Identifying Targeted Attacks

Six Tell-Tale Signs

PRESENTED BY:  Matt Hastings  

AUGUST 19, 2014
Introductions

Matt Hastings

- Consultant
- 2.5 years with Mandiant
- Incident Response
  - Financial crime
  - APT
- Penetration Testing
Agenda

- Threat actors
- Targeted attack life cycle
- Six ways to identify targeted attacks
  - The situation
  - What to look for
  - Real world example
- Proper response
## All Threat Actors Are Not Equal

<table>
<thead>
<tr>
<th>Objective</th>
<th>Nuisance Threats</th>
<th>Economic Espionage</th>
<th>Organized Crime</th>
<th>Hacktivists</th>
</tr>
</thead>
<tbody>
<tr>
<td>Launch Points &amp; Nuisance</td>
<td>Economic Advantage</td>
<td>Financial Gain</td>
<td>Defamation, Press &amp; Policy</td>
<td></td>
</tr>
<tr>
<td>Example</td>
<td>Botnets &amp; Spam</td>
<td>Advanced Persistent Threat</td>
<td>Credit Card Theft</td>
<td>Anonymous &amp; Lulzsec</td>
</tr>
<tr>
<td>Targeted</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Persistent</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
</tr>
</tbody>
</table>

*Attacks which are targeted and persistent pose the greatest challenge and the greatest risk.*
Anatomy of a Targeted Attack

Initial Compromise
- Gain Initial Access into Target
- Establish Foothold
- Strengthen Position within Target

Escalate Privileges
- Steal Valid User Credentials

Maintain Presence
- Identify Target Data

Move Laterally
- Package & Steal Target Data

Deploy Persistence Mechanisms

Complete Mission
- Access Other Servers & Files
The Incident Response Process

1. **DETECT**
   - Identify & Validate Security Incidents
   - Alerting Technologies
   - Mandiant Intelligence

2. **CONTAIN**
   - Contain & Remediate Threats

3. **RESPOND**
   - Investigate & Scope Incident

Mandiant, A FireEye Company.
Detecting a Compromise - 2013

33% of victims discovered the breach internally

Down from 37% in 2012

67% of victims were notified by an external entity
Six Ways to Identify Targeted Attacks

1. Phishing emails
2. Anomalous privileged account activity
3. Anomalous VPN logons
4. Malware alerts
5. Anomalous scheduled tasks
6. Persistence mechanisms
Phishing Emails
The Situation

- Many targeted attacks use phishing emails
  - Part of the initial compromise phase
  - Easy method of entry
  - APT favorite
- Only need one victim
- Sometimes difficult to detect
  - Technology getting better
Some Users Still Don’t Get It

Could you summarize it for me, I’m kinda busy.

From: [Redacted]
Sent: [Redacted]
Subject: URGENT
Importance: High

Hello,

Please read the following article, its very important:

[Redacted]

Thanks & Regards
But Some Do

Nope. Sh*t. Got hacked.

On [redacted] wrote:

Is this for real? Looks spammy.

Sent: Monday, [redacted]
Subject: News
Importance: High
Hello,

Please read the following article, its very important:

http://www.washingtonpost.com/world/

Thanks & Regards
What to Look For

- Alerts from relevant devices
- Suspicious attachments
- Suspicious links
- Poor grammar
- Scare tactics
Real World Example

**TIMELINE OF SEA ATTACK ON A NEWS AGENCY**

**DAY 1**
- **Initial Spear Phish Attack**
  - SEA targets a news agency with initial phishing emails

**DAY 2**
- **22 Min Later**
  - SEA actors log into webmail accounts using stolen employee credentials
- **31 Min Later**
  - SEA sends second round of emails from internal email accounts
- **3 Hours Later**
  - SEA uses valid credentials from the phishing campaign to access the news agency’s network and to authenticate the content management system

**DAY 3**
- **4 Hours Later**
  - SEA defaces the news agency’s public website, publishes unauthorized articles and tweets from the agency’s websites and Twitter account
- **26 Hours Later**
  - News agency issues a network-wide password reset that successfully blocks the SEA’s 25 attempts to regain access
Anomalous Privileged Account Activity
The Situation

- Attackers love legitimate credentials
  - Lateral movement
  - Data theft
- Target privileged accounts
  - Local administrators
  - Domain administrators
  - Service accounts
- Can be difficult to detect
  - Lack of understanding
  - Not many people looking for this
What to Look For

- Define normal activity
  - Business need only
- Suspicious logons
  - Interactive logons with service accounts
  - Logons during abnormal business hours
  - Logons to non-related systems
- Focus on privileged accounts
  - Narrow the scope
  - Daily reports
# Real World Example

<table>
<thead>
<tr>
<th>Date</th>
<th>Type</th>
<th>Event</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>06/11/14</td>
<td>Audit</td>
<td>4624</td>
<td>An account was successfully logged on. Logon Type: 10 &lt;br&gt; Account Name: service_account &lt;br&gt; Account Domain: CORP &lt;br&gt; Logon ID: 0x1231a3d4 &lt;br&gt; Workstation Name: CORP_DC &lt;br&gt; Source Network Address: 10.10.10.10</td>
</tr>
<tr>
<td>12:33:46</td>
<td>Success</td>
<td></td>
<td></td>
</tr>
<tr>
<td>06/11/14</td>
<td>Audit</td>
<td>4634</td>
<td>An account was logged off. Logon Type: 10 &lt;br&gt; Account Name: service_account &lt;br&gt; Account Domain: CORP &lt;br&gt; Logon ID: 0x1231a3d4 &lt;br&gt; Logon Type: 10</td>
</tr>
<tr>
<td>12:45:59</td>
<td>Success</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Anomalous VPN logons
The Situation

- Attackers love single factor VPN
  - Usually tied to AD authentication
  - Generally not monitored very well
  - Typically full access to network
- Allows for a smaller malware footprint
  - Less need for backdoors
What to Look For

- Asset verification failure
  - Is it a company laptop?
- Logon origin
  - Hosting providers
  - Geolocation
- Abnormal logon times
# Real World Example

<table>
<thead>
<tr>
<th>Date/Time</th>
<th>Source IP Address</th>
<th>User name</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>06/21/14</td>
<td>5.5.5.3</td>
<td>user1</td>
<td>Login succeeded for user1/Users (session:00000000) from 5.5.5.3.</td>
</tr>
<tr>
<td>06/22/14</td>
<td>5.5.5.1</td>
<td>user1</td>
<td>Login succeeded for user1/Users (session:00000000) from 5.5.5.1.</td>
</tr>
<tr>
<td>06/23/14</td>
<td>5.5.5.5</td>
<td>user1</td>
<td>Login succeeded for user1/Users (session:00000000) from 5.5.5.5.</td>
</tr>
<tr>
<td>06/24/14</td>
<td>1.2.3.4</td>
<td>user1</td>
<td>Login succeeded for user1/Users (session:00000000) from 1.2.3.4.</td>
</tr>
<tr>
<td>06/25/14</td>
<td>5.5.5.1</td>
<td>user1</td>
<td>Login succeeded for user1/Users (session:00000000) from 5.5.5.1.</td>
</tr>
</tbody>
</table>
Malware Alerts
The Situation

- Existing technology can still help
- Alerts often overlooked/misunderstood
- Partial containment/remediation
- Malware alerts can signal a portion of the attack
  - Password dumpers
  - Backdoors
What to Look For

- Password dumpers
  - Indicator of privilege escalation
- Backdoors
  - Need to filter out the noise
- Binaries location
  - Suspicious/critical folders

Real World Example

- FireEye detected large number of callbacks
  - Company thought it was a worm
  - Continued to remove malware
- Stayed at low level in the SOC
  - No escalation based on number
  - No malware analysis
- Misguided containment/remediation

<table>
<thead>
<tr>
<th>Malware</th>
<th>Callbacks</th>
<th>Last CnC Server</th>
<th>Ports Used</th>
<th>Protocols</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malware.ZerodayMatch</td>
<td>45</td>
<td>1.2.3.4</td>
<td>80</td>
<td>TCP</td>
</tr>
</tbody>
</table>
Anomalous Scheduled Tasks
The Situation

- Popular method for tool execution
  - Reconnaissance
  - Backdoor installation
  - Password dumping
What to Look For

- Unnamed scheduled tasks
  - Created when using the Windows “at” command
- Lots of available sources
  - Event logs
  - Scheduled task log
  - File system
### Real World Example

<table>
<thead>
<tr>
<th>Date</th>
<th>Event ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>07/11/14 06:19:44</td>
<td>106</td>
<td>User “CORP\service_account” registered Task Scheduler task &quot;\At1&quot;</td>
</tr>
<tr>
<td>07/11/14 06:21:00</td>
<td>107</td>
<td>Task Scheduler launched &quot;{…}&quot; instance of task &quot;\At1&quot; due to a time trigger condition.</td>
</tr>
<tr>
<td>07/11/14 06:21:00</td>
<td>200</td>
<td>Task Scheduler launched action &quot;cmd&quot; in instance &quot;{…}&quot; of task &quot;\At1&quot;.</td>
</tr>
<tr>
<td>07/11/14 06:21:30</td>
<td>201</td>
<td>Task Scheduler successfully completed task &quot;\At1&quot;, instance &quot;C:\Windows\system32\cmd.EXE&quot;, action &quot;{…}&quot;.</td>
</tr>
</tbody>
</table>
Real World Example

```xml
<?xml version="1.0" encoding="UTF-16"?>
...

<Triggers>
    <TimeTrigger>
        <StartBoundary>2014-07-11T01:21:00</StartBoundary>
    </TimeTrigger>
</Triggers>

<Principals>
...

<Actions Context="Author">
    <Exec>
        <Command>cmd</Command>
        <Arguments>/c "c:\evil.exe -a >c:\hashes.txt"</Arguments>
    </Exec>
</Actions>
</Task>
```
Persistence Mechanisms
The Situation

- Backdoors need to maintain persistence
- Attackers leverage a number of methods
  - Registry
  - Services
  - Search order hijacking
  - Startup paths
What to Look For

- Stack services to find the outliers
- Unsigned binaries
  - Most attackers don’t sign their backdoors
- Suspicious services
  - Unusual locations
  - Unusual names
## Real World Example

<table>
<thead>
<tr>
<th>Service Name</th>
<th>Number of Occurrences</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft afdsjal Support</td>
<td>1</td>
</tr>
<tr>
<td>Microsoft 9fadfa Support</td>
<td>1</td>
</tr>
<tr>
<td>umrdpservice</td>
<td>2,539</td>
</tr>
<tr>
<td>adobeflashplayerupdatesvc</td>
<td>3,813</td>
</tr>
<tr>
<td>eventsystem</td>
<td>3,407</td>
</tr>
</tbody>
</table>
Proper Response
Proper Response

- Triage the alert
  - Identify the root-cause
  - Obtain IOCs for incident
- Scope the environment
- Contain incident
  - Find the right strike zone
- Implement remediation items
  - Strengthen the environment
Questions