Phishing Scenario #5

On November 25, 2013 at 8:05 AM we sent out our fifth phishing simulation from phishme.com. This was a two-day week for EMU employees as it was the week of Thanksgiving. We sent out 952 emails to emich.edu mailboxes. Of those recipients, only 2 provided a password when prompted.

The Phishing Email

From: <security@emich.edu>
Subject: Important: Virus Outbreak

IMPORTANT - VIRUS OUTBREAK

The recent spike in traffic on our internal network was successfully correlated to a computer virus outbreak. We have taken several measures to limit the impact of the virus on our information systems and cure those affected by it. However, we require your cooperation to confirm eradication of the virus.

Please perform a quick virus check against your machine to ensure that it is not affected by the W32.Amirecivel.C virus by clicking here, at your earliest convenience.

NOTE: This virus will not be detected by your desktop anti-virus as there is no comprehensive detection signature for it

For more information about this virus please refer to:
http://securityresponse.symantec.com/avcenter/venc/data/w32.amirecivel.c.html#technicaldetails

Thank you once again for your cooperation.

Information Security
Eastern Michigan University

The Landing Page

The Virus Control Center

Important Notice!

The corporate network was recently affected by an outbreak of the W32.Amirecivel.C worm. The information security group has taken several measures to ensure a limited impact on critical information systems and to fix the affected computers. To confirm eradication we need to locally run a virus check against each computer.

To assist in this process please do the following:

- Click **Start** -> **Search** -> **For Files or Folders...**
- In the **Look In** textbox type **c:winnt or c:Windows**
- Enter ***.pic.bat** in the text box labeled **Search for Files or Folders Named**
- Click **Search Now**
- If Windows detects any files that match this search criteria please notify Information Security.

You must also authorize Information Security to scan your computer for remnants of the worm by entering your information below.

I authorize the Information Security group to perform a scan of my computer to ensure that it is not affected by the W32.Amirecivel.C virus.

Username:

Password: ••••••••••••

Submit

What is the W32.Amirecivel.C worm?

W32.Amirecival.C is a worm that attempts to spread via the Kazaa file-sharing network and hides security related windows and infects other .exe files. It has a HIGH potential for disrupting the normal operations of affected Windows 2000, Windows 2003, and Windows XP systems by altering key registry and configuration file settings.

For more information please refer to:

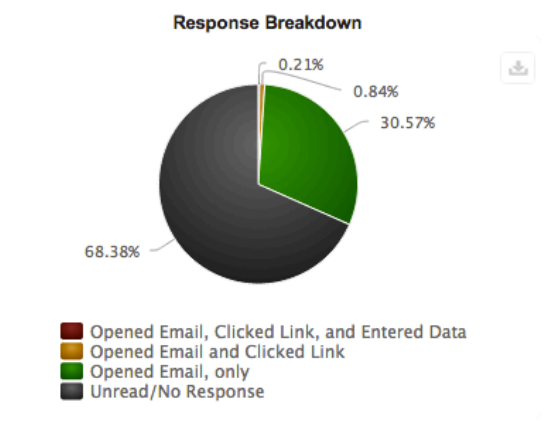
http://securityresponse.symantec.com/avcenter/venc/data/w32.amirecivel.c.html#technicaldetails

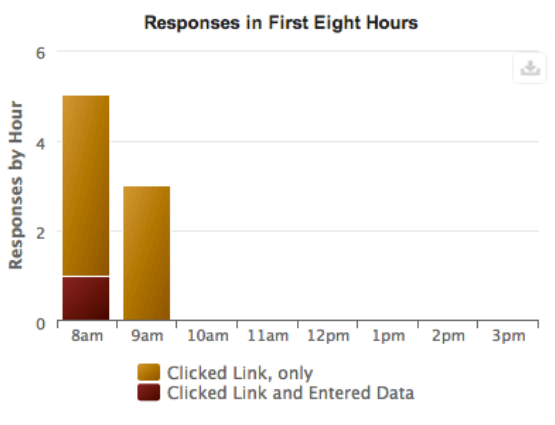
The Education Page

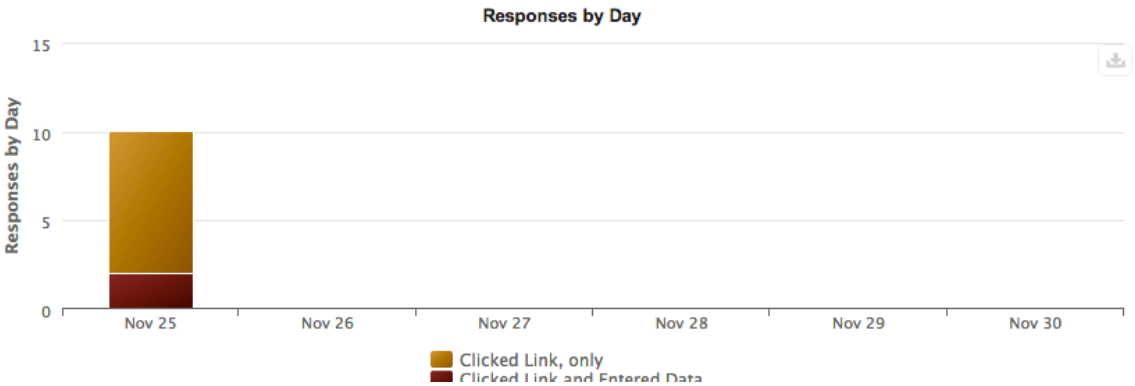
How it Works

When the recipient opens the email they are enticed to click on the link provided, in this case “clicking here” This link would have actually brought them to the landing page at “http://emich.virus-control.com/” where they would be asked for their username and password. If they submitted the form they would have been redirected to the education page.

The results







- Of the individuals emailed **291** opened the message in a way we can track, only **10** clicked on the link, and only **2** of those entered a username and password.
    - This is **47** fewer views, **48** fewer clicks, and **33** fewer entered passwords than last moth.
- **122** recipients used the Zimbra 

button to report these messages as Spam. About **30** fewer than normal.
    - The first 25 individuals to use the Spam button were rewarded with a security awareness month T-Shirt.
- One of the individuals who entered a password viewed the education video the other did not.
- Both individuals who entered a password a repeat offenders.
    - They each entered their password in one previous phishing scenario.

Conclusion

It seems that because of vacation week we received a reduced number of results in each category. We will use this knowledge to schedule future scenarios more effectively.