The weakest link of Office 365 security

1st Nestori Syynimaa

[1]Enterprise Architect, CSC – IT Center for Science, Espoo, Finland, nestori.syynimaa(at)csc.fi
[1]Senior consultant and founder, Gerenios Ltd, Tampere, Finland, nestori.syynimaa(at)gerenios.com

Keywords
Office 365, security, mitigation, risk.

1. ABSTRACT

Office 365 service is widely adopted in Higher Education field all around the world. It is a cloud service provided by Microsoft, including Office applications and services like Exchange Online and SharePoint Online. Although the Office 365 is audited by many external bodies, there have been continuous discussions about the information security of the service.

One of the top current security risks of web applications is Security Misconfiguration. This paper introduces some techniques a rogue administrator may use in order to exploit users' confidential information. Symptoms, detection techniques, forensics, and mitigation techniques of these are also introduced. As a conclusion, it can be argued that the weakest point of Office 365 security is organisation's on-premise misconfiguration. This paper helps organisation's security officers and IT administrators auditing their on-premise environment security.

2. INTRODUCTION

Office 365 (O365) is a cloud service provided by Microsoft. There are several different service plans available, which usually includes Office applications, such as Word and PowerPoint, but also other productivity services, such as Exchange Online and SharePoint Online. In Higher Education field O365 is widely adopted, especially due to its aggressive pricing. For instance the E1 plan (Office applications not included) is free for students and faculty staff, and the E3 plan £1.80 and £3.30 per month per user, respectively (Microsoft, 2015b). Besides the Office 365 platform, Microsoft has also published productivity tools for education. For instance in September 2014, OneNote Class Notebook Creator was launched to help teachers to easily set up their classes (Microsoft, 2014a).

As the adoption rate of Office 365 is increasing, so are the security concerns. Especially the concerns about the confidentiality of data and information has generated discussion (see for example University of Bradford, 2014; University of Concordia, 2014). To address these issues contractually, some government bodies, such as janet in the UK, has negotiated amendments to standard Office 365 agreements (janet, 2013).

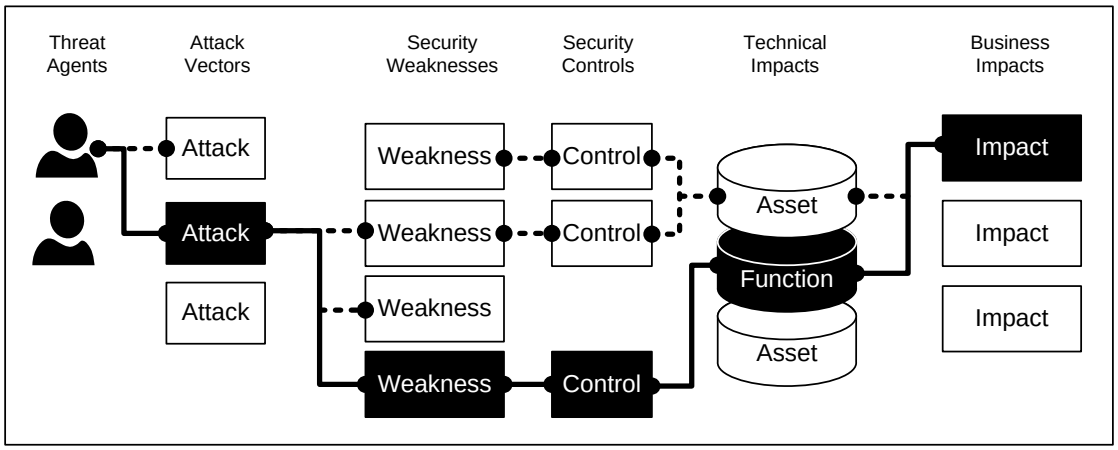

Figure 1: Application security paths (adapted from OWASP, 2013)

There are many different paths to impact organisations business through security weaknesses, as illustrated in Figure 1. Sometimes these paths are easy to find, sometimes they are difficult. After identification of a weakness, actions need to be taken to control it. In this paper, we will introduce some of the paths how a rogue administrator may gain access to users' confidential data in O365. We start by introducing the Office 365 security basics, including three O365 identity options. Next we demonstrate how the misconfigured on-premise security allows exploitation of O365 confidential data. We will also show how to detect such rogue behaviour, how to forensic, and finally how to mitigate it.

3. OFFICE 365 CORE SECURITY

Office 365 runs on another Microsoft cloud service, Microsoft Azure. Azure is an infrastructure-as-a-service (IaaS) and a platform-as-a-service (PaaS) (Microsoft, 2015c). O365 is a software-as-a-service utilising the Azure IaaS and PaaS services. It is accessible from the internet regardless of the user's location and is therefore exposed to massive security attacks.

In cloud services, the service provider is taking care of the hardware level security, and most parts of the software security. O365 is provided using a defence-in-depth strategy (Microsoft, 2014b) as illustrated in Figure 2. The physical layer consists of facility and network security, the logical layer host, application, and admin user security, and the data layer the data security. These layers are taken care of Microsoft. Customers also have a number of security controls. They can control for instance data integrity, data encryption, and end-user access.

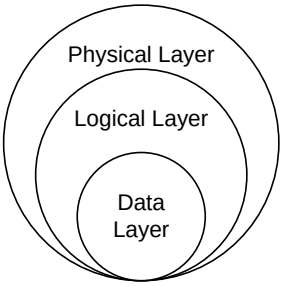

Figure 2: Defence in depth (Microsoft, 2014b)

The Open Web Application Security Project (OWASP) has identified ten most critical web application risks (see OWASP, 2013). In O365, all server-side risks are handled by Microsoft. However, when O365 is integrated with on-premise environment, the Security Misconfiguration risk needs to be mitigated by the customer. Description of the Security Misconfiguration is as follows:

> *Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and platform. Secure settings should be defined, implemented, and maintained, as defaults are often insecure. Additionally, software should be kept up to date. (OWASP, 2013, p. 6)*

3.1. Users and admin roles

Office 365 uses role-based access control (RBAC) system. Accessing O365 requires an identity, e.g. an entry in the O365 internal directory. O365 uses Azure Active Directory (AAD) as a directory solution. Each user added to AAD, either using the O365 admin center, DirSync, or PowerShell, is given by default a user role. A summary of O365 admin roles can be seen in Table 1. Adding user to AAD does not require a license. However, in order to use O365 services, such as Exchange Online or SharePoint Online, a license such as E1 or E3 needs to be assigned. It should be noted that Exchange Online has its own RBAC which is different from the O365 RBAC. Having said that, the O365 *Global admin* role maps to *Organization admin* role in Exchange Online. Similarly, SharePoint Online has its own access control, which is different to the O365.

Table 1: Office 365 Administrator roles and rights (Microsoft, 2015a)

Role	Description
Global admin	Access to all administrative features. Only role that can be used assign admin rights to others.
Billing admin	Can make purchases, manage subscriptions and support tickets, and monitor service health.
User management admin	Resets passwords, monitors service health, and manages user accounts, user groups, and service requests.
Password admin	Resets passwords, manages service requests, and monitors service health. Password admins are limited to resetting passwords for users and other password admins.
Service admin	Manages service requests and monitors service health.
User	No access to administrative features.

Each O365 environment (tenant) has at least one domain. The default domain, also called a service domain, is formed when the tenant is deployed. The form of the service domain is <*tenant*>.*onmicrosoft.com*, where tenant refers to the name of the tenant. Customers may also use their own domains in O365, as long as they are registered and their ownership verified. Domains can be used in identities, in email addresses, and in public site url in SharePoint Online.

3.2. Identity scenarios

Office 365 has three identity scenarios as illustrated in Figure 3. The first scenario is called *cloud identity*. In this scenario identities are managed in AAD, either by using O365 admin center or PowerShell. This suits for small organisations or organisations not having an internal Active Directory (AD). Each time users accesses O365, the authentication is performed against the AAD. This means that users have two sets of credentials, one for O365 and one for the on-premise environment. These credentials may or may not be same in terms of username and password.

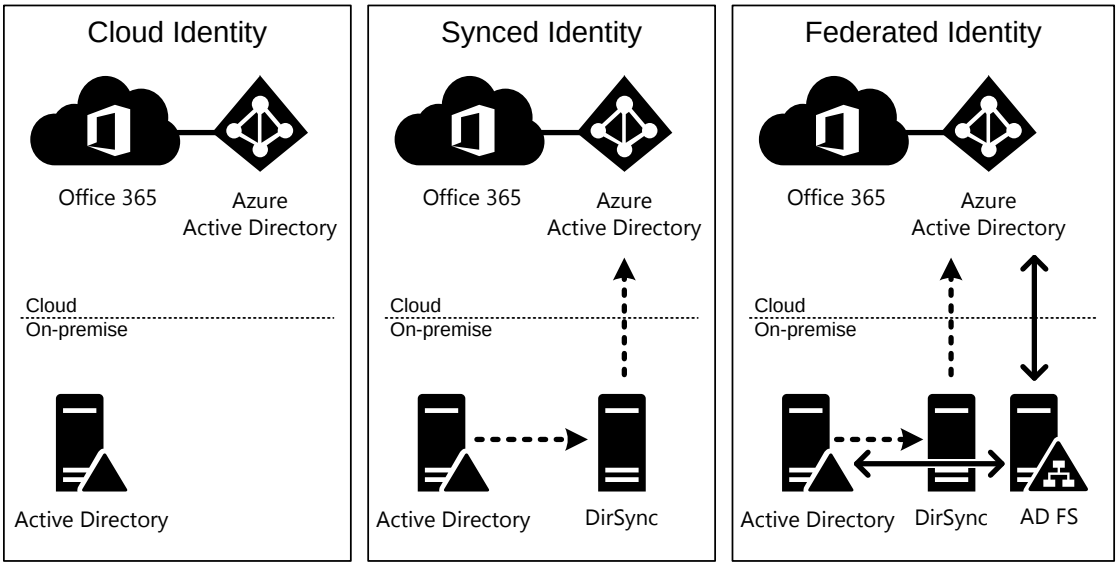

Figure 3: Office 365 identity scenarios

The second scenario is called *synced identity*, which suits for larger organisations having internal AD. In this scenario identities in on-premise AD are synced to AAD using a directory synchronisation software, such as DirSync, AADSync, or FIM. Synchronisation can be configured to sync also the users' passwords, which enables same-sign-on. This way users can use their on-premise credentials to access O365. However, authentication is still performed against the AAD, although the credentials are

populated from internal AD. By default, synchronisation takes place in every 3 hours, passwords are synced in every two minutes. Objects which are synced from the on-premise AD, i.e. users and groups, cannot not be edited in AAD. It should be noted that the directory synchronisation does not prevent creating users directly to AAD. The DirSync software requires *Global admin* level access to AAD, and *Enterprise admin* level access to internal AD.

Third scenario is called *federated identity*, which suits for large organisations and for organisations willing to use single-sign-on (SSO). Also in this scenario, identities are synced to AAD. However, the authentication is performed against the organisation's on-premise AD. Technically this is implemented by using Active Directory Federation Service (AD FS). AD FS needs to be installed on a domain joined server. Accessing such a server directly from the internet would be a security risk, so the access is provided by using internet facing AD FS proxies. When SSO is used, authentication requires access to AD FS each time users are logging in. This makes AD FS a single-point-of-failure. Therefore both AD FS and proxy services needs to be provided using at least two servers in a high availability configuration. This requires in total 2+2=4 servers.

When SSO is turned on, one of the organisation's domains are converted to a federated domain. Every users using that domain as an identity, is switched to using SSO. Only way to add users to the federated domain is to use directory synchronisation. From technical point-of-view AD FS provides a claims-based identity service. Claims are statements made about users, such as identity information (Microsoft, 2011). In O365, AD FS is using UPN and organisation' on-premise AD GUID for user identification. These claims are transferred in security tokens, which are signed by AD FS server by a certificate.

When the domain is converted to federated, on-premise AD FS server and O365 are exchanging information needed in SSO. This information includes two key components; FQDN of the on-premise AD FS server, and the token signing certificate. When user is accessing O365 with a federated username, O365 uses this information to forward the authentication to a correct on-premise AD FS.

There are three authentication endpoints in AD FS for different clients, as illustrated in Figure: 4. *Active endpoint* is used by Outlook and devices using Active Sync protocol, such as mobile phones. These devices are sending username and password to Exchange Online, which authenticates user with AD FS proxy on behalf of the user and acquires the security token. *MEX endpoint* is used by rich clients, such as Lync and Office 365 ProPlus subscription. Those applications are connecting either AD FS or AD FS proxy directly, regarding to their location (on-premise/internet). *Web endpoint* is used by web browsers accessing O365 services, such as Outlook Web App and SharePoint Online. When authenticating, web browser is redirected to AD FS server or proxy. Authentication information is transferred in HTTP POST data.

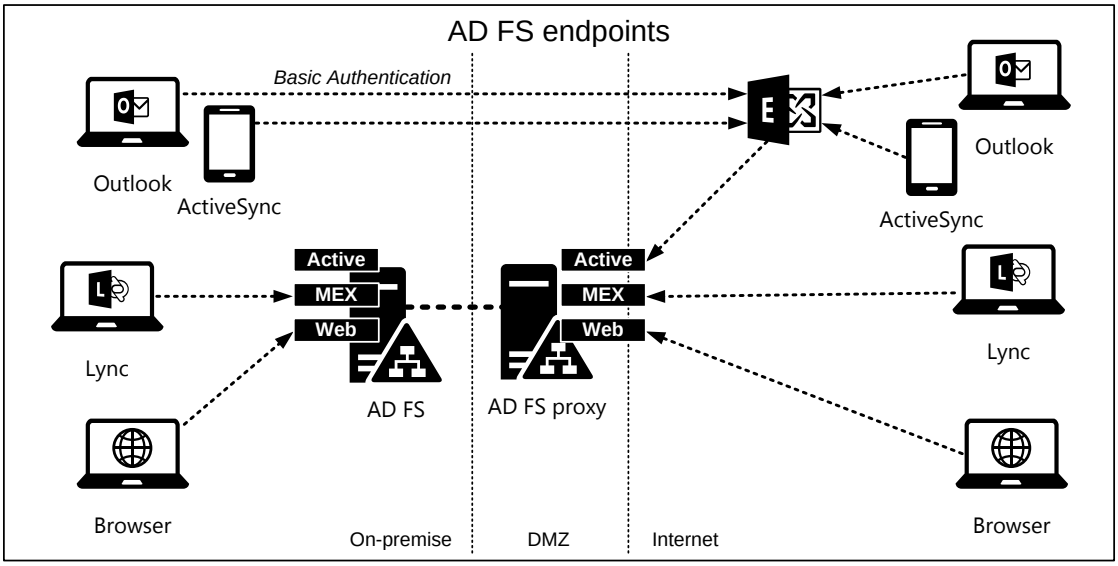

Figure: 4 AD FS Endpoints

4. ACCESSING CONFIDENTIAL INFORMATION

Office 365's internal security certified being high level, which guarantees that users can only access information they are allowed to access. All control for giving access is on customer's hands. Therefore only way to access other users' information is to use administration privileges.

In this section, we will demonstrate techniques a rogue administrator can use to access confidential data, how to identify and detect such an activity, and techniques for mitigation.

4.1. Accessing information by altering permissions

Simplest way to access user's mailbox is to give someone permissions to user's mailbox. This can be performed with a simple PowerShell command (Figure 5).

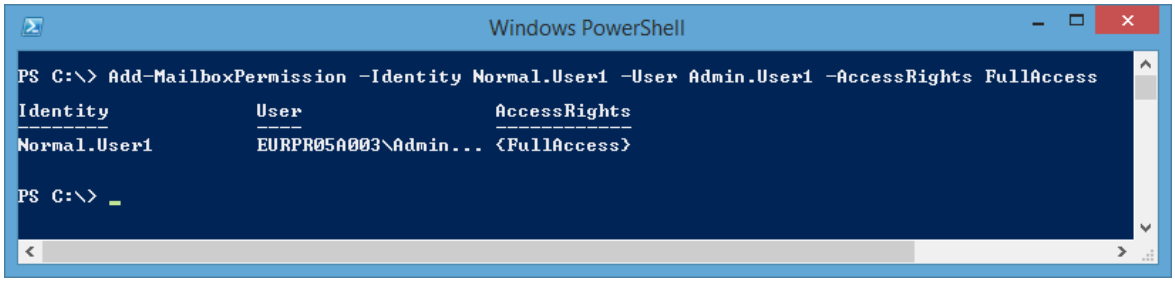

Figure 5: Giving FullAccess permissions to user's mailbox

Similarly, in SharePoint Online, administrators may change the owner(s) of the site collections.

4.2. Accessing identities by changing password

Simplest way to access other user's identity is to change the user's password. This can be performed in O365 admin center, or by using PowerShell (Figure 6). Naturally, user would notice the change of the password when next time accessing O365.

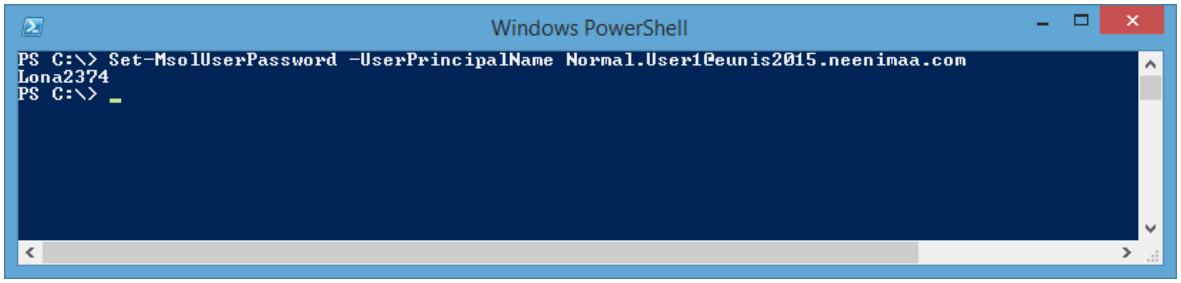

Figure 6: Changing user's password

Changing users' passwords in AAD is possible only in *cloud identity* scenario, and in *synced identity* without password sync.

4.3. Accessing identities by changing password of synchronised user

It is also possible to change user's password in *synced identity* scenario with password sync enabled, although it is more difficult. As stated earlier, when using directory synchronisation, synced objects are not editable in AAD. When objects are synchronised, the object in AAD has an attribute *ImmutableID* which contains the GUID of the corresponding object in internal AD (Figure 7). This is called a hard link.

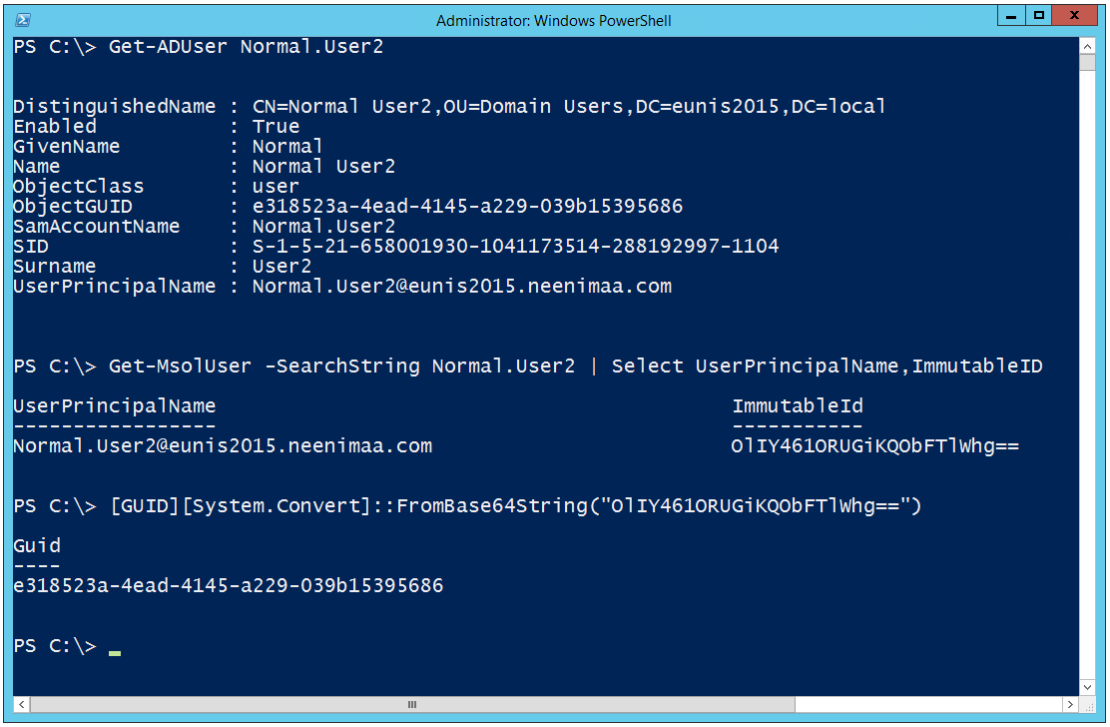

Figure 7: AAD ImmutableId refers to user's internal AD GUID

First step to change the user's password in this scenario is to make user to unsynced. By default, the whole AD forest is synchronised by directory synchronisation. Typically this is not the case, as the sync is usually limited to a certain scope, such as seen in Figure 8. In this case, the *Domain Users* container is synced but *Do not sync* OU is excluded from the synchronisation.

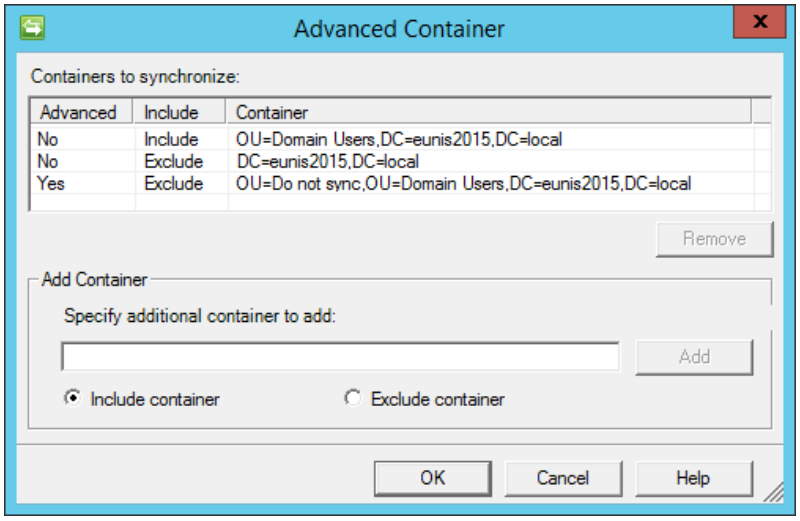

Figure 8: Directory synchronisation scope

Next step is to simply move the user to the excluded OU using Active Directory Users and Computers (ADUC), as in Figure 9, or by PowerShell. This stops the user being synced.

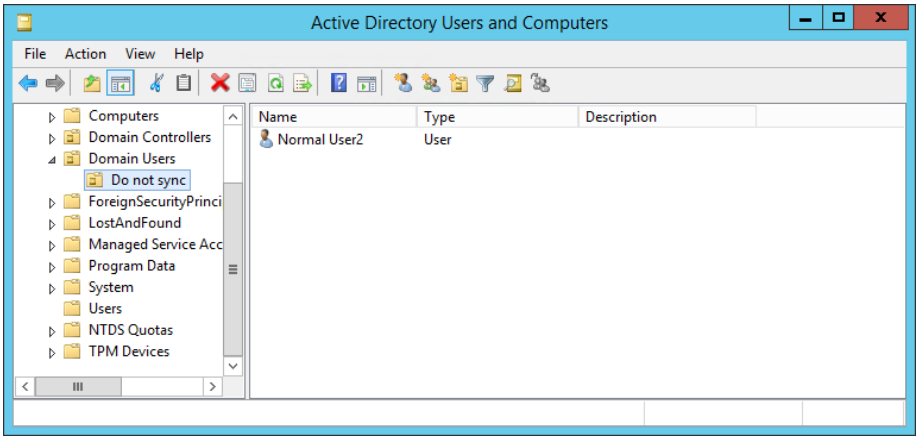

Figure 9: Moving user to OU excluded from synchronisation

After moving the user to another OU, the synchronisation needs to be started manually. When synchronisation is completed, the user will be deleted from AAD if it was originally created by directory synchronisation. In the PowerShell example in Figure 10, we first check the last synchronisation time, start the synchronisation manually, and restore the user. As the user is restored within the grace period (30 days) no data is lost. Finally, the password is changed for the user and O365 may be accessed with the user's identity.

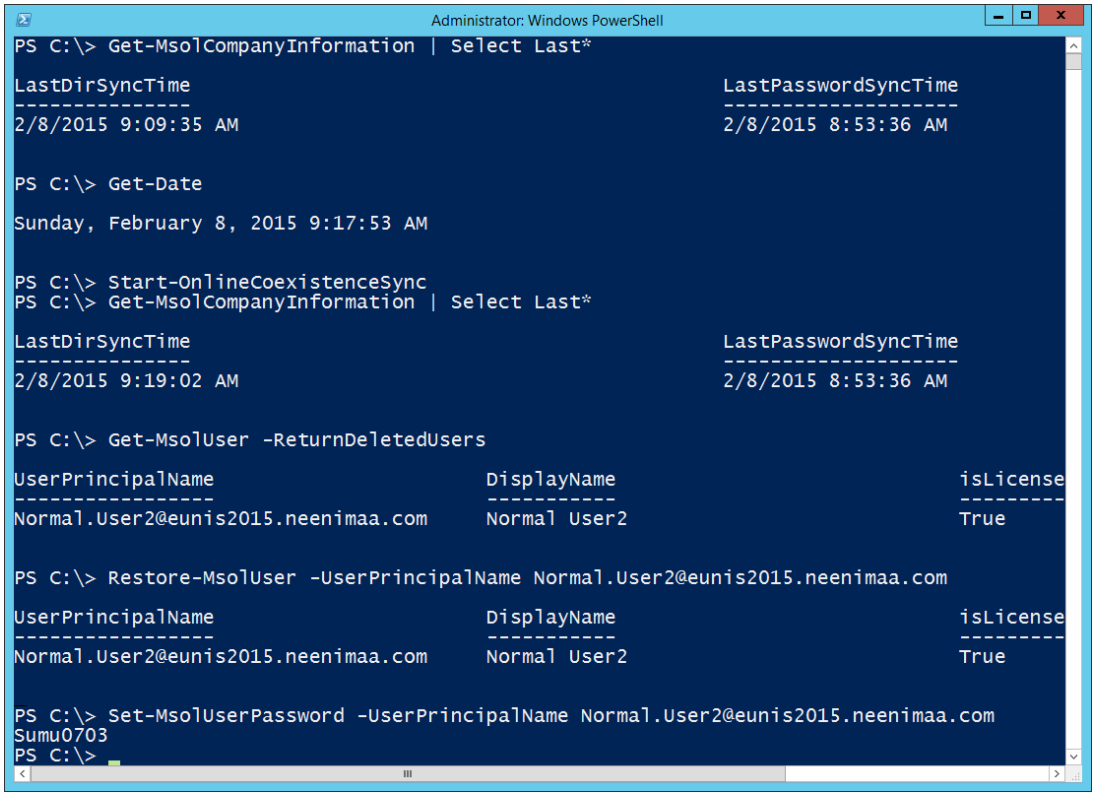

Figure 10: Restoring the deleted sync user and changing user's password

After accessing O365 with the user's identity, changes needs to be reversed so that the user does not notice that the identity has been compromised. First the user is returned to the original container in AD, which makes it again synced user. Next step is to manually start the synchronisation and check the *miisclient* for any errors. Sometimes the user is not properly linked, if so, the *Windows Azure Active Directory* connector needs to be disconnected (Figure 11) in *miisclient*. After another directory synchronisation the user should be linked properly.

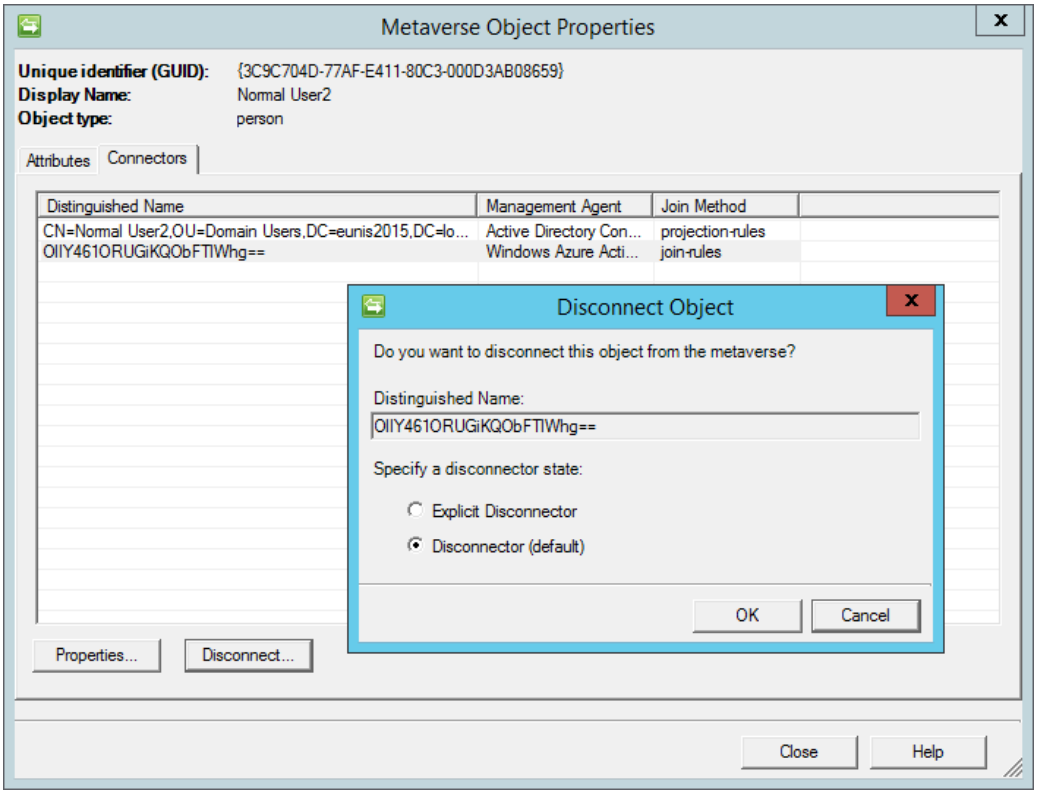

Figure 11: Disconnecting Windows Azure Active Directory connector

When the user in AAD is linked properly with AD, we need to force full synchronisation of passwords. Otherwise the AD password is not synced, because it is triggered only when the password is changed in AD. Password synchronisation can be initiated using PowerShell (Figure 12).

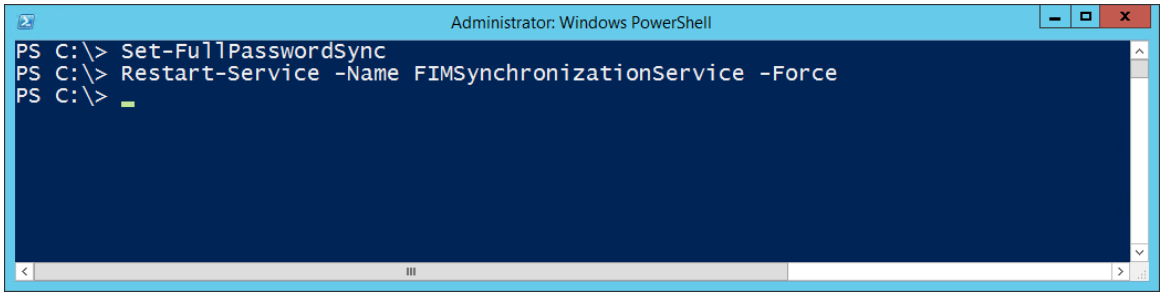

Figure 12: Forcing password full synchronization

After the password synchronisation, everything is returned to original state. So the user may use O365 normally, using the same credentials. This means that the user might not even notice that the account has compromised.

4.4. Accessing federated identities by configuring AD FS

AD FS uses claims to provide authentication information to O365, as described earlier. In AD FS claims are issued using *claim rules*. When the domain is converted to federated, a Relaying Party Trust is created to AD FS. The name of the party is *Microsoft Office 365 Identity Platform* and has contains 2 or 3 issuance transform rules, depending on the configuration. These rules extract UPN and GUID of the authenticated user from the internal AD and issues corresponding claims.

Accessing other user's identity can be achieved simply by altering these claim rules. As an example, in Figure 13, claim rules are altered so that no matter which user logs in, the user is having the identity of Normal User6. The first rule issues the UPN claim and the second one user's ImmutableID claim. ImmutableID is a Base64 encoded GUID of user's AD object.

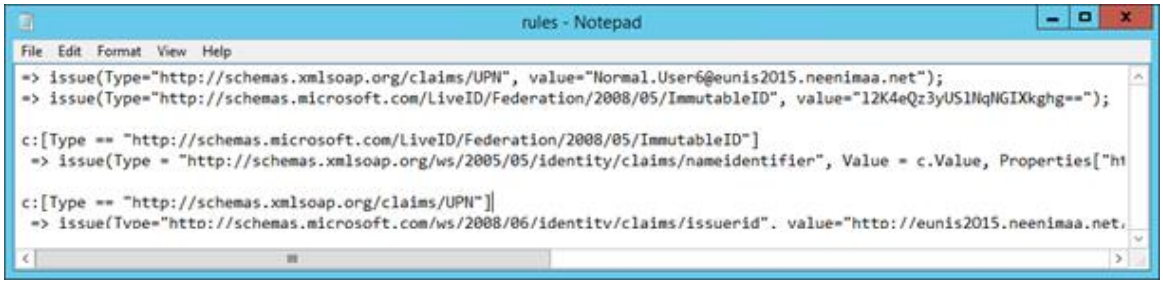

Figure 13: Altering claim issuance transform rules

The altered claim rules can easily be imported to AD FS using PowerShell (Figure 14). This can be performed remotely without a need for desktop access.

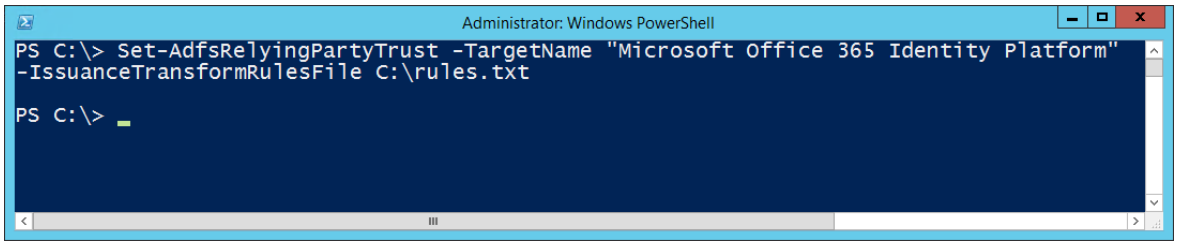

Figure 14: Importing claim issuance transform rules to AD FS

Obviously, in our example, the changes in the rules would be noticed by users as they would be logged in as another user. In real life, rogue administrator would use more sophisticated rules which would give another identity only to a specific user. The user used to log in does not have to be in AAD, or not even use the same identity domain. As long as the user is in AD and can log in, AD FS can be used to access other user's identity.

As we have demonstrated, the rogue administrator can quite easily access other users' information. All of the techniques presented above can be detected and actions can be taken to prevent their exploitation. However, the rogue administrator may have access to backups or virtual hard disks used by the servers. These can easily be copied to a different location and a copy of the on-premise environment could be started. Given the AD FS web endpoint implementation technique, one can alter the name resolution so that the FQDN of the AD FS points to the new environment. In this case, the AD FS configuration could be altered without any chance of noticing it. Therefore the physical protection of backups and limiting access to virtual machines is crucial.

4.5. Gaining administrator access to Windows

Gaining administrator access to Windows and AD is relatively trivial (see Laiho, 2013), as long as certain conditions are met. First, you need to be able to boot from external media, such as the Windows installation media. Secondly, Bitlocker must not be used. If these conditions are met, you may take following steps to gain administrator rights to the computer (or server):

1. Boot the computer from the Windows installation media and start the command prompt
2. Go to C:\Windows\System32 and copy cmd.exe to sethc.exe
3. Boot the computer normally and in the login screen hit the left shift key five times. Command prompt starts as SYSTEM account and you may add yourself as an admin (Figure 15).

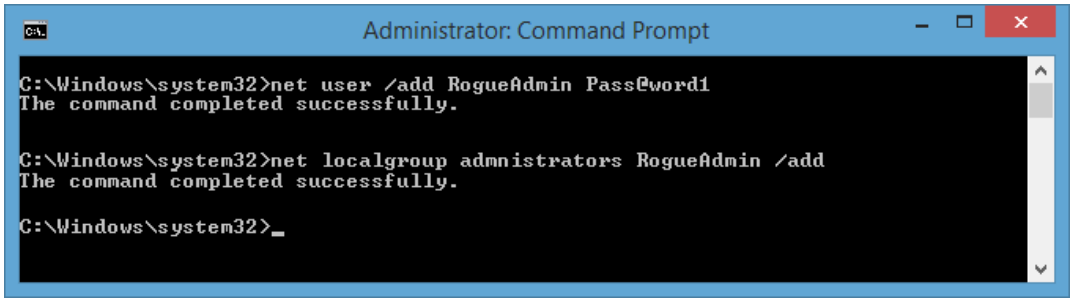

Figure 15: Adding user as local administrator

Getting a domain admin rights is a bit trickier as it requires help from an existing administrator:

1. Create a scheduled task that runs the following command on every logon:

   `NET GROUP "Domain Admins" RogueAdmin /add /domain`

2. Get an existing administrator to log on to your computer, for instance by using excuse such as a need for help in configuring a printer. Note that the user needs to exist in AD.

4.6. Summary

A summary of techniques how a rogue administrator may access other users' information in Office 365 is listed in Table 2, including the end-user symptoms, detection and forensics methods, and mitigation techniques.

Table 2: Summary of information access techniques

Accessing information by giving permission	
End-user symptoms	None, unless content is altered.
Detection	None.
Forensics	For Exchange Online, run *Mailbox access by non-owners* report in Office 365 admin center. For SharePoint Online, view audit log reports in *Site Collection Administrator* section.
Mitigation	Give only minimum admin rights.

Accessing identities by changing user's password	
End-user symptoms	Unable to log in. Multi-factor authentication requested when not logging in (if configured).
Detection	None.
Forensics	Check the value of *LastPasswordChangeTimestamp* property of the user with *Get-MsolUser* cmdlet. View the *LastLogonTime* property of the user mailbox with *Get-Mailbox* cmdlet. Check audit reports from Azure AD, such as *Password reset activity* (requires Azure premium).
Mitigation	Give only minimum admin rights. Configure Multi-factor authentication.

Accessing identities by changing password of synchronised user	
End-user symptoms	Unable to log in. After a some period of time login may be possible. Multi-factor authentication requested when not logging in (if configured).
Detection	Monitor directory synchronisation events in *Application log* with *Event Viewer* using for instance Source filter for *FIMSynchronizationService, Directory Synchronization*, and *MSOnlineSyncScheduler*.
Forensics	Check the value of *LastPasswordChangeTimestamp* property of the user with *Get-MsolUser* cmdlet. Check the value of *LastDirSyncTime* property of the user with *Get-MsolUser* cmdlet. View the *LastLogonTime* property of the user mailbox with *Get-Mailbox* cmdlet. Check audit reports from Azure AD. Check *miisclient* for synchronisation events.
Mitigation	Give only minimum admin rights. Configure Multi-factor authentication for users. Prevent unnecessary access to DirSync server.

Accessing federated identities by configuring AD FS	
End-user symptoms	None (if rules configured properly)
Detection	Monitor Kerberos authentication events in *Security log* in *Event Viewer* for event IDs 4768 and 4769. Compare for instance to Azure AD login logs.
Forensics	View the *LastLogonTime* property of the user mailbox with *Get-Mailbox* cmdlet. Check audit reports from Azure AD.
Mitigation	Give only minimum admin rights. Configure Multi-factor authentication for users. Prevent unnecessary access to AD FS server. Disable remote PowerShell.

Gaining administrator rights to Windows	
End-user symptoms	None
Detection	Monitor event logs for unnormal activity
Forensics	View *Domain Admins* group members, check the computer and server logs.
Mitigation	Give only minimum admin rights. Never log on as Domain Admin to other user's computer. Use Bitlocker.

5. CONCLUSIONS

In this paper, we have demonstrated techniques a rogue administrator may exploit users' confidential information in Office 365. Some of the techniques cause symptoms that end-users may notice, most of them not. Administrator may detect usage of some of these techniques but not all. All of these weaknesses are related to organisation's on-premise security.

It can be argued that the weakest point of Office 365 security is the customer's on-premise security misconfiguration. Organisation's security officers and IT administration may use this paper as a guideline when auditing their on-premise security. Software and service versions used in demonstrations are listed in Table 3.

Table 3: Software versions used in the demonstrations

Product/Service	Version
Office 365 plan	E3
Windows Server 2012 R2 Data center	6.3.9600
Microsoft Online Services Sign-in Assistant	7.250.4551.0
Windows Azure Active Directory Module for Windows PowerShell	1.0.0
Windows Azure Active Directory Sync Tool	1.0.7020.0

6. REFERENCES

janet. (2013). Cloud services for education agreements. Microsoft Office 365. Retrieved from https://www.ja.net/sites/default/files/Cloud%20for%20Ed%20-%20Office%20365%20info.pdf

Laiho, S. (2013). 7 Ways to Crack Windows 7. Retrieved from http://www.inuit.se/download.php?file=gogn/Avecto/avecto_article__sl_7_ways_to_crack_windows_7.pdf

Microsoft. (2011). AD FS 2.0 Design guide Retrieved Feb 7th 2015, from https://technet.microsoft.com/en-gb/library/dd807036%28v=ws.10%29.aspx

Microsoft. (2014a). OneNote Class Notebook Creator Retrieved Feb 7th 2015, from http://aka.ms/OneNoteEDUapp

Microsoft. (2014b). Security in Office 365 White Paper. Retrieved from http://www.microsoft.com/en-us/download/details.aspx?id=26552

Microsoft. (2015a). Assigning admin roles Retrieved Feb 7th 2015, from https://support.office.com/client/Assigning-admin-roles-eac4d046-1afd-4f1a-85fc-8219c79e1504

Microsoft. (2015b). Office 365 Education plans and pricing Retrieved Feb 7th 2015, from http://products.office.com/en-gb/academic/compare-office-365-education-plans

Microsoft. (2015c). What is Microsoft Azure? Retrieved Feb 7th 2015, from http://azure.microsoft.com/en-gb/overview/what-is-azure/

OWASP. (2013). OWASP Top 10 - 2013. The Ten Most Critical Web Application Security Risks Retrieved from http://owasptop10.googlecode.com/files/OWASP%20Top%2010%20-%202013.pdf

University of Bradford. (2014). Office 365 Privacy Impact Assessment Retrieved Feb 7th 2015, from http://www.bradford.ac.uk/it-services/media/itservices/allfiles/documents/projects/office-365/o365-privacy-impact.pdf

University of Concordia. (2014). Microsoft Office 365 for education - Privacy FAQ Retrieved Feb 7th 2015, from http://www.concordia.ca/content/dam/concordia/docs/IITS/office365-privacy-faq.pdf

7. AUTHOR'S BIOGRAPHY

Dr. Nestori Syynimaa MBCS CITP works as an Enterprise Architect for CSC - Finnish Center of Science, as a freelance trainer for the leading Finnish ICT-training company Sovelto Plc, and is the founder of Gerenios Ltd. His is experienced trainer in Enterprise Architecture and Office 365. Previously he has worked as CIO, CTO, and senior consultant in ICT industry since 2000. He holds BBA from Seinäjoki University of Applied Sciences and M.Sc. (Econ. & BusAdm with major in CS) from University of Vaasa, Finland. He received his Ph.D. from Henley Business School, University of Reading, UK. He also holds several industry certificates including TOGAF, ITIL, Microsoft Certified Trainer, Microsoft Certified Educator, and MCSA (Office 365). http://www.linkedin.com/in/nestori