Detecting and Responding

PANDAS AND BEARS

Chris Scott, Director of Remediation, CrowdStrike Services
Wendi Whitmore, Global Partner, IBM Security Services
TODAY’S SPEAKERS

14+ YEARS
Incident response and security breach investigations experience

PRIOR TO IBM
Vice President, CrowdStrike Services
Managing Director, Mandiant
Special Agent, Air Force Office of Special Investigations

CONNECT
LINKEDIN: Wendi Whitmore
TWITTER: @WendiLou2
wwhitmor@us.ibm.com

WENDI WHITMORE
PARTNER, IBM SECURITY SERVICES
Defended networks for the Defense Industrial Base

18+ YEARS
 Conducting security assessment, incident response, insider threat analysis, and security architecture.

PRIOR TO CROWDSTRIKE
 Defended networks for the Defense Industrial Base

CONNECT
 LINKEDIN: Christopher Scott
 TWITTER: @NetOpsGuru
 chris@crowdstrike.com

TODAY’S SPEAKERS

CHRIS SCOTT
DIRECTOR OF REMEDIATION
IR & HUNTING
EVOLUTION & BEST PRACTICES
Remove affected machine from network immediately

Collect data from one machine at a time

Automation!

Search for indicators of compromise

Clean entire network before beginning to remediate

Conduct forensics for months before containment of the adversary

Track attackers and actively hunt for them in real-time

Search for indicators of attack

Begin posturing for remediation on Day 1 of IR

Contain the adversary quickly
INDICATORS OF COMPROMISE ARE JUST THE BEGINNING. WE NEED TO TRACK HUMAN BEHAVIORS AND ATTACK METHODOLOGY AS WELL. **WE NEED TO COMBINE IOC AND IOA METHODOLOGIES TO BE SUCCESSFUL.**
We need a shift in detection capabilities from indicators of compromise to Indicators of Attack.
DEEP PANDA

CASE STUDY
Forces attackers to change behaviors

Not all behaviors change - good intel and pattern analysis can identify the new TTPs

Analysts need the ability to tailor intel and extract relevance via tools and skillsets

Understanding your adversaries helps you gain focus and understand what intel is relevant
<table>
<thead>
<tr>
<th>Attacker TTP</th>
<th>Historic Trends</th>
<th>New Trends</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial Attack Vector</td>
<td>Spearphish and Vulnerable External Facing Applications (Most Common)</td>
<td>No Significant Changes - Why change if it still works?</td>
</tr>
<tr>
<td>Malware - Persistence Mechanism</td>
<td>Installed as Service, Run Key, etc.</td>
<td>No Persistence</td>
</tr>
<tr>
<td>Malware - Command &amp; Control</td>
<td>Beacon to malicious IP or Domain</td>
<td>No Standard Beacon Activity</td>
</tr>
<tr>
<td>Malware - Functionality</td>
<td>Simple functionality (provide shell or basic upload/download functionality)</td>
<td>Memory resident - robust functionality</td>
</tr>
<tr>
<td>Lateral Movement</td>
<td>Net Use, RDP or utilities (PSEexec)</td>
<td>WMI, Service Accounts - Evade Logging and blend in</td>
</tr>
<tr>
<td>Obfuscation</td>
<td>Time Stamp Standard Times (Windows API)</td>
<td>Time Stamp both Standard and File times (Windows API and MFT)</td>
</tr>
<tr>
<td>Data Extraction</td>
<td>Compress data and send to compromised host provider</td>
<td>No Significant Changes</td>
</tr>
</tbody>
</table>
CASE STUDY: DEEP PANDA

- **February**
  - Customer #1 investigation commences
  - Traditional tactics

- **March**
  - Intel community shares TTPs shared widely
  - Customer #1 partial remediation: logging & monitoring old tactics

- **April**
  - Customer #1 re-compromised
  - New TTPs

- **May**
  - Customer #2 investigation commences
  - New tactics
TTPs are now rapidly changing
Some things must still remain

What are adversaries adjusting to?
Better intelligence
Hiding from forensics
Better analysts
Better technology

How many adversaries are attacking you?
BEAR vs PANDA
WHY ATTRIBUTION MATTERS
TTPs point to Russia; earliest activity occurred Jan 2015

Complete set of tools for lateral movement copied to network and executed

Toolset attributed to China; use went back several years, but recently inactive

Forensic analysis identifies lateral movement and malware created BEFORE spear-phish

Successful spear-phish in Jan 2015

Attackers identified as “living off the land” and largely using tools readily available on the system

TTPs point to Russia; earliest activity occurred Jan 2015

Two attacker profiles emerge

Toolset #1:
- Sloppy coding
- Compile time and debug info intact
- Chinese character set information present

Attribution: Eloquent Panda

Toolset #2:
- Professional and sanitized code
- Use of valid digital signatures
- Attempts to frustrate reverse engineering

Attribution: Cozy Bear
Complete set of tools for lateral movement copied to network and executed

Toolset attributed to China; use went back several years, but recently inactive

TTPs point to Russia; earliest activity occurred Jan 2015

Toolset #1:
- Sloppy coding
- Compile time and debug info intact
- Chinese character set information present

Attribution: Eloquent Panda

Attackers identified as “living off the land” largely using tools readily available on the system

Toolset #2:
- Professional and sanitized code
- Use of valid digital signatures
- Attempts to frustrate reverse engineering

Attribution: Cozy Bear
POS Malware “Big Picture”
Multiple Adversaries?
- Multiple Locations – Franchise Expansion
- Different POS Software and Vendors
- Different Support Vendors
- Different Concerns on Security

Hunting and Responding
- Understand the Environment
- Do You Have Access to the Endpoint?
  - This is not a technical question ;-) 
- Do You Have Tools to Respond?
  - This is a technical question
Mergers & Acquisitions
Multiple Adversaries?
- Plans to purchase
- What adversaries would be interested?
- Understand the negotiation plans

Hunting and Responding
- Do you have access in multiple environments?
  - Law firm?
  - Other company?
- Targeted hunting on people key to the M & A
  …and their assistants
DETERMINING MULTIPLE ADVERSARIES

• Why would you care?
  – Understand who is targeting your intellectual property
  – Plan to spend your security budget better
  – Employ more effective containment and mitigation strategies
    • What areas of the kill chain is the adversary targeting?
    • Where is the weakness?

• What would better help you identify?
  – Context of the incident
    • M & A, Franchises, Development Plans
  – Malware tools used
  – Sequencing of commands
  – Known C2 channels
THE SPEED OF CONTAINMENT

• Why?
  – Intellectual property leaving the building during the attack
  – What makes you unique is quickly being taken
  – Containment is not “Remediation”

• How?
  – Visibility, Visibility, Visibility
  – Isolate in real time
  – New technologies allow for this
  – Look at the IOAs
    • Where in the attack cycle?

• When?
  – As soon as possible
  – Before forensics is complete? YES. Are you crazy? No.
THE TAKEAWAYS
Intel-Driven Response

Not every adversary group is created equal. Groups have differing skills, resources, and capabilities.

Do not fit data into your expectations – Look for anomalies in your findings focusing on timing, behavior, and tradecraft

The likelihood of being targeted by multiple adversaries is high. In this example, remediation had to include both actors simultaneously!
REMEDIATION PLANNING SHOULD COINCIDE WITH INITIAL INCIDENT RESPONSE
REMEDIATION ACTIONS

• All Adversaries
  – Privileged Account Control
    • Think outside of the box on ways to do this
  – Blacklisting known IOCs?
    • What is the effort vs the reward?
  – Service Accounts
    • Can you reset them?
    • Who has the source code?
    • How long to fix it?
REMEDIATION ACTIONS

• Where is the adversary in the kill chain?
• The earlier in the kill chain, the more options at your disposal.
  – Visibility, Visibility, Visibility
  – If you can find them at: exploitation, installation, command and control
    • You can stop them quickly
  – If you understand the pattern of the attack you have additional options
    • Anticipate the next move
    • Use the intel you collected
CONTAINMENT ASAP
ACHIEVE VISIBILITY AND ISOLATE THE ADVERSARIES