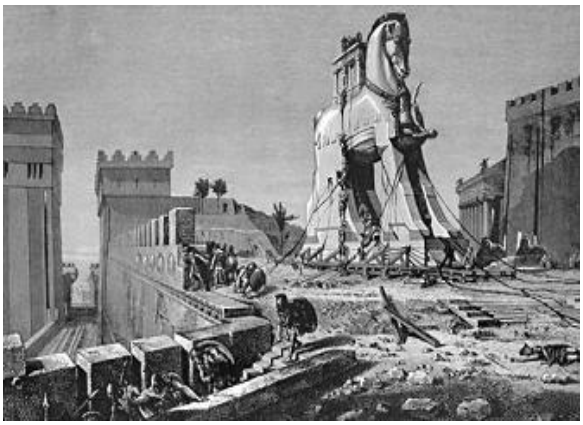
The Treasures of Troy

A Security Perspective, by Robin Proctor



Between 1300 and 1200 BC, according to Greek mythology, the Greeks waged war against the City of Troy. Troy was known to be rich in treasure. The Trojans built massive walls around the city in its defense. The Greeks defeated the Trojans in many battles, but could never break through the walls of Troy.

Seeking to gain entrance to Troy, Odysseus, a very clever man, ordered a large wooden horse to be built. The inside was hollow where soldiers could hide. Once the statue had been built, Odysseus and a number of Greek warriors climbed inside. The Greek fleet sailed away hoping to deceive the Trojans. They left behind one man, a Greek spy named Sinon. Sinon was to trick the Trojans into believing the wooden horse was safe and would bring them good luck. Celebrating their perceived victory, the Trojans dragged their trophy into the city behind the very walls that had kept them safe.

When the time was right, probably while the city was sleeping; Sinon opened a secret door and freed Odysseus and the Greek warriors from the wooden horse. They slaughtered the Trojans, ravaged the City of Troy, and stole their treasures.

Welcome to the 21st century. The clever ruse designed by Odysseus is no longer just a myth; it is a serious threat to Network Security. According to industry security experts, the biggest security vulnerability facing computer users and networks is email with concealed Trojan Horse software—destructive programs that masquerade as benign applications and embedded links to seemingly innocent websites that download malicious code. In 2005, targeted Trojan attacks - as opposed to computer worm outbreaks - became a greater concern. Unlike the more indiscriminate assaults by viruses and worms, Trojans can be delivered with precision to target organizations network infrastructure.

Security experts believe the most important line of defense in computer security is the user. User training and awareness about social engineering attack techniques and safe web browsing practices are integral to a sound computer security posture. Social Engineering makes attacks easier. Recent Trojan Horse attacks have been similar in using social engineering methods to enter the targeted computer network. Social engineering exploits the weakest link in computer network defense—the user—by persuading or deceiving the user, through trust or intimidation, to act out of character.

So what can you (the user) do to help prevent these sorts of attacks and defend our Network? ALL users should be wary of emails with ANY of the following characteristics:

- Email messages written as if they are part of an ongoing conversation, but the user was never part of the original thread.
- Email messages disseminated by people or organizations with whom the user never has had contact or that entice the user to click on a link or open an attachment for more information.
- Emails with attachments the user was not expecting. This can be any type of attachment, including files with common extensions, such as ".doc" for Microsoft Word files, ".jpg" for photo files, and ".wmv" for video files.
- Emails that claim to originate from someone familiar to the user, but the "From" displays differently than in previous messages, such as with a misspelled name or only an email address instead of the sender's name.
- Email messages that do not display the recipient in either the "To:" or "cc:" fields, or have unfamiliar people in the "To:" field.

While firewall architecture (the walls of Troy) blocks direct attacks, email (with an embedded Trojan Horse) provides a vulnerable route into an organization's internal network (the city of Troy) through which attackers can destroy or steal information (our treasure).

Look before you click. In today's world of Cyber Crime, theft of proprietary information is BIG business. Don't let the Odysseus of today lure you into a false sense of security. If you receive any suspicious email, please DO NOT open it. Send it to COTSecurityServicesISS@ky.gov by opening a new email message, then drag and drop the suspicious email as an attachment.