LIBRA ESVA
email security virtual appliance

THE GUIDE TO EMAIL THREATS 2018

INCOMMSEC

A user is almost twice as likely to encounter malware through email than they are through exploit kits

A targeted organization has 5.2 BEC emails sent to them in a given month.

Approximately 8,000 businesses each month are targeted by BEC scams.

1 in 9 email users encountered email malware last year

Anatomy of an email attack

01. An attacker sends an email with a malicous link or attachment

02. The email contains an attachment, usually a JavaScript (JS) file or an office file containing a macro.

03 When the file is launched, it will either prompt users to execute a macro or will launch PowerShell to download and execute the final payload

04 The final payload is typically ransomware but may also be one of a multitude online threats.

Spam

Spam is one of the more common methods of both sending information out and collecting it from unsuspecting people. While ordinary spam is simply considered a nuisance, it is also frequently used to deliver malware.

Phishing

Phishing uses psychological manipulation to bait victims into divulging logon data or other sensitive information that criminals sell or use for malicious purposes Many email recipients believe the message is from a trusted individual and will open infected attachments or click on malicious links.

Malicious Links/Attachments

Emails often include dangerous attachments or links to malicious web pages that install keyloggers, ransomware, and other malware when opened by the victim. According to reports, hackers delivered two-thirds of all successful malware via malicious email attachments.

Spoofing

Because email protocols lack effective mechanisms for authenticating email addresses, hackers are able to use addresses and domains that are very similar to legitimate ones, deceiving victims into believing that fraudulent emails are from a trusted individual.

Business Email Compromise

This is a type of social engineering scam where an attacker sends an email to someone in the organisation who has the ability to execute a financial transaction. The email looks like it's from the CEO (or another empowered individual), and requests an immediate financial transaction such as a vendor payment, direct deposit, or wire transfer.

Ransomeware

Most commonly delivered via email, ransomware encrypts the victim's data and demands a fee to restore it. According to CNBC, ransomware spiked 6,000% in 2016, and most ransomware victims, in an attempt to recover their data, paid the ransom.

Zero-Day Attacks

A zero-day vulnerability refers to a security weakness that is unknown to the software developerand is exploited by hackers before the vendor has created a fix. Zero-day attacks are frequently delivered via malicious emails, and hackers use them to gain unauthorized access and steal sensitive information.