EVER-EVOLVING EMAIL ATTACKS

In a continuous cycle of evasion and adaption, email attackers are getting smarter every day. Some of the latest tactics include URL-based attacks, using HTTPS, location-dependent strikes, and file sharing scams.

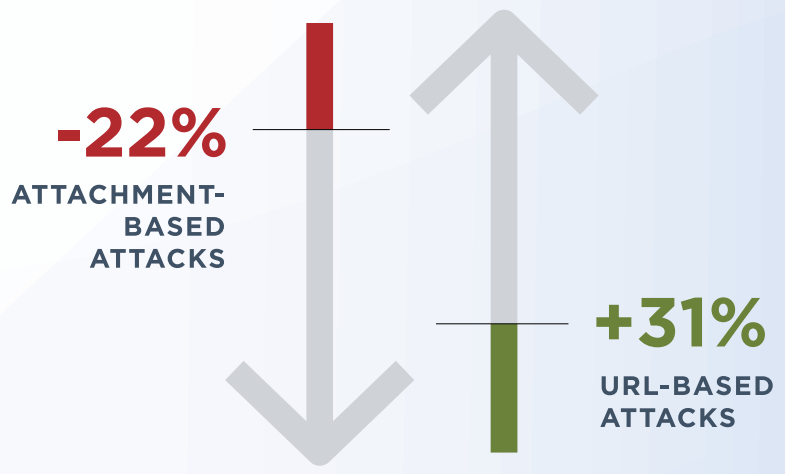
31%
more URL-based attacks[1]

35%
of phishing and malicious URLs used HTTPS[1]

5%
reduction in content management system related phishing campaigns[1]

Shifting methods

Feeling safe because you don't click on unknown attachments? Attachments aren't the only bait. URL-based attacks are easier for attackers to deploy and are more difficult to detect.



In 2018, there were 22% fewer attachment-based attacks and **31% more URL-based attacks**.[1]

URL-based attacks are challenging for some security vendors because they require a level of dynamic advanced threat detection capability not always found in SEGs.

Smarter Phishers

35% of phishing and malicious URLs used HTTPS in 2018, which means secure domains aren't as secure as we might believe.

Phishing attacks aren't just Word docs and PDF attachments anymore. Phishers are turning to Internet Shortcut Files (.url), Excel Web Query and Internet Inquiry files (.iqy).

Some phishing attacks can recognize if they are being accessed by a security engine or a person and wait until a person clicks on a link or attachment to deliver malicious content.

Some phishing kits recognize the request origin location and serve malicious content only if the request comes from the targeted location.

Phishing attacks are using security measures like Sleep, Captcha, Display-links and buttons to appear legitimate and then link to malicious docs.

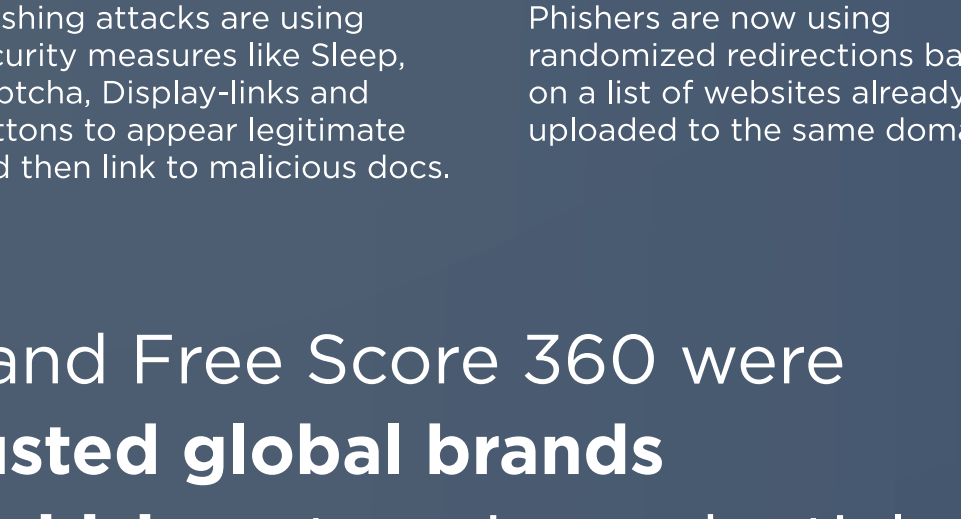
Phishers are now using randomized redirections based on a list of websites already uploaded to the same domain.

Microsoft, Netflix and Free Score 360 were among the **top trusted global brands impersonated by phishers** to gain credentials and access in 2018.[2]

File Sharing Dangers

Sometimes danger is hiding in plain sight. Attackers are now using popular file sharing services like WeTransfer, Dropbox, Google Drive and OneDrive to host malicious/phishing files.

By using the preview link in popular file sharing services, attackers evade content filters and get victims to click on phishing URLs without even downloading the file.



To download the latest email threat report, visit www.FireEye.com/offers/rpt-email-threat.html

1 FireEye Labs, Q4'18 compared to Q4'17
2 FireEye Labs