Advanced Persistent Threats - Detection and Countermeasure

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

PURDUE UNIVERSITY

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]

- Stegobot: A Covert Social Network Botnet [Nagaraja, Houmansadr, Agarwal, Kumar, Borisov, IH 2011]

PURDUE UNIVERSITY

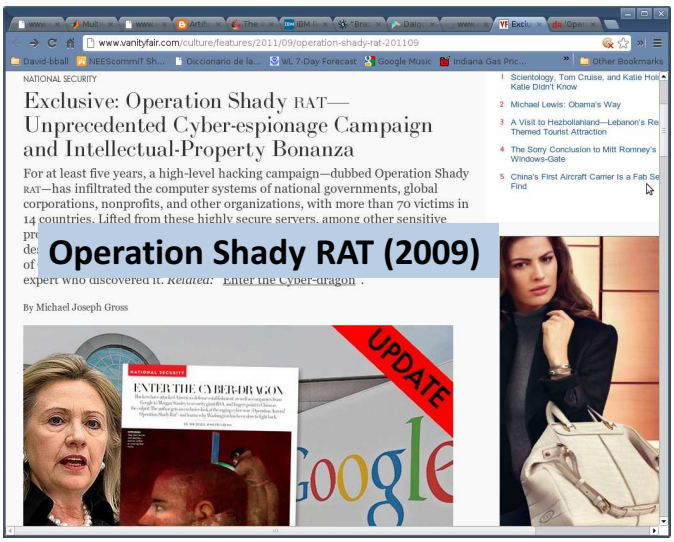
Sherlock Holmes and the Case of the Advanced Persistent Threat

Ari Juels, Ting-Fang Yen

Usenix LEET 2012

PURDUE UNIVERSITY

In The News



PURDUE UNIVERSITY

In The News

Slide 5

PURDUE UNIVERSITY

In The News

Slide 6

PURDUE UNIVERSITY

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

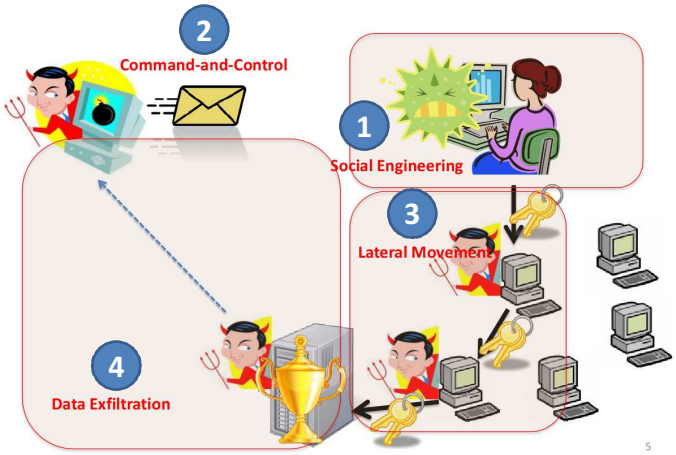
PURDUE UNIVERSITY

Is This New?

	Traditional Attackers	APT
Means of exploitation	Software vulnerabilities, social engineering	
Objective	Spam, DoS attack, identity theft	Espionage, intellectual property theft
Motive	Fame, Financial gain	Military, political, technical
Target	Machines with certain configuations	Users
Scope	Promiscuous	Specific
Timing	Fast	Slow
Control	Automated malware	Manual intervention

PURDUE UNIVERSITY

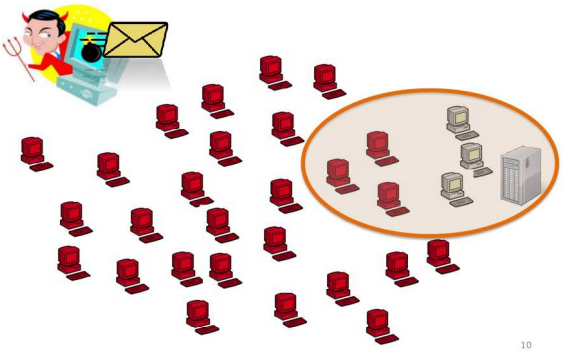
How does it Work?



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

Possibilities

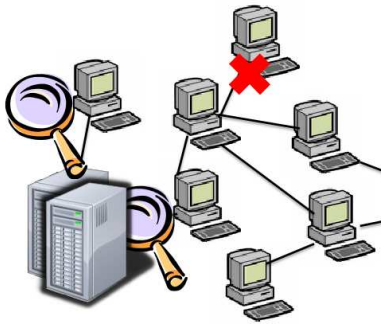
- The Adventures of the Red Headed League
  - Deception Strategy: encompass a victim in a general event that conceals a targeted attack



- The Adventure of the Blue Carbuncle
  - Deception Strategy: Concel 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

PURDUE UNIVERSITY

Possibilities

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

PURDUE UNIVERSITY

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

PURDUE UNIVERSITY

Modeling User Search Behavior for Masquerade Detection

Malek Ben Salem, Salvatore Stolfo

RAID 2011

PURDUE UNIVERSITY

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 classificer (SVM) to develop behavior models
  - No need to define a priori what masquerader behavior looks like

Table 1. Summary of Accuracy Performance of Anomaly Detectors Using the Schonlau Data Set

Method	True Pos. (%)	False Pos. (%)
Uniqueness [15]	39.4	1.4
Bayes one-step Markov [15]	69.3	6.7
Hybrid multi-step Markov [15]	49.3	3.2
Compression [15]	34.2	5.0
Sequence Match [8,15]	26.8	3.7
IPAM [6,15]	41.1	2.7
Naïve Bayes (w. Updating) [10]	61.5	1.3
Naïve Bayes (No Upd.) [10]	66.2	4.6
Semi-Global Alignment [4]	75.8	7.7
Sequence Alignment (w. Upd.) [5]	68.6	1.9
Eigen Co-occurrence Matrix [12]	72.3	2.5

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: intente to steal information
  - 60 students, 3 groups (malicious, benign, neutral)

PURDUE UNIVERSITY

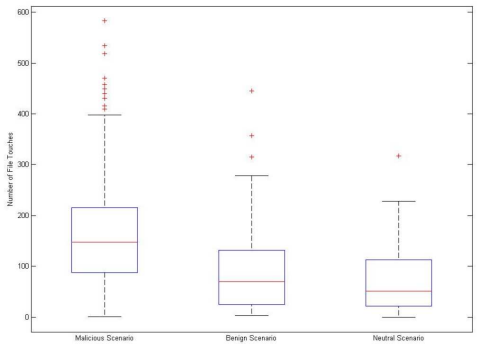
User Study Experiment (1)

- 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

PURDUE UNIVERSITY

User Study Experiment (2)

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

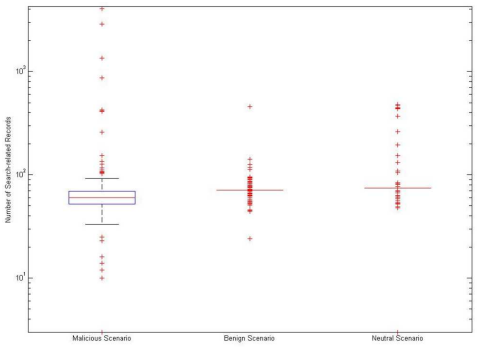


Slide 21

PURDUE UNIVERSITY

User Study Experiment (3)

- Distribution of search-related queries to the registries and accesses to search-related DLLs and applications

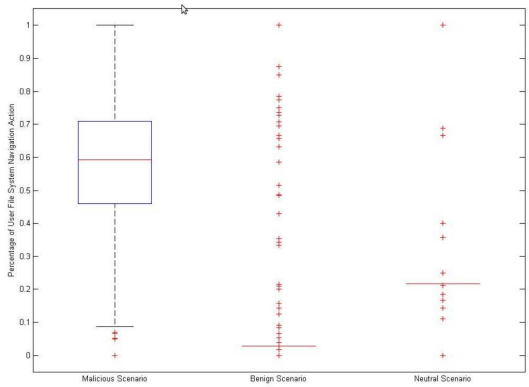


Slide 22

PURDUE UNIVERSITY

User Study Experiment (4)

- Distribution of the Percentage of File System navigation User Actions

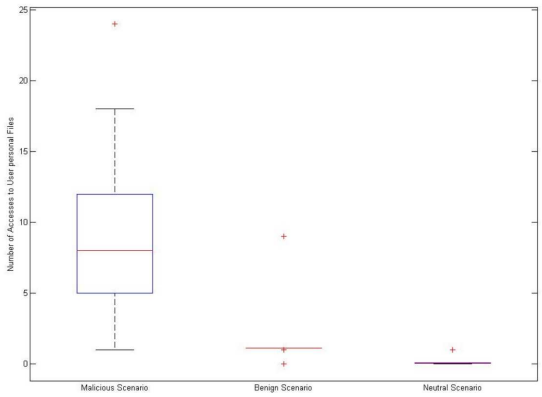


Slide 23

PURDUE UNIVERSITY

User Study Experiment (5)

- Distribution of the Percentage of File System navigation User Actions



Slide 24

PURDUE UNIVERSITY

RUU Experiment

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

PURDUE UNIVERSITY

Detection Accuracy Evaluation (1)

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

Table 2. Experimental results of ocSVM modeling approaches using search-behavior related features and application frequency features

Method	True Pos. (%)	False Pos. (%)
Search-behavior ocSVM	100	1.1
App.-freq. ocSVM	90.2	42.1

PURDUE UNIVERSITY

Detection Accuracy Evaluation (2)

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

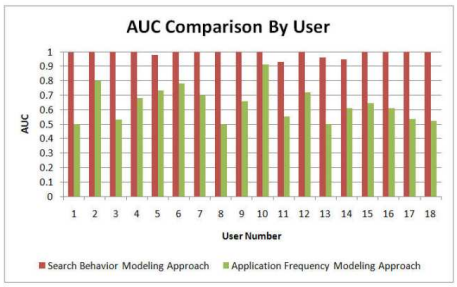


Fig. 3. AUC Scores By User for the Search Behavior and Application Frequency-Based Modeling Approaches using one-Class Support Vector Machines

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

- Juels, A., Yen, T. Sherlock Holmes and The Case of the Advanced Persistent Threat. Usenix LEET 2012
- Altshuler, Y., Aharony, N., Pentland, A., Elovici, Y., Cebrian, M. Stealing Reality: When Criminals Become Data Scientists (or viceversa). IEEE Intelligent Systems. 2011
- Bind, B., McRee, R., O'Connor, T. Assessing Outbound Traffic to Uncover Advanced Persistent Threat. The SANS Institute. 2011
- Ben Salem, M., Stolfo, S. Modeling User Search Behavior for Masquerade Detection. RAID 2011
- Maloof, M., Stephens, G. ELICIT: A System for Detection Insiders Who Violate Need-to-Know. RAID 2007