National Cyber Security Centre
a part of GCHQ

Advisory: The rise of O365 compromise and how to mitigate

Version 1.0

Reference: NCSC-Ops/32-18

04 December 2018

About this Document

This NCSC advisory provides details on the compromise of Microsoft Office 365 and details mitigation advice that organisations of all sizes should consider adopting. Organisations should remember that a risk-based approach should be taken when considering the mitigation strategies set out in this advisory.

Handling of the Report

Information in this report has been given a Traffic Light Protocol (TLP) of WHITE, which means it can be shared within the Cyber Security Information Sharing Partnership (CiSP) community with no handling restrictions. You must ensure that you store, handle and transmit the report in the manner appropriate to its TLP.

Disclaimer

This report draws on information derived from the NCSC and industry sources. Any NCSC findings and recommendations made have not been provided with the intention of avoiding all risks and following the recommendations will not remove all such risk. Ownership of information risks remains with the relevant system owner at all times.

Introduction

Microsoft Office 365 (O365) is an online version of Microsoft's Office application. The service is delivered to users through the cloud on a monthly paid subscription basis and has become increasingly popular. Because O365 has been rapidly adopted across sectors and organisations of all sizes, it has become a prime target for cyber actors, in particular those seeking to profit financially. According to the FBI, attacks on business email cost businesses over $5.3 billion dollars in losses between 2013 and 2016.[1]

The NCSC is aware of several incidents involving the compromise of O365 accounts within the UK, including the use of such methods in targeted supply chain attacks. The ultimate objective of this type of targeting is not clear and the attacks appear not to be limited to any particular sector or attributed to any single threat actor.

This NCSC advisory outlines the different techniques used by cyber actors to compromise O365 and provides detailed guidance on steps an organisation can take to reduce the risk of such breaches occurring.

Details

O365 compromise objectives

The impact of an O365 account compromise can vary in severity depending on an actor's objectives. Once an actor has obtained credentials for an O365 account, not only can the account access be used to access documents across a user's O365 surface (SharePoint, OneNote etc.) but it can also be used as a launchpad to carry out further compromises within an organisation. Some of the ways in which an actor can use a compromised O365 account are detailed below:

- Impersonation of the compromised O365 account owner to manipulate the movement of money or to gain access to information within an organisation;
- Steal sensitive commercial information from the compromised account either to leak publicly causing reputational damage to a company, or to sell;
- Use of the compromised O365 account to distribute spear phishing emails, prompting recipients to give up user credentials and allowing the actor access to further O365 credentials within the victim organisation and its supply chain;
- Use of the compromised O365 account credentials to try and access the accounts of the individual on social media or other places where they might find sensitive information that the actor can use or sell;
- Set up forwarding rules so that the compromised O365 account covertly sends copies of incoming emails to the actor's email account.

[1] https://www.itproportal.com/features/office-365-and-linkedin-integration-a-goldmine-for-fraudsters/

Gaining access to O365 accounts

Actors typically use two common hacking techniques to gain access to O365 accounts, brute force attacks and spear phishing.

Brute force attacks

Brute force attacks involve password guessing, often in an automated manner. In attacks on O365 accounts, brute force techniques have often been used to target specific individuals in organisations rather than targeting multiple employees, primarily to reduce the chances of attack detection by the cloud service provider.[2]

Spear phishing

An actor sends spear phishing emails requesting victims to click on a link which redirects them to a spoofed login page. This login page allows the actor to harvest victim O365 credentials.[3]

Why MFA is so important to preventing O365 compromise

One of the most important steps an organisation can take to reduce the risk of O365 account compromise via brute force attacks or spear phishing is the implementation of Multi-Factor Authentication (MFA) across the O365 platform. As users tend to re-use passwords across online and enterprise services,[4] MFA reduces the potential of password compromise through adding another layer of security.

MFA works by requiring two or more of the following authentication methods:

- Something you know (typically a password);
- Something you have (a trusted device such as a mobile phone);
- Something you are (biometrics);

The O365 platform supports a number of different MFA mechanisms and depending on the subscription, organisations are able to use a mixture of different deployments.

To implement MFA effectively across an organisation's O365 platform will require IT departments to understand the user group to which they are intending to roll it out. This is especially crucial when organisations are dealing with a diverse workforce. As an example, organisations that have employees deployed in locations with poor mobile phone coverage may have problems receiving SMS tokens, causing difficulties in access to the O365 platform. In this scenario, organisations should consider the different MFA mechanisms available to them to avoid reluctance in adoption across the wider organisation.

The NCSC has recently published publicly available guidance on 'MFA for Online Services' (https://www.ncsc.gov.uk/guidance/multi-factor-authentication-online-services).

[2] https://www.tripwire.com/state-of-security/featured/new-type-brute-force-attack-office-365-accounts/

[3] https://threatpost.com/office-365-phishing-campaign-hides-malicious-urls-in-sharepoint-files/136525/

[4] https://www.ncsc.gov.uk/guidance/password-collection

Organisations should review this guidance along with the mitigation advice below, which has been tailored for organisations using O365 to deliver online services.

Mitigation

This section details a minimum set of mitigations that all organisations should implement, and it identifies some extra features that could also be considered.

The NCSC also suggests referring regularly to the Office 365 Secure Score which analyses aspects of an organisation’s configuration, tracks it over time, and makes recommendations for further security-impacting improvements. While the numerical score itself is not particularly useful, the analytics and recommendations that feed into it are a good way of auditing which controls an organisation has implemented and identifying newly released security capabilities. More information on the Office 365 Secure Score and how to get the most out of it can be found on Microsoft's support site.

We strongly recommend that all organisations implement Microsoft's published security best practices for Office 365. These include the following:

Authentication

Organisations need to ensure that a type of Multi-Factor Authentication (as outlined in NCSC's MFA guidance) is enabled for **all** accounts and enforced by Conditional Access. The type of extra factor will vary depending on how users currently access the service, but will usually be one (or more) of:

- An authenticator app - either using a single-use code or accepting approve/deny prompt;
- Accessing the service from a known work device, including Azure AD registered devices, joined devices or compliant devices;
- Accessing the service from a trusted network, including remote access to that network via a VPN;
- An SMS or phone call to a pre-registered number. SMS is not the most secure type of 2FA, but any multi-factor authentication is better than not having it at all.

The NCSC recommends that users with privileged or administrative access both use an authenticator app and prove that they are accessing the service from a known, trusted device or network.

Some legacy authentication protocols do not fully support modern authentication, requiring security controls such as MFA to be turned off or bypassed. These are generally used by older Office clients (e.g. Office 2010) or apps that use mail protocols such as IMAP/SMTP/POP. The NCSC therefore strongly recommend that legacy authentication protocols are disabled as part of an organisation’s Conditional Access policy.

Audit and Monitoring

Organisations should ensure that they are collecting enough audit data to give insight into any attempted or successful breaches. While Office 365 has some auditing enabled by default, we recommend also enabling:

- Audit Log data recording, which logs how users are interacting with the service. This action can take up to 24 hours to be applied consistently across all services.
- Mailbox auditing, to give visibility of the timeline of any compromise – as by default only non-owner access to mailboxes is audited.

Optional services such as Office 365 Cloud App Security can generate reports and raise alerts for suspicious or anomalous authentication and access events for standard and privileged users.

Service hardening

Organisations should configure the Office 365 service and the devices from which it is accessed to attempt to filter out and reduce the impact of attempted attacks. As a minimum organisations should:

- Configure Exchange Online to prevent e-mails from automatically forwarding outside of your organisation, as documented by Microsoft.
- Configure Office Anti-malware protection, ensuring that Exchange Online Protection and Spam Filtering are enabled. Optional services such as Office 365 ATP can perform more advanced analytics on email attachments, files stored in SharePoint/OneDrive and links in emails and documents, and should be enabled if included in an organisation's license. Third party mail filters can also be configured as part of mail flow.
- Configuration of Exchange Online to prevent others spoofing emails from your organisation's domain(s) by configuring SPF, DKIM and DMARC as described in NCSC's e-mail security and anti-spoofing guidance. Office 365 enforces DMARC on inbound email by default; Microsoft provides documentation to set up SPF, DKIM and DMARC for outbound email. Optional services such as ATP anti-phishing and third-party services can reduce the number of malicious e-mails delivered to an organisation's users. We suggest also referring to NCSC's phishing guidance.
- Organisations should review the permissions that it and its users have granted to others, ensuring that it is understood what permissions have been granted to third party services via Integrated Apps.

Device hardening

Most mitigations for Office 365 are applied to the service itself, but it is also important to consider the security posture of the devices being used to access the service.

As a minimum, organisations need to ensure that devices are fully patched, are not using administrative privileges, have malware defences in place and are collecting security logs. The NCSC recommend referring to relevant NCSC guidance including:

- Mitigating malware
- End User Devices security guidance
- Macro security for Microsoft Office
- Preventing lateral movement
- Introduction to logging for security purposes
- Phishing guidance