WHY EMAIL IS SUCH A DANGEROUS ATTACK PLATFORM

(AND HOW TO PROTECT YOURSELF)

ThreatSTOP

Email Attacks

Malicious emails are one of the cyber realm's most widespread epidemics. Over 215 billion business and consumer emails are received daily, and with such an overwhelming flow of emails arises a very attractive opportunity for threat actors to easily penetrate victims' online activity and lure them in to giving up credentials, downloading malware and more. According to the Symantec Internet Threat Security Report, one out of 412 emails contains a malware attack.

Although it seems as though cyber awareness is somewhat increasing due to the attempt to keep up with rapid advances in attack techniques, preying on human error continues to be extremely rewarding for threat actors. In retrospect, many email attack victims are dumbfounded when they realize that the email they so willingly acted upon is quite obviously suspicious upon second look. On top of that are highly thought out, sometimes tailored malicious emails, which do not even alert relatively cyber-aware people.

People tend to assume that recognizing suspicious emails is an easy task, yet on top of the fact that many victims act upon malicious emails without noticing, 58% of emails reported by users as suspicious are actually legitimate, as discovered in a Baraccuda Networks survey. Inadequate identification abilities lead to attacks, fraud and theft on one hand and to false identification, confusion and a waste of time and energy on the other.

In this article, we will outline five common email attack types, and explain how to protect yourself and your organization from these attacks.

Phishing

Email phishing is a form of fraud in which an attacker poses as a legitimate and usually reputable individual or organization, luring victims to perform a target action on a malicious email – whether it's opening a link or attachment, performing a money transfer, or handing over valuable information such as credentials and credit card information. Usually, phishing emails will convey a sense of urgency, inducing victims in to acting quickly and carelessly. After stealing victims' credentials and data, cyber attackers can use them for hacking or sell them to other criminals.

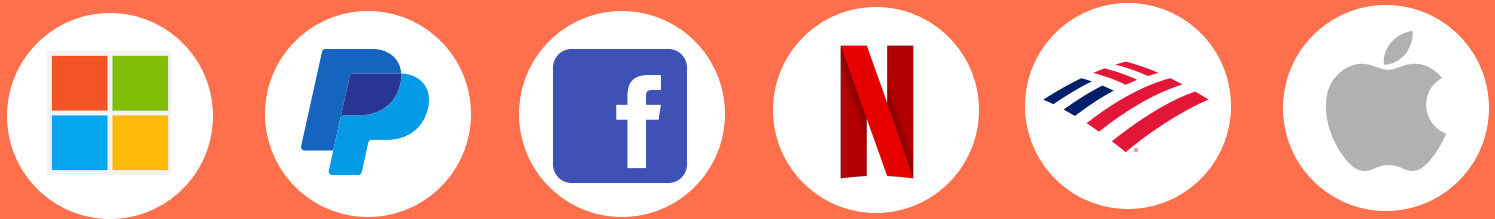
Spear phishing is a type of phishing in which attackers target a specific person or organization, rather than sending out bulk emails. This attack is usually much more convincing, since the perpetrator bases the email on extensive research about the target, including information on company personnel, current projects, and email, text and logo styles. Therefore, spear phishing emails are very hard to recognize, and they can be similar or even identical to a legitimate email sent just the day before.

Business Email Compromise

Possibly the most dangerous of all are spear phishing attacks targeting high profile individuals such as senior executives. These are called Whaling attacks, or Business Email Compromise - an attack that attempts to persuade the victim in to authorizing high-value wire transfers.

Top Brands Abused for Phishing

Threat STOP



Malware and Ransomware

Email is a classic platform for malware and ransomware distribution. Victims caught in a moment of wavering attention or irresponsible curiosity will almost instinctively open an attachment or click on a link the moment it lands in their inbox. Malicious links will oftentimes contain typo squat domains of legitimate, large corporations. Attached files may also have seemingly-legitimate names, but since people do not always use indicative, appropriate file names for their own files, even email attachments with weird-looking names are quite easily opened. Malicious macro abuse in legitimate files can also lead to malware infections. In addition, some attackers try to fool victims by appending a standard file type ending to the name of a malicious executable, causing the victim to think that, for instance, a .exe file is actually a .pdf file (by using a .pdf.exe name ending). In other cases, threat actors will disguise suspicious file types by displaying a different file type icon (continuing the previous example – a .exe file with a PDF viewer icon). Once a victim clicks on the malicious link or attachment, the malware will start infecting their machine.

Common Malicious Email Attachment File Types

Threat STOP

Identity Theft

Gaining access to a victim's accounts and private information may be even more valuable than tricking them in to making a wire transfer. Sometimes, it's just a lot easier. Identity thieves craft well-designed emails posing as online services such as social media platforms, retailers or the victim's bank, persuading the latter to hand over their account information. Gaining access to the victim's accounts allows the attackers to easily commit many types of fraud, such as credit card, bank, tax-related, utilities, loan, or government benefits fraud.

Spam

Bulk, unsolicited emails, also known as spam, are the most commonly known email attack. The only thing amusing about spam emails is their name, which comes from a Monthy Python sketch illustrating how Spam meat is ubiquitous and unavoidable, traits widely associated with spam emails. Spammers collect addresses from various platforms such as chat rooms, websites, customer lists, and newsgroups. Although spam is mostly commercial, cyber attackers are also involved in some spamming activity, oftentimes utilizing botnets they've created by hacking and enslaving unknowing victims' machines. Whether it's malicious or just plain annoying, any form of spam wastes the victim's time and energy, making it worthy of appearing in this list.

How to Protect Yourself

As stated by Kevin Epstein, vice president of threat operations at Proofpoint, “More than 99% of cyberattacks rely on human interaction to work”. Therefore, the first line of defense against email attacks should be a people-oriented security strategy and mindset. Establishing and adhering to companywide cybersecurity policies can greatly reduce the amount of employees that fall victim to these types of attacks. Offering awareness training is also extremely important, as it is crucial that employees possess the ability to identify email threats ahead of time.

Proactive Protection Methods

- Implement email filters that use machine learning and natural language processing to detect suspicious email messages
- Enforce strict password management policies, such as demanding frequent password change and not allowing reuse of passwords for multiple applications
- Block malicious outbound traffic to prevent malware and ransomware from contacting their C&C servers and leaking information
- Use prenotes in payroll management to validate bank accounts prior to transfers
- Use Two Factor Authentication incorporating two methods of identity confirmation

Identifying Suspicious Emails

- Contains misspelled or suspicious URLs
- Email sent from Gmail or other public email address rather than a corporate one
- Content invokes fear or a sense of urgency
- Contains requests to verify personal information, such as financial details or a password
- The message is poorly written and has spelling and grammatical errors
- Contains "too good to be true" offers
- Contains unexpected attachments, especially .exe files
- Use of plain text and logo absence

Email attacks are a prevalent, growing threat. Organizations should make sure that they choose and implement the right security measures to keep their employees safe from these attacks. In addition to awareness and training, using the latest threat intelligence provides protection from countless attacks and malware. ThreatSTOP curates hundreds of sources of intelligence to stop these attacks. To see how ThreatSTOP can protect your organization, sign up for a 14-Day Trial here or request a quick demo.

Threat STOP