LOGIX ACADEMY

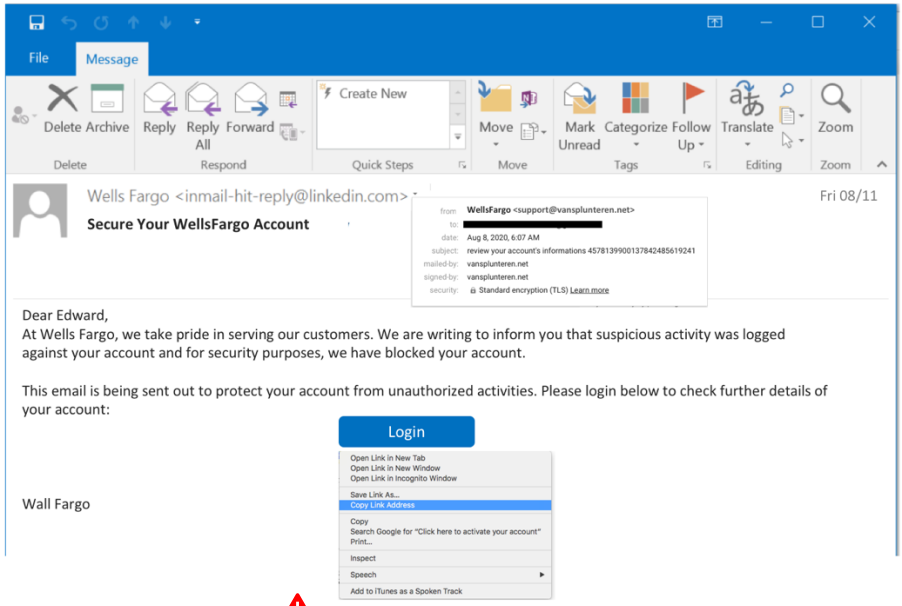
Lab: Investigating Phishing Incident

Note: URLs in this lab should only be used as input to the tools specified. Do Not open the links in a browser!

Purpose

In this lab, we are going to investigate a phishing email and carry out the following activities:

1. Check whether URL in the email is malicious
2. Check whether the file attachment in the email is malicious
3. Check reputation of the sender domain



URL: http://russellvillea.buzz/1/2/3
Sender: support@vansplunteren.net

Please do not open phishing links directly in the browser. For safety, you must manually type the URL in the security tools.

1. Check If URLs Are Malicious

Engine	Result
Zulu ZScaler (https://zulu.zscaler.com)	Malicious
Virus Total (https://www.virustotal.com)	Malicious

2. Check If Attachments Are Malicious

Engine	Result
MD5Hash (https://md5file.com/calculator)	Not Malicious
Virus Total (https://www.virustotal.com)	Not Malicious

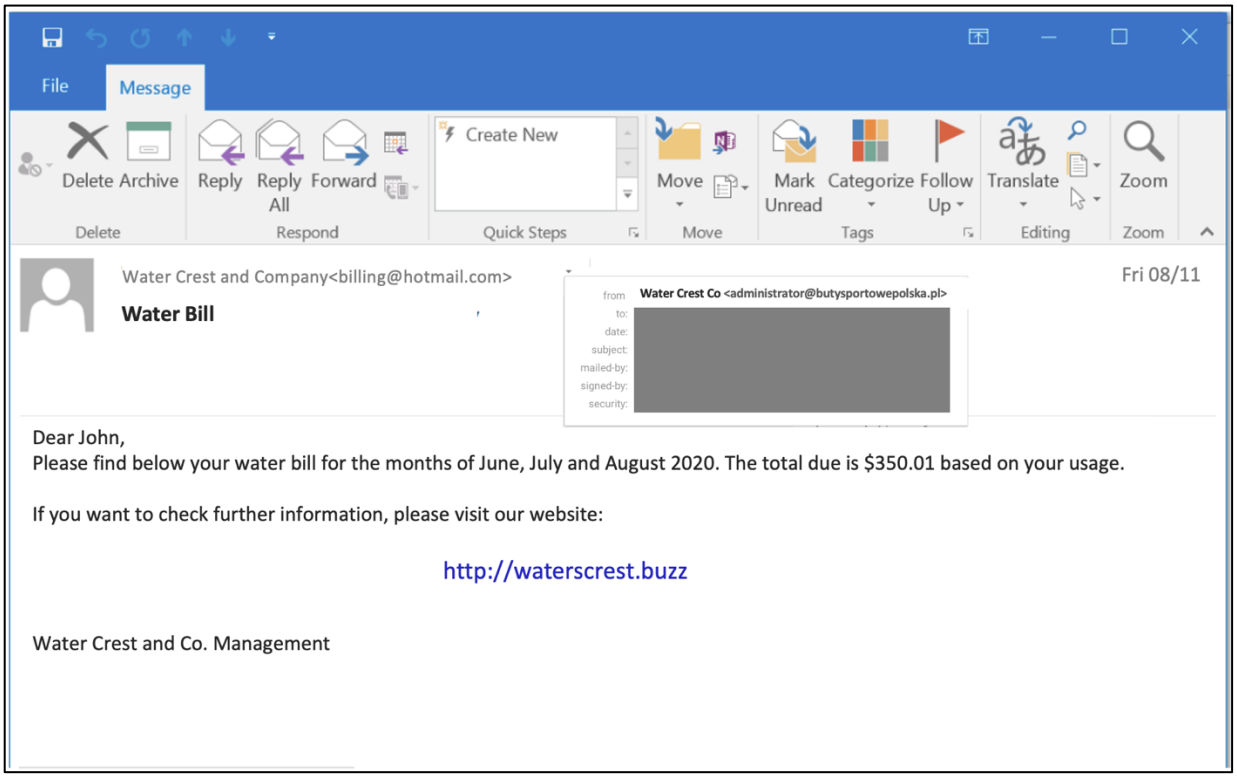
3. Check Reputation of Sending Domain

Engine	Result
CISCO Talos Intelligence (https://talosintelligence.com)	

LOGIX ACADEMY

Task

You have received a suspected phishing email with the information below:



URL: http://waterscrest.buzz
Sender: administrator@butysportowepolska.pl

⚠ Please do not open phishing links directly in the browser. For safety, you must manually type the URL in the security tools.

File Hash (MD5): `31cf9a5d5b8347bdb8c22b2a93ddc1f5`

Complete the incident investigation and decide whether:

A. It is a phishing email or not?
B. Is the file malicious (based on the given hash)?
C. Is the sending domain reputable?

(Solution on Next Page)

LOGIX ACADEMY

Solution

Complete the incident investigation and decide whether:

A. It is a phishing email or not? URL http://waterscrest.buzz is definitely malicious
B. Is the file malicious (based on the given hash)? No
C. Is the sending domain reputable? Not flagged as malicious