Insider Threat Visualization

Raffael Marty, GCIA, CISSP
Chief Security Strategist @ Splunk

Hack In The Box - September 07 - Malaysia
Who Am I?

- Chief Security Strategist and Product Manager @ Splunk
- Manager Solutions @ ArcSight, Inc.
- Intrusion Detection Research @ IBM Research
  - [http://thor.cryptojail.net](http://thor.cryptojail.net)
- IT Security Consultant @ PriceWaterhouse Coopers
- Open Vulnerability and Assessment Language (OVAL) board
- Common Event Enumeration (CEE) founding member
- Passion for Visualization
Agenda

- Convicted
- Visualization
- Log Data Processing
  - Data to Graph
  - AfterGlow and the Splunk Integration
- Insider Threat Visualization
- Insider Detection Process
  - Precursors
  - Scoring
  - Watch Lists
- Visual Conviction
Convicted

In February of 2007 a fairly large information leak case made the news. The scientist Gary Min faces up to 10 years in prison for stealing 16,706 documents and over 22,000 scientific abstracts from his employer DuPont. The intellectual property he was about to leak to a DuPont competitor, Victrex, was assessed to be worth $400 million. There is no evidence Gary actually turned the documents over to Victrex.
DuPont Case
How It Could Have Been Prevented

What’s the answer?
DuPont Case
More Generic Solution
Visualization - Questions

• Who uses visualization for log analysis?
• Who is using visualization?
• Who is using AfterGlow?
• Have you heard of SecViz.org?
• What tools are you using for log processing?
Visualization

Answer questions you didn’t even know of

Increase Efficiency
✓ Quickly understand thousands of data entries
✓ Facilitate communication
✓ Increase response time through improved understanding

Make Informed Decisions
Insider Threat Visualization

• Huge amounts of data
• More and other data sources than for the traditional security use-cases
• Insiders often have legitimate access to machines and data. You need to log more than the exceptions.
• Insider crimes are often executed on the application layer. You need transaction data and chatty application logs.
• The questions are not known in advance!
• Visualization provokes questions and helps find answers.
• Dynamic nature of fraud
• Problem for static algorithms.
• Bandits quickly adapt to fixed threshold-based detection systems.
• Looking for any unusual patterns
Visualizing Log Data

Jun 17 09:42:30 rmarty ifup : Determining IP information for eth0...
Jun 17 09:42:35 rmarty ifup :  failed; no link present. Check cable?
Jun 17 09:42:38 rmarty network: Bringing up interface eth0:  failed
Jun 17 09:42:38 rmarty sendmail :  sendmail shutdown succeeded
Jun 17 09:42:39 rmarty sendmail :  sendmail startup  succeeded
Jun 17 09:42:39 rmarty sendmail :  sm-client  shutdown  succeeded
Jun 17 09:42:39 rmarty sendmail :  sm-client startup  succeeded
Jun 17 09:43:39 rmarty vmmnet-dhcpd : DHCPOFFER from 172.16.48.128
Jun 17 09:45:42 rmarty last message repeated 2 times
Jun 17 09:45:47 rmarty vmmnet-dhcpd : DHCPIFORM from 172.16.48.128
Jun 17 09:56:02 rmarty vmmnet-dhcpd : DHCPDISCOVER from 00:0c:29:b7:b2:47 via vmmnet8
Jun 17 09:56:03 rmarty vmmnet-dhcpd : DHCPOFFER on 172.16.48.128 to 00:0c:29:b7:b2:47 via vmmnet8

✓ Interpret Data
✓ Knows Data Formats
✓ Re-use don’t re-invent
✓ Find some at: http://secviz.org/?q=node/8
Charts - Going Beyond Excel

• Multi-variate graphs
  - Link Graphs
  - TreeMaps
  - Parallel Coordinates
Beyond The Boring Defaults For Link Graphs
Link Graph Shake Up

[**] [1:1923:2] RPC portmap UDP proxy attempt [**]

[Classification: Decode of an RPC Query] [Priority: 2]

06/04-15:56:28.219753 192.168.10.90:32859 ->

192.168.10.255:111

UDP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:148

192.168.10.90 portmap 192.168.10.255 192.168.10.90 192.168.10.255 111 Len: 120

192.168.10.90  32859  111  RPC portmap 192.168.10.90 192.168.10.12
TreeMaps

What is this?
TreeMaps Explained

Configuration Hierarchy: Protocol -> Service

- UDP
- DNS
- SNMP
- TCP
- HTTP
- SSH
- FTP

80%

20%

Size: Count
Color: Service
Generating Graphs - For Free

• Log Collection
  - Database
  - Files
  - Syslog Collector
  - Splunk

• Graphing
  - AfterGlow (http://afterglow.sourceforge.net)
  - Treemap2 (http://www.cs.umd.edu/hcil/treemap)
digraph structs {
  graph [label="AfterGlow 1.5.8", fontsize =8];
  node [shape=ellipse, style=filled,
      fontsize =10, width=1, height=1, fixedsize =true];
  edge [len =1.6];
  "aaelenes" -> "Printing Resume";
  "abbe" -> "Information Encryption";
  "aanna" -> "Patent Access";
  "aatharuy" -> "Ping";
}
Why AfterGlow?

• Translates CSV into graph description
• Define node and edge attributes
  - color
  - size
  - shape
• Filter and process data entries
  - threshold filter
  - fan-out filter
  - clustering

```plaintext
# Variable and Color
variable=@violation=("Backdoor Access", "HackerTool Download");
color.target="orange" if (grep(/$fields[1]/,@violation));
color.target="palegreen"

# Node Size and Threshold
maxnodesize=1;
size.source=$fields[2]
size=0.5
sum.target=0;
threshold.source=14;

# Color and Cluster
color.source="palegreen" if ($fields[0] =~ /^111/) color.source="red"
color.target="palegreen"
cluster.source=regex_replace("(\d+)\d+").
```
What’s Splunk?

1. Universal Real Time Indexing
2. Ad-hoc Search & Navigation
3. Distributed / Federate Search
4. Interactive Alerting & Reporting
5. Knowledge Capture & Sharing

The IT Search Engine
AfterGlow - Splunk

./splunk <command>
./splunk search "<search command>" -admin <user>::<pass>

./splunk search "ipfw | fields + SourceAddress DestinationAddress DestinationPort | afterglow" -auth admin:changeme
Insider Threat Definition

"Current or former employee or contractor who

• intentionally exceeded or misused an authorized level of access to networks, systems or data in a manner that

• targeted a specific individual or affected the security of the organization’s data, systems and/or daily business operations"

Three Types of Insider Threats

**Fraud** deals with the misuse of access privileges or the intentional excess of access levels to obtain property or services unjustly through deception or trickery.

**Information Theft** is concerned with stealing of confidential or proprietary information. This includes things like financial statements, intellectual property, design plans, source code, trade secrets, etc.

**Sabotage** has to do with any kind of action to harm individuals, organizations, organizational data, systems, or business operations.
Insider Threat Detection

• Understand who is behind the crime.
• Know what to look for.
• Stop insiders **before** they become a problem.

• Use *precursors* to monitor and profile users.
• Define an insider detection process to analyze precursor activity.
## Insider Detection Process

- **Build List of Precursors**
- **Assign Scores to Precursors**

<table>
<thead>
<tr>
<th>Action</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accessing job Web sites such as monster.com</td>
<td>1</td>
</tr>
<tr>
<td>Sales person accessing patent filings</td>
<td>10</td>
</tr>
<tr>
<td>Printing files with &quot;resume&quot; in the file name</td>
<td>5</td>
</tr>
<tr>
<td>Sending emails to 50 or more recipients outside of the company</td>
<td>3</td>
</tr>
</tbody>
</table>
Insider Detection Process

• **Build List of Precursors**
• **Assign Scores** to Precursors
• **Apply Precursors** to Log Files

Aug 31 15:58:06 [68] cmd "loginwindow" (0x5c07) set hot key operating mode to all disabled
Aug 31 15:58:06 [68] Hot key operating mode is now all disabled
Apr 04 19:45:29 rmarthy Privoxy(b65ddba0) Request:
www.google.com/search?q=password+crack
Insider Detection Process

• Build List of Precursors
• Assign **Scores** to Precursors
• Apply Precursors to Log Files
• Visualize Insider Candidate List
Insider Detection Process

- Build List of Precursors
- Assign **Scores** to Precursors
- Apply Precursors to Log Files
- Visualize Insider Candidate List
- Introduce User Roles
Insider Detection Process

- Build List of Precursors
- Assign Scores to Precursors
- Apply Precursors to Log Files
- Visualize Insider Candidate List
- Introduce User Roles
- Where Did the Scores Go?
Tiers of Insiders

- Nothing to worry about just yet
- On a bad track of going malicious
- Very likely has malicious intentions
- Malicious Insiders

Scale:
- 0
- 20
- 60
- 80
- 100
The Insider? Finally?

Big, dark areas!
Thank You

www.secviz.org
rafael.marty@splunk.com