Gladiator NetTeller® Enterprise Security Monitoring™ Online Fraud Detection
Foreword
The consumerization of IT and the explosive growth in worldwide Internet users have contributed to a sustained growth of online banking activity. Following this trend, Corporate Account Takeover and other fraudulent attacks against the online channel continue to rise at an alarming pace. Traditional multi-factor authentication and other common validation controls are now being defeated regularly by increasingly sophisticated attacks.

Corporate Account Takeover and electronic banking fraud have become a billion-dollar underground industry, comprised of many well-organized criminal organizations and sophisticated social networks of attackers. Phishing and data breach attacks also continue to pose a risk that all financial institutions must acknowledge and guard against. However, in recent years there has been a significant shift toward more mass-distributed malware and banking Trojans targeting online users directly. This malicious code is mass-infecting financial institution customers' devices, often unbeknownst to the victim, as the malware is covertly installed during seemingly routine Web browsing or while reading emails. Protecting account holders from dangerous banking Trojans cannot be accomplished with education alone, since many of the methods of infection involve activity not traditionally considered dangerous, such as browsing the Web.

Banking Trojans’ attack mechanisms include methods of stealing credentials, hijacking the user's workstation, or even hijacking the user's active online banking session through a method called Man-in-the-Browser attacks. As attackers’ methods continue to evolve, approaches to protecting online banking activity must also adapt to remain effective. Traditional “strong” authentication security no longer provides adequate protection, and monitoring activity conducted within the online session is necessary to provide security to online banking customers. Modern online banking attacks pose unique threat patterns compared to fraud associated with credit or debit cards.
Defeating Statistical Analysis and Page Navigation Behavioral Analytics

Statistical Analysis
Statistical analysis models, such as those based upon transaction frequency and deviations from normal transaction amounts, can be powerful tools for detecting certain types of fraud. However, these methods assume that transactions initiated by fraudsters will differ from the normal baseline activity of the compromised account. This model works well for systems such as debit or credit card fraud detection, since the normal behavior of the account holder is often not known to the fraudsters. However, in online banking fraud, criminals typically have direct access to the victim’s transaction history and can initiate transactions that appear to be within the normal pattern of activity for the account. For example, a fraudster may compromise a commercial banking account and immediately check the account’s ACH batches and see that the customer has a payroll batch that typically goes out on the 1st and 15th of each month. If the fraudster edits the payroll ACH batch to send some of the money to a mule account instead of employee accounts but leaves the batch total the same, most statistical analysis models will miss the fraud due to the fact that it is within the normal financial range, time, and frequency for that account.

Page Navigation Analysis
Page navigation models attempt to baseline the way a user typically traverses the online banking site and looks for significant deviations in behavior as a precursor to fraud. For example, if a user typically logs in, signs into cash management and processes some ACH transactions, but then all of the sudden that same user account starts logging in and checking the account balance and immediately logging off repeatedly, alerts may fire. This method may be effective at catching certain fraud attempts where the criminal has compromised the user’s account and is logging into the system remotely. However, a majority of commercial account compromises today are facilitated by browser-hijacking malware which “steals” the real user’s active session. This allows the criminal to see what pages the user typically visits so that they can follow the same pattern to avoid detection.
NetTeller ESM

At the end of the day, for fraudsters to steal funds they have to transfer money outside of the financial institution to new locations (mule accounts). With advanced tools and adapting methodologies, today's criminals are becoming more adept at mimicking the normal behavior of their victims and flying “under the radar” of traditional behavioral analysis models such as those previously mentioned. To provide consistent and reliable online banking fraud detection, fraud detection models must assume the attackers can mimic a user’s typical behavior. Gladiator’s behavioral models do just that. Our solution focuses on actionable threat intelligence, activity spanning the entire online banking session, including logins, and especially activity where funds are leaving the institution destined to previously unobserved locations.

Gladiator NetTeller ESM’s 24x7x365 holistic online session monitoring provides FIs with superior protection from modern online banking fraud attacks. Real-time data feeds to Gladiator’s correlation technology deliver the timeliest analysis and alerting of suspicious and potentially fraudulent activity. Activity conducted throughout the online session is streamed directly from both the NetTeller data center hosted in Lenexa, Kansas, and from client core systems/JHA OutLink Processing Services™.

Advanced correlation logic incorporates threat intelligence feeds, including findings from Gladiator’s Security Research department, along with numerous partnerships including FSISAC and Jack Henry's internal corporate security team. Intelligence feeds provide regular updates about where fraud attacks originate, tracked accounts being used as money mules, and early warnings of legitimate online banking accounts that are communicating with financial fraud botnets. These attributes of suspicious activity are compared across all NetTeller activity in real time. Threat intelligence feeds provide an effective early indication of fraudulent activity or accounts becoming compromised. Gladiator has also incorporated an Online Fraud Database which is integrated into our correlation engine, capable of detecting logins to NetTeller from known fraudulent locations.

THREAT INTELLIGENCE SOURCES

- Identify NT users that are communicating with financial fraud botnets
- Reverse engineer malware to learn new behaviors and infection methods
- Locate and track hostile domains, botnets, and hosts on the Internet
- Access current financial fraud methods and track money mule accounts

Through regular and dynamic integration of threat intelligence feeds, Gladiator’s detection quickly adapts to new patterns of fraudulent behavior.
Analysis begins from the time a login first takes place to identify fraudulent activity taking place in the NetTeller session. Threat intelligence feeds along with Gladiator ESM’s real-time NetTeller data flows from IP Restrict failed logon attempts, successful authentication, and activity that a user conducts online such as CM user creation, ACH Create, ACH Edit, ACH Initiate, ACH Uninitiate, wire edit, wire initiate, bill pay payee creation, etc. Analyzing NetTeller activity as it takes place provides the most responsive protection for securing online banking.

NetTeller ESM’s unique fraud detection model provides review of each individual line item of ACH batches at the time the line items are created and/or edited through NetTeller. This unique and proven approach is capable of detecting elaborate fraud schemes very early in the transaction. The analysis of line items within the batch compares where funds are being configured along with a learned history of where the NetTeller account normally transacts. This in-depth analysis gets to the underlying commonality of the various fraud schemes used, which is that funds ultimately go to a new destination (often a money mule account). Since fraud involves fund transfers to abnormal locations, fraudulent activity is detected despite the prevalence of advanced attack methods that can make every other part of the transaction look normal.

Fraudulent attacks continually shift to the most vulnerable target. Since retail bill pay often has significantly less protection, these accounts are also frequently targeted. NetTeller ESM leverages our threat intelligence feeds to protect all online banking activity for both commercial and retail accounts. Another layer of protection for retail accounts is provided through monitoring bill payment activity. When NetTeller bill payment attacks are carried out, fraudsters will commonly either find an existing payee to modify the destination account or will simply create a new payee to receive the stolen funds. The ESM correlation engine incorporates these actions along with analysis of the payments that are configured to detect suspicious activity.
Gladiator NetTeller ESM Real-World Examples

$20,000 – ACH Fraud Attempt

Result: Fraudulent activity identified prior to ACH initiation. No loss.

Logon
Cash Management user tried logging in and received an error message. At the same time, the fraudster hijacked the customer’s login session to bypass token security.

ACH Batches Created
The fraudster created two batches totaling $20,000.

Gladiator’s behavior analysis identified that the destination account’s routing and account number combination did not match the normal commercial account’s behavior. Client was notified within five minutes of the suspicious ACH activity.

After receiving the alert from Gladiator, the FI reached out to the commercial account holder to review the activity and was told that the legitimate customer did attempt to login but received a screen showing that the NetTeller site was down for maintenance. The commercial account holder informed the bank that this activity was not authorized, and the bank suspended the account before the fraudulent batches were ever initiated.

Following investigation, it was found that the commercial account holder’s workstation was infected with a banking Trojan.
$580,000 – Fraudulent Wire and ACH Attempt

Result: Fraudulent activity identified prior to ACH and wires were processed. No loss.

Gladiator’s behavioral analysis first flagged the ACH uninitiated event, then identified that the ACH edit activity included destinations that did not match the commercial account’s normal behavior. Finally, the three wires together reached a large sum which exceeded the norm for the account, triggering further notification. The client was notified within five minutes of each of the ACH uninitiated and suspicious ACH edit events.

Bank received security tickets from Gladiator regarding the activity and deleted the ACH batch and the three wire transfers, resulting in no loss.
Unknown Dollar Amount – Corporate Account Takeover Attempt

Result: Malware activity identified prior to fraudulent activity in NetTeller.

The bank received a security ticket from Gladiator regarding the probable banking Trojan infection at the commercial account holder’s location. The NetTeller account was disabled while the commercial account holder cleaned the infected workstation. The imminent threat was terminated before the fraudster was able to tunnel in over the user’s session and commit fraud.