A Forensic Analysis of APT Lateral Movement in Windows Environment

AhnLab
Junghoon Oh
Introduction
Lateral Movement ?

Lateral Movement

Initial Breach~!!!

Accomplishing Goal of Attack~!!
Introduction

Need for Tracing Lateral Movement
Method of Lateral Movement
Method of Lateral Movement

Active Directory Environment (in Same Domain)

- Using Domain Administrator Account
- RDP
- Compromised System
- Copy Backdoor
- Run Backdoor
- Normal System
- sc, at, wmic, reg, psexec, winrs

Administrator System

Normal System

Compromised System
Method of Lateral Movement

Multi-Domain Environment

A Domain  Trust Relationship  B Domain

DC  DC

Copyright (C) AhnLab, Inc. All rights reserved.
Method of Lateral Movement

Non-Active Directory Environment

Stealing Local Administrator’s ID/PW (Kerberos.dll, Wdigest.dll) and NTLM Credentials (Msv1_0.dll) From Memory

All Systems have same Local Administrator Account (Same ID/PW)

Network Share Point

Copy Backdoor

Run Backdoor

sc, at, wmic, reg, psexec, winrs
Forensic Analysis
Forensic Analysis

Layout of Lateral Movement

- Escalation of Privileges
- Network Share Point
- Copy Backdoor
- Run Backdoor
- Victim System
- Anti Forensics

Commands:
- sc, at, wmic, reg, pseexec, winrs
Forensic Analysis

Program Execution

- Location: Attacker System
- Artifact
  - Prefetch

![Prefetch Image]

WCE Execution ~!!

![WCE Execution Screen]

Cain&Abel Execution~!!

![Cain&Abel Execution Screen]
Forensic Analysis

Program Execution

- Location: Attacker System
- Artifact
  - RecentFileCache.bcf

  ![RecentFileCache.bcf](image)

  - Launching Job Scheduler for Installing Malware and Erasing Event Log With `wevtutil`
  - Launching Malware for Stealing NTLM Credentials
  - Launching WCE~!!

- Strings in Memory

  ```
  0963359048WCE v1.3beta (Windows Credentials Editor) - (c) 2010, 2011, 20
  096335910812 Amplia Security - by Hernan Ochoa (hernan@ampliasecurity.com)
  0963359197Use -h for help.
  0963359192
  0963359194ACTIVATEDIRECTORY\:NTLMTEST::00000000000000000000000000000000::B
  0963359254602C4D74A4C9470047AC1B9BBAD530E5
  0963359287Administrator\:NTLMTEST::00000000000000000000000000000000:6019
  0963359347DA498CB790C61C66D405A24101F
  ```

Copyright (C) AhnLab, Inc. All rights reserved.
Forensic Analysis

Program Execution

- Location: Attacker System
- Artifact: wceaux.dll

✓ Dropped DLL from wce.exe

- This DLL is injected to LSASS.EXE and used for acquiring/replacing Credentials.

<table>
<thead>
<tr>
<th>Time</th>
<th>Process</th>
<th>PID</th>
<th>Operation</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>12:16:51</td>
<td>wce.exe</td>
<td>321</td>
<td>CREATE</td>
<td>C:\WOCUME<del>1\forensics\WLOCALS</del>1\Temp\Wwceaux.dll</td>
</tr>
<tr>
<td>12:16:52</td>
<td>wce.exe</td>
<td>321</td>
<td>DELETE</td>
<td>C:\WOCUME<del>1\forensics\WLOCALS</del>1\Temp\Wwceaux.dll</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Source Process</th>
<th>Target Process</th>
<th>API</th>
<th>Inj Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>wce.exe</td>
<td>lsass.exe(PID:696)</td>
<td>WriteProcessMemory</td>
<td>0x950000</td>
</tr>
<tr>
<td>wce.exe</td>
<td>lsass.exe(PID:696)</td>
<td>WriteProcessMemory</td>
<td>0x960000</td>
</tr>
<tr>
<td>wce.exe</td>
<td>lsass.exe(PID:696)</td>
<td>WriteProcessMemory</td>
<td>0x960818</td>
</tr>
<tr>
<td>wce.exe</td>
<td>lsass.exe(PID:696)</td>
<td>CreateRemoteThread</td>
<td>0x960818</td>
</tr>
</tbody>
</table>

- Usually, malware uses these functions~!!
Forensic Analysis

Program Execution

- Location: Attacker System
- Artifact: sekursa.dll
  - DLL used by mimikatz.exe
    - This DLL is injected to LSASS.EXE and used for acquiring/replacing Credentials and Passwords

Malware uses these functions~!!
Forensic Analysis

Logon Attempt

- **Location**: Attacker System
- **Artifact**: Security Event Log
  - The event occurs when attempting to logon to another system ✗ ID: 552(evt) or 4648(evtx)
    - A logon was attempted using explicit credentials (using ID/PW).
    - Information
      - Targeted system name
      - Process information
        - Process ID, name
        - Normal case: lsass.exe (to Remote), winlogon.exe (to Local), taskhost.exe (to Local), consent.exe (to Local)
        - Suspicious case: 0x4(system), cscript.exe, svchost.exe (to Remote)
  - Characteristics of this behavior
    - Attempting 10 times logon per second through automation
    - There is no information whether logon succeeds or not.
Forensic Analysis

NTLM Authentication

- **Location**: Victim System
- **Artifact**: Security Event Log
  - Network Logon through NTLM authentication  ☑  ID: 540(evt) or 4624(evtx)
    - **Condition**
      - Logon Type: 3
      - Logon Process: NtLmSsp
      - Package Name: NTLM V2  ☑ In Case of XP SP3, NTLM
    - **Information**
      - New Logon: Account Name, Domain
      - Network Information: Workstation Name, IP, Port

![Using NTLM Authentication~!!](image-url)
Forensic Analysis

NTLM Authentication

- **Real Case: Finding Lateral Movement**
  - Online Game Company
  - The Security Event Log of Compromised DC (Domain Controller) Server \( \times \) **3158244 records**
  - The filtering result with "Logon Type : 3" keyword (Network Logon) \( \times \) **176006 records**

<table>
<thead>
<tr>
<th>Type</th>
<th>Date</th>
<th>Time</th>
<th>Event</th>
<th>Source</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit Success</td>
<td>2/16/2013</td>
<td>7:11:53 AM</td>
<td>4624</td>
<td>Microsoft-Windows-SeLogon</td>
<td></td>
</tr>
<tr>
<td>Audit Success</td>
<td>2/16/2013</td>
<td>7:11:54 AM</td>
<td>4634</td>
<td>Microsoft-Windows-SeLogoff</td>
<td></td>
</tr>
<tr>
<td>Audit Success</td>
<td>2/16/2013</td>
<td>7:11:55 AM</td>
<td>4634</td>
<td>Microsoft-Windows-SeLogoff</td>
<td></td>
</tr>
<tr>
<td>Audit Success</td>
<td>2/16/2013</td>
<td>7:12:05 AM</td>
<td>4634</td>
<td>Microsoft-Windows-SeLogoff</td>
<td></td>
</tr>
<tr>
<td>Audit Success</td>
<td>2/16/2013</td>
<td>7:12:17 AM</td>
<td>4634</td>
<td>Microsoft-Windows-SeLogoff</td>
<td></td>
</tr>
</tbody>
</table>

- Performing cross-analysis with other artifacts.

<table>
<thead>
<tr>
<th>Type</th>
<th>Date</th>
<th>Time</th>
<th>Event</th>
<th>Source</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit Success</td>
<td>2/19/2013</td>
<td>12:12:27 PM</td>
<td>4624</td>
<td>Microsoft-Windows-SeLogon</td>
<td></td>
</tr>
<tr>
<td>Audit Success</td>
<td>2/25/2013</td>
<td>4:05:15 PM</td>
<td>4624</td>
<td>Microsoft-Windows-SeLogon</td>
<td></td>
</tr>
</tbody>
</table>
Forensic Analysis

Copying Backdoor

- **Location**: Victim System
- **Artifact**: Security Event Log

  - File share ID: 5140 (Not default)
    - Information
      - New Logon: Account Name, Domain
      - Network Information: System IP, Network Share Point

![Security Event Log Table]

![Network Share Access Log]

Copyright (C) AhnLab, Inc. All rights reserved.
Forensic Analysis

Remote service registration/execution

- **Location**: Victim System
- **Artifact**: Security Event Log
  - Service Installation  ID: 4697 (Not Default)
    - Information
      - Account Name, Domain
      - Service Name, Service File Name
Forensic Analysis

Remote service registration/execution

- **Location**: Victim System
- **Artifact**: SYSTEM Event Log
  - **Service Installation**  ID: 7045
    - Information
      - Service Name
      - Service File Name
  - **Changing Service State**  ID: 7036
    - Information
      - Whether backdoor is executed or not

<table>
<thead>
<tr>
<th>Type</th>
<th>Date</th>
<th>Time</th>
<th>Event</th>
<th>Source</th>
<th>Category</th>
<th>User</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information</td>
<td>7/13/2013</td>
<td>4:09:50 PM</td>
<td>7045</td>
<td>Service Control Manager</td>
<td>None</td>
<td>S-1-5-21-2313365137-</td>
</tr>
<tr>
<td>Information</td>
<td>7/13/2013</td>
<td>4:09:53 PM</td>
<td>7036</td>
<td>Service Control Manager</td>
<td>None</td>
<td>N/A</td>
</tr>
</tbody>
</table>

**Description**

- A service was installed in the system.
- Service Name: uytmjkoby
- Service File Name: %SystemDrive%\uytmjkoby.exe /s
- Service Type: ??????
- Service Start Type: ??
- Service Account: LocalSystem

- The uytmjkoby service entered the ?? state.
Forensic Analysis

Remote job schedule registration, execution and deletion

- **Location**: Victim System
- **Artifact**: Task Scheduler Event Log (since win7)
  - **Registering Job schedule**  
    - ID: 106
      - Account Name used to registration
      - Job Name: Usually “At#” form
  - **Starting Job schedule**  
    - ID: 200
      - The path of file executed for job
  - **Deleting Job schedule**  
    - ID: 141
      - Account Name used to registration

---

<table>
<thead>
<tr>
<th>Type</th>
<th>Date</th>
<th>Time</th>
<th>Event</th>
<th>Source</th>
<th>Category</th>
<th>User</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information</td>
<td>1/30/2013</td>
<td>11:05:29 PM</td>
<td>106</td>
<td>Microsoft-Windows-TaskScheduler</td>
<td>Task registered</td>
<td>SYSTEM</td>
</tr>
</tbody>
</table>

**Log Entry**

User "AA-WORLD-24\zmfisprotm" registered Task Scheduler task "At1".

---

<table>
<thead>
<tr>
<th>Type</th>
<th>Date</th>
<th>Time</th>
<th>Event</th>
<th>Source</th>
<th>Category</th>
<th>User</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information</td>
<td>1/30/2013</td>
<td>11:06:00 PM</td>
<td>200</td>
<td>Microsoft-Windows-TaskScheduler</td>
<td>Action started</td>
<td>SYSTEM</td>
</tr>
</tbody>
</table>

**Log Entry**

Task Scheduler launched action "c:\windows\help\update.bat" in instance "(FC22253A-361B-4A21-8A67-C110D3F60757)" of task "At1".

---

<table>
<thead>
<tr>
<th>Type</th>
<th>Date</th>
<th>Time</th>
<th>Event</th>
<th>Source</th>
<th>Category</th>
<th>User</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information</td>
<td>1/30/2013</td>
<td>11:06:04 PM</td>
<td>141</td>
<td>Microsoft-Windows-TaskScheduler</td>
<td>Task registration deleted</td>
<td>SYSTEM</td>
</tr>
</tbody>
</table>

**Log Entry**

User "NT AUTHORITY\System" deleted Task Scheduler task "At1".
Forensic Analysis

Remote job schedule registration, execution and deletion

- **Location**: Victim System
- **Artifact**: Tasks Folder
  - Creating “At#.job” file under “Tasks” folder

<table>
<thead>
<tr>
<th>Name</th>
<th>File Created</th>
<th>Last Written</th>
<th>Last Accessed</th>
<th>Entry Modified</th>
</tr>
</thead>
</table>

- Last Written
- Last Accessed
- MFT Entry Modified

![Image of Task Folder](image.png)
Forensic Analysis

Remote execution with wmic

- **Location**: Victim System
- **Artifact**: Security Event Log
  - Creating Process ✗ ID : 4688 (Not Default)
    - After creating "WmiPrvSE.exe" process, "WmiPrvSE.exe" creates backdoor process.
Forensic Analysis

Remote registry registration

- Location: Victim System
- Artifact: Registry
  - Changing “Last Written Time” of relevant key

![Registry Key Properties and Data](image1.png)

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
  - Value Name: VMware Tools, Value Type: REG_SZ, Value Data: "C:\Program Files\VMware\VMware Tools"
  - Value Name: VMware User Process, Value Type: REG_SZ, Value Data: "C:\Program Files\VMware\VMware Tools"
  - Value Name: myentry, Value Type: REG_SZ, Value Data: "C:\backdoor.exe"
Forensic Analysis

Remote execution with psexec

- **Location**: Victim System
- **Artifact**: Security Event Log
  - **File Share**  \(\text{ID: 5140}\) (Not Default)
    - Copying backdoor to “SYSTEM32” folder \(\text{ADMIN}\$\) share
  - **Creating Process**  \(\text{ID: 4688}\) (Not Default)
    - After creating “PSEXESVC.EXE” process, “PSEXESVC.EXE” creates backdoor process.
Forensic Analysis

Remote execution with psexec

• Location: Victim System
• Artifact: SYSTEM Event Log
  ✓ Changing Service State  ID: 7036
    ▪ Starting PsExec Service

<table>
<thead>
<tr>
<th>Type</th>
<th>Date</th>
<th>Time</th>
<th>Event</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information</td>
<td>12/11/2013</td>
<td>6:33:21 PM</td>
<td>7036</td>
<td>Service Control Manager</td>
</tr>
</tbody>
</table>

The PsExec service entered the ?? state.
Forensic Analysis

Remote execution with winrs

- **Location**: Victim System
- **Artifact**: Security Event Log

- **Creating Process** ▪ **ID: 4688** (Not Default)
  - After Creating "winrshost.exe" process, "winrshost.exe" creates backdoor process through `cmd.exe` process.
  - The subject of executing backdoor is User Account unlike psexec.
Forensic Analysis

Countermeasure for Anti Forensics

- Anti Forensic behavior
  - After installing backdoor, attacker deletes of “Event Log”, job file and backdoor installation file

```plaintext
copy c:\windows\system32\net.exe c:\windows\net1.exe /y
del c:\windows\net1.exe del c:\windows\tasks\*.job
wevtutil cl Application
wevtutil cl System
wevtutil cl security
del c:\windows\net1.bat
```

- Countermeasure
Forensic Analysis

Countermeasure for Anti Forensics

• Recovering Deleted Event Records
Forensic Analysis

Countermeasure for Anti Forensics

- Countermeasure (continue...)
  - Deleting job file
    - Job file is in $MFT with form of resident file due to the file size (< 870 byte)  Searching within $MFT
    - “MFT Modified Time” of “Tasks” folder is used to find attack time
Forensic Analysis

Countermeasure for Anti Forensics

- Countermeasure (continue…)
  - Deleting malware file
    - Analyzing file system log ($LogFile, $UsnJrnl)
    - NTFS Log Tracker: https://sites.google.com/site/forensicnote/ntfs-log-tracker

<table>
<thead>
<tr>
<th>TimeStamp</th>
<th>USN</th>
<th>FileName</th>
<th>Full Path (from $MFT)</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>2012-12-25 00:58:55</td>
<td>461968376</td>
<td>net6.bat</td>
<td>\Windows\debug\net6.bat</td>
<td>File_Created</td>
</tr>
<tr>
<td>2012-12-25 00:58:55</td>
<td>461968456</td>
<td>net6.bat</td>
<td>\Windows\debug\net6.bat</td>
<td>File_Created, File_Added</td>
</tr>
<tr>
<td>2012-12-25 00:58:55</td>
<td>461968536</td>
<td>net6.bat</td>
<td>\Windows\debug\net6.bat</td>
<td>File_Created, File_Added, Data_Overwritten</td>
</tr>
<tr>
<td>2012-12-25 00:58:55</td>
<td>461968616</td>
<td>net6.bat</td>
<td>\Windows\debug\net6.bat</td>
<td>File_Created, Attr_Changed, File_Added, Data_Overwritten</td>
</tr>
<tr>
<td>2012-12-25 00:58:55</td>
<td>461968696</td>
<td>net6.cpl</td>
<td>\Windows\debug\net6.cpl</td>
<td>File_Created</td>
</tr>
<tr>
<td>2012-12-25 00:58:55</td>
<td>461968776</td>
<td>net6.cpl</td>
<td>\Windows\debug\net6.cpl</td>
<td>File_Created, File_Added</td>
</tr>
<tr>
<td>2012-12-25 00:58:55</td>
<td>461968856</td>
<td>net6.cpl</td>
<td>\Windows\debug\net6.cpl</td>
<td>File_Created, File_Added, Data_Overwritten</td>
</tr>
<tr>
<td>2012-12-25 00:58:55</td>
<td>461968936</td>
<td>net6.cpl</td>
<td>\Windows\debug\net6.cpl</td>
<td>File_Created, Attr_Changed, File_Added, Data_Overwritten</td>
</tr>
<tr>
<td>2012-12-25 00:58:55</td>
<td>461969016</td>
<td>net6.exe</td>
<td>\Windows\debug\net6.exe</td>
<td>File_Created</td>
</tr>
<tr>
<td>2012-12-25 00:58:55</td>
<td>461969096</td>
<td>net6.exe</td>
<td>\Windows\debug\net6.exe</td>
<td>File_Created, File_Added</td>
</tr>
<tr>
<td>2012-12-25 00:58:55</td>
<td>461969176</td>
<td>net6.exe</td>
<td>\Windows\debug\net6.exe</td>
<td>File_Created, File_Added, Data_Overwritten</td>
</tr>
<tr>
<td>2012-12-25 00:58:55</td>
<td>461969256</td>
<td>net6.exe</td>
<td>\Windows\debug\net6.exe</td>
<td>File_Created, Attr_Changed, File_Added, Data_Overwritten</td>
</tr>
<tr>
<td>2012-12-25 00:58:55</td>
<td>461969336</td>
<td>net6.bat</td>
<td>\Windows\debug\net6.bat</td>
<td>File_Created, Attr_Changed, File_Added, Data_Overwritten, File_Closed</td>
</tr>
<tr>
<td>2012-12-25 00:58:55</td>
<td>461969416</td>
<td>net6.cpl</td>
<td>\Windows\debug\net6.cpl</td>
<td>File_Created, Attr_Changed, File_Added, Data_Overwritten, File_Closed</td>
</tr>
<tr>
<td>2012-12-25 00:58:55</td>
<td>461969496</td>
<td>net6.exe</td>
<td>\Windows\debug\net6.exe</td>
<td>File_Created, Attr_Changed, File_Added, Data_Overwritten, File_Closed</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TimeStamp</th>
<th>USN</th>
<th>FileName</th>
<th>Full Path (from $MFT)</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>2012-12-25 01:59:12</td>
<td>462450008</td>
<td>net6.bat</td>
<td>\Windows\debug\net6.bat</td>
<td>File_Closed, File_Deleted</td>
</tr>
<tr>
<td>2012-12-25 01:59:12</td>
<td>462450088</td>
<td>net6.cpl</td>
<td>\Windows\debug\net6.cpl</td>
<td>File_Closed, File_Deleted</td>
</tr>
<tr>
<td>2012-12-25 01:59:12</td>
<td>462450163</td>
<td>net6.exe</td>
<td>\Windows\debug\net6.exe</td>
<td>File_Closed, File_Deleted</td>
</tr>
</tbody>
</table>
Forensic Analysis

Countermeasure for Anti Forensics

- Disk Destruction (ex: 3.20 / 6.25 Cyber Attack in South Korea)
Forensic Analysis

Countermeasure for Anti Forensics

- Countermeasure for Disk Destruction
  - Recovering VBR by Backup VBT located in end of volume
  - Creating New MBR

![Diagram showing disk structure with MBR, VBR, and Backup VBR layers]
Forensic Analysis

Forensic Readiness

• Event Log
  - Remote backup Server
    - Real-time Backup
    - The backup server should be excluded in domain.

  - Audit policy : Turn on all audits

  ```
  wevtutil sl <LogName> /ms:<MaxSizeInBytes>
  ```
Forensic Analysis

Forensic Readiness

- **LogFile, UsnJrnl**
  - **LogFile**: Changing size of log file
    - `chkdsk /L:<size>(KB)`
    - Usually 64M log data is saved for about 3 hours
    - One percent of volume size is recommended.

- **UsnJrnl**: fsutil usn createjournal m=<size>(byte) a=<size>(byte) <volume>
  - Usually 32M log data is saved for about 1~2 days
  - One percent of volume size is recommended.
## Forensic Analysis

### Summary

- **Attacker System**

<table>
<thead>
<tr>
<th>Behavior</th>
<th>Artifact</th>
<th>Detail</th>
</tr>
</thead>
<tbody>
<tr>
<td>Escalation of Privileges</td>
<td>Prefetch</td>
<td>Program Execution</td>
</tr>
<tr>
<td>Application Compatibility Cache</td>
<td>RecentFileCache.bcf</td>
<td>Program Execution</td>
</tr>
<tr>
<td></td>
<td>wceaux.dll</td>
<td>DLL of WCE</td>
</tr>
<tr>
<td></td>
<td>sekurlsa.dll</td>
<td>DLL of Mimitakz</td>
</tr>
<tr>
<td>Memory</td>
<td>String search</td>
<td></td>
</tr>
<tr>
<td>Attempting Logon</td>
<td>Security Event Log</td>
<td>Attempting Logon to another system with explicit credentials ID: <strong>552(evt)</strong> or <strong>4648(evtx)</strong></td>
</tr>
</tbody>
</table>
# Forensic Analysis

## Summary

- **Victim System**

<table>
<thead>
<tr>
<th>Behavior</th>
<th>Artifact</th>
<th>Detail</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>NTLM Authentication</strong></td>
<td>Security Event Log</td>
<td>Network Logon (ID: 540 or 4624)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Network Traffic</td>
<td>Protocol: SMB2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Characteristics</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1. SessionSetup: NTLMSSP_NEGOTIATE</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. SessionSetup: NTLMSSP_AUTH, Domain, Username</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. TreeConnect: &lt;IP or Host Name&gt;\IPC$</td>
</tr>
<tr>
<td><strong>Copying Backdoor</strong></td>
<td>Security Event Log</td>
<td>File Share (ID: 5140)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Protocol: SMB2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Characteristics</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1. TreeConnect: &lt;IP or Host Name&gt;&lt;Share Point: C$, D$ &gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Create</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Write</td>
</tr>
<tr>
<td><strong>Remote service registration/execution</strong></td>
<td>Security Event Log</td>
<td>Installing Service (ID: 4697)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Protocol: SVCCTL</td>
</tr>
<tr>
<td></td>
<td>System Event Log</td>
<td>Installing Service (ID: 7045)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Changing Service State (ID: 7036)</td>
</tr>
<tr>
<td></td>
<td>Network Traffic</td>
<td>Protocol: SVCCTL</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Characteristics</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1. OpenSCManager</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. CreateService or OpenService, StartService</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. CloseServiceHandle</td>
</tr>
</tbody>
</table>
### Forensic Analysis

#### Summary
- **Victim System (continue...)**

<table>
<thead>
<tr>
<th>Behavior</th>
<th>Artifact</th>
<th>Detail</th>
</tr>
</thead>
</table>
| Remote job schedule registration and execution, deletion | Task Scheduler Event Log | Registering Job (ID: 106)  
Starting Job (ID: 200)  
Deleting Job (ID: 141)  
Tasks folder | Changing time information of “Tasks” folder by Creating “At#.job” file |
| Network Traffic | Protocol: ATSVC  
Characteristics: JobAdd |
| Remote registry registration | Software Registry | HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run |
| Network Traffic | Protocol: WINREG  
Characteristics:  
1. OPENHKLM  
2. CreateKey  
3. QueryValue  
4. SetValue  
5. CloseKey |
| Remote execution with psexec | Security Event Log | File Share (ID: 5140) → $ADMIN share  
Creating Process (ID: 4688) → PSEXESVC.EXE  
System Event Log | Changing Service State (ID: 7036) → starting PsExec service |
| Network Traffic | Protocol: SMB2  
Characteristics:  
TreeConnect: \<IP or Host Name>\ADMIN$  
Create: PSEXESVC.EXE  
Create: svcctl  
Create: 실행 파일 |
## Forensic Analysis

### Summary

- **Victim System (continue...)**

<table>
<thead>
<tr>
<th>Behavior</th>
<th>Artifact</th>
<th>Detail</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote execution with <strong>winrs</strong></td>
<td><strong>Security Event Log</strong></td>
<td>Creating Process (ID: 4688) [ winrhost.exe ]</td>
</tr>
</tbody>
</table>
|                   | **Network Traffic**           | Protocol: **HTTP** Characteristics: 
|                   |                               | 1. NTLMSSSP_NEGOTIATE: /wsman 
|                   |                               | 2. NTLMSSP_AUTH: Domain, Username |

- **Countermeasure for Anti Forensics**

<table>
<thead>
<tr>
<th>Behavior</th>
<th>Response</th>
<th>Detail</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deleting Event Log</td>
<td>Recovering Event Log</td>
<td><strong>Record Carving</strong></td>
</tr>
<tr>
<td>Deleting Job file</td>
<td>Keyword Search</td>
<td>Searching within $MFT</td>
</tr>
<tr>
<td>Deleting Job file</td>
<td>Confirming <strong>MFT Modified Time</strong></td>
<td>Guessing creation and deletion time of job file</td>
</tr>
<tr>
<td>Deleting file</td>
<td>Analyzing File System Log($LogFile, $UsnJrnl)</td>
<td><strong>Using “NTFS Log Tracker”</strong></td>
</tr>
</tbody>
</table>

- **Forensic Readiness**

<table>
<thead>
<tr>
<th>Target</th>
<th>Response</th>
<th>Detail</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event Log</td>
<td>Remote Backup Server</td>
<td>Real-time backup</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Backup server not included in domain</td>
</tr>
<tr>
<td></td>
<td>Setting Audit Policy</td>
<td>Turn On all audits</td>
</tr>
<tr>
<td>$LogFile, $UsnJrnl</td>
<td>Changing size of log file</td>
<td>wevtutil sl</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$LogFile [ chkdsk ]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$UsnJrnl [ fsutil ]</td>
</tr>
</tbody>
</table>
Case Study

Case Study 1: Defense Contractor in South Korea

Office Network (Not AD Environment)

“This system is compromised.”
From. Mandiant

All systems have same local administrator ID/PW...

Military Research Institute’s Web Server

Watering Hole Attack~!!

Drive by Download

: Back Tracking
Case Study

Case Study 2: Online Game Company in South Korea

Server Farm (AD Environment)

Fabricating Game Money~!!

Gateway Server
Connected to Office Network

Office Network (AD Environment)

Using Domain administrator’s Credentials…

Can’t find any traces Before Formatting

File Server

Download
Nvidia Driver Installation Program
(Malicious)

Using Domain administrator’s Credentials…

VPN

Keylogging

Can’t find any traces Before Formatting

Analyzing FTP Log

Gateway Server
Connected to Office Network

Using Domain administrator’s Credentials…

Recovering Deleted Event Records

Can’t find any traces Before Formatting

VPN

Using Domain administrator’s Credentials…

Analyzing FTP Log
Case Study

Case Study 3: 6.25 Cyber Attack in South Korea

Cable TV Company

A branch's Server Farm

B branch's Server Farm

C & C Server~!!

Malware Functions
1. Changing password
2. Lateral Movement via Network share
3. Disk Destruction

All systems's password and wall paper are changed.

All systems have same local administrator ID/PW...

Private Line

Recovering Destroyed File System

C & C Connection

C & C Connection

C & C Connection

C & C Connection

System become unbootable...

Copyright (C) AhnLab, Inc. All rights reserved.
Conclusion
Conclusion

• APT Lateral Movement
  ✓ Moving laterally to find targeted server in internal network
  ✓ Using windows authentication protocol
  ✓ Necessity of Forensic Analysis
  ✓ Difficulty of classification
  ◆ Removing Root cause through tracebacking.

• Forensic Analysis
  ✓ Malware Execution
  ✓ Tracing NTLM Authentication
  ✓ Countermeasure for Anti Forensics
  ✓ Forensic Readiness
Thank you.
Reference