Subject: PhishPrevent Notification
Date: Tuesday, September 22, 2020 at 8:44:39 PM Pacific Daylight Time
From: PhishPrevent Reports
To: Trevor Smith
Attachments: ATT00001.png, ATT00002.png

PhishPrevent

Breach Assessment Report

Contoso Industries

Logins From Foreign Countries

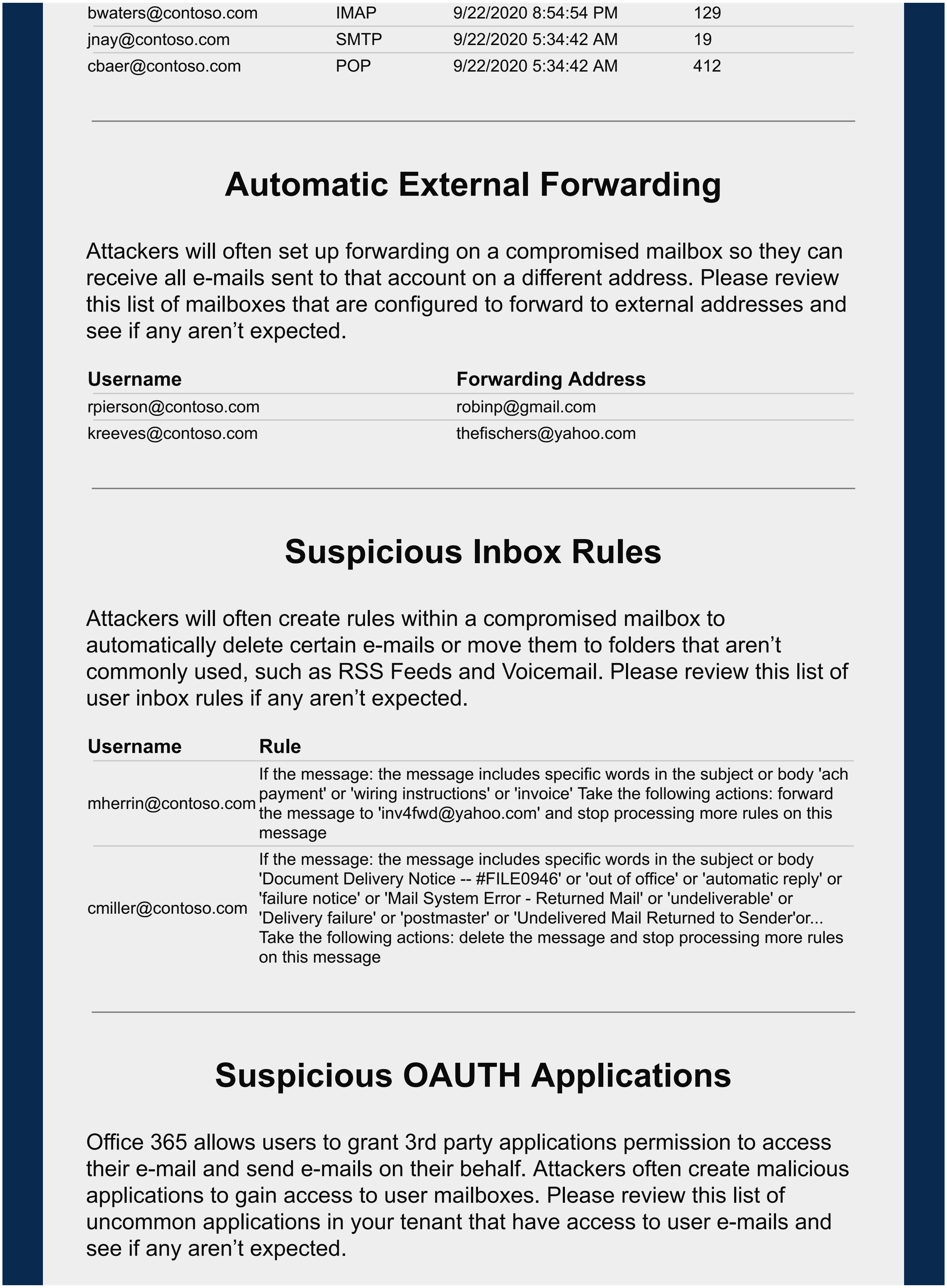
One of the most obvious signs of a breach is if a user has logged in from a country that they haven’t been to. Please review this list of users that have successfully logged in from outside North America in the last 30 days and see if any aren’t expected.

Username	Country	Last Login	Login Count
cdavis@contoso.com	Croatia	8/28/2020 6:57:51 AM	42
cmendenhall@contoso.com	Switzerland	9/17/2020 12:06:20 PM	179
dlyles@contoso.com	Taiwan	9/22/2020 9:50:24 AM	18

Suspicious E-mail Protocols

When attackers compromise user credentials they often attempt to access the user mailbox using older e-mail protocols, such as IMAP and POP, which bypass MFA and other security controls. Please review this list of users that have successfully logged in with suspicious e-mail protocols in the last 30 days and see if any aren’t expected.

Username	Protocol	Last Login	Login Count



bwaters@contoso.com	IMAP	9/22/2020 8:54:54 PM	129
jnay@contoso.com	SMTP	9/22/2020 5:34:42 AM	19
cbaer@contoso.com	POP	9/22/2020 5:34:42 AM	412

Automatic External Forwarding

Attackers will often set up forwarding on a compromised mailbox so they can receive all e-mails sent to that account on a different address. Please review this list of mailboxes that are configured to forward to external addresses and see if any aren’t expected.

Username	Forwarding Address
rpierson@contoso.com	robinp@gmail.com
kreeves@contoso.com	thefischers@yahoo.com

Suspicious Inbox Rules

Attackers will often create rules within a compromised mailbox to automatically delete certain e-mails or move them to folders that aren’t commonly used, such as RSS Feeds and Voicemail. Please review this list of user inbox rules if any aren’t expected.

Username	Rule
mherrin@contoso.com	If the message: the message includes specific words in the subject or body 'ach payment' or 'wiring instructions' or 'invoice' Take the following actions: forward the message to 'inv4fwd@yahoo.com' and stop processing more rules on this message
cmiller@contoso.com	If the message: the message includes specific words in the subject or body 'Document Delivery Notice -- #FILE0946' or 'out of office' or 'automatic reply' or 'failure notice' or 'Mail System Error - Returned Mail' or 'undeliverable' or 'Delivery failure' or 'postmaster' or 'Undelivered Mail Returned to Sender'or... Take the following actions: delete the message and stop processing more rules on this message

Suspicious OAUTH Applications

Office 365 allows users to grant 3rd party applications permission to access their e-mail and send e-mails on their behalf. Attackers often create malicious applications to gain access to user mailboxes. Please review this list of uncommon applications in your tenant that have access to user e-mails and see if any aren’t expected.

Name	Publisher	Permissions	Granted For	URLs
Email	Test	EWS.AccessAsUser.All	jstuckey@contoso.com	https://localhost
Dialpad	Dialpad, Inc	Mail.Read	Entire Organization	https://dialpad.com https://dialpadbeta.com
production-nimble	Unknown	Mail.ReadWrite Mail.Send	lgrissom@contoso.com pcooper@contoso.com sramsay@contoso.com	https://app.nimble.com/

E-mails From Suspicious Domains

Attackers will often register domain names that look visually similar to domains that you own in order to trick your users. Please review this list of domains that your users have received e-mails from in the last 90 days that look similar to yours and see if any aren't expected. A message trace can be performed in Office 365 to get more details.

Original Domain	Suspicious Domain	Type	Messages Received
contoso.com	contaso.com	Vowel swap	14
fabrikam.com	fabrkam.com	Omission	2

Questions? Contact us