Advanced Persistent Threats - Detection and Countermeasure

Gaspar Modelo-Howard, Christopher Gutierrez
Dependable Computing Systems Lab (DCSL)

Agenda

1. Introduction to Advanced Persistent Threats
   – Sherlock Holmes and The Case of the Advanced Persistent Threat [Juels, LEET 2012]

2. Attacks Phases
   – Social Engineering
   – Command and Control
   – Lateral Movement
   – Data Exfiltration

3. Case Study
   – Stuxnet [Symantec Report, 2011]
Sherlock Holmes and the Case of the Advanced Persistent Threat

Ari Juels, Ting-Fang Yen
Usenix LEET 2012

In The News
In The News

RSA SecurID (2011)

RSA SecurID Hack Shows Danger of APTs

By Tony Bowness, PCWorld

May 16, 2011 11:10 AM

RSA revealed in an open letter posted to its website that it has been the target of an attack, and that data may have been compromised. The attack against the RSA network is an example of a so-called advanced persistent threat (APT), flying under the radar and going after bigger prey.

RSA describes the attack as an advanced persistent threat (APT). The "APT" acronym, CTO of RSA, announced that APTs represent a significant change in the security landscape. An APT attack involves patient, skilled, well-funded attackers going after the really big...
What is an APT?

- Advanced
  - Operates in the full spectrum of computer intrusion
  - Involves 0-day attacks
- Persistent
  - Maintains presence
  - Targeted
- Threat
  - Well-resourced, organized, motivated

Is This New?

<table>
<thead>
<tr>
<th></th>
<th>Traditional Attackers</th>
<th>APT</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Means of exploitation</strong></td>
<td>Software vulnerabilities, social engineering</td>
<td>Espionage, intellectual property theft</td>
</tr>
<tr>
<td><strong>Objective</strong></td>
<td>Spam, DoS attack, identity theft</td>
<td>Espionage, intellectual property theft</td>
</tr>
<tr>
<td><strong>Motive</strong></td>
<td>Fame, Financial gain</td>
<td>Military, political, technical</td>
</tr>
<tr>
<td><strong>Target</strong></td>
<td>Machines with certain configurations</td>
<td>Users</td>
</tr>
<tr>
<td><strong>Scope</strong></td>
<td>Promiscuous</td>
<td>Specific</td>
</tr>
<tr>
<td><strong>Timing</strong></td>
<td>Fast</td>
<td>Slow</td>
</tr>
<tr>
<td><strong>Control</strong></td>
<td>Automated malware</td>
<td>Manual intervention</td>
</tr>
</tbody>
</table>
How does it Work?

- An APT isn’t a playbook, it’s a campaign.

Possibilities

- The Adventures of the Red Headed League
  - Deception Strategy: encompass a victim in a general event that conceals a targeted attack
• The Adventure of the Blue Carbuncle
  – Deception Strategy: Conceal unauthorized communications within commonplace objects or activities

Possibilities

• A Scandal in Bohemia
  – Create disturbances to the victim to obtain intelligence about a target resource
  – Recommended responses to a breach can reveal
    • Location of valuables
    • Critical services
    • What you know about the attack
Possibilities

• The Adventure of the Speckled-Band
  – Deception Strategy: Breach a security perimeter through unconventional means

Possibilities

• Other ropes and ventilators
  – Infected digital photo frames
  – Infected mobile phones
  – Bluetooth vulnerabilities
  – Compromised device drivers
  – The locked-room illusion
Conclusions

• APT is a campaign
• Necessary to expand definition of APTs
  – No formula or playbook of tactics
  – Necessary to include 0-day attacks
• How about detection?
  – Behavior profiling
  – Defensive deception
  – Information sharing

Modeling User Search Behavior for Masquerade Detection

Malek Ben Salem, Salvatore Stolfo
RAID 2011
Introduction

• Masquerade attack
  – A user of a system illegitimately poses as, or assumes the identity of another legitimate user

• Assumption
  – Masquerader doesn’t attempt to escalate the privileges of the stolen identity, simply accesses whatever the victim can access

• Conjecture
  – Masquerader is unlikely to have the depth of knowledge of the victim’s machine
  – Likely first engage then in info gathering and search activities

Objective and Approach

• Uses 1-class maximal marginal classifier (SVM) to develop behavior models
  – No need to define a priori what masquerader behavior looks like

<table>
<thead>
<tr>
<th>Method</th>
<th>True Pos. (%)</th>
<th>False Pos. (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uniqueness</td>
<td>39.4</td>
<td>1.4</td>
</tr>
<tr>
<td>Bayes one-step Markov</td>
<td>49.3</td>
<td>6.7</td>
</tr>
<tr>
<td>Hybrid multi-step Markov</td>
<td>59.3</td>
<td>3.2</td>
</tr>
<tr>
<td>Compression</td>
<td>34.2</td>
<td>5.0</td>
</tr>
<tr>
<td>Sequence Match</td>
<td>26.8</td>
<td>3.7</td>
</tr>
<tr>
<td>IPAM</td>
<td>41.1</td>
<td>2.7</td>
</tr>
<tr>
<td>Naive Bayes (w. Updating)</td>
<td>61.5</td>
<td>1.3</td>
</tr>
<tr>
<td>Naive Bayes (No Upd.)</td>
<td>66.2</td>
<td>4.6</td>
</tr>
<tr>
<td>Semi-Global Alignment</td>
<td>75.8</td>
<td>7.7</td>
</tr>
<tr>
<td>Sequence Alignment (w. Upd.)</td>
<td>68.6</td>
<td>1.9</td>
</tr>
<tr>
<td>Eigen Co-occurrence Matrix</td>
<td>72.3</td>
<td>2.5</td>
</tr>
</tbody>
</table>
Datasets Collection

- Host Sensor
  - Monitors registry-based activity, process creation and destruction, windows GUI and file accesses, DLL libraries’ activity
- Normal User Data
  - 18 students / > 10 GBytes / ~4 days / ~500K records per user
- Simulated Masquerader Data
  - Independent variable: intent to steal information
  - 60 students, 3 groups (malicious, benign, neutral)

User Study Experiment (1)

- Objective: provide evidence for conjecture that masquerader’s intent has a significant effect on her search behaviour
- Three features were extracted
  - Number of files touched during an epoch of two minutes
  - Number of automated search-related actions initiated by masquerader
  - Percentage of manual search actions during same epoch
User Study Experiment (2)

- Distribution of number of accesses to all files residing on the file system per a 2-minute epoch

User Study Experiment (3)

- Distribution of search-related queries to the registries and accesses to search-related DLLs and applications
User Study Experiment (4)
- Distribution of the Percentage of File System navigation User Actions

User Study Experiment (5)
- Distribution of the Percentage of File System navigation User Actions
RUU Experiment

- Objective: model normal user search behavior and use it to detect masqueraders
- Training set: normal user data (80%)
- Testing set: simulated masquerader data

Detection Accuracy Evaluation (1)

- False positives rate is significantly reduced compared to the application frequency-based modeling approach
  - Frequency of applications and processes within the 2-min epoch as features for ocSVM model
  - Monitoring file access and fetching patterns proved to be most effective feature

<table>
<thead>
<tr>
<th>Method</th>
<th>True Pos. (%)</th>
<th>False Pos. (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search-behavior ocSVM</td>
<td>100</td>
<td>1.1</td>
</tr>
<tr>
<td>App.-freq. ocSVM</td>
<td>90.2</td>
<td>42.1</td>
</tr>
</tbody>
</table>
Detection Accuracy Evaluation (2)

- Comparison of ROC curves using AUC scores
  - Each user has her own model with its own detection threshold

![AUC Comparison By User](image)

**Fig. 3.** AUC Scores By User for the Search Behavior and Application Frequency-Based Modeling Approaches using One-Class Support Vector Machines

Conclusions

- Use of search behavior profiling for masquerade attack detection permits limiting the range and scope of the user profiles
  - Limits potentially large sources of prediction errors
- Insight that a masquerader is likely to perform untargeted and widespread search
  - TP: 100%, FP: 1.1% for RUU dataset
- Limitations
  - Attacker’s ignorance of victim’s behavior
  - Copy of data using USB drive
References

- Ben Salem, M., Stolfo, S. Modeling User Search Behavior for Masquerade Detection. RAID 2011