Analytics, Big Data, & Threat Intelligence: How Security is Transforming

Jason Sloderbeck
Director, Product Management
RSA Web Threat Detection
Presentation Overview

• The Largest Threat
• How Can Big Data and Analytics Help?
• Blind Spot: Web Threats
• RSA Web Threat Detection
The Largest Threat
The Largest Threat

Attacks are increasing in...
- Volume
- Complexity
- Damage

Which is the largest threat?
- Zero-hour exploits?
- Botnets?
- Mobile malware?
- Application security vulnerabilities?
Human Intelligence: The Largest Threat

natal cubrilovic
@nikcub

posting an email address as JSON to appleid.apple.com/account/validation/appleid returns if it is a valid account or not. no rate limit.
Security Defense Spectrum

Awareness
• Individual vs. organizational

Visibility
• How usable?

Detection
• Historical vs. real-time
• False positive rate

Mitigation
• Manual vs. automated
How Can Big Data and Analytics Help?
What is Big Data?

“High-volume, high-velocity and high-variety information assets that demand cost-effective, innovative forms of information processing for enhanced insight and decision making.”

– Gartner

“Big data is not defined by how you can measure data in terms of volume, velocity, and variety.”

– Forrester
Benefits of Big Data

• Depth
  – Summary versus full content
  – Logs and packets

• Time
  – Historical versus real-time
  – Process past and present

• Storage, Processing, and Analysis

• Flexibility
  – Change detection rules on-the-fly

• Usability
  – Help humans understand what is important
  – Give context-sensitive information
Statistical Analytics

• Real-time statistical analysis
  – Population-based (crowd) statistical analysis
  – User-based statistical analysis (profiling)

• Behavior analytics
  – Velocity, navigation, content/device variance

• Long-term and short-term trends

• Cross-channel correlation
In-House Data Science
Playing Catch-up

"By 2016, 25% of large global companies will have adopted big data analytics for at least one security or fraud detection use case."

- Gartner, 2014
Adoption Hurdles

- Unclear organizational ownership
  - Minimal collaboration between fraud and infosec

- Inadequate staffing for new, complex information

- New budget justification

- Waiting for the silver bullet
  - Real-time detection with automated in-line mitigation for all types of attacks
Blind Spot: Web Threats
Evolution of the Web

- PC
- Mobile
- App Stores & Marketplaces
- User Account
- Electronic Downloads
- Sweepstakes & Rewards
- Wire Transfer
- Shopping Cart
- Reviews
- Local Stores
- Social Networks
- Login
How are Websites Protected Today?

- **User**
  - 2 Factor Authentication
  - Device ID

- **Network**
  - Firewall
  - IPS/IDS

- **Application**
  - WAF
  - Penetration Testing
  - Dynamic Scanning
  - Log Analysis/SIEM
  - Source Code Analysis
Web Threat Landscape

In the Wild

• Phishing
• Site Scraping
• Vulnerability Probing
• Layer 7 DDoS Attacks

Begin Session

• Password Cracking/Guessing
• Parameter Injection
• New Account Registration Fraud
• Advanced Malware (e.g. Trojans)
• Promotion Abuse

Login

• Man in the Middle/Browser
• Account Takeover
• New Account Registration Fraud
• Unauthorized Account Activity
• Fraudulent Money Movement

Transaction

Logout

InfoSec

Pre-Authentication Threats

• Phishing
• Site Scraping
• Vulnerability Probing
• Layer 7 DDoS Attacks

Fraud

Post-Authentication Threats

• Man in the Middle/Browser
• Account Takeover
• New Account Registration Fraud
• Unauthorized Account Activity
• Fraudulent Money Movement
Industry Survey: Web Threats

Everyone is Losing Money

90% Report Lost Revenue due to Web Fraud

Web Sessions Appear the Same

74% Can’t tell if a web session is a customer or a criminal

IT Needs Tools

64% Report that they do not have clear visibility of their web session traffic

It’s Not My Job

1/3 Do not know who is responsible for addressing web threats

Source: Ponemon Institute ‘The Risk of Business Logic Abuse: U.S. Study’
Mobile: Another Blind Spot

- Third-party developers
- Runs over SSL, but not web requests
- API-level communication
- New message formats
  - JSON
  - XML
What is JSON?

{"response":{"numFound":95219,"start":0,"docs":
[{"id":"10.1371/journal.pone.0092642","doi":
"10.1371/journal.pone.0092642"},"publication_date":"2014-03-21T00:00:00Z","author":
[Frieda Beauregard","Sylvie de Blois"],"title_display":"Beyond a Climate-Centric View of Plant Distribution: Edaphic Variables Add Value to Distribution Models"},
{"id":"10.1371/journal.pone.0092604","doi":
"10.1371/journal.pone.0092604"},"publication_date":"2014-03-21T00:00:00Z","author":
[Liping Hao","Fan Lü","Qing Wu","Liming Shao","Pinjing He"],"title_display":"High Concentrations of Methyl Fluoride Affect the Bacterial Community in a Thermophilic Methanogenic Sludge"},
{"id":"10.1371/journal.pone.0092629","doi":
"10.1371/journal.pone.0092629"},"publication_date":"2014-03-21T00:00:00Z","author":
[Cheng-Fei Liu","Shu-Yan Liu","Xiao-Yun Min","Yuan-Yuan Ji","Na Wang","Dan Liu","Ning Ma","Zong-Fang Li","Ke Li"],"title_display":"The Prognostic Value of CXCR4 in Ovarian Cancer: A Meta-Analysis"},
{"id":"10.1371/journal.pone.0092617","doi":
"10.1371/journal.pone.0092617"},"publication_date":"2014-03-21T00:00:00Z","author":
[François Brischoux","Yurii V Korniliev"],"title_display":"Hypernatremia in Dice Snakes (<i>Natrix tessellata</i>) from a Coastal Population: Implications for Osmoregulation in Marine Snake Prototypes"},
{"id":"10.1371/journal.pone.0092584","doi":
"10.1371/journal.pone.0092584"},"publication_date":"2014-03-21T00:00:00Z","author":
[Ryosuke O Tachibana","Naoya Oosugi","Kazuo Okanoya"],"title_display":"Semi-Automatic Classification of Birdsong Elements Using a Linear Support Vector Machine"}]}
RSA Web Threat Detection
Visibility

- Access to Transaction Data
- Easy integration into other systems
- Flexible formats
- Mobile Application Parsing

Detection

- Real-time Threat Groups
- Anonymous IP Scoring
- Profile History Timeline
- Enhanced Rules

Ease of Use

- Search enhancements
- Analyst Summary Dashboard
- Granular Access roles/controls
- UI Enhancements
- IE 11 Support
- Simplified Upgrades
Profile Timeline

User/IP Sessions’ Summary (no time boundaries)

Profile Timeline
2014/05/16 07:00 UTC - 2014/05/14 23:55 UTC

Multiple Locations
Multiple IPs
Top 10 Score
Incidents
Unique Pages
Response Codes
User Agents
Click Speeds
Alerts
Notes

Direct Navigation

Score Generated by Analytics Engine

Scores This Hour: 0 21 28 12 22
Case Study: Vulnerability Probing

- Spike in number of clicks
- Short time period
- High number of Unique URLs
- Single or multiple Ips

Example

- Typical active use case ~150
- Unique URLs targeted ~ 4000
- ~70% of URLs were invalid
- Requests were still received by web server application
Case Study: Password Guessing

- Same User ID, Guess password
- Same password, Guess User ID
- Do you
  - Allocate user IDs based on numbers?
  - Use a common initial P@ssword1
  - Have the ability to identify the machine running the request to the web server Linux machine common for scripted attacks
Case Study: DDoS

• Full Visibility & Real Time Data
  – Behavioral Clustering of DDoS attack & correlating clustered Botnet Attack IP’s with activity on other high risk parts of the site (ie. Wires to high risk recipients)
  – Real time alerting & visibility into what the DDoS attack is actually doing on the site
    ▪ Other systems could tell a DDoS was happening but, would take 6 hrs to get the logs to understand how they were trying to take down the site
Case Study: Account Takeover

• Account Takeover
  – Fraudsters taking over account adding exit account and executing money withdrawals with minimal clicks & session time.
    ▪ WTD has helped stop very high-dollar transfers ($100K+)

• Short Sell Scam – Account Takeover
  – Rings of short-sell scammers purchase thousands of shares of low-priced stocks to increase the demand/price, then turn around and sell the stock for a loss. WTD has helped prevent losses
    ▪ When someone short-sells using another person's account, the real account holder doesn't pay for the losses, Scottrade does
Mobile Visibility

- Native support for JSON content
- Rule creation on mobile application elements
- Mobile data
  - Included in Streaming Analytics
  - Visible in Clickstream Details
Closing Thoughts

1. Evolution and innovation is **rapid**
2. Often the **only effective layer**
3. **Amplifies** the right human assets, but doesn’t replace
4. Establish organization **ownership**
5. Build **awareness**: problem & budget
6. Plenty of room to grow – **don’t wait** for perfection