Learnings from the Cloud: What to Watch When Watching for Breach

Sara Manning Dawson
Principle Group Program Manager, Office 365 Security
Microsoft Corporation
We will shed light on

- What are common attack patterns?
- How do I watch for them?
- How do I protect myself and my organization?
Foot In
Phish ➔ Identity Theft ➔ Fraud

URL to Attachment
URL to Credential Theft
Malware In Attachment
URL to Malware

Keep people safe
You are receiving this email because you have signed up for BECU online eStatements. Your monthly BECU eStatement is now available. To protect you from email phishing, direct links to our website are not provided within this email. To view your eStatement, visit the BECU website and login to your Online Banking account.

Use Cloud Tooling
SPF, DMARC, DKIM, EXTERNAL
Account Access = Keys To The Kingdom

Permissions

Trust

Goodwill

What To Do About It

MFA

PKI, Hardware

PKI, Biometrics
Organization Attacks: Case Study #1

- **Initial Breach**
  - Phishing email from consumer email provider
  - “invoice.doc” embedded malware

- **Method**
  - Targeted initial breach, likely researched. Account creds dumped to C2.
  - Exec admin account used to send invoice.doc malware to rest of company, expanding account breach.
  - Spoofed email sent to CFO from CEO asking for bank transfer
  - Hmmm...Discovery point by CFO

- **Impact**
  - Nearly successful whaling attempt with potential **high five figure** loss.
Organization Attacks: Case Study #2

- **Initial Breach**
  - Cred harvesting (likely through spoofed login page)

- **Method**
  - Attacker created shadow admin account, used to create regular user account. Cleaned up.
  - Granted delegate perms to payables clerk account, created mail forwarding rules to external domain.
  - Gathered intelligence on accounting and downstream payments.
  - Spoofed downstream supplier from external domain, asked for bank routing update.
  - Six weeks of $30K+ weekly, before actual downstream supplier asked about missing payment.

- **Impact**
  - **Six figure** loss.
  - Customer reputation impact
Organization Attacks

Phishing is the “foot in”
90% of the time

Attackers take time to
learn financial processes

FADS
aren’t just a fad

Audit FADS

Assessment and Monitoring

What To Do About It
Malicious Insiders

### In Practice

<table>
<thead>
<tr>
<th>Industry</th>
<th>Ideology</th>
<th>Financial</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Analytic Indicator Category

- **Social**
  - Disregard
  - Personal Inflexibility
  - Unusual Business Travel
  - Unusual Personal Travel
  - Unauthorized or Inappropriate Associations
  - Withdrawal
  - Workplace Events
  - Workplace Satisfaction

- **Health**
  - Mental Instability
  - Impulsive Control

- **Human Resources**
  - Major Life Events
  - Complaints Against the User
  - Negative Reviews

#### Content-Based Analytics

<table>
<thead>
<tr>
<th>Indicator</th>
<th>Attack Types</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Accidental</td>
</tr>
<tr>
<td></td>
<td>Espionage</td>
</tr>
<tr>
<td></td>
<td>Financial</td>
</tr>
<tr>
<td></td>
<td>Fraud</td>
</tr>
<tr>
<td></td>
<td>Misuse</td>
</tr>
<tr>
<td></td>
<td>Opportunity</td>
</tr>
<tr>
<td></td>
<td>Data Theft</td>
</tr>
<tr>
<td></td>
<td>Physical</td>
</tr>
<tr>
<td></td>
<td>Theft</td>
</tr>
<tr>
<td></td>
<td>Product</td>
</tr>
<tr>
<td></td>
<td>Alteration</td>
</tr>
<tr>
<td></td>
<td>Sabotage</td>
</tr>
<tr>
<td></td>
<td>Violence</td>
</tr>
</tbody>
</table>

#### Inferential Analytics

<table>
<thead>
<tr>
<th>Indicator</th>
<th>Attack Types</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Accidental</td>
</tr>
<tr>
<td></td>
<td>Espionage</td>
</tr>
<tr>
<td></td>
<td>Financial</td>
</tr>
<tr>
<td></td>
<td>Fraud</td>
</tr>
<tr>
<td></td>
<td>Misuse</td>
</tr>
<tr>
<td></td>
<td>Opportunity</td>
</tr>
<tr>
<td></td>
<td>Data Theft</td>
</tr>
<tr>
<td></td>
<td>Physical</td>
</tr>
<tr>
<td></td>
<td>Theft</td>
</tr>
<tr>
<td></td>
<td>Product</td>
</tr>
<tr>
<td></td>
<td>Alteration</td>
</tr>
<tr>
<td></td>
<td>Sabotage</td>
</tr>
<tr>
<td></td>
<td>Violence</td>
</tr>
</tbody>
</table>

Mistaken Insiders

Sharing

Sending

Syncing

Saving

What To Do About It

Retention and Deletion

Device and App Management

DLP
Attacks on a Cloud Service

**BIGGER SURFACE AREA but FEWER VECTORS**

Lean and Automated = minimal human interaction

Control and Uniformity in code execution and communications stack

Difficult to target at scale: 100,000’s of machines

In TheorY

Espionage via Judicial Systems

In Practice

blogs.microsoft.com/on-the-issues
It’s all about the money, honey
Invest in account and identity protection
Watch for FADS
Mind your inner “Hmm...”
Stay Safe

- **Account Breach**

- **Phishing**

- **Protect Identity through FIDO**
  - [https://fidoalliance.org](https://fidoalliance.org)

- **Asses and Protect yourself in Office 365**
  - [https://securescore.office.com/](https://securescore.office.com/)

- **Ransomware**