Conquer the Beast - How to Effectively Manage Open-source Intelligence Outbursts

Naveed ul Islam
Kevvie Fowler
SecTor Presentation
October 2\textsuperscript{nd} 2012
Introduction
Introduction

- **About us:**
  - Who we are
    - Naveed ul Islam (BEE Telecom/DSP, CISSP, GCFA, MCSE, CCNA)
      - Security Intelligence architect within the TELUS Intelligent Analysis team
      - Leads Application Security and Code Analysis Program for TELUS in Health
      - Experienced Web 2.0 developer
    - Kevvie Fowler (GCFA Gold, SANS Forensicator, CISSP)
      - Leads the TELUS Intelligent Analysis practice
      - Founder and principal consultant of Ringzero
      - Author of “SQL Server Forensic Analysis” and contributing author to several forensics and security books
  
- **What we do at TELUS**
  - Intelligence Analysis
  - Research
  - Forensics
  - Vulnerability Management
  - Security Quality Assurance Program
  - Incident Management
  - Penetration Testing
Introduction

Agenda

- Presentation format
  - Security Landscape
  - Intelligence
  - Sources
  - Information Collection Tools
  - Classification Tool
    - Overview
    - Customization
    - Implementation
  - Intelligent Process
  - Question and Answer
Security Landscape
Security Landscape

The industry today is more dangerous than ever before

- Today’s threats are evolved and bypass traditional detection measures
  - Increased complexity
  - Increased stealth (bypass FW, IPS, UTM, WCF)
  - Dynamic

- Hactivism is a threat affecting everyone

- Targeted attacks are now common in the industry
  - Attacks leveraging zero-day vulnerabilities
  - Custom malware

- Your industry DOES affect your probability of attack
  - Patterns and attack volume vary significantly between industries (healthcare, energy, finance, etc.)
  - “Intelligence” will help improve your defenses against industry attacks
Intelligence
Intelligence – What is Intelligence?

- Relevant information put into context and in a form that can be acted upon
- Intelligence is derived from data

Most organizations have the data but can not convert it into “intelligence”

- Focusing on intelligence will allow you to add
  - Context to real-time activity
  - Identify and protect yourselves against present and emerging threats
Sources
Sources – Internet

- **Communication**
  - Chat
  - Email
  - News
  - Newsgroup
  - Webcam
  - Webcast
  - Weblog
  - Social Sites

- **Databases**
  - Commerce
  - Education
  - Government
  - Military
  - Organizations

- **Web pages**
  - Commerce
  - Education
  - Government
  - Military

- **Services**
  - Dictionary
  - Directory
  - Downloads
  - Finance
  - Geospatial
  - Search
  - IP Lookup/Who is
  - Technical Support
  - Translation
  - URL Lookup

**Estimated size:**
- Roughly **5 million terabytes**

**Expanding by:**
- **100 terabytes** per month
Sources – Activity in 60 Seconds

- 168m Emails
- 695k FB Status Updates
- 510k FB Comments
- 98k Tweets
- 79k Wall Posts
- 6.6k Pictures
- 1.5k Blog Posts
- 600 Videos
- 1 New Article
Information Collection Tools
Tools – Information Collection

Google Alerts

- Search query: lulzsec
- Result type: Everything
- How often: As-it-happens
- How many: Only the best results
- Deliver to: Feed

Google Alert for today

From: Google Alerts <googlealerts-noreply@google.com>

News  Web

News

Second accused LulzSec hacker arrested in Sony Pictures breach
Reuters
While Rivera was the only person named in the indictment, the FBI said his co-conspirators included Cody Kretsinger, 24, a confessed LulzSec member who pleaded guilty in April to federal charges stemming from his role in the Sony attack. Following the ...
See all stories on this topic ➤

Accused LulzSec Hackers Attended College Together
InformationWeek
Two men who've been arrested on charges that they hacked into the website of Sony Pictures Entertainment and posted stolen data
Tools – Information Collection

- Google Alerts RSS
  - LulzSec shuts down, posts final leak of data
    - Notorious hacking group LulzSec is no more, according to a Pastebin document purportedly posted by the group. However, the group did NOT confirm via...
  - Twitter / bengoldacre: This documentary on lulzsec, ...
    - Instantly connect to what's most important to you. Follow your friends, experts, favorite celebrities, and breaking news.
    - twitter.com/bengoldacre/statuses/2495792453461477585
  - Second accused LulzSec hacker arrested in Sony Pictures breach
    - LOS ANGELES (Reuters) - A second suspected member of the clandestine hacking group LulzSec was arrested on Tuesday on charges he took part in an extensive computer breach of Sony Pictures Entertainment, the FBI said. Raynaldo Rivera, 20, of...
    - See all stories on this topic

- Rich Site Summary
- Really Simple Syndication
Tools – Information Collection

- Silobreaker.com

Sources:
- News
- Blogs
- Web Content
- Press Releases
- Audio/Video
- Reports/Research
Tools – Information Collection

- Silobreaker.com Entity-based Search
Tools – Information Collection

Search results for: Organization:"Anonymous group" AND legion

Entities

<table>
<thead>
<tr>
<th>Entity</th>
<th>Type</th>
<th>~Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>American Legion</td>
<td>Organization</td>
<td>6075</td>
</tr>
<tr>
<td>Légion d'honneur (a.k.a Legion of Honor)</td>
<td>Organization</td>
<td>345</td>
</tr>
<tr>
<td>Royal British Legion</td>
<td>Organization</td>
<td>228</td>
</tr>
<tr>
<td>Royal Canadian Legion</td>
<td>Organization</td>
<td>212</td>
</tr>
<tr>
<td>Legion of Merit</td>
<td>Keyphrase</td>
<td>208</td>
</tr>
<tr>
<td>The Royal British Legion</td>
<td>Organization</td>
<td>94</td>
</tr>
<tr>
<td>French Foreign Legion</td>
<td>Organization</td>
<td>55</td>
</tr>
<tr>
<td>Legion of Christ</td>
<td>Organization</td>
<td>39</td>
</tr>
<tr>
<td>Roman Legion</td>
<td>Keyphrase</td>
<td>7</td>
</tr>
<tr>
<td>Jewish Legion</td>
<td>Keyphrase</td>
<td>5</td>
</tr>
</tbody>
</table>

Anonymous Operation Spain

6:00 PM ET USA Greetings World – Anonymous sends its solidarity to our brothers and sisters in Spain who at this very moment have completely surrounded the Parliament Building in Madrid. They are calling for the resignation of a government that lies... [Published Sep 26 2012 by San Francisco Bay Area Independent Media Center]

Entities: Anonymous group, Spain, Brutality, Madrid, Distributed Denial-of-Service Attack

Doku: We Are Legion – The Story of the Hacktivists

Youtube Direktanons, via Waxy Brian Knappenberger hat seine Anon-Doku „We Are Legion: The Story of the Hacktivists“ komplett online gestellt. Ich habe bisher nur die ersten zehn Minuten gesehen, die sind aber schon ziemlich großartiwig und bei welchem... [Published Sep 24 2012 by Nidore]
Tools – Information Collection

- Silobreaker.com Search Results RSS
Tools – …Collection

Social Media Sources:
- Documents
- Crowdsourced Content
- Wikis
- Video
- Pictures
- Location
- Reputation
- Interest Networks
- Forums
- Social Networks
- Twitter Ecosystem
- Micromedia
- Blog Communities
Tools – Social Information Collection

- Socialmention.com’s 100+ Social Media Sources:

Socialmention*
Real-time social media search and analysis:

Trends: Airline Baby Ban, Vitamin D Study, Blood Sugar, JFK Turtles, Bernard Madoff, Tina Brown, Bathroom Cleaning Tips

Social Media Alerts
Like Google Alerts but for social media.
Receive free daily email alerts of your brand, company, CEO, marketing campaign, or on a developing news story, a competitor, or the latest on a celebrity.

Create an alert

Realtime Buzz Widget
Display realtime buzz on your site or blog.

Get the widget
Tools – Social Information Collection

Top Hashtags

<table>
<thead>
<tr>
<th>Hashtag</th>
<th>Mentions</th>
</tr>
</thead>
<tbody>
<tr>
<td>anonymous</td>
<td>137</td>
</tr>
<tr>
<td>sxsw</td>
<td>8</td>
</tr>
<tr>
<td>25s</td>
<td>8</td>
</tr>
<tr>
<td>docu</td>
<td>5</td>
</tr>
<tr>
<td>hacktivists</td>
<td>5</td>
</tr>
<tr>
<td>legion</td>
<td>5</td>
</tr>
<tr>
<td>ows</td>
<td>4</td>
</tr>
<tr>
<td>expects</td>
<td>4</td>
</tr>
<tr>
<td>spam</td>
<td>4</td>
</tr>
<tr>
<td>idea</td>
<td>2</td>
</tr>
</tbody>
</table>

Mentions about anonymous legion

Sort By: Date Results: Anytime
Results 1 - 15 of 434 mentions.

- **We Are Legion - The Story of the Hacktivists (2012)[FULL DOCUMENTARY]** http://t.co/CLGxwa5n via @liveleak
  anonymous hacktivism
  twitter.com/domineef/statuses/25067789601747968
  6 minutes ago - by @domineef on twitter

- **RT @Anon_Prole: #Colombia_RT @LegionJJ #Anonymous in the streets fighting against the hunger caused by politicians** http://t.co/O4rPXVLL
  twitter.com/iansully/statuses/2508738143632272785
  22 minutes ago - by @iansully01 on twitter

- **We are Anonymous We are Legion We do not Forgive We do not Forget Expect Us.**
  www.facebook.com/profile.php?id=10663331211&v=wall&story_fbid=3870247623798
  1 hour ago - by Namus MfPL on facebook

- **RT @Anne_R_u_Ok: "@Anonymous_SA: Remember, We Are LEGION, WE ARE #ANONYMOUS"** http://t.co/Z9Z64gWq
  twitter.com/Therefore_I_am_/statuses/250555157205778432
  1 hour ago - by @Therefore_I_am_ on twitter
Tools – Social Information Collection

- Socialmention.com RSS:

![Image of FeedDemon Lite 4.1 with an example of social media posts from Operation Anonymous]
Tools – Location-based Collection

Trendsmap Toronto
@TrendsToronto
Real-time local Twitter trends for Toronto
Toronto, Canada http://trendsmap.com/local/ca/toronto

Tweet to Trendsmap Toronto
@TrendsToronto

Tweets
1. Trendsmap Toronto @TrendsToronto
   ‘beckham’ is now trending in #Toronto trendsmap.com/ca/toronto
   Expand

2. Trendsmap Toronto @TrendsToronto
   ‘decreasing’ is now trending in #Toronto trendsmap.com/ca/toronto
   Expand

3. Trendsmap Toronto @TrendsToronto
   ‘grove’ & ‘crescent’ are now trending in #Toronto trendsmap.com/ca/toronto
   Expand

4. Trendsmap Toronto @TrendsToronto
   ‘jamestown’ is now trending in #Toronto trendsmap.com/ca/toronto
   Expand
Tools – Twitter to RSS

- Twittertorss.com
Tools – Twitter to RSS

- Convert Twitter to RSS
Tools – Filter Your RSS

- FeedRinse.com

- http://pipes.yahoo.com/pipes/
Tools – Summary

- Data Aggregators
  - Silobreaker.com
  - Socialmention.com
  - Google.com

- Selected Search Feeds
  - Silobreaker Advance Search
  - Socialmention social media search
  - Google Alerts
  - Trendsmap location based stream

- Feed Convertors
  - twittertorss.com
  - mmmmail.com
  - mailinator.com

- Feed Filters
  - Yahoo Pipes
  - FeedRinse

- Select Feeds
  - Feed burner
  - Google Reader
  - Browser Plugin
Classification
Classification – NewsPet Overview

Configurable RSS feeds
Web-based interface
Automatic Categorization
Ability to re-categorize to train the system

- Michael Fulker
- Tony Hauber
- Tyson Williams

Summary
NewsPet is a news-reader web application that categorizes RSS news items using a trainable engine.
Classification – NewsPet Architecture

User

Network

Django
- Web Application

SQLite
- Database

Java
- Reader/Classifier Service

RSS Feeds

NewsPet

RSS feeds
- $feed_0$
- $feed_1$
- $feed_n$

Categories:
- $category_A$
- $category_B$
- $category_C$
- $category_D$
- trash

MALLET
- machine learning for language toolkit
Classification – NewsPet Overview

- Statistical Natural Language Processing

- Document
  - Classification
  - Clustering
  - Topic Modeling
  - Information extraction
  - Other machine learning applications

- Naïve Bayes
- Maximum Entropy
- Decision Trees

- Named-entity extraction
- Topic models

- http://mallet.cs.umass.edu/
- Andrew McCallum

- Mallet
  - machine learning for language toolkit

- UMass Amherst

- Other machine learning applications
Classification – NewsPet Overview

Naive Bayes classifier using Mallet Library

- Bayes’ Theorem
  - Probabilistic classifier
  - Strong Independence

- Red
- Round
- 4 Inches in Diameter
Classification – NewsPet Categories

Creation of Categories

Manage Categories

- Trash
- External
- Anomalies
- Attacks
- Malware
- Breach
- Industry: SP
- Industry: Finance
- Industry: Media
- Industry: Oil & Gas

Add a Category

Name:

Industry: Health

Category for Initial Categorization:

Industry: Health

Create
Classification – NewsPet Accuracy

The categories = Required training

% Accuracy

# of Training Items

66 categories
30 categories
5 categories
Intelligence Process
Intelligence Process

Internet Sources

Prepared Feeds

Java Process with Artificial Intelligence

5. New Feeds are collected and classified

Intelligence Analyst

0. Maintains Sources

1. Sources are read

Source Research Team

3. Tools serve prepared feeds

4. Server grabs new content

2. Server Polls for RSS

6. Sent for storage

7. Reviews and Corrects

Source Research Team

new content

previously collected
Intel. Process – Analyst Interface

- Review all news that comes in
  - Star important articles
  - Move mislabeled articles to proper categories
  - This enhances the artificial intelligence further

**Categories**
- Un Categorized
- #Security
- #Hackers
- Attack
- Security Watch
- Dormant (5)
- Industry (2)
- -Organizations
- -People (4)
- -Place (9)

**Industry**
mark all as read

**Report: ‘Hacktivism’ on the rise**
from Hacker's groups on Wednesday 28 Mar 2012 15:32

58 percent of all data stolen in 2011 was due to “hacktivism,” according to a recent from Verizon Wireless. Hacktivists are computer hackers that specifically target companies primarily for political reasons. The Verizon 2012 Data Breach Investigations ...

**Hacktivists dominate 2011 data thefts, report says**
from Hacker's groups on Wednesday 28 Mar 2012 15:32

The vast majority of data breaches analyzed in the latest annual report from Verizon were unsophisticated and easily avoidable, and most were carried out against targets of opportunity. This corresponds with the increase in the amount of hacktivism in ...

'Hacktivists' biggest data thieves in 2011: Verizon
Intelligence Process – Correlation

- NewsPet
- Goes to SIEM
- Correlated Alerts are sent to screen
- Analyst II analyses correlation
Intelligence Process – Actionable Results

- Calculated the overall risk to a customer from a particular attack using several vectors.
  - Asset Value
  - Relevance to a particular customers environment
  - Damage Severity
  - Certainty that this will cause damage
  - Mitigating Controls
  - Threat Activity
  - Industry Intelligence
Process – Summary

Data Sources
• Overt
• Covert

Classification
• AI
• Human

Collection
• Aggregators
• Convertors
• Filters

Analysis
• Human

Actionable Intelligence
Process – Mirage Example

- Oil Companies
- Canadian Oil Companies in Philippines
- Telvent Software Company
- CnC is in China
- Spear Phishing
- CNOOC Involved
- November 2012
Questions?

the future is friendly®
References

- Malware Graph
  http://androidspeichern.com/2012/09/gdata-darwinian-evolution-is-transferred-to-computer-viruses/
- Google.com/alerts – Web Service
- News.silobreaker.com – Web Service
- Socialmention.com – Web Service
- FeedRinse.com – Web Service
- Pipes.yahoo.com – Yahoo Pipes
- Microsoft – Infograph
- Intelligence – US Military DoD – Open Source Intelligence
  Fas.org/irp/dodir/army
- Go-Globo.com – Sixty Second Infograph
- Conversation in Social Media Infograph – www..ethroty.de
- Trendsmap.com
- Tittertorss.com
- Naïve Bayes Classifier
  http://en.wikipedia.org/wiki/Naive_Bayes_classifier
- Mallet
  http://mallet.cs.umass.edu/
- NewsPet
  http://code.google.com/p/news-pet/
- NewsPet Accuracy Graph – NewsPet documentation
- Intellectual Data and Research – Telus.com
- Mailinator.com
- Mmmmail.com