Office 365 Email Account Compromise Remediation SOP

If a user or PoC reports a user’s Office 365 email account as compromised, which can be identified by spam messages to contacts (internal or external), changed passwords, or other strange behavior, it is likely that they have been subjected to a phishing attack and a malicious threat actor has commandeered their Office 365 email account for nefarious means.

To remediate, simply run the Powershell script linked below, and obtain the [Exchange Online Powershell Module](https://docs.microsoft.com/en-us/powershell/exchange/exchange-online/connect-to-exchange-online-powershell/mfa-connect-to-exchange-online-powershell?view=exchange-ps) by going to any Office 365 administrative console, and going to Exchange Admin Console > Settings > Hybrid > Setup > Install

To run this script, you will not need to know the exactly location of this module on your PC because the script leverages a sorting technique to install it from ISE. Additionally, if you want to check on OAuth compromises, which is a more recent type of attack vector, you will need to save the following [.ps1 script from Microsoft/Azure’s official Github page](https://gist.github.com/psignoret/9d73b00b377002456b24fcb808265c23) to C:\Temp on your local machine. This step, however, is optional, and you can opt to skip this by choosing **NO** or **n** when it prompts: Do you want to check OAuth access? (Y/n)

Ad the conclusion of the script’s runtime, make sure you grab the email template and send it out to the PoC of that client, or send it out directly to the users who received the initial spam, if you have permission from the PoC. The message template is also linked at the bottom of this document.

**SOP**

To remediate a compromised Office 365 account, first: disable sign in to that account. Then, change the password to a temporary password and enable the switch to force new password creation when it is first used. While this account is disabled, connect through the Exchange Online Powershell Module linked above, and list out forwarding rules for that user. There currently is no option to do this from the GUI-based admin console at Portal.Office.com – and instead it must be completed by Powershell.

Connect to the admin console of that client with:

Connect-EXOPSSession

Here, you will sign in with the admin credentials. Then, to test connectivity to Office 365, enter the following command. If it returns error code or nothing, then something went wrong:

Get-MailBox

If this returned the mailboxes of the employees of that company, then you know you are good to go. To list forwarding rules, enter the following (obviously replacing the [user@clientdomain.org](mailto:user@clientdomain.org) with the correct compromised user, but making sure to encase the real user with **“**apostrophes**”**):

Get-InboxRule -Mailbox “user@clientdomain.org”

You can then remove these rules with:

Get-InboxRule -Mailbox “[user@clientdomain.org](mailto:user@clientdomain.org)” | Remove-InboxRule

Once the account is locked out, and the inbox rules were removed, and the password was changed, then check the message trace of Office 365 or Mimecast to identify any outbound spam. Collect the recipients of the spam, and send that list to the PoC. The pre-written script will collect recipient addresses into an array and return it to the operator, and addition to providing the body of the mail message, but it will not send the messages automatically. If not using the script, the operator should send the PoC the content of the message with the message template.

Now, the operator can re-enable the account, and call the PoC and ensure that the password is only told to the user OVER THE PHONE. The new temporary password can NOT be sent over email.