Phishing Incident Response Process:

9/19/2017

ADS – Spam Administrator (Exchange Administrators, ADS - Service Desk Information and DII – Information Security) receives notification from user of a malicious email. The notification is received as a result of the directions that are found on the ADS website.

a. A member from one of the groups notified will go to PaloAlto Test A Site and reclassify the site if needed. https://urlfiltering.paloaltonetworks.com/TestASite.jsp

b. Exchange Admins alert the Service Desk that a notification needs to be sent out.

c. Service Desk sends phishing warning email with spam/phishing reporting instructions including a screen shot of the email to the ADS – Spam and Phishing Notifications distribution list; ensuring there are not active links in the example before sending out.

If it is suspected that a user fell for the phishing scam (clicked link, opened attachment), the Service Desk resets user's password, forces a password change, and has the user disconnect completely from the network until Desktop Solutions contacts them and instructs otherwise.

a) A member from one of the groups notified will go to PaloAlto Test A Site and reclassify the site if needed. https://urlfiltering.paloaltonetworks.com/TestASite.jsp

b) If a user contacts the Service Desk and is from a domain that ADS does not support, (ADS Support and Services.xls) The Service Desk will tell the users to contact their IT. (Foreign Domains should weigh in here). This includes contact via telephone, email, or ticket.

c) If the user is from a ADS supported domain - Service Desk will create a critical ticket and assign to EAS, adding ADS – Spam Administrator as a cc. The ticket needs to contain the machine name, IP address, and the time frame of the event.

d) The responsible AD administrators will then disable the users account and reset the password.

e) The responsible department's Desktop team then scans the user's PC for malware.

f) If no malware is found, then Security will perform network forensics. Security will then reassign the task back to Desktop Solutions with updated IoCs or to EAS for closing.

g) After all malware has been removed, the user's account can be enabled and the user notified.