Agenda

- Fraud threat trends and business challenges
- Web fraud protection
- Mobile fraud protection
- Security operations center
- Example architecture
Everything Evolves

Network Firewall  SSL  Application Security  Access Control  DDoS Protection  DNS Security

Anti-Fraud, Anti-Malware, Anti-Phishing
Fraud and Malware Remains a Challenge

**Malware/Fraud Statistics**

- **15%** increase in malware  
  ~ McAfee threat report 2013

- **196 Million** Unique malware samples in 2013  
  ~ McAfee threat report 2013

- **70%** of malware targeting financial services companies

**Mobile Malware**

- **22,750** new modifications of malicious programs target mobile devices throughout the year

- **99%** of newly discovered mobile malware attacks target Android devices

**Phishing Attacks**

- **37.3** million users around the world were subjected to phishing attacks 2012-2013

- **72,758** unique phishing attacks recorded in 1st half 2013 (worldwide)

Data sources include Symantec, Microsoft, Kaspersky, McAfee, DarkReading, Gartner, and Cybersource
Malware Threat Landscape – Growth and Targets

- 25% of real-world malware is caught by anti-virus
- 50% of malware code is logic to bypass defenses
- 79% existing malware strains are Trojans
- 82% of institutions learned about fraud incidents from their customers

Data sources: Dark Reading, PandaLabs, and ISMG

Source: McAfee Labs, 2014.
The Increasing Complexity of Securing Users to Apps
Traditional Malware Solutions Focus on the Enterprise

Enterprise

Rising Security Threats/Attacks

Hacktivism

Malware

State Sponsored Attacks

Attacker

Copied Pages and Phishing

Enterprise Anti-Malware

Firewall

Internet

Database

Applications

DMZ

[Some protection]

[Unprotected]
Securing Against Banking Fraud Can Be Complex

Ownership
Customers expect the banks to secure against all forms of fraud regardless of devices used or actions taken.

Changing threats
Increasing in complexity requiring full threat reconnaissance.

Browser the weakest link
Trojans, MitB attack the client browser or device where the bank has no security footprint.

Attack visibility
Often lacking details to truly track and identify attacks and their source.

Compliance
Ensuring compliance with regulations and FFIEC requirements.

Endless customer devices
Desktop, laptop, tablet, phone, internet café, game consoles, smart TVs.
Web Fraud Protection
Protecting Against Fraud, Phishing, and Malware

- Device ID
- Generic malware detection
- Phishing and MitM detection
- Credential protection
- Targeted malware (injections)
- Behavioral and click analysis
- Automatic transaction
- Transaction integrity checks
- Customer fraud alerts

Phishing Threats

Credential Grabbing

Malware Injections

Transaction Manipulation

Automatic Transactions
Anti-Fraud, Anti-Phishing, Anti-Malware
Best practices for anti-fraud, anti-phishing, and anti-malware services

Prevent Fraud
Targeted malware, MitB, zero-days, MitM, phishing automated transactions

Protect Online User
Clientless solution, enabling 100% coverage
Application level encryption

On All Devices
Desktop, tablets, and mobile devices

Full Transparency
No software or user involvement required

In Real Time
Alerts and customisable rules

Security Operations Center
24x7 research, investigation, and site take-down
Anti-Fraud Solution: Key Functionality Needed

**Fraud Detection and Protections**
- Detect targeted malware, Bots, MitM, MitB, Zero-day, credential grabbers, session hijacking
- Identify extensive scans and searches
- Monitor and alert when site copy is loaded to spoofed sites
- Detect DNS hijacking

**Transaction Protection**
- Perform real-time transaction analysis
- Offer comprehensive request analysis
- Support clientless layer 7 encryption
- Application level encryption

**Security Operations Research Center**
- Provide 24x7 security reports and alerts
- Identify and investigate attacks in real-time
- Research and investigate new global fraud technology and schemes
- Provide detailed incident reports
- Offer optional site take-down
Generic and Targeted Malware Detection

• Identify compromised sessions, malicious scripts, phishing attacks, and malware
  • Including MitM, MitB, Bots, and fraudulent transactions with real-time analysis

• Analyse browser for traces of common malware (Zeus, Citadel, Carberp, etc.)

• Detect browser redressing

• Perform checks on domain and other components
Advanced Application-Layer Encryption
Secure the credentials and other valuable data submitted on webforms

• Encrypt any sensitive information at the message level
• Encrypt then submitt user credentials and information
• Decrypt data using web fraud protection solution
• Render intercepted information useless to MitM attacker
Automatic Transaction Detection

1. Analyse the way users interact with browser
2. Analyse the way users interact with website
3. Conduct track site navigation
4. Trigger alerts upon detecting non-human behavior

• Gather client details related to the transaction
• Run a series of checks to identify suspicious activity
• Assign risk score to transaction
• Send alert based on score
• Apply L7 encryption to all communications between client and server
Advanced Phishing Attack Detection and Prevention
Identify phishing threats early on and stop attacks before emails are sent

- Alert of extensive site copying or scanning
- Alert on uploads to a hosting server or company
- Alert upon login and testing of phishing site
- Shut down identified phishing server sites during testing
- Capture user credentials
Key Features of a Web Fraud Protection Solution

Provide transparent anti-fraud solution

Combine fraud detection and protection

Simplify product rollout

Ensure compliance

Protect users data in use

Prevent phishing attacks

Protect all customers on all devices
Mobile Fraud Protection
Fraud Protection for Mobile Device Users

**Fraud Detection and Protections**
- Detect targeted malware Bots, MitM, MitB, Zero-day, SMS grabbers, key loggers
- Provide jail broken device detection and risk score adjustment

**In App Encryption**
- Encrypt user sensitive data in the app (e.g. user name, passwords, account numbers)
- Render mobile device traffic sniffing malware ineffective

**Security Operations Research Center**
- Provide 24x7 security reports and alerts
- Identify and investigate attacks in real-time
- Research and investigate new global fraud technology and schemes
Fraud Protection for Mobile Users: Key Functionality
Identify malware and MitM attacks in real time

- Detect mobile site phishing and pharming
- Provide advanced mobile malware detection capabilities
- Execute various DNS checks and SSL certificate verification
- Perform app signature checks to identify application tampering
- Flag obsolete or vulnerable device OS and send alerts
- Discover rooted/jailbroken devices
- Identify each device and assign a risk score
Real-Time Mobile Transaction Protection

• Capture key information on each transaction
• Associate each transaction with unique device id
• Provide clientless, application-level encryption on top of standard SSL encryption
• Use transparent virtual key-pad
Key Features of a Mobile Fraud Protection Solution

- Secure against targeted and generic malware
- Minimise product rollout
- Protect all mobile device users

- Render intercepted information useless
- Ensure regulatory compliance
- Provide immediate reduction in fraud loss
Security Operations Center
Security Operations Center (SOC)

• Leverage a 24x7x365 fraud analysis team that extends your security team
• Research and investigate new global fraud technology and schemes
• Provide detailed incident reports
• Offer continuous web fraud component checks
• Send real-time alerts by phone, SMS, and email
• Take down phishing sites and brand abuse sites
Cyber Intelligence
Always on cyber research and analysis

• Source information from a variety of resources

• Analyse malware files and research drop zones

• Provide quarterly dedicated reports

• Deliver the right information
  • Identify attackers, command & control, drop zones, mule accounts, compromised users

• Identify social network scheming, sophisticated online fraud and brand abuse
Phishing Site Take-Down Service
Quickly identify and shut down brand abuse websites

MONITORING AND RESPONSE TEAM

• Complete attack assessment and post-partum attack report
• Leverage relationships with ISPs, anti-phishing groups, and key international agencies
• Offer malicious site take-down in minimal time
• Provide recommendations for counter security measures
Key Benefits of Using a Security Operations Center

- **Provide 24x7 expert security watch**
- **Integrate with SIEM and risk management systems**
- **Turn on services immediately**

- **Offer immediate phishing site shutdown**
- **Provide up-to-date threat intelligence**
- **Reduce fraud loss**
Example Architecture
Example of a Web Fraud Protection Architecture

Customer Scenarios
- Malware detection and protection
- Anti-phishing
- Transaction analysis
Anti-Fraud, Anti-Phishing, Anti-Malware

- Prevent Fraud
- Protect Online User
- On All Devices
- Full Transparency
- In Real Time
- Security Operations Center
Solutions for an Application World.