

## TREASURY MANAGEMENT SOLUTIONS

# COMMON FRAUD THREATS

### *Glossary of Common and Advanced Trojan Fraud Threats*

The following glossary of terms provides a comprehensive look at the advanced types of Trojan threats that are targeting financial institutions and their customers.

The term Trojan refers to a family of malicious software (“Malware”) which resides on a user’s computer and has the capability to perform certain actions transparently, all without the end user’s knowledge. For simplicity, Trojans can be divided into several families:

*Phishing/Pharming Trojans* - Performs a redirect to a fraudulent website without the user’s knowledge. Financial institutions that are targeted face risks similar to those of a phishing attack.

*Page-in-the-middle* - Waits until the user logs in to a specific site, performs a redirect to a page for data collection without the user’s knowledge, and then redirects the user back to the financial institution’s genuine site. These Trojans are more reliable than traditional phishing attacks, but serve the same purpose for a fraudster.

*Active Trojans* (man-in-the-middle Trojan) - Installs a type of proxy on the user’s computer that interacts with the financial institution’s genuine site on the user’s behalf. As the Trojan is interacting with the financial institution’s site through the user’s computer, it allows the fraudster to imitate the user’s profile. Some Trojans of this type wait until the user logs in to the genuine site and performs a concurrent web session automatically. Thus, the Trojan will appear to be transacting from the same IP and device as the user.

*Keyloggers/Screen-scrapers* - Captures the user’s keystrokes or tiny images of on-screen selection (for targeting financial institutions that use virtual keyboards at login). Details are then sent to a “drop zone” (an e-mail account or a remote server).

*Active Keylogger+Proxy* (Botnet) Trojan - Steals a user’s credentials using a keylogger or screen-scrapers and then sends the information to the fraudster. The fraudster will access the financial institution’s site from his computer, using the user’s PC as a proxy (botnet). While the fraudster, is imitating the user’s IP, the device credentials of the fraudster’s and end user’s PC are not the same.

*Man-in-the-middle Attacks* - A man-in-the-middle (MITM) server attack involves an end user interacting with a website that appears to be the financial institution’s genuine site, but is actually a spoofed site. At the same time and unnoticed in the background, a fraudster, serving as “a man in the middle,” is feeding the data entered by the user in real-time to the actual financial institution’s site, validating the user and performing a malicious transaction. If the user is challenged to provide additional authentication, the MITM server will pass the request to the user and validate himself. These types of attacks may appear genuine, even to the most sophisticated end user.

*Botnet* - A series of Internet computers that have been compromised with malicious software and are used to send transmissions (of mostly spam or malware) to other computers on the Internet.

**PARK BANK**

DRIVEN BY YES®

Users are often unaware that their computer has been infected. Online users can become part of a botnet in several ways. First, if their computer is left unprotected, fraudsters can install malicious software through “open doors.” Second, software can also be sent through attachments, links or images embedded within e-mails and when a user clicks on them, they will install malicious

software in the background. Finally, a user can be infected with this software just by visiting a website or downloading files (often called a “drive-by download”).

For more information, please visit [www.ftc.gov](http://www.ftc.gov) and [www.ongaurdonline.gov](http://www.ongaurdonline.gov).

**PARK BANK**

DRIVEN BY YES®