In this week we studied about message security, but in specific email message security. Per Symantec’s 2017 Internet Security Threat Report (Volume 22), Symantec witnessed a resurgence of email as the favored attack channel. One in every 131 emails sent were malicious, the highest rate they’ve witnessed in 5 years.

Furthermore, the availability of spam botnets-for-hire , such as Necurs, allowed ransomware groups to mount massive email campaigns during 2016. It’s believed spear-phishing emails were used in the DNC attacks of 2016.

Below are some statistics found within the Symantec 2017 ISTR.

Below is a link where you can download the 2017 Symantec ISTR:

<https://www.symantec.com/security-center/threat-report>

A growing trend in email phishing is the Business email compromise fraud, most commonly known as BEC. Per the FBI’s public service announcement in May 2017, BEC is defined as a sophisticated scam targeting businesses working with foreign suppliers and/or businesses that regularly perform wire transfer payments. In total, the scam has accounted for more than $5 billion dollars lost by victims of the scam. Between January 2015 and December 2016, there was a 2,370% increase in identified exposed losses.

Below is a link to the FBI’s PSA:

<https://www.ic3.gov/media/2017/170504.aspx>

Furthermore, the attackers are target specific industries known to operate/conduct financial transactions via wire transfers. In specific, certified public accountants, lawyers/law firms, and real estate firms. They will initiate transfer while impersonating a high ranking officer of the firm and funds are intended to arrive to a mule account. If the wire transfer is completed the client is fully liable since the transactions was initiated by the authorized signer’s of the accounts.

However, there security researchers have found effective way’s for filtering out spam emails. Per this week’s lectures there are two known tools for detecting spam.

1. Reputation driven information tools
2. Content driven information tools

Also, in recent years there have been the development of various authentication methods for emails. In example:

* Sender Policy Framework (SPF) which is a simple email-validation system designed to detect email spoofing by providing a mechanism to allow receiving mail exchangers to check that incoming mail from a domain comes from a host authorized by that domain’s administrators. The list of authorized sending hosts for a domain is published in the DNS records for that domain in the form of a specially formatted TXT record.
* Domain Keys Identified Mail (DKIM) which is an email authentication method designed to detect email spoofing. DKIM let’s a domain associate it’s name with an email message by affixing a digital signature to it. Verification is carried out using the signer’s public key published in the DNS. A valid signature guarantees that some parts of the email (possibly including attachments) have not been modified since the signature was affixed.
* Domain Based Message Authentication Reporting and Conformance (DMARC) is an email-validation system designed and intended to combat certain techniques used in phishing and email spam, such as emails with forged sender addresses that appear to originate from legitimate organizations. DMARC is built on top of SPF and DKIM .

Overall,