Hi All

Thank you for sending through the Office 365 audit logs as requested. From an initial analysis, we were able to identify the following.

Findings and Chain of Event Summary

i. On the 25/06/2020, eight attempted suspicious unsuccessful login attempts were identified in trying to gain access to the system. Based on the source IP information in the audit logs, the activity was confined to two distinct IP addresses resolving out of Lagos, Nigeria

   a) 193.238.28.55 – Nigeria Mtn Nigeria Communication Limited

   b) 168.253.114.9 – Nigeria Lagos Ngcom

ii. On the 26/06/2020 and 27/06/2020, two successful login attempts were made from 168.253.114.9. No further activity was recorded on these days besides the login activity.

iii. On the 28/06/2020, a suspicious login was recorded at approximately 4.30am from 193.238.28.55.

iv. Following on from this successful login, 13 minutes later at 4.43am a bulk email was sent to the ExecCo mailboxes. As was highlighted in the Office 365 audit and risk logs. Seen below.

Operations	ClientIP	AuditData
BulkMailOut	193.238.28.55	{ "Name": "BulkMail", "OrganizationId": "240445d8-adfd-4029-b8f3-2afa6dca780a", "UserId": "Hacky.McHackFace@domain.com", "ClientIPAddress": "193.238.28.55", "LogonUserSid": "S-1-5-21-3151364413-2125736233-906098302-10958315", "MailboxGuid": "953a9063-ac26-47a3-9272-eac4b8a7fbc0", "Activity": Send to ExecCoMailboxes "MailboxOwnerSid": "S-1-5-21-3151364413-2125736233-906098302-10958315", "MailboxOwnerUPN": "Hacky.McHackFace@domain.com" }

v. One minute following the bulk mail out identified above at 4.44am, an effort was made to cover the tracks of the threat actors activities by moving all recently sent items to the RSS feeds of the victim mailbox. This was also seen in the Office 365 audit and risk logs.

In summary, there were 11 total login attempts made from IPs resolving in Lagos, Nigeria (8 Unsuccessful, 3 Successful). It was evident from the activity on the 28/06/2020 that the threat actor successfully gained access, navigated and created rules in the victims mailbox in an attempt to gain further access to the ExecCo mailboxes by sending further phishing emails.

Operations	ClientIP	AuditData
MailMove	193.238.28.55	{ "Name": "MailMove", "OrganizationId": "240445d8-adfd-4029-b8f3-2afa6dca780a", "UserId": "Hacky.McHackFace@domain.com", "ClientIPAddress": "193.238.28.55", "LogonUserSid": "S-1-5-21-3151364413-2125736233-906098302-10958315", "MailboxGuid": "953a9063-ac26-47a3-9272-eac4b8a7fbc0","Acitivty":"Move recently sent to RSS Feeds" "MailboxOwnerSid": "S-1-5-21-3151364413-2125736233-906098302-10958315", "MailboxOwnerUPN": "Hacky.McHackFace@domain.com" }