The Future of Cyber Threat Detection

Julie Conroy
Research Director
Aite Group

Nick Edwards
Director, Identity Protection Solutions
RSA

Tuesday, 9 July
14:00 BST

U.S./Canada Toll-Free
1-866-289-3291 PIN: 8272

International Toll
Dial 001-503-295-8000, then enter 866-289-3291 and PIN: 8272

Or listen via your computer speakers:
Under the Voice & Video tab select “Join Audio”
Threats Span Across Customer Interaction Points

Pre-Authentication Threats
- InfoSec
- New Account Registration Fraud
- Password Guessing
- Parameter Injection
- Man In The Browser
- Trojan Attacks
- Rogue Mobile Apps
- Phishing Attacks
- DDOS Attacks
- Site Scraping
- Vulnerability Probing

Post-Authentication Threats
- Fraud
- Unauthorized Account Activity
- Access From High Risk Country
- Man In The Middle
- High Risk Checkout
- Fraudulent Money Movement

In the Wild
- Login
- Transaction
- Logout

Web and Mobile Channels
- Beginning of Session
- Web and Mobile Channels
- Login
- Transaction
- Logout
Defense in-Depth is Critical for Fraud Prevention

Shared Intelligence

Anti-Phishing /Trojans

Behavioral Analysis

Risk-Based Authentication

Knowledge-based Authentication

Risk-Based Transaction Monitoring

In the Wild

Beginning of Session

Login

Transaction

Logout

Web and Mobile Channels
RSA Fraud Prevention – Comprehensive Visibility

Threat Intelligence • eFraudNetwork

- Adaptive Authentication
- Identity Verification
- AA for eCommerce
- Transaction Monitoring

In the Wild
Beginning of Session
Login
Transaction
Logout

Web and Mobile Channels
Agenda

The Threat Landscape

- Account takeover
- Mobile channel threats
- DDoS

Best Practices for Addressing Today’s Threats
Account takeover
and increasing use of manual assisted cyber attacks
How does account takeover happen?

- **Data breach**
- **Malware**
- **Phishing**
The username/password combo is officially broken

Zappos hacked, 24 million user credentials stolen

LinkedIn hacked, 6 million user passwords stolen

And now...
150,000+
Number of unique strains of malware deployed per day

50%
Percent of malware designed to compromise credentials

55%
Number of consumers that use the same credentials across multiple online relationships
Consumers’ experiences substantiate the rising tide of fraud

Q. Have you experienced more than one incident of debit or credit card fraud in the past 5 years?
(2011, N=4,200; 2012, N=4,247)

- 2011 respondents: 6%
- 2012 respondents: 14%

Source: Aite Group, ACI Worldwide study of 5,223 consumers in 17 countries, Q3 2012
The criminals’ innovation is paying off

Global Corporate Account Takeover Losses, 2011 to e2016
(In US$ millions)

Source: Aite Group, 2012
FIs and merchants do not have the luxury of resting on their laurels

Fraudsters’ pace of innovation is just too fast
Big Data Analytics
Fraud Prevention: RSA FraudAction Services

In the Wild
Beginning of Session
Login
Transaction
Logout

Web and Mobile Channels

Threat Intelligence • eFraudNetwork

In the Wild
Beginning of Session
Login
Transaction
Logout

Web and Mobile Channels

FraudAction
Silver Tail

Adaptive Authentication
Identity Verification

AA for eCommerce
Transaction Monitoring

In the Wild
Beginning of Session
Login
Transaction
Logout

Web and Mobile Channels

FraudAction
Silver Tail

Adaptive Authentication
Identity Verification

AA for eCommerce
Transaction Monitoring
RSA FraudAction Services

External Threat Intelligence

- Real-time threat detection and handling
- Attack intelligence sharing
- Actionable intelligent threat data feeds
- Forensics and baits operations
RSA FraudAction Service
Anti-Phishing Blocking Network

Unparalleled Blocking Network

• Broad Partnerships
  • Partners include large ISPs, anti-virus, toolbar and anti-spam firms
  • FraudAction customers benefit from added-value at no additional cost

• Proactive Alerting
  • RSA alerts partners, who then block access to phishing URLs
  • Limits fraud exposure while fraud site is in process of being shut down
RSA FraudAction Service
Anti-Trojan Service

Stop the Threat of Trojans and Crimeware

Identification:
WHAT crimeware is targeting you and your customers
Aggregated detection via RSA and AV partner network

Analysis:
HOW the crimeware works that is targeting you and your customers
Aggregated analysis via RSA and AV partner network

Blocking:
WHERE the crimeware infects, and WHERE it drops credentials
Data feed to browser, ISP, and firewall partners

Credential Recovery:
WHO of your customers have been infected

Targeted Shutdown:
Infection Points and Drop Zones

Targeted Baits:
Track the movement of online criminals and gain insight into their tactics

Money Mules:
Trace mules to prevent transactions

RSA® FraudAction™ Anti-Trojan Service

RSA® eFraudNetwork™
Risk-based Authentication

• Transparent real-time fraud detection and authentication without sacrificing user experience

• Monitor and authenticate both login and post login activities

• Risk based self-learning engine which rapidly adjusts policies and controls to predict and protect against future attacks

• Collaborative real-time cross-institution fraud intelligence sharing
How Risk is Determined - RSA Risk Engine

- Payment activity
- Non-payment activity
- RSA eFraudNetwork
- Anti-Trojan analysis
- Geo location
- Cross-channel information
- RSA case management feed-back
- Fraud intelligence
- IP information
- Behavioral profile
- Mobile activity
- Device profile
Risk-Based Fraud Mitigation

Risk Engine

Activity details

Policy Mgr.

Authenticate

Continue

Step-up Authentication

Out-of-band
Challenge
Knowledge
Others

Feedback

Case Mgmt
Fraud Prevention: RSA Silver Tail

---

**Threat Intelligence • eFraudNetwork**

- **Adaptive Authentication**
- **Identity Verification**
- **AA for eCommerce**
- **Transaction Monitoring**

**FraudAction**

- **In the Wild**
- **Beginning of Session**
- **Login**
- **Transaction**
- **Logout**

**Web and Mobile Channels**

---
Evolution of the Web

- PC
- User Account
- App Stores & Marketplaces
- Mobile
- Electronic Downloads
- Sweepstakes & Rewards
- Wire Transfer
- Shopping Cart
- Reviews
- Local Stores
- Social Networks
- Login
They know when the brinks truck arrives to drop off money.

They know when the tellers go on their smoke breaks.

They know when the guards change shifts.

Banking Circa 2013
Anomalous Behaviour Detection

*Criminals Look Different than Customers*

- Velocity
- Page Sequence
- Origin
- Contextual Information
Excessive Logins – Password Guessing/Running

Using search to expand investigation
Numerous password values and username values
Consistent with password guessing

Multiple user accounts tied to single IP
Fraud Investigations: High Risk Registration Activity

- Only two IPs associated with registration page
- High risk countries: RU and UA
- Large amount of activity, periodic spikes
- All User Accounts generated can be collated and shut down quickly
As the world Goes Mobile
cyber crime will follow
Mobile is an increasing point of pain

Q. How has your mobile fraud rate changed year-over-year? (N=9)

Lower, 1

Higher, 3

Flat, 5

Source: Aite Group interviews with merchants, issuers, and payment gateways, Q1 2013

Criminals are taking advantage of the unique properties of the mobile channel
Mobile malware is increasing at a scary pace

Source: McAfee Threat Report, Q4 2012

97% of the mobile malware is on the Android platform
Games
RSA Adaptive Authentication: Mobile Channel

- Leverages RSA Risk Engine with unique Mobile Model
- Mobile transaction normalization
- User profiles built using multiple channel information
- Mobile device identifiers taken into consideration
RSA FraudAction Anti-Rogue App Service

- Monitors major app stores:
- Detects apps targeting customers
- Works with store and developer to shutdown apps based on customer guidance
IP coming via the mobile channel with high hits to the login page. IP originating from Sweden. Further investigation reveals a deposit of 900 followed by numerous login attempts. Behaviour could indicate attempted account takeover as login attempts occur following logout request.
RSA Silver Tail: Mobile Traffic (High-Risk Transaction)

Deposit is carried out. Then login is attempted numerous times. Search shows password iterations attempted following deposit amount.
TREND 3

DDOS

Hacktivists, Cybercriminals, Nation-States
DDoS on steroids

Hacktivism  Fraud
Make, distributed denial-of-service (DDoS), a legal form of protesting.

With the advance in internet technology, comes new grounds for protesting. Distributed denial-of-service (DDoS), is not any form of hacking in any way. It is the equivalent of repeatedly hitting the refresh button on a webpage. It is, in that way, no different than any “occupy” protest. Instead of a group of people standing outside a building to occupy the area, they are having their computer occupy a website to slow (or deny) service of that particular website for a short time.

As part of this petition, those who have been jailed for DDoS should be immediately released and have anything regarding a DDoS, that is on their “records”, cleared.

Created: Jan 07, 2013
Issues: Civil Rights and Liberties, Human Rights, Technology and Telecommunications

SIGNATURES NEEDED BY FEBRUARY 06, 2013 TO REACH GOAL OF 25,000

21,456 TOTAL SIGNATURES ON THIS PETITION 3,544
DDoS Attacks

About:
We are here to provide you a Professional DDOS service.
We are capable of taking down small personal website/server to huge protected website/server for days.

FAQ:

Question:
What is DDOS?

Answer:
A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attack on the availability of a target service. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists in making a site or service from functioning efficiently or at all, temporarily or indefinitely.
DDoS Evolution

- DoS
  - ICMP Flood
  - Nuke
  - NAPTHA
  - Teardrop
  - Ping of Death
- Solution
  - Firewalls
  - Switches and Routers
  - IPS

DDoS
- Layer 4 Attack
- Peer-to-Peer Attack
- Spoofed Attack
- SYN Flood
- UDP Flood
- Bandwidth Consumption

Solution
- Firewalls
- Session DDoS
- Beyond Layer Attack
- Session Flood
- Request Flood
- User Agent Randomization
- Device Id Randomization
- Crowd Sourced Opt-in Attacks
- Resource Consumption

Session DDoS
- Beyond Layer Attack
- Session Flood
- Request Flood
- User Agent Randomization
- Device Id Randomization
- Crowd Sourced Opt-in Attacks
- Resource Consumption

Solution
- Real-Time Web Session Visibility
- User Behavior Patterns
- Population Activity Clustering
- Deep Data Visibility
- Real-Time Detection Logic
- Cross Session Visibility
- Historical Profile Analysis

© Copyright 2011 EMC Corporation. All rights reserved.
What we learned

- In one hour, 43 IP addresses were clustered together based on their activity on the login page.
- In subsequent hours, as few as 1, or as many as 320 IPs were behaviorally clustered.

How we used it

- The ‘DDoS’ threat cluster behaviorally linked this trend across hours
- The behavioral clustering provided visibility into the full attack scale & duration which – beyond what the customer had identified by other means
Dissecting the Attack

*Using Page Details to isolate the target*

What we learned
• ≈2.6 million hits were made to the login page in one hour.
• 213,098 of those hits came from one IP address.

How we used it:
• Visibility into which parts of the site are being attacked

The login page is being hit **52 times** more frequently than the subsequent landing page.
There is little in the way of deterrent

Q. What percentage of fraud incurred against your company do you prosecute? (n=19)

Source: Aite Group surveys and interviews with 22 e-commerce merchants, March and April 2012
The problem will only get worse

- Data breaches provide plenty of fodder
- Retailers and FIs continue to be attractive targets
- Arrival of EMV in the U.S. market will displace current counterfeit fraud volume to other fraud mechanisms
With the U.S. migration to EMV, issuers and merchants globally will see significant spikes to CNP fraud and account takeover.

Change in U.K. Card Fraud Composition, 2005 to 2012

With the increasing use of 3D-Secure, CNP fraud is a problem for merchants and issuers alike.

Source: Financial Fraud Action UK, Aite Group
The bad guys are also aware of 3DS

Source: RSA
FIs and merchants continue to build their layered strategies

- Behavioral analytics and device fingerprinting favored for their effectiveness and transparency
- OOBA picking up steam, while KBA is losing power
- Periodic risk assessments are necessary given the pace of fraudsters’ innovation
- Assume the endpoint is compromised, and build your defense strategy from there
- Stay nimble—fraud prevention is about the journey, because there is no final destination
InfoSec

Pre-Authentication Threats

Fraud

Post-Authentication Threats

In the Wild

Beginning of Session

Login

Transaction

Logout

Web and Mobile Channels

Site Scraping
Trojan Attacks
Rogue Mobile Apps
Phishing Attacks
Vulnerability Probing
DDOS Attacks
Parameter Injection
New Account Registration Fraud
Promotion Abuse
Password Guessing
Access From High Risk Country
Account Takeover
Man In The Browser
Unauthorized Account Activity
Man In The Middle
High Risk Checkout
Fraudulent Money Movement

Threats Span Across Customer Interaction Points
Defense in-Depth is Critical for Fraud Prevention

**Shared Intelligence**

- Anti-Phishing /Trojans
- Behavioral Analysis
- Risk-Based Authentication
- Knowledge-based Authentication
- Risk-Based Transaction Monitoring

**Channels:**
- Web and Mobile

**Phases:**
- In the Wild
- Beginning of Session
- Login
- Transaction
- Logout
RSA Fraud Prevention - Intelligent Risk-Based Solutions

Threat Intelligence • eFraudNetwork

In the Wild • Beginning of Session • Login • Transaction • Logout

Web and Mobile Channels

FraudAction • Silver Tail • Silver Tail

Adaptive Authentication • Identity Verification

AA for eCommerce • Transaction Monitoring

eFraudNetwork • FraudAction • Silver Tail

Identity Verification

Login

Transaction Monitoring

Web and Mobile Channels