Spamming and phishing

Spam and phishing emails are the most common delivery methods for malware. The volume of spam email as a percentage of total global email traffic fluctuates widely from month to month – typically 45 to 75 percent. Although most end users today are readily able to identify spam emails and are savvier about not clicking links, opening attachments, or replying to spam emails, spam remains a popular and effective infection vector for the spread of malware.

Phishing attacks, in contrast to spam, are becoming more sophisticated and difficult to identify.

Spear phishing is a targeted phishing campaign that appears more credible to its victims by gathering specific information about the target and thus has a higher probability of success. A spear phishing email may spoof an organization (such as a financial institution) or individual that the recipient actually knows and does business with, and it may contain very specific information (such as the recipient's first name, rather than just an email address). According to Symantec's *2018 Internet Security Threat Report*, "Spear-phishing emails emerged as by far the most widely used infection vector, employed by 71 percent of [140 known targeted attack] groups."[1]

Whaling is a type of spear phishing attack that is specifically directed at senior executives or other high-profile targets within an organization. A whaling email typically purports to be a legal subpoena, customer complaint, or other serious matter.

Spear phishing, and phishing attacks in general, is not always conducted via email. A link is all that is required, such as a link on Facebook or on a message board, or a shortened URL on Twitter. These methods are particularly effective in spear phishing attacks because they allow the attacker to gather a great deal of information about the targets and then lure them through dangerous links into a place where the users feel comfortable.

Watering hole attacks compromise websites that are likely to be visited by a targeted victim, for example, an insurance company website that may be frequently visited by healthcare providers. The compromised website will typically infect unsuspecting visitors with malware (known as a "drive-by download"). Watering hole attacks are the second most popular infection vector for targeted attack groups (24 percent), according to Symantec.[2]

A *pharming* attack redirects a legitimate website's traffic to a fake site, typically by modifying an endpoint's local hosts file or by compromising a DNS server ("DNS poisoning").

[1] "Internet Security Threat Report, Volume 23." Symantec. 2018. https://www.symantec.com/security-center/threat-report.

[2] Ibid.

Key Terms

Spear phishing is a highly targeted phishing attack that uses specific information about the target to make the phishing attempt appear legitimate.

Whaling is a type of spear phishing attack that is specifically directed at senior executives or other high-profile targets within an organization.

Watering hole attacks compromise websites that are likely to be visited by a targeted victim to deliver malware via a drive-by download. A *drive-by download* is a software download, typically malware, that happens without a user's knowledge or permission.

Pharming is a type of attack that redirects a legitimate website's traffic to a fake site.