Behavioral Analytics – A Closer Look

Mike Huckaby
VP, Global Systems Engineering
RSA
The world is full of obvious things which nobody by any chance ever observes.

Sherlock Holmes
Patterns – Signal And The Noise
Agenda

- UBA / UEBA Defined
- Practical Uses Today
- What does the future hold?
Attacker Capabilities

Time to Discovery

Percent of breaches where time to compromise (red)/time to Discovery (blue) was days or less

© Copyright 2015 EMC Corporation. Confidential and Proprietary. NDA Required
Defender’s Challenges

The attack surface is expanding

Attackers are becoming more sophisticated

Existing strategies & controls are failing

Security teams need comprehensive visibility from endpoint to cloud

Teams need to increase experience & efficiency

Tools & processes must adapt to today’s threats
At first, there were HACKS
Preventative controls filter known attack paths

Successful HACKS
At first, there were HACKS
Preventative controls filter known attack paths

Then, ATTACKS
Despite increased investment in controls, including SIEM

Successful ATTACKS
Now, successful ATTACK CAMPAIGNS target any and all whitespace.

Complete visibility into every process and network sessions is required to eradicate the attacker opportunity.

Unified platform for advanced threat detection & investigations
Behavior what?

- UBA
  - General Term – Fraud and Security

- UEBA
  - Analysis On Users and Entities
  - Algorithms
  - Machine Learning
Visibility & Analytics

- **User Behavior:**
  - Anomalous Logins Suspect Access Patterns

- **Suspicious tools:**
  - Live Off The Land Anomalous Usage

- **Malware Behavior:**
  - Suspicious Domains Mechanized Activity

- **Campaign Detection:**
  - Related entities Related indicators Related behaviors
A Typical Attack Utilizing C2

1. Spear phishing email with link to malicious URL
2. User clicks link
3. Dropper is downloaded
4. Dropper downloads Gh0st RAT
5. C2 Beaconing (Gh0st Protocol)
6. Attacker issued command

COMMAND Examples:
- Capture webcam
- Download file
- Keystroke logging
- Remove existing rootkits
- Remote shell
- System inventory
- ...
Spotting C2 Exploit Early

**LEADING INDICATORS OF A PLANNED C2 EXPLOIT**

- **Real-time Analytics**
  - Data Science algorithms
  - Scores on multiple C2 behavior indicators
  - Utilizes streaming HTTP activity

- **Low False Positives**
  - Learns from ongoing and historical activity
  - Supervised whitelisting option

- **Beaconing Behavior**
- **Rare Domains**
- **Rare User Agents**
- **Missing Referrers**
- **Domain Age (WhoIS)**
- **Suspicious Domains aggregate score**
Workflow for Investigating a C2 Exploit

High Risk Score Indicating a C2 exploit

Activities indicating and used to calculate risk score of C2 exploit

Enable analyst to pivot into associated network sessions

Network Session Details

### Enrichment
- Domain Registration
  - No domain registration data available
- Overall Command And Control Risk
  - Command and Control Risk Score:
  - Contribution of Rare Domain Score (This Network)
  - Contribution of No Domain Referrer Score
  - Contribution of Rare User Agent
  - Beaconing Score
  - Beaconing Period
- Domain Age Indicator
  - Domain Age Score (This Network)
  - Domain Age (This Network)
- Expiring Domain Indicator
  - No domain registration data available
- Rare Domain Indicator
  - Rare Domain Score (This Network)
  - IPs Associated With The Domain
  - Occurrences in the last week
- No Referers Indicator
  - No Referers Score
  - IPs With No Referers
  - Percentage of IPs With No Referers
  - Occurrences in the last week
- Rare User Agent
  - Rare User Agent Score

### Image
- Network Session Details with date range from 2014-09-01 13:51:00 to 2014-10-31 21:01:59
- Concentrator Source:
  - loki (144)
- Decoder Source:
  - (1 value)
Lateral Movement Detection

- Identifies suspicious Windows login activity to reveal lateral movement attempts
  - Windows Credential Harvesting Services
  - Suspicious Login activity
  - Explicit logins
  - File move + Services
Resource Shift Needed: Budgets & People

Today’s Priorities:
- Prevention: 80%
- Monitoring: 15%
- Response: 5%

Future Requirements:
- Prevention: 33%
- Monitoring: 33%
- Response: 33%
Detection: A Layered Approach

- Identify risky authentications (Individuals, Peers, Population)
- User/Resource context (Priv users, OU, Critical assets, etc.)
- Correlation with attack events (IDS/IPS, DLP, C2, etc.)
- Host based behavior analytics (LOTL, Etc.)
- Central user ID (All events per user)
- Automated “Look Left”
Combining Analytics, Context & Content

Behavior profiling
2. User authentication behavior is highly anomalous

GRC/CMDB Context
1. Host is a critical asset
2. Client Using Multiple DHCP Servers

Content

Suspect login + 2 medium/high for this user/host/IP

High Priority Incident
“Apply” Slide

1. Evaluate Your Internal Spending Patterns
   - Look for a balanced approach

2. Start Collecting Data
   - Context doesn’t appear out of thin air

3. Consult on Data Science Approach
   - You know your business – apply analytics to your unique view