Insiders: The Threat is Already Within

Shiri Margel & Itsik Mantin
June 2016
About us

• Shiri Margel
  • Data Security Research Team Leader
  • M. Sc. in Applied Math and Computer Science from the Weizmann Institute

• Itsik Mantin
  • Director of Security Research
  • M. Sc. in Applied Math and Computer Science from the Weizmann Institute
Agenda

• Introduction
• Behavioral Analysis
• Deception
• Summary
People are the WEAK LINK
Compromised  Careless  Malicious
The Nature of Insider Breach

- Acquire small amount of sensitive information over a long period of time
- Noticed after damaging events
- Almost impossible to prevent

Verizon DBIR 2016
Our Research

- Behavioral Analysis
- Deception
Our Research

- Behavioral Analysis
- Deception
Our Research – Behavioral Analysis

- Collect live production data from several customers of Imperva
- Full database and file server audit trail - SecureSphere audit logs
- Machine learning algorithms identify “Actors” and “Good Behavior” in order to identify “Meaningful Anomalies”
Actors
Good Behavior
Behavioral Analysis Findings

- Malicious Insider
- Negligent Insider
- Compromised Insider
Behavioral Analysis Findings

- **Malicious Insider**
  - Hoarding IP before leaving the company
  - A DBA accessed financial information

- **Negligent Insider**
- **Compromised Insider**
Malicious Insider: Behavioral Analysis finds the IP Hoarder

- A Technical Writing employee copied > 100,000 files
- Employee was authorized to access data
- Operation took 3 weeks
- Each copy contained a few thousand files
- Some copies - in the middle of the night and/or on the weekend
Malicious Insider: Behavioral Analysis finds the IP Hoarder

- The employee / department never copied this amount of files
- The employee never worked on weekends / middle of the night

Figure 1: Number of files accessed by user in a week
Malicious Insider: Behavioral Analysis finds the IP Hoarder

- The employee / department never copied this amount of files
- The employee never worked on weekends / middle of the night

Employee was authorized to access data
Malicious Insider: Behavioral Analysis finds the IP Hoarder

Organization Feedback:

• The employee was planning to leave the organization shortly after the incident took place
Behavioral Analysis Findings

- **Malicious Insider**
  - Hoarding IP before leaving the company
  - A DBA accessed financial information

- **Negligent Insider**

- **Compromised Insider**
Malicious Insider: Behavioral Analysis flags DBA abusing privileges
A DBA from IT retrieved and modified multiple records from PeopleSoft application tables on a specific day.

- Didn’t access these tables through the PeopleSoft interface
  → bypassed PeopleSoft logging and retrieval limitations
Malicious Insider: Behavioral Analysis flags DBA abusing privileges

- Retrieved many records

Compared to other users -

Compared to himself -
Malicious Insider: Behavioral Analysis flags DBA abusing privileges

- Modified several thousands of records in one table
- The tables contained sensitive financial information
Malicious Insider: Behavioral Analysis flags DBA abusing privileges

• Modified several thousands of records in one table
• The tables contained sensitive financial information

Should a DBA access financial information ???
Malicious Insider: Behavioral Analysis flags DBA abusing privileges

**Organization Feedback:**

- A DBA from IT should never be exposed to financial information
- Certainly not modify this information outside of application processes
Behavioral Analysis Findings

- Malicious Insider
- Negligent Insider
  - Account Sharing
- Compromised Insider
Negligent Users: Behavioral Analysis flags Account Sharing

- Bypass organization permissions and privileges
- Provide people with access that they are not entitled to
- Leave incorrect access trail to the data

• **Sharing is not caring!**
Negligent Users: Behavioral Analysis flags Account Sharing

- A and B share privileges
- C and D use B’s account
- H uses the accounts of E, G
- J uses the accounts of G, I
- L uses the account of K
Behavioral Analysis Findings

- Malicious Insider
- Negligent Insider
- **Compromised Insider**
  - Multiple failed login attempts
Compromised Users: How failed logins are flagged as anomalous

<table>
<thead>
<tr>
<th></th>
<th>Baseline</th>
<th>Day of incident</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Successful logins</td>
<td>Failed logins</td>
</tr>
<tr>
<td>DB1 (user's normal DB)</td>
<td>1,954</td>
<td>6</td>
</tr>
<tr>
<td>DB2 (anomalous DB for this user)</td>
<td>3</td>
<td>1</td>
</tr>
</tbody>
</table>

- **Baseline period**
  - the user always successfully logs into DB1 using “red” account
  - never logs into DB2
- **On the day of the incident**
  - the user tried and failed to log into DB2 11 times using 4 different account
  - Succeeded using 5\(^{th}\) account
Behavioral Analysis - Summary
Behavioral Analysis - Summary

- We found interesting incidents for all insiders options
- It was hard to find them without behavioral analysis methods
  - Used valid privileges
  - Chose “meaningful” anomalies
- Concentrated on the **actors** and on their access to the **data**
Our Research

- Behavioral Analysis
- Deception
Deception Why?

• Because **Compromise is Inevitable**
  – No Perimeter: BYOD, Cloud Apps, VPN
  – Legitimate apps (TeamViewer, DropBox)
  – Zero Days
  – Social Engineering

• Find **Data Breach within Compromises**
  – Compromises happen all the time… **few** of them may turn into a breach!
  – Response team have to prioritize
  – **100 alerts << 1 alert**

• **Detect** a breach **ASAP**
  – Reconnaissance & Lateral Movement
Attack Cycle

• Compromise
  • Reconnaissance
  • Lateral Movement
• Data Access
• Exfiltration

Files
Web Apps
Databases
Data Center
Deception Tokens

• **Point** the attacker towards a **Trap**
  – Web, File, DB Server (etc)
  – Local / Domain Account
  – Passwords, Cookies, Authentication Tokens

• **Trap Server is Real**
  – Not a Honeypot

• **Detection** = Harvest + Use token
  – Deliberate attempt at the data center / gain more privileges
Using Sensors for Deception

File Sensors
File Server

Database Sensors
Databases

Cloud App Sensors
Cloud Applications

The Perimeter
Browser Passwords

• Where are autocomplete passwords saved?

• Are they safe?
Browser Passwords

WebBrowserPassView v1.75
Copyright (c) 2011 - 2016 Nir Sofer

See Also

- Recover deleted files on Mac & Windows - Desk Drill recovers your lost data and protects your storage media from future data loss.
- Windows Password Recovery Tools
- Saved Password Locations For Popular Windows Applications
- BrowsingHistoryView - View browsing history of your Web browsers.

Description

WebBrowserPassView is a password recovery tool that reveals the passwords stored by the following Web browsers: Internet Explorer (Version 4.0 - 11.0), Mozilla Firefox (All Versions), Google Chrome, Safari, and Opera. This tool can be used to recover your lost/forgotten password of any Website, including popular Web sites, like Facebook, Yahoo, Google, and Gmail, as long as the password is stored by your Web Browser.

After retrieving your lost passwords, you can save them into text/html/csv/xml file, by using the 'Save Selected Items' option (Ctrl+S).
MimiKatz

- Pulling plaintext passwords from Windows
- Relies on Wdigest interface through LSASS

- Wdigest: a DLL used to authenticate users against HTTP Digest authentication and Simple Authentication Security Layer (SASL) exchanges.

- (un)fortunately, these require the plain-text password
Compromised User Scenario

- Trojan got through to the endpoint via phishing
- Planted credentials inside Windows Vault, Internet Explorer were used
- Determine the source and scope of the attack without tipping off the attacker

*Figure 5: Example of credential dumps*