Recent Local Spearphishing Attacks

Posted At : March 28, 2019 9:16 AM | Posted By : Admin
Related Categories: Security

Over the recent week, Cornell and other companies and organizations have been hit with several spearphishing attacks. As you might expect, Cornell is a constant target for nefarious attacks (as are most large institutions), however this one has hit a large number of "Cornell.edu" email accounts. And over the last 24 hours, we've been made aware of several other attacks as well.

What makes this attack particularly challenging, is that the Sender and Subject appear to be legitimate.

However, once the email is opened the content reads something like:

READ THIS MESSAGE (in a clickable banner)

05:59:47 (Cornell)
Re: "Subject"
Watch before: Thursday

If you clicked on the banner, you are taken to a page with a legitimate company logo - the one we looked at (safely) had the Xerox Logo with lines requesting our Xerox Login Name and Password.

IF YOU OPEN THIS EMAIL, DO NOT CLICK ON THE BANNER AND ABSOLUTELY DO NOT FILL IN ANY LOGIN OR PASSWORD INFORMATION!

Cornell has an excellent page on its site discussing this and other phishing attacks and how to recognize them: **https://it.cornell.edu/phish-bowl**

When we first saw this attack, we notified the "sender" who happens to be a long-time Computing Center client and friend. Cornell had already discovered the spam acitivity, notified him, and changed/scrambled his Cornell Outlook 365 email password. After some discussion, we decided to have him run a full antivirus and antiMalware scan on his computer. Those scans appear to be clean. He then changed his Cornell password and also changed the other sites where the same password was used.(We all know that using the same password on multiple sites is a bad idea, but it does happen.)

Additional information on Spearphishing

A lot of Office 365 customers (especially universities, but also corporate accounts) have been aggressively targeted by spearphishing attacks with the intent to compromise one or more O365 accounts and then use the compromised accounts for either spam relay or additional spearphishing to ‘trusted’ people. In a few cases, specific individuals in key departments such as Finance, HR or Administration (CEO/CFO/COO) have been explicitly targeted for attempted fraud where financial transaction requests to partners were forged. These forged e-mails were often based off of previous legitimate transactions, but an unauthorized offshore account was specified for the payment destination instead; because of the resemblance to existing correspondence, these can be highly effective and difficult to secure against. O365/Outlook rules were commonly set up by the attacker to help obscure these attacks by diverting relevant (or all) messages away from the Inbox and Sent Items.

Microsoft strongly recommends use of 2-factor/Multi-factor authentication for Office 365; this greatly reduces the effectiveness of account compromise through spearphishing attacks or other methods of gaining a user's password (easily guessed, reused from other compromised accounts/sites, other social engineering, etc.)