IBM Security

Protection against email-borne attacks

IBM Australia whitepaper - Vijayalakshmi Adluru

IBM

Executive summary

This paper starts with the highlights of recent cyber-attack threats and exploitation techniques, with a focus on one of the weakest channels of attack – e-mail. Then we share some of the best practice recommendations to help reduce malware infections from cyber-attacks and discuss some of the advanced security features in Email Security Products that can help protect organisations from email-borne attacks.

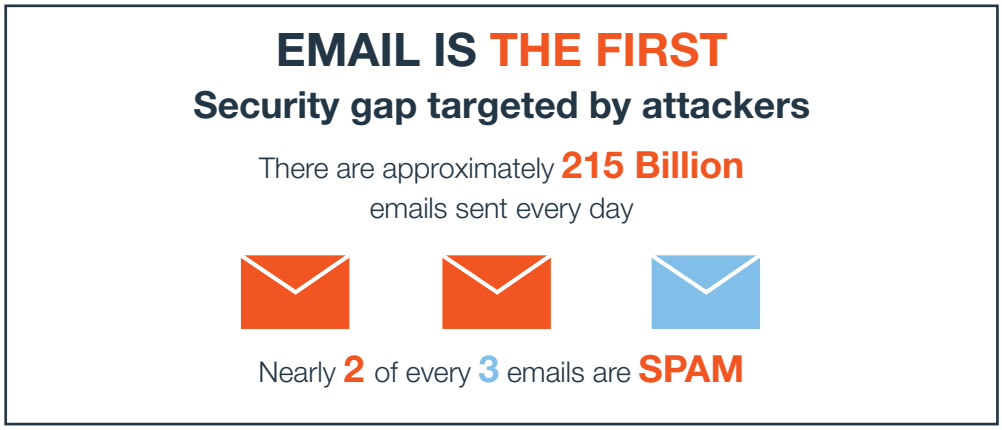

Figure 1: *FireEye Infographic[1] (Source: FireEye)*

Cyber Security Incident Highlights

- Losses from Business Email Compromise Scams Top $3 Billion. Losses went up by 1,300% since Jan 2015 – https://www.fbi.gov/news/stories/business-e-mail-compromise-on-the-rise
- According to https://www.ibm.com/security/xforce/xfisi/, a spear phishing attack on bank employees which led to hacked ATM's, an international crime ring targeted banks to steal money in 14 European countries (Aug 2016).
- The FBI estimates that ransomware will net criminals $1 billion in 2016 – http://money.cnn.com/2016/04/15/technology/ransomware-cyber-security/index.html
- JavaScript attachments led to an explosion of malicious message volume, 230% quarter over quarter – https://www.proofpoint.com/us/threat-insight/post/what-spring-proofpoint-q2-threat-summary-tracks-ransomware-exploit-kits-and-more
- 98% of Microsoft Office-targeted threats use macros – https://blogs.technet.microsoft.com/mmpc/2016/03/22/new-feature-in-office-2016-can-block-macros-and-help-prevent-infection/?platform=hootsuite, 2016
- Malicious WSF files have been used in a number of recent major spam campaigns spreading Locky (Ransomware). Symantec blocked more than 1.3 million emails with an attachment that consisted of a WSF file within a .zip archive between October 3-4 2016 – https://www.symantec.com/connect/blogs/surge-email-attacks-using-malicious-wsf-attachments
- According to Proofpoint, 600%+ increase in attachment-based vs. URL delivered malware attacks from mid-2014 to 2015 – https://www.clearswift.com/blog/2016/05/24/10-shocking-malware-and-ransomware-statistics, 2016

- Whaling attack in January which cost FACC $56 million, the company has sacked both its CFO and CEO – https://www.scmagazineuk.com/ceo-sacked-after-aircraft-company-grounded-by-whaling-attack/article/530984/
- https://www.cnet.com/au/news/wannacry-wannacrypt-uiwix-ransomware-everything-you-need-to-know/, a massive ransomware attack has hit more than 150 countries and 200,000 computers, shutting down hospitals, universities, warehouses and banks.

Email-borne attacks

Current security trends and attacks suggest that **email** is the one of the most common channels used to spread malware and intrude into an organisation's network.

Spear phishing[2], a targeted form of Phishing attack, is one of the most popular exploitation techniques used. Spear Phishing emails contain malicious attachment or a URL which links to malicious code. Although most organisations have anti-spam and antivirus solutions, they may not be able to completely block spear phishing emails. Detection of spear phishing emails, since these emails are often sent only to a small group of targeted email accounts rather than a mass-mailer, can be difficult. Such emails can also be carefully crafted to look legitimate.

Ransomware emails spiked in 2016 with 6000% increase compared to 2015 and most victims paid the attackers, according to an **IBM Study**[3]. Ransomware is a type of malware that encrypts a victim's data and demands a ransom be paid to obtain the key required to decrypt it. Attached files such as JavaScript, VBScript, Office files with macros and WSF file types are known to have been used in the Ransomware emails.[4]

Threat actors target unsuspecting victims during seasonal times like Tax filling, Black Friday, using the cover of enticing offers. Some of the other malicious email campaigns are government notice scams, bank fraud emails, CEO email scams, parcel/order delivery, invoice, billing, payment receipts, shipping related emails and traffic infringement notices.[5]

How do Email attacks work?

The attacker gathers the intelligence about an individual or the target organisation. Then a personalised email is sent to the victim with a link or attachment from a spoofed sender email address.[6]

The sender address and the email content lures the victim to open the email attachment. The malware code in the attachment infects the system and opens a backdoor to the attacker. The Attacker may then be able to access or transfer confidential data. The malware typically hides its presence in the system. With the unauthorised access the attacker can exfiltrate data. This may occur through an encrypted channel to avoid detection.

These malicious email campaigns can be created to avoid traditional spam filter detection as the email content, subject, attachment name, URL and sender address/domain differ with each email.

Challenges

Malicious Email Attachments

Many organisations have already deployed solutions or rules to block specific malicious file types like executables or script files to prevent malware infection. According to Proofpoint Threat Report 2016[7] *[Refer Fig 2: Malicious Email volume by attack type – Proofpoint 2016],* recent attack trends show a significant increase in the number of attacks using attachment types like office documents, PDF, ZIP, RAR and RTF files which are used by the business and hence difficult to block based on file type. Also the attachment file names, sender address/domain, email subject often change with every email making it hard for traditional spam filtering solutions to block it.

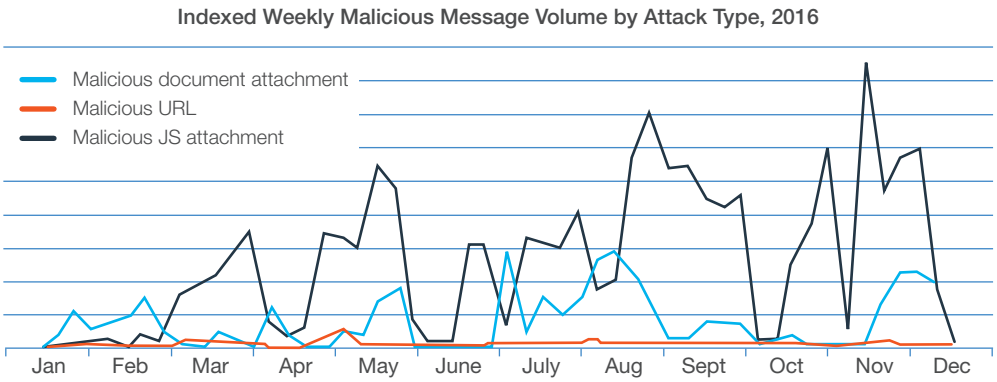

Figure 2: *Malicious Email volume by attack type –2016[8] (Source: Proofpoint)*

Malicious URLs in Email

The dynamic nature of the threat email campaigns makes it harder to be identified or blocked by a traditional Email Security solution. A URL in an email is scanned by the Gateway systems or verified against its URL database to mark it as clean or malicious URL. A URL that is classified under a safe category now may later be infected and used to spread malware. Also, a safe URL can potentially redirect to a malicious URL when a victim clicks on the link in the email. Another challenge is that attackers may keep changing the web domain and URL links, so blocking a particular URL today may not protect your organisation from future attacks.[9]

Recommendation

Organisations should consider advanced Email Security Solutions which have the following capabilities to address the targeted, dynamic nature of cyber-attacks and zero-day threats:

Global Threat Intelligence – It collects and redistributes real-time threat intelligence across web, email, file, and endpoint products. This information helps to block unknown malicious files/ URLs in real-time. The Sender IP and file reputation information provided by a Threat intelligence solution helps block more sophisticated attacks.

URL Filtering and Categorisation – The content and embedded links in the URL are scanned and assigned a category in the URL Master database, which is a static category. A secure shopping category website may be injected with a malware link, so the system should perform a real-time content and security analysis aside from matching it across the URL database's static

classification. There is potential for a delayed malware infection scenario where a non-malicious URL is included in an email which was scanned by the Gateway system and allowed through as safe. Later, malware may be dropped into the destination webpage. If the user clicks on the link, malware may be downloaded. To help address this issue, an additional Time-of-Click protection is available with some products which can scan the URL when a user clicks the link from the email.[10]

Sandboxing- is a dynamic / behavioural analysis technique which uses an isolated virtual environment to analyse the attached file or URL in the email.[11] The file or URL is accessed or executed in the sandbox environment to monitor any suspicious behavior. A file or URL is blocked if any suspicious actions like contact to command and control servers, dropping files, modifying registry keys and system changes are observed. This can be an effective technique in helping to block zero-day attacks.

Block malicious file type attachments - As many of the recent cyber-attacks have used attachment based emails as a means to send malware according to the Bit Defender Q1 2016 report, we recommend blocking these malicious files types at the Gateway. To decide which file types to block, we should consider any file types that can contain malicious code, script or can execute commands. *[Refer - Fig 3: Percentage of File types attached to spam emails - on the following page].*

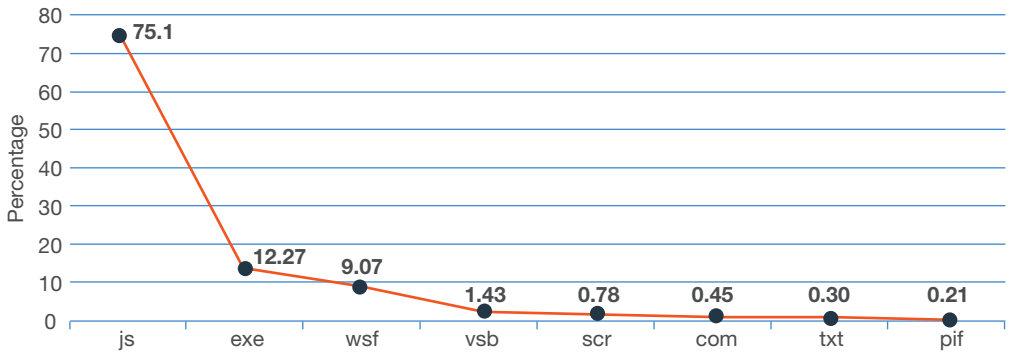

Figure 3: *Percentage of File types attached to spam emails – Q1 2016[12]*
(Source: Bit Defender)

Scanning emails to detect threats, filtering malicious files and disabling macros along with patching the vulnerabilities could be the best prevention against ransomware attack including the latest Wannacry ransomware.[13]

The Email Security solution should be able to block potentially dangerous files based on the file types and not based on file extensions[14], the difference is file extension can be modified. For example, file.exe can be renamed as file.txt. The system should be capable of scanning the content within a compressed file as malicious files are often embedded inside a compressed file. Attackers spread malicious code through macros which is used to automate routine tasks, resulting in potential impacts such as unauthorised access to sensitive information.

This is not an extensive list but just a baseline we recommend starting with. Which attachment types are to be blocked depends on each organisation's requirements.

Quarantining emails, rather than blocking them, allows the emails to be further analysed and to cross reference parameters such as the sender of the email, content or email pattern. By quarantining emails with suspicious file attachments, they can be released later if they are determined to be safe.

Malicious File Types to Block[15]

.EXE – An executable program file.
.PIF – A program information file for MS-DOS programs.
.DLL – Microsoft binary libraries
.APPLICATION – An application installer deployed with Microsoft's ClickOnce technology.
.GADGET – A gadget file for the Windows desktop gadget technology introduced in Windows Vista.
.MSI – A Microsoft installer file.
.MSP – A Windows installer patch file.
.PRG – Program file
.COM – The original type of program used by MS-DOS.
.SCR – A Windows screen saver. Windows screen savers can contain executable code.
.HTA – An HTML application.
.CPL – A Control Panel file. All of the utilities found in the Windows Control Panel are .CPL files.
.MSC – A Microsoft Management Console file. Applications such as the group policy editor and disk management tool are .MSC files.
.JAR – .JAR files contain executable Java code.

Scripts

.BAT – A batch file.
.CMD – A batch file.
.VB, .VBS – A VBScript file. Will execute its included VBScript code if you run it.
.VBE – An encrypted VBScript file.
.JS – A JavaScript file.
.JSE – An encrypted JavaScript file.
.WS, .WSF – A Windows Script file.
.WSC, .WSH – Windows Script Component and Windows Script Host control files.
.PS1, .PS1XML, .PS2, .PS2XML, .PSC1, .PSC2 – A Windows PowerShell script.
.KSH – UNIX Shell Script

Shortcuts

.SCF – A Windows Explorer command file.
.LNK – A link to a program on your computer. A link file could potentially contain command-line attributes that do dangerous things, such as deleting files without asking.
.INF – A text file used by AutoRun. If run, this file could potentially launch dangerous applications it came with or pass dangerous options to programs included with Windows.

Other

.REG – A Windows registry file. .REG files contain a list of registry entries that will be added or removed if you run them. A malicious .REG file could remove important information from your registry, replace it with junk data, or add malicious data.

Office Macros

.DOCM, .DOTM, .XLSM, .XLTM, .XLAM, .PPTM, .POTM, .PPAM, .PPSM, .SLDM – New file extensions introduced in Office 2007. The M at the end of the file extension indicates that the document contains Macros.

Email Gateway Products

Email security products offer **on-premise** appliances or **cloud-based** email filtering. In regard to the malware threats over email, the cloud based solutions filter malicious files in the cloud, before they enter an organisation's network.

The Features of a number of vendor products as advertised online are set out in the below table to serve as a guide to help organisations to choose an Email Security Product that best suits their requirements and environment.

Product Vendor	Features
Forcepoint	• Forcepoint offers private cloud, on-premise and hybrid deployment options. • The messaging security product provides various features likes signatureless anti-spam/anti-phishing, data loss prevention, encryption, phishing education, image analysis, sandboxing and adopt to cloud technologies such as Microsoft Office 365. • Real-time threat intelligence from the Forcepoint ThreatSeeker Intelligence Cloud, real-time identification and classification of threats using Forcepoint ACE (Advances Classification Engine) https://www.forcepoint.com/product/cloud-security/forcepoint-email-security
FireEye	• The FireEye Email Threat Prevention (ETP) is a cloud email security solution that filters emails for spam and known viruses first. It then uses the signature-less FireEye Multi-vector Virtual Execution (MVX) engine to analyse every attachment and URL to detect threats and stop APT attacks in real time. • Offers on-premise, cloud and hybrid deployment options. • Analyses emails for threats, such as zero-day exploits, attacks hidden in ZIP/RAR/TNEF archives, and malicious URLs. https://www.fireeye.com/products/ex-email-security-products.html
Trend Micro	• Trend Micro provides spear phishing email detection with Trend Micro Social Engineering Attack Protection, protection for Business Email Compromise (BEC). • Web reputation analysis for URLs, email reputation check for email from spam sources, time-of-click protection against malicious URLs in email messages and advanced threat protection with sandbox malware analysis https://www.trendmicro.com/en_us/business/products/user-protection/sps/email-and-collaboration.html
Fortinet	• FortiMail provides antispam, anti-phishing, anti-malware, sandboxing, data loss prevention (DLP), encryption, and message archiving. • Available as hardware, virtual appliance, cloud-based service. https://www.fortinet.com/products/email-security.html

Product Vendor	Features
Symantec	• Symantec Cynic sandboxing leverages advanced machine learning-based analysis combined with Symantec's global intelligence to detect stealthy and persistent threats. • Symantec Click-Time URL protection and Real-Time Link following to protect against spear phishing and other advances threats. • Easily export the threat intelligence on malicious emails to your Security Operations Centre through integration with third-party SIEMs https://www.symantec.com/products/messaging-security
Cisco	• Cisco Advanced Malware Protection for Email Security defends against spear phishing, ransomware and other sophisticated attacks. Advanced sandboxing capabilities perform static and dynamic malware analysis of unknown files. • Cisco Email Security provides 4 deployment options – cloud, hybrid, virtual, on-premise. • If malicious behaviour is spotted later, AMP sends you a retrospective alert to contain and remediate the malware. http://www.cisco.com/c/en/us/products/security/email-security/index.html
Proofpoint	• Proofpoint's email protection product features include Dynamic classification and control of email across spam, phishing, impostor, bulk, adult and malware. • Proofpoint provides protection against Business Email Compromise (BEC) and business continuity capabilities keep email communications flowing, even when your email server fails. https://www.proofpoint.com/us/products/email-protection
Barracuda	• Barracuda offers features including Spam Protection, Virus Protection, Archiving, Malware Protection, Link Protection and Typo squatting, Data Leak Prevention, Anti-Phishing Protection, Advanced Threat Detection, Email Spooling. • Barracuda provides a unique feature to protect against denial-of-service attack. https://www.barracuda.com/products/emailsecuritygateway
Sophos	• Sophos secure email gateway offers antivirus and phishing detection technology, sandbox technology, DLP, Encryption, advanced protection by blocking emails containing suspicious content, attachments or URLs, also block unwanted content using MIME type and extension filters. • Sophos Time-of-Click protection blocks malicious email URLs to protect against stealthy, delayed, spear phishing attacks. https://www.sophos.com/en-us/products/secure-email-gateway.aspx

Product Vendor	Features
Mimecast	• Mimecast offers Anti-spam and anti-virus protection, data leak prevention, URL re-writing, impersonation protection, malware blocking, internal monitoring, sandboxing, encryption and graymail control for email. • Large File Send offers a quick and easy way to Send and receive large file attachments from within email, but that are greater than traditional size limits. • In addition to email security, Mimecast provides technology for email continuity and for archiving email. https://www.mimecast.com/products/email-security/
Dell SonicWALL	• Dell SonicWALL Email Security provides Antispam filter, multi-layer antivirus protection, reputation checks including sender IP reputation, reputation of content, structure, links, images, attachments and real time threat information from the SonicWall GRID Network. • The technology also provides directory harvest attack (DHA) protection, Denial of Service (DoS) protection and sender validation. Outbound email scanning safeguards organisation reputation by scanning for — and blocking — traffic from zombies, unauthorised senders and email containing malicious viruses. http://www.sonicwall.com/en-us/products/secure-email
Retarus	• Retarus E-mail Security provides anti-spam filters, multi-level virus protection and gateway-based encryption. • Retarus supports the exporting of any archived emails, which provides business continuity in case your email system fails or messages are eliminated after deleting employee email accounts by the time they leave the company. https://www.retarus.com/us/services/email/

Conclusion

The impact of a cyber-attack can involve financial loss, reputational damage, legal implications and cost of remediation.[16] An organisation should consider investing in an Email Security solution that can combat advanced threats.

An Email Security solution should be a first line of defence blocking unwanted and malicious emails through anti-spam/anti-virus filtering and advanced level of protection through threat intelligence and sandboxing technology combined with file and URL analysis.

Footnotes

1 https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/email/fireeye-infographic-spear-phishing.pdf

2 https://acsc.gov.au/publications/ACSC_Threat_Report_2016.pdf

3 https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=WGL03135USEN&

4 http://blog.trendmicro.com/trendlabs-security-intelligence/rar-javascript-ransomware-figures-fluctuations-email-attachments/

5 http://www.news.com.au/finance/money/tax/watch-out-for-these-tax-time-scams/news-story/6f48e0df0a896a61caee9fe0df253f5f, https://auspost.com.au/about-us/about-our-site/online-security-scams-fraud/scam-alerts, http://www.news.com.au/technology/online/security/police-issue-warning-about-fake-delivery-emails-over-christmas/news-story/fda0b2be827a22ff009adb49e751d575, http://www.heraldsun.com.au/news/australians-falling-victim-to-fake-agl-energy-bills-in-virus-scam/news-story/ad09cda6f1b3c995fe46bfa317453991, http://asic.gov.au/about-asic/media-centre/find-a-media-release/2017-releases/17-005mr-asic-warns-customers-about-scam-emails/, http://www.mailguard.com.au/blog/fake-driving-infringement-notice-floods-inboxes

6 https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/spear-phishing-101-what-is-spear-phishing

7 https://www.proofpoint.com/sites/default/files/q4_threat-summary-final-cm-16217.pdf

8 https://www.proofpoint.com/sites/default/files/q4-fig-1_0.png

9 http://webobjects.cdw.com/webobjects/media/pdf/FireEye/FireEye-email-Cyber-attacks-with-Gartner.pdf

10 https://www.trendmicro.com/en_au/business/products/user-protection/sps/email-and-collaboration/interscan-messaging.html

11 https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/email/rpt-frost-sullivan-advanced-malware-sandbox.pdf

12 http://download.bitdefender.com/resources/files/News/CaseStudies/study/104/Bitdefender-2016-Spam-A4-04-en-EN-screen.pdf

13 https://www.us-cert.gov/ncas/alerts/TA17-132A

14 https://www.asd.gov.au/publications/protect/malicious_email_mitigation.htm

15 https://www.howtogeek.com/137270/50-file-extensions-that-are-potentially-dangerous-on-windows/, http://support.proofpointessentials.com/index.php?/Knowledgebase/Article/View/179/7/essentials-filters-file-extensions, http://www.websense.com/content/support/library/email/hosted/admin_guide/av_per_user.aspx, https://support.symantec.com/en_US/article.INFO3768.html

16 https://acsc.gov.au/publications/ACSC_Threat_Report_2016.pdf

Copyright