 6E 67 74 68 3A 20 33 30 39 30 0D 0A 45 78 70 65 63 74 3A									
000002A6	20 31 30 30 2D 63 6F 6E 74 69 6E 75 65 0D 0A 41 63 63 65 70 74 2D 45 6E 63 6F 64 69 6E 67									
000002C4	3A 20 67 7A 69 70 2C 20 64 65 66 6C 61 74 65 0D 0A 0D 0A 02 0B 01 73 04 0B 01 61 06 56									
000002E2	08 44 0A 1E 00 82 99 66 68 74 74 70 3A 2F 2F 73 63 68 65 6D 61 73 2E 6D 69 63 72 6F 73 6F									
00000300	66 74 2E 63 6F 6D 2F 6F 6E 6C 69 6E 65 2F 61 77 73 2F 63 68 61 6E 67 65 2F 32 30 31 30 2F									
00000318	30 31 2F 49 50 72 6F 76 69 73 69 6F 6E 69 6E 67 57 65 62 53 65 72 76 69 63 65 2F 47 65 74									
00000336	43 6F 6D 70 61 6E 79 43 6F 6E 66 69 67 75 72 61 74 69 6F 6E 40 09 53 79 6E 63 54 6F 6B 65									
00000354	6E 1E 8A 01 98 2A 75 72 6E 3A 6D 69 63 72 6F 73 6F 66 74 2E 6F 6E 6C 69 6E 65 2E 61 64 6D									
00000372	69 6E 69 73 74 72 61 74 69 76 65 73 65 72 76 69 63 65 08 2A 75 72 6E 3A 6D 69 63 72 6F 73									
00000390	6F 66 74 2E 6F 6E 6C 69 6E 65 2E 61 64 6D 69 6E 69 73 74 72 61 74 69 76 65 73 65 72 76 69									
000003A8	63 65 09 01 69 29 68 74 74 70 3A 2F 2F 77 77 72 6E 77 73 2E 6F 72 67 2F 32 30 31 2F 58									
000003C6	4D 4C 53 63 68 65 6D 61 2D 69 6E 73 74 61 6E 63 65 40 0D 41 70 70 6C 69 63 61 74 69 6F 6E									
000003E4	49 64 08 36 68 74 74 70 3A 2F 2F 73 63 68 65 6D 61 73 2E 6D 69 63 72 6F 73 6F 66 74 2E 63									

0x02 : <Envelope>  
0x0B : <Header>

Headers

TextView

SyntaxView

WebForms

HexView

WCF Binary

Auth

Cookies

Raw

JSON

XML

<s:Envelope xmlns:s="http://www.w3.org/2003/05/soap-envelope" xmlns:a="http://www.w3.org/2005/08/addressing">

<s:Header>

<a:Action s:mustUnderstand="1">

http://schemas.microsoft.com/online/aws/change/2010/01/IProvisioningWebService/GetCompanyConfiguration

<SyncToken s:relay="um:microsoft.online.administrativeservice" xmlns="um:microsoft.online.administrativeservice" xmlns:i="http://www.w3.org/2001/XMLSchema-instance">

<a:MessageID>

<a:SequenceAcknowledgement>

<a:ReplyTo>

http://www.w3.org/2005/08/addressing/anonymous

<a:To s:mustUnderstand="1">

https://adminwebservice.microsoftonline.com/provisioningservice.svc

<s:Body>

<GetCompanyConfiguration xmlns="http://schemas.microsoft.com/online/aws/change/2010/01">

<includeLicenseInformation>

false

0x1E	Identifier
0x20	http://schemas.xmlsoap.org/ws/2005/02/rm
0x22	Transforms
0x24	Transform
0x26	DigestMethod
0x28	DigestValue
0x2A	Address
0x2C	ReplyTo
0x2E	SequenceAcknowledgement
0x30	AcknowledgementRange
0x32	Upper
0x34	Lower

```

dict.Add("Identifier");
dict.Add("http://schemas.xmlsoap.org/ws/2005/02/rm");
dict.Add("Transforms");
dict.Add("Transform");
dict.Add("DigestMethod");
dict.Add("Address");
dict.Add("ReplyTo");
dict.Add("SequenceAcknowledgement");
dict.Add("AcknowledgementRange");
dict.Add("Upper");
dict.Add("Lower");

```

[Pull requests](#) [Issues](#) [Marketplace](#) [Explore](#)[waf](#) / [WCF-Binary-Message-Inspector](#)[Watch](#)

12

[★ Star](#)

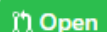
52

[Fork](#)

16

[Code](#)[Issues](#) 0[Pull requests](#) 1[Projects](#) 0[Wiki](#)[Insights](#)

## Added the missing dictionary element "DigestValue" #2

[Edit](#)NestoriSyynimaa wants to merge 1 commit into [waf:master](#) from [NestoriSyynimaa:patch-1](#)[Conversation](#) 1[Commits](#) 1[Checks](#) 0[Files changed](#) 1

Changes from all commits ▾ Jump to... ▾ +1 -0 ■■■■■

[Diff settings](#) ▾[Review changes](#) ▾

### Added the missing dictionary element "DigestValue"

I added the missing dictionary element "DigestValue" between "DigestMethod" and "Address".

NestoriSyynimaa committed 6 hours ago [Verified](#)

commit 56e553d1c3eb039185e83daca331d854a9034083

1 ■■■■■ BinaryMessageFiddlerExtension/WcfBinaryConverter.cs

[View](#)

@@ -75,6 +75,7 @@ private static XmlDictionary CreateWcfBinaryDictionary()			
75	dict.Add("Transforms");	75	dict.Add("Transforms");
76	dict.Add("Transform");	76	dict.Add("Transform");
77	dict.Add("DigestMethod");	77	dict.Add("DigestMethod");
		78 +	dict.Add("DigestValue");
78	dict.Add("Address");	79	dict.Add("Address");
79	dict.Add("ReplyTo");	80	dict.Add("ReplyTo");
80	dict.Add("SequenceAcknowledgement");	81	dict.Add("SequenceAcknowledgement");

💡 ProTip! Use [n](#) and [p](#) to navigate between commits in a pull request.

Headers | TextView | SyntaxView | WebForms | HexView | WCF Binary | Auth | Cookies | Raw | JSON | XML

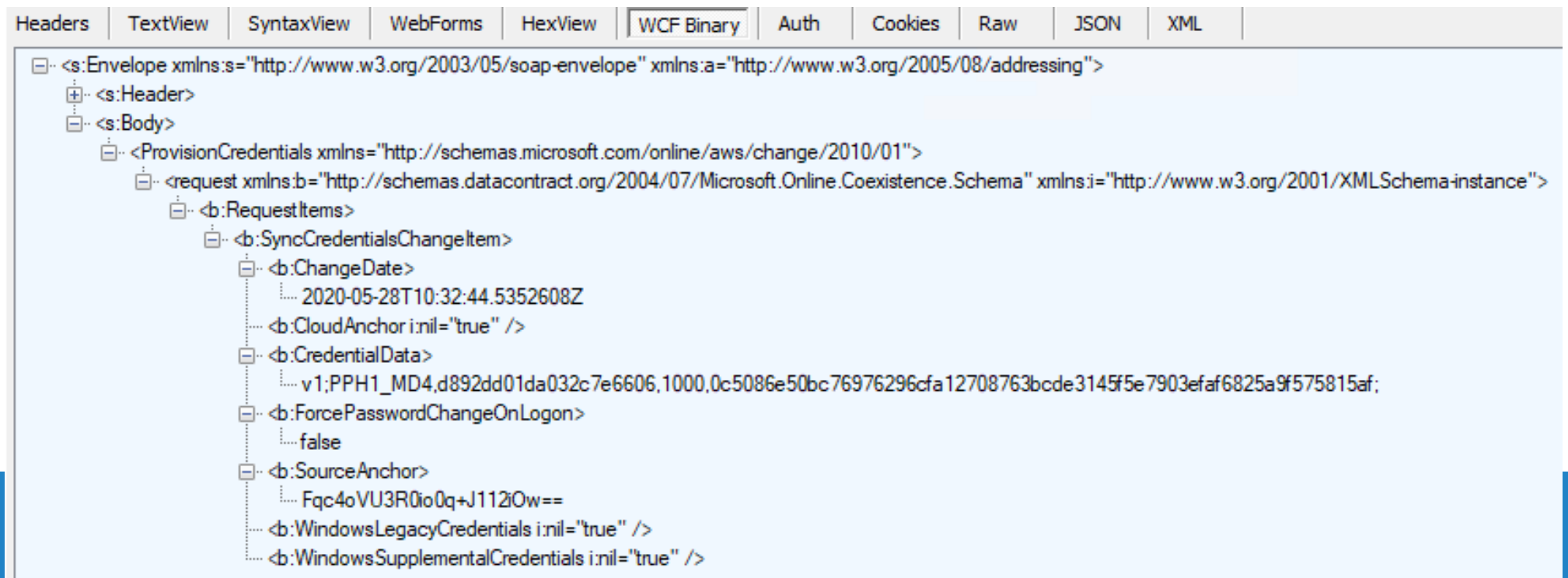
```
<s:Envelope xmlns:s="http://www.w3.org/2003/05/soap-envelope" xmlns:a="http://www.w3.org/2005/08/addressing">
  <s:Header>
    <a:Action s:mustUnderstand="1">
      http://schemas.microsoft.com/online/aws/change/2010/01/ProvisioningWebService/GetCompanyConfiguration
    </a>
    <SyncToken s:relay="um:microsoft.online.administrativeservice" xmlns="um:microsoft.online.administrativeservice" xmlns:i="http://www.w3.org/2001/XMLSchema-instance">
    </SyncToken>
    <a:MessageID>
    </a>
    <a:SequenceAcknowledgement>
      <a:ReplyTo>
        http://www.w3.org/2005/08/addressing/anonymous
      </a>
      <a:To s:mustUnderstand="1">
        https://adminwebservice.microsoftonline.com/provisioningservice.svc
      </a>
    </a>
  </s:Header>
  <s:Body>
    <GetCompanyConfiguration xmlns="http://schemas.microsoft.com/online/aws/change/2010/01">
      <includeLicenseInformation>
        false
      </includeLicenseInformation>
    </GetCompanyConfiguration>
  </s:Body>
</s:Envelope>
```

Headers | TextView | SyntaxView | WebForms | HexView | WCF Binary | Auth | Cookies | Raw | JSON | XML

```
<s:Envelope xmlns:s="http://www.w3.org/2003/05/soap-envelope" xmlns:a="http://www.w3.org/2005/08/addressing">
  <s:Header>
    <a:Action s:mustUnderstand="1">
      http://schemas.microsoft.com/online/aws/change/2010/01/ProvisioningWebService/GetCompanyConfiguration
    </a>
    <SyncToken s:role="um:microsoft.online.administrativeservice" xmlns="um:microsoft.online.administrativeservice" xmlns:i="http://www.w3.org/2001/XMLSchema-instance">
    </SyncToken>
    <a:MessageID>
    </a>
    <a:ReplyTo>
      <a:Address>
        http://www.w3.org/2005/08/addressing/anonymous
      </a>
      <a:To s:mustUnderstand="1">
        https://adminwebservice.microsoftonline.com/provisioningservice.svc
      </a>
    </a>
  </s:Header>
  <s:Body>
    <GetCompanyConfiguration xmlns="http://schemas.microsoft.com/online/aws/change/2010/01">
      <includeLicenseInformation>
        false
      </includeLicenseInformation>
    </GetCompanyConfiguration>
  </s:Body>
</s:Envelope>
```

# Set-AADIntUserPassword

- Password Hash, change timestamp, and force password change
- Hash is a PBKDF2 (Password-Based Key Derivation Function 2)
- Only hash synchronised -> cloud pwd restrictions not applied ☺



The screenshot shows a SOAP message in a debugger's XML view. The message is a request to set an AAD user password. The XML structure is as follows:

```
<s:Envelope xmlns:s="http://www.w3.org/2003/05/soap-envelope" xmlns:a="http://www.w3.org/2005/08/addressing">
  <s:Header>
  <s:Body>
    <ProvisionCredentials xmlns="http://schemas.microsoft.com/online/aws/change/2010/01">
      <request xmlns:b="http://schemas.datacontract.org/2004/07/Microsoft.Online.Coexistence.Schema" xmlns:i="http://www.w3.org/2001/XMLSchema-instance">
        <b:RequestItems>
          <b:SyncCredentialsChangeItem>
            <b:ChangeDate>
              2020-05-28T10:32:44.5352608Z
            <b:CloudAnchor i:nil="true" />
            <b:CredentialData>
              v1:PPH1_MD4,d892dd01da032c7e6606,1000,0c5086e50bc76976296cfa12708763bcde3145f5e7903efaf6825a9f575815af;
            <b:ForcePasswordChangeOnLogon>
              false
            <b:SourceAnchor>
              Fqc4oVU3R0io0q+J112iOw==
            <b:WindowsLegacyCredentials i:nil="true" />
            <b:WindowsSupplementalCredentials i:nil="true" />
          </b:SyncCredentialsChangeItem>
        </b:RequestItems>
      </request>
    </ProvisionCredentials>
  </s:Body>
</s:Header>
</s:Envelope>
```



# Get-AADIntOneDriveFiles

- Downloads all files from user's OneDrive
- Sync client sends to OneDrive
  - Domain guid in http header **X-MachineDomainInfo**
  - Machine type in http header **User-Agent**
    - Microsoft SkyDriveSync 19.192.0926.0012 ship; windows NT 10.0 (17763)
    - Microsoft SkyDriveSync 20.169.0823.0006 ship; Mac OS X 10.15.7"



# Azure AD and Microsoft 365 kill chain

	Recon	Compromise	Persistence	Actions on Intent
Outsider	Get-AADIntTenantDomains Get-AADIntOpenIDConfiguration Get-AADIntLoginInformation Invoke-AADIntReconAsOutsider Invoke-AADIntUserEnumerationAsOutsider	Invoke-AADIntPhishing		
Guest	Get-AADIntAzureTenants Get-AADIntAzureInformation Get-AADIntSPOSiteUsers Get-AADIntSPOSiteGroups Invoke-AADIntReconAsGuest Invoke-AADIntUserEnumerationAsGuest			
User	Get-AADIntTenantDetails Get-AADIntGlobalAdmins Get-AADIntSyncConfiguration Get-AADIntCompanyInformation Get-AADIntSPOServiceInformation Invoke-AADIntReconAsInsider Invoke-AADIntUserEnumerationAsInsider			
Admin	Get-AADIntAzureSubscriptions	Grant-AADIntAzureUserAccessAdminRole Set-AADIntAzureRoleAssignment Invoke-AADIntAzureVMScript Register-AADIntPTAAgent Set-UserMFA Set-UserMFAApps	ConvertTo-AADIntBackdoor Set-AADIntPassThroughAuthentication	New-AADIntSAMLToken New-AADIntKerberosTicket Open-AADIntOffice365Portal
On-prem admin		Export-AADIntADFSSigningCertificate Get-AADIntSyncCredentials Set-AADIntUserPassword Install-AADIntPTASpy		New-AADIntSAMLToken New-AADIntKerberosTicket Open-AADIntOffice365Portal

# Invoke-AADIntUserEnumerationAsGuest

- Dumps Azure AD users and groups of target tenant
- Introduced Aug 7<sup>th</sup>, MS reacted next day
- Public preview for mitigation Aug 22<sup>nd</sup>



**TunaMania** @tuna\_gezer · Aug 8

Great post Nestori, as always! Current guest permissions are around limiting enumerate, anyone who doesn't read the doc miss this detail! We are working on a new feature which will address a large set of your points in the blog, you might need to update the post very soon 🤖



1



3



**Dr. Nestori Syynimaa** @NestoriSyynimaa · Aug 8

Looking forward to that!



2



## External collaboration settings



Save



Discard

### Guest user access

Guest user access restrictions (Preview) ⓘ

[Learn more](#)



Guest users have the same access as members (most inclusive)



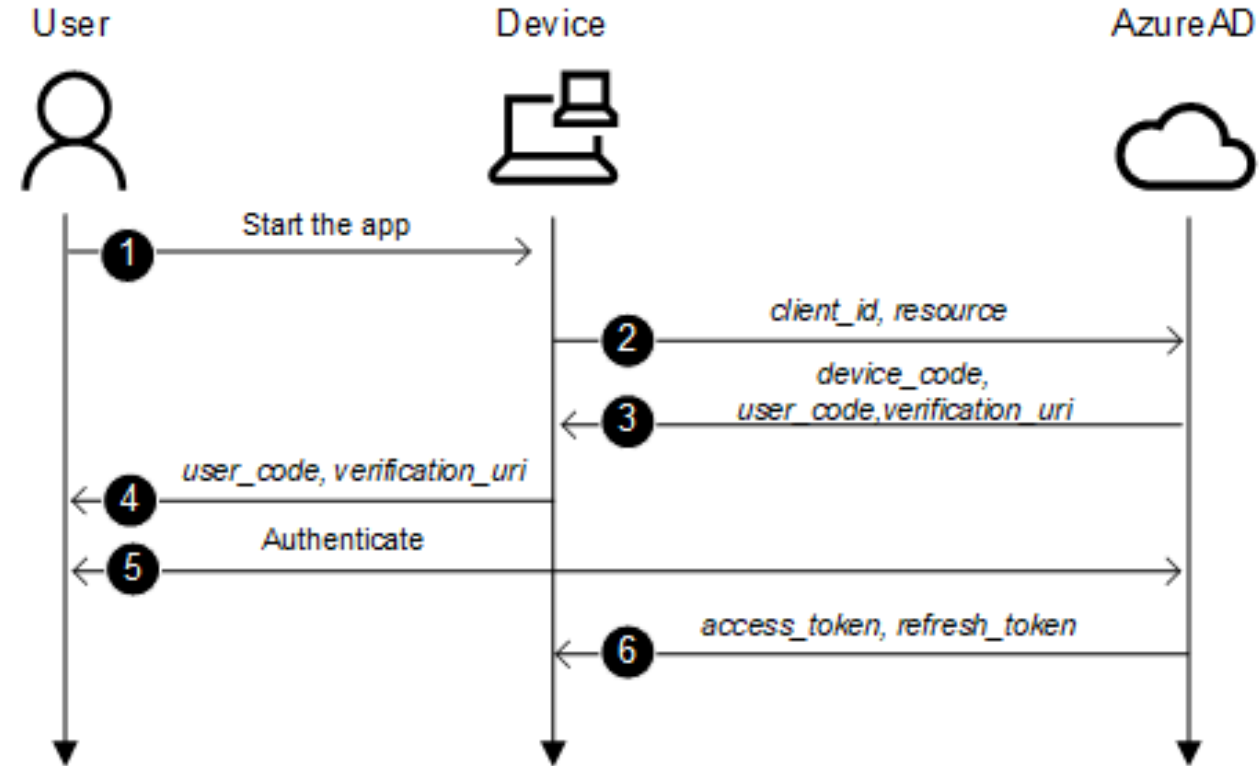
Guest users have limited access to properties and memberships of directory objects



Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)

# Invoke-AADIntPhishing

- Generates phishing messages (email / Teams)
- Utilises “device code authentication flow”
- Steals the user’s identity



# Summary

- Every client is communicating with cloud
  - Cloud only does what the client asks
  - Cloud only knows what client tells
- PowerShell module is a great way to share your knowledge!
  - Remember to document what you do (both the code and functionality)
  - Add help with examples! (Get-Help xxx -Examples)
- Cloud changes all the time..





# CLOUD IDENTITY SUMMIT '20

Your Feedback is important!

<http://feedback.identitysummit.cloud/>

Thanks to our sponsors!

