A Forensic Analysis of APT Lateral Movement in Windows Environment

AhnLab
Junghoon Oh

AhnLab

Agenda

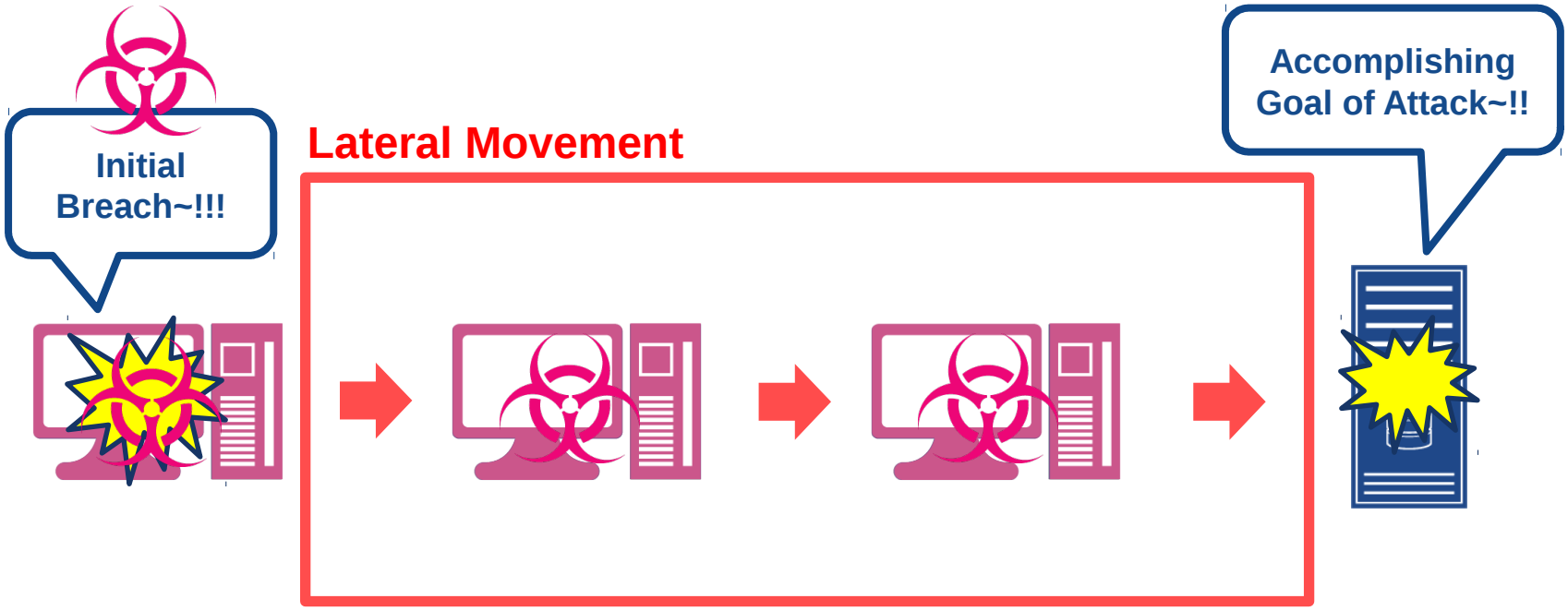
AhnLab

Introduction

AhnLab

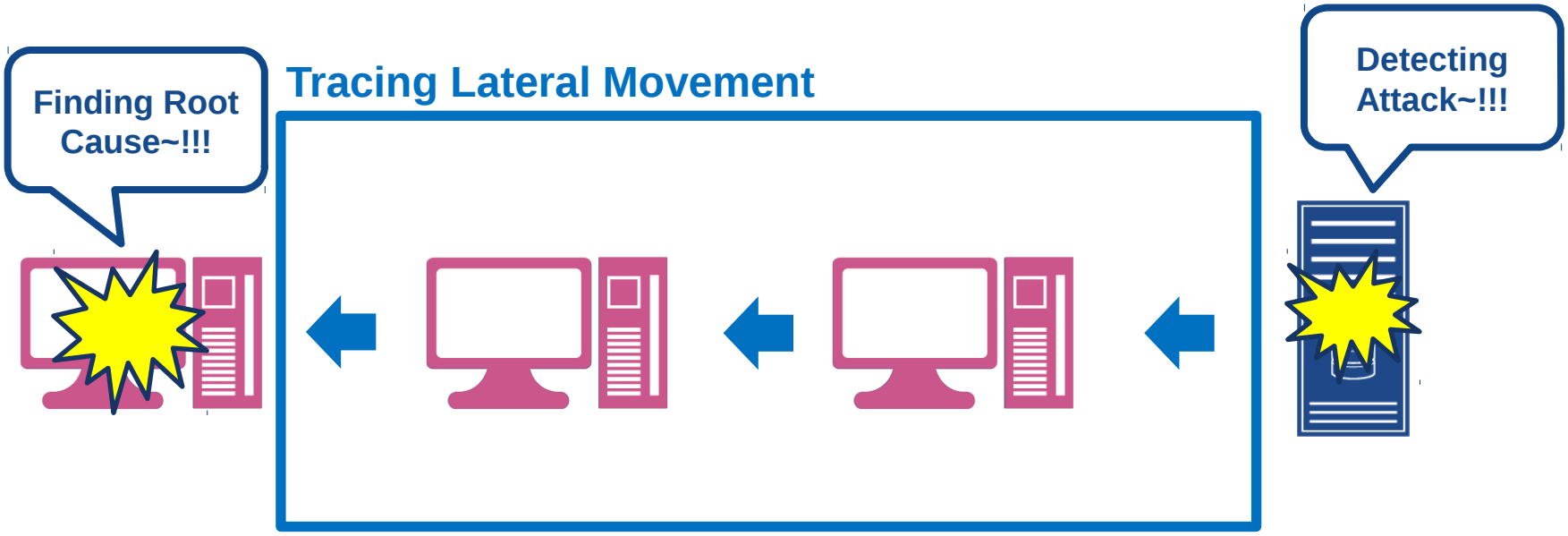
Introduction

Lateral Movement ?



Introduction

Need for Tracing Lateral Movement

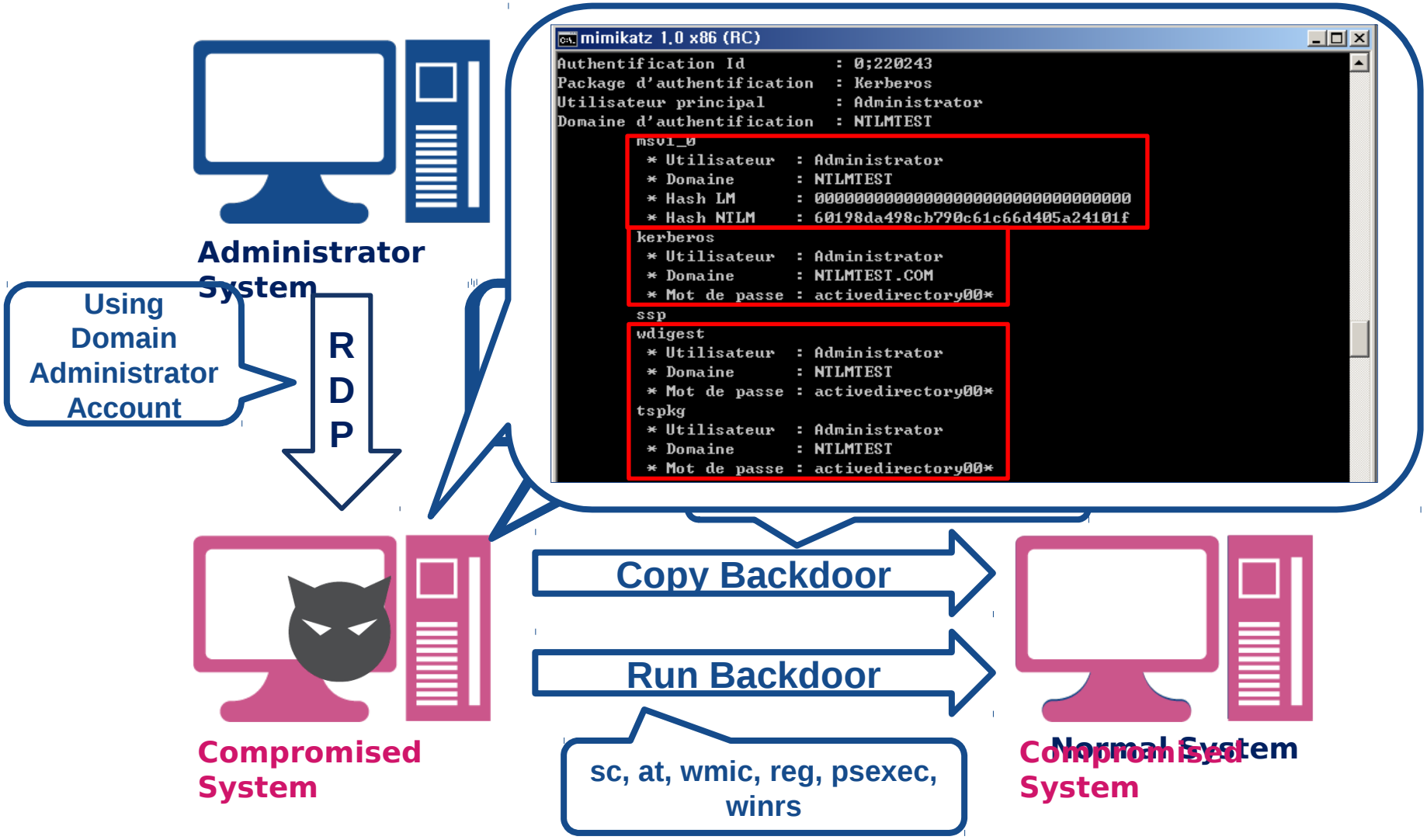


Method of Lateral Movement

AhnLab

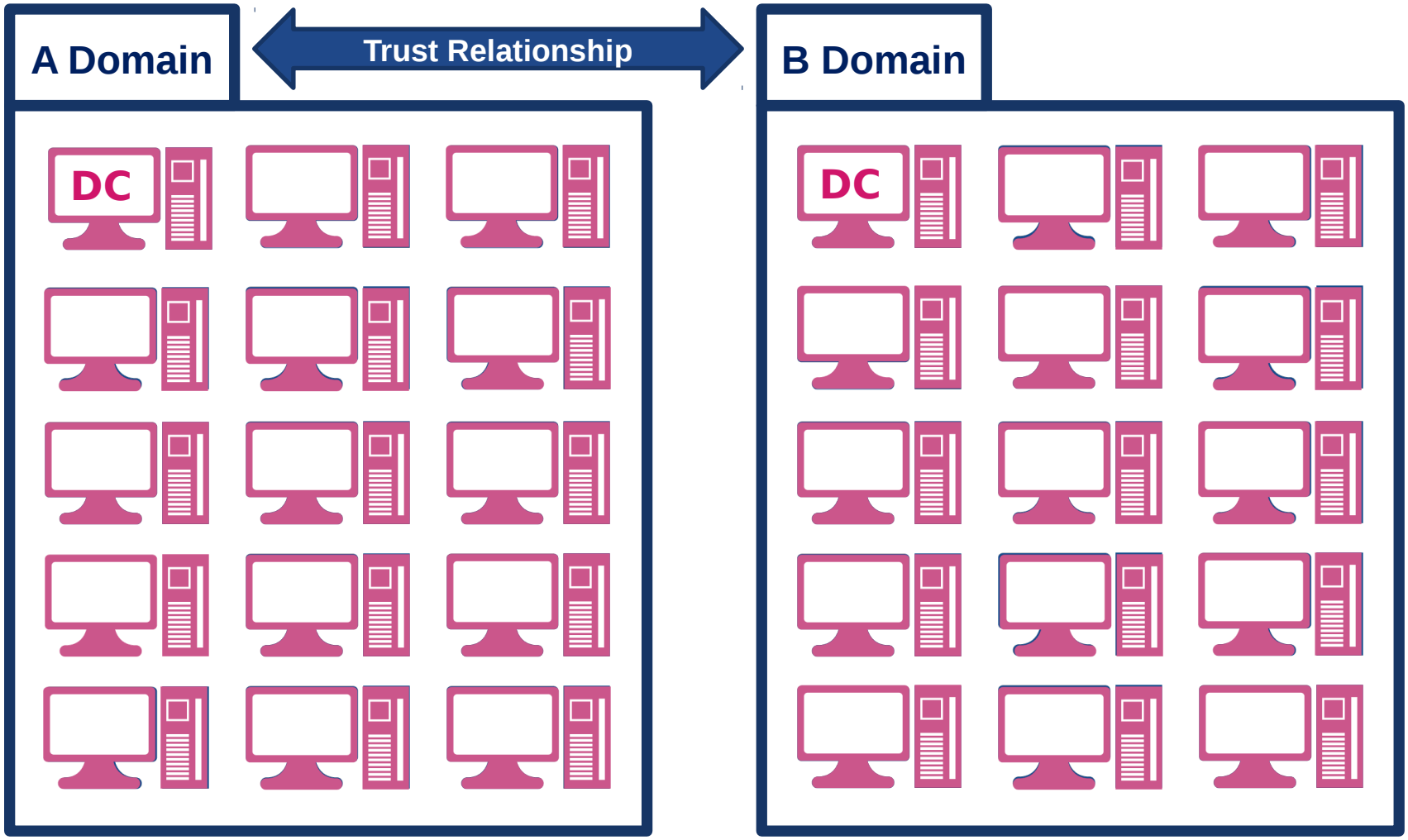
Method of Lateral Movement

Active Directory Environment(in Same Domain)



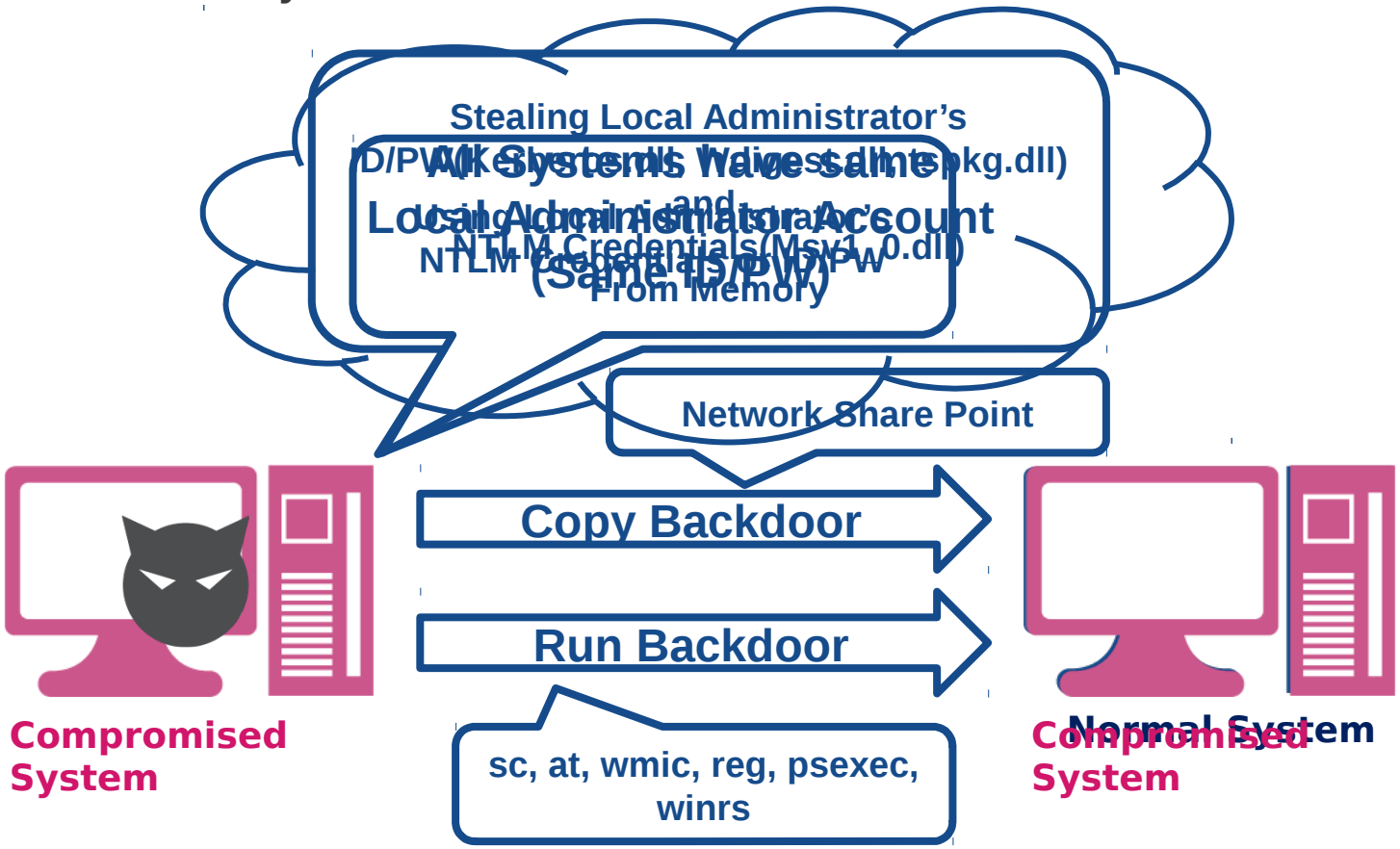
Method of Lateral Movement

Multi-Domain Environment



Method of Lateral Movement

Non-Active Directory Environment

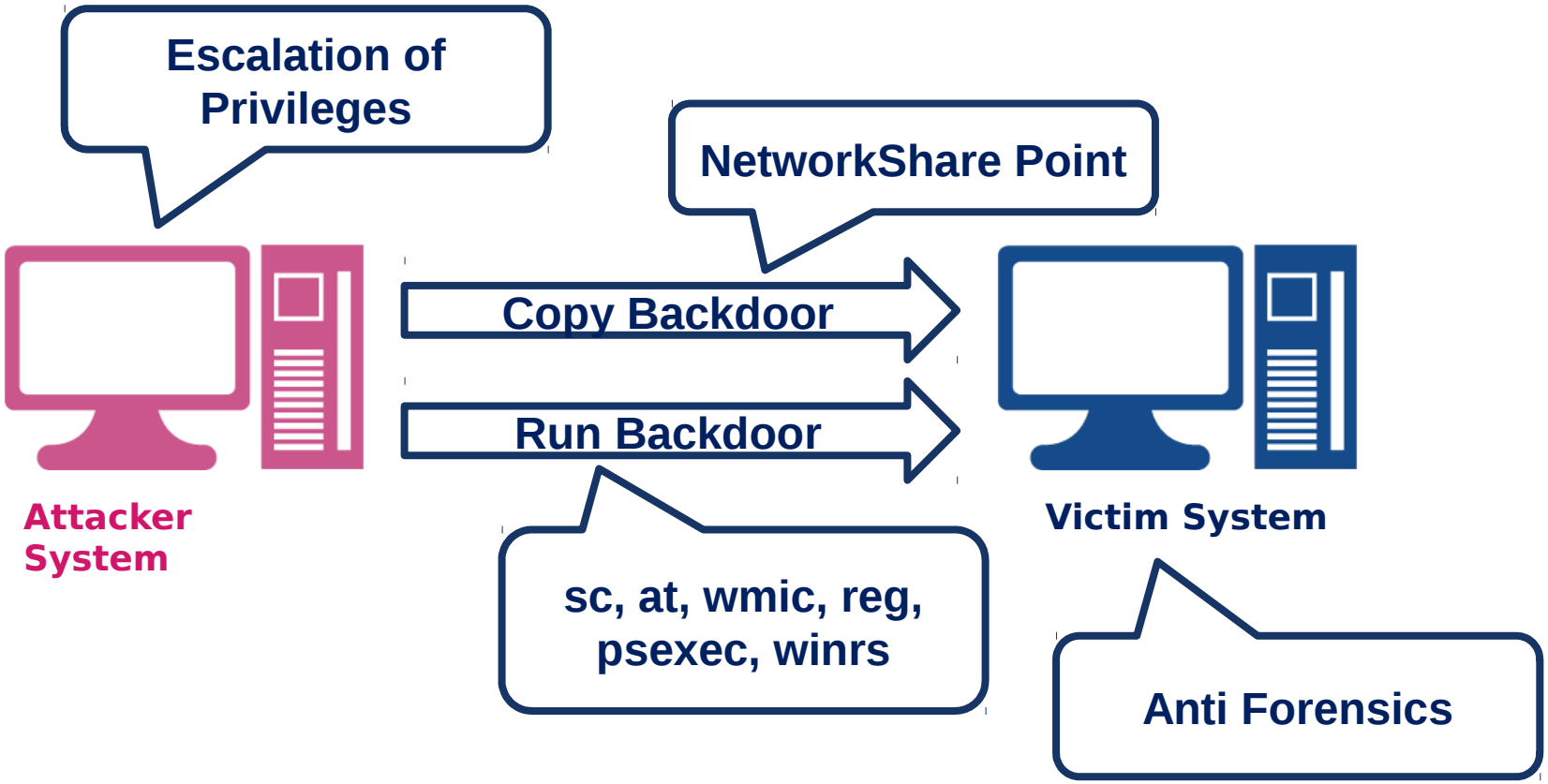


Forensic Analysis

AhnLab

Forensic Analysis

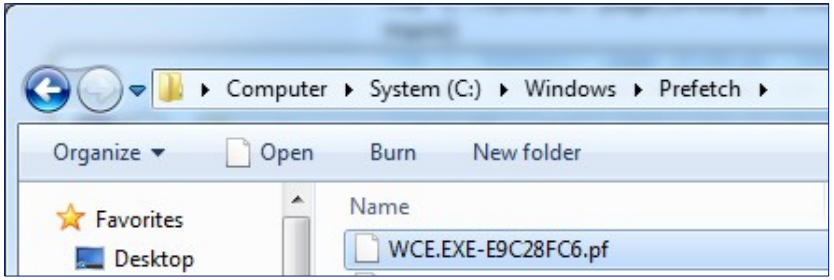
Layout of Lateral Movement



Forensic Analysis

Program Execution

- Location : Attacker System
- Artifact
  - ✓ Prefetch



WCE Execution ~!!

  - ✓

Timeline | Bookmarks | Search Result | Application Compatibility Cache

ControlSet: ControlSet001 (Current) Filter: Enter filter text here

Executable File Path	Last Modified Time (UTC+09:00)	Last Update Time (UTC+09:00)	Filesize
C:₩wce.exe	2012-03-09 06:43:19 Fri	none	none

Cain&Abel Execution~!!

Timeline | Bookmarks | Search Result | Application Usage Log

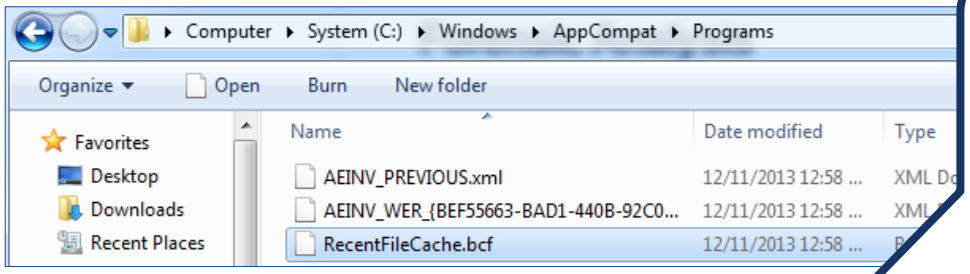
Account: View all Filter: Enter filter text here

User Account	Name	Type	Last Execution Time (UTC+09...
vmuser	{7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}₩Cain₩Cain.exe	CTLSESSION	2013-12-11 15:59:10 Wed
vmuser	₩Users₩vmuser₩Desktop₩Cain.lnk	CTLSESSION	2013-12-11 15:59:10 Wed

Forensic Analysis

Program Execution

- Location : Attacker System
- Artifact
  - ✓ RecentFileCache.bcf




```
000000015A1C  000000015A1C  0  c:\windows\system32\at.exe
000000015A56  000000015A56  0  c:\windows\ime\net6.exe
000000015A8A  000000015A8A  0  c:\windows\system32\wevtutil.exe
000000015AD0  000000015AD0  0  c:\windows\system32\logoff.exe
000000015B12  000000015B12  0  c:\windows\system32\query.exe
000000015B52  000000015B52  0  c:\windows\system32\quser.exe
000000015B92  000000015B92  0  c:\windows\system32\cacls.exe
000000015BD2  000000015BD2  0  c:\windows\system32\attrib.exe
000000015C14  000000015C14  0  c:\windows\system32\qprocess.exe
000000015C5A  000000015C5A  0  c:\windows\debug\nvidia.exe
000000015C96  000000015C96  0  c:\windows\system32\systeminfo.exe
```

Launching Job Scheduler for Installing Malware and Erasing Event Log With wevtutil

Launching Malware for Stealing NTLM Credentials

  - ✓ Strings in Memory

```
0963359048WCE v1.3beta (Windows Credentials Editor) - (c) 2010,2011,20
0963359108 12 Amplia Security - by Hernan Ochoa (hernan@ampliasecurity.
0963359168com)
0963359174Use -h for help.
0963359192
0963359194ACTIVEDIRECTORY$:NTLMTEST:00000000000000000000000000000000:B
0963359254602C4D74AAC9470047AC19BBAD5305E
0963359287Administrator:NTLMTEST:00000000000000000000000000000000:6019
09633593478DA498CB790C61C66D405A24101F
```

Launching WCE~!!

Forensic Analysis

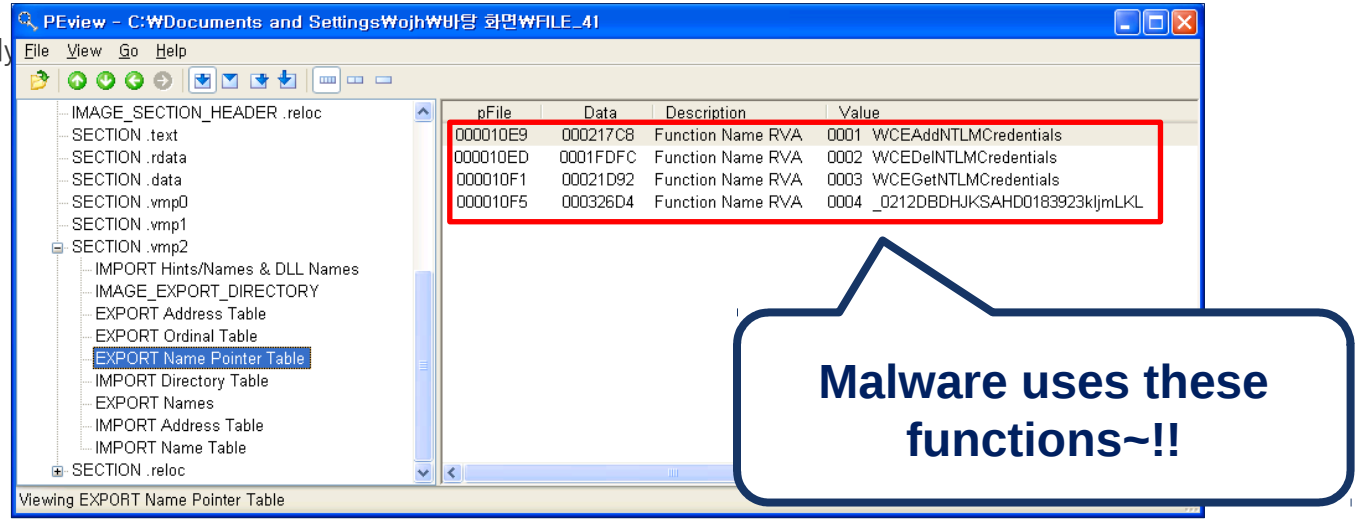
Program Execution

- **Location : Attacker System**
- **Artifact : wceaux.dll**
  - ✓ Dropped DLL from wce.exe
    - This DLL is injected to LSASS.EXE and used for acquiring/replacing Credentials.

Time	Process	PID	Operation	Path
start...				
*오후 12:16:51	wce.exe	321	CREATE	C:₩DOCUME~1₩forensic₩LOCALS~1₩Temp₩wceaux.dll
*오후 12:16:52	wce.exe	321	DELETE	C:₩DOCUME~1₩forensic₩LOCALS~1₩Temp₩wceaux.dll

Source Proc...	Target Process	API	Inj Address
wce.exe	lsass.exe(PID:696)	WriteProcessMemory	0x950000
wce.exe	lsass.exe(PID:696)	WriteProcessMemory	0x960000
wce.exe	lsass.exe(PID:696)	WriteProcessMemory	0x960818
wce.exe	lsass.exe(PID:696)	CreateRemoteThread	0x960818

- Usually

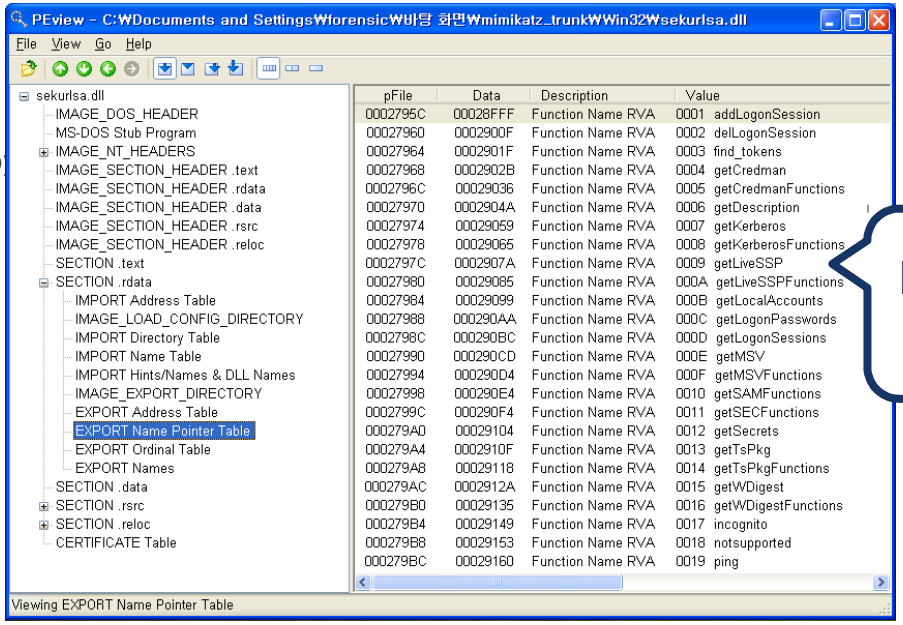


Forensic Analysis

Program Execution

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

- This DLL is used b



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.

Attack Automation~!!

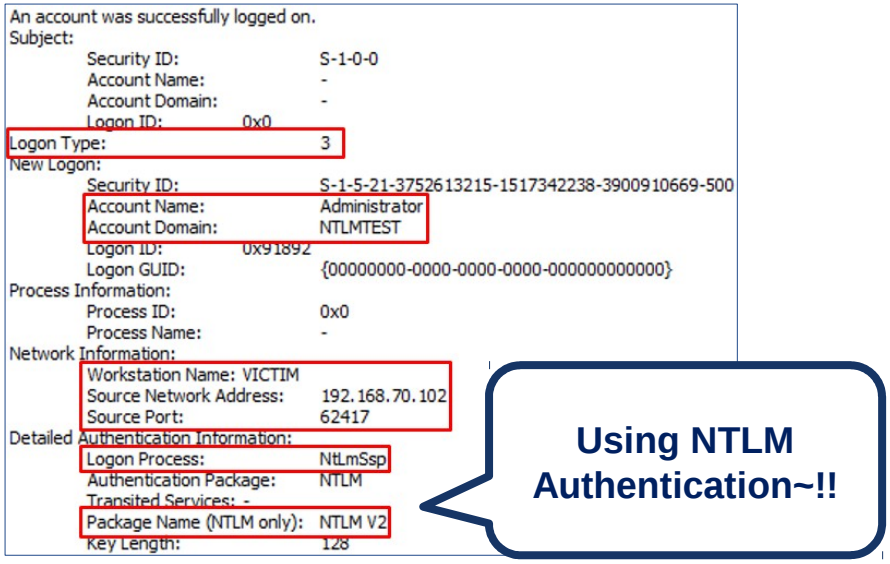
```
A logon was attempted using explicit credentials.
Subject:
        Security ID:            S-1-5-21-1992302423-290508237-277687817-1000
        Account Name:           vmuser
        Account Domain:         VICTIM
        Logon ID:       0x424ee
        Logon GUID:             {00000000-0000-0000-0000-000000000000}
Account Whose Credentials Were Used:
        Account Name:           administrator
        Account Domain:         ntlmtest
        Logon GUID:             {00000000-0000-0000-0000-000000000000}
Target Server:
        Target Server Name:     mssql.ntlmtest.com
        Additional Information: mssql.ntlmtest.com
Process Information:
        Process ID:             0x4
        Process Name:
Network Information:
        Network Address:        -
        Port:                   -
```

Type	Date	Time	Event	Source	Category
Audit Success	7/13/2013	4:15:13 PM	4648	Microsoft-Windows-Security-Auditing	Logon
Audit Success	7/13/2013	4:15:13 PM	4648	Microsoft-Windows-Security-Auditing	Logon
Audit Success	7/13/2013	4:15:13 PM	4648	Microsoft-Windows-Security-Auditing	Logon
Audit Success	7/13/2013	4:15:13 PM	4648	Microsoft-Windows-Security-Auditing	Logon
Audit Success	7/13/2013	4:15:13 PM	4648	Microsoft-Windows-Security-Auditing	Logon
Audit Success	7/13/2013	4:15:13 PM	4648	Microsoft-Windows-Security-Auditing	Logon
Audit Success	7/13/2013	4:15:13 PM	4648	Microsoft-Windows-Security-Auditing	Logon
Audit Success	7/13/2013	4:15:13 PM	4648	Microsoft-Windows-Security-Auditing	Logon
Audit Success	7/13/2013	4:15:13 PM	4648	Microsoft-Windows-Security-Auditing	Logon
Audit Success	7/13/2013	4:15:13 PM	4648	Microsoft-Windows-Security-Auditing	Logon
Audit Success	7/13/2013	4:15:14 PM	4648	Microsoft-Windows-Security-Auditing	Logon
Audit Success	7/13/2013	4:15:14 PM	4648	Microsoft-Windows-Security-Auditing	Logon
Audit Success	7/13/2013	4:15:14 PM	4648	Microsoft-Windows-Security-Auditing	Logon
Audit Success	7/13/2013	4:15:14 PM	4648	Microsoft-Windows-Security-Auditing	Logon
Audit Success	7/13/2013	4:15:14 PM	4648	Microsoft-Windows-Security-Auditing	Logon

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**

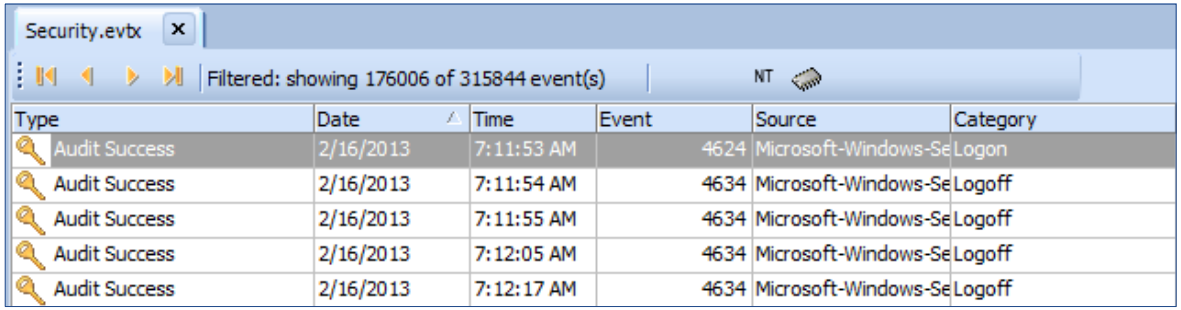


Forensic Analysis

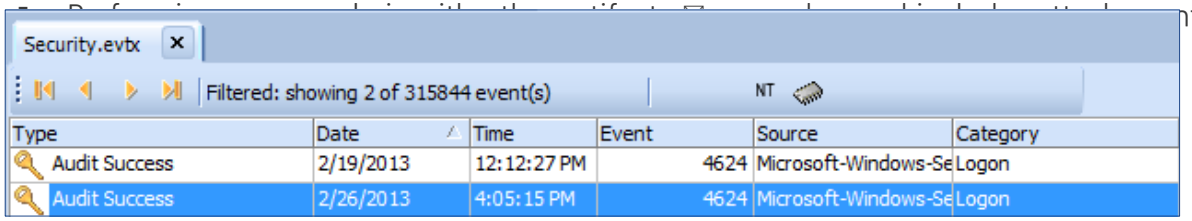
NTLM Authentication

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

✓



Type	Date	Time	Event	Source	Category
Audit Success	2/16/2013	7:11:53 AM	4624	Microsoft-Windows-Se	Logon
Audit Success	2/16/2013	7:11:54 AM	4634	Microsoft-Windows-Se	Logoff
Audit Success	2/16/2013	7:11:55 AM	4634	Microsoft-Windows-Se	Logoff
Audit Success	2/16/2013	7:12:05 AM	4634	Microsoft-Windows-Se	Logoff
Audit Success	2/16/2013	7:12:17 AM	4634	Microsoft-Windows-Se	Logoff

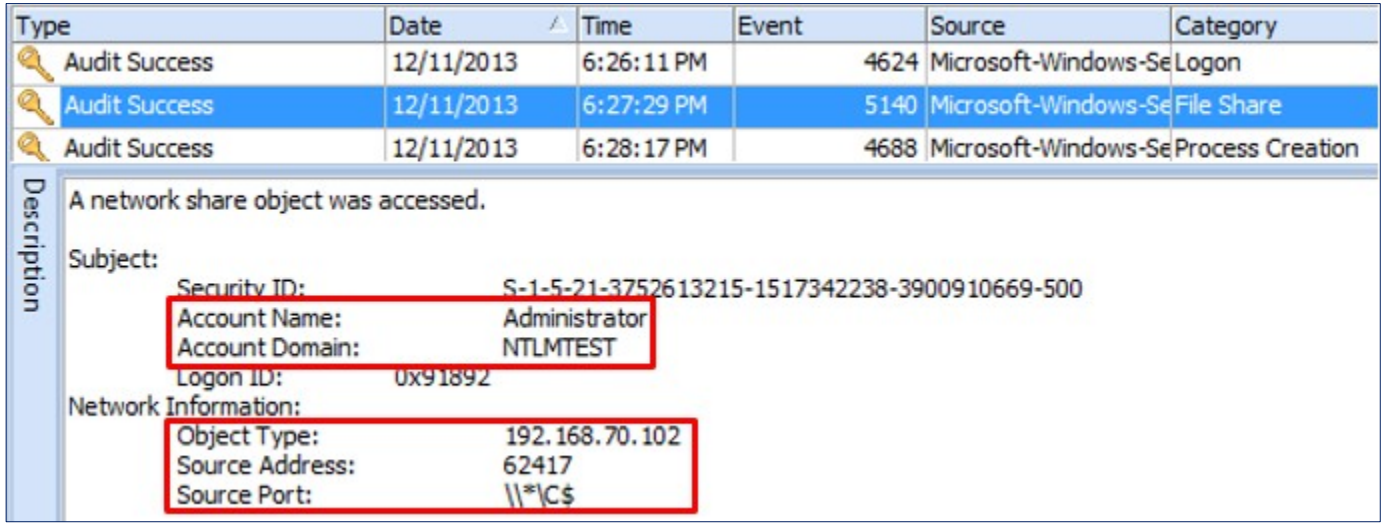


Type	Date	Time	Event	Source	Category
Audit Success	2/19/2013	12:12:27 PM	4624	Microsoft-Windows-Se	Logon
Audit Success	2/26/2013	4:05:15 PM	4624	Microsoft-Windows-Se	Logon

Forensic Analysis

Copying Backdoor

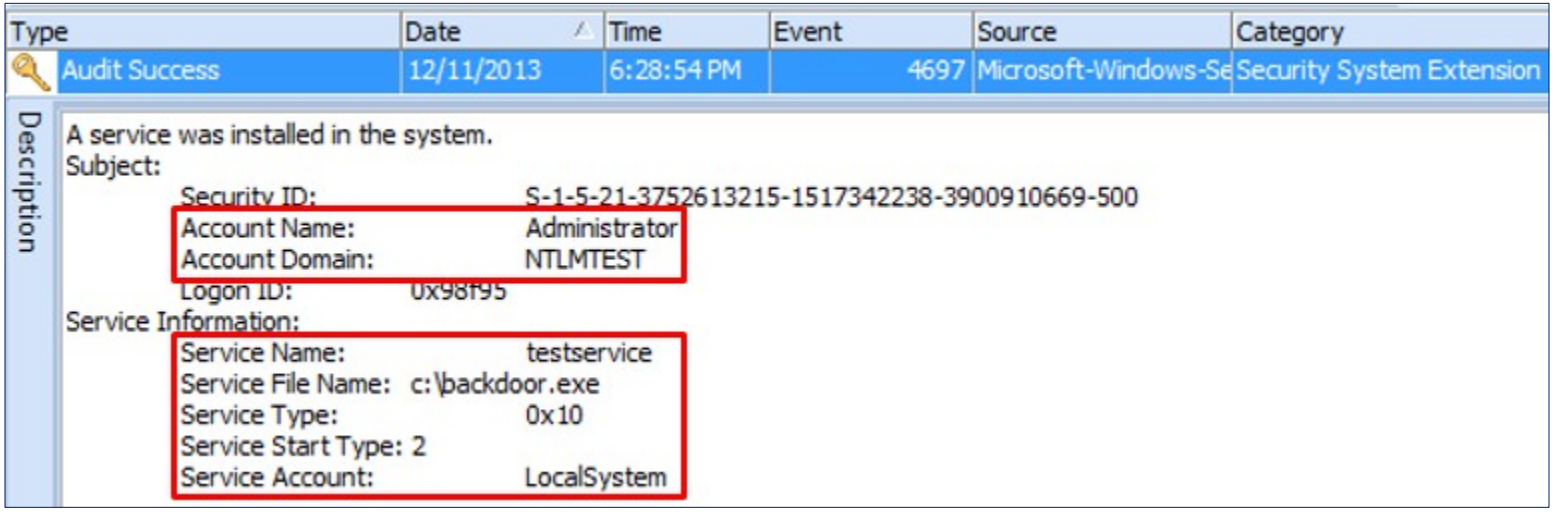
- **Location : Victim System**
- **Artifact : Security Event Log**
  - ✓ **File share** ☒ ID : **5140** (Not default)
    - Information
      - New Logon : Account Name, Domain
      - Network Information : System IP, Network Share Point



Forensic Analysis

Remote service registration/execution

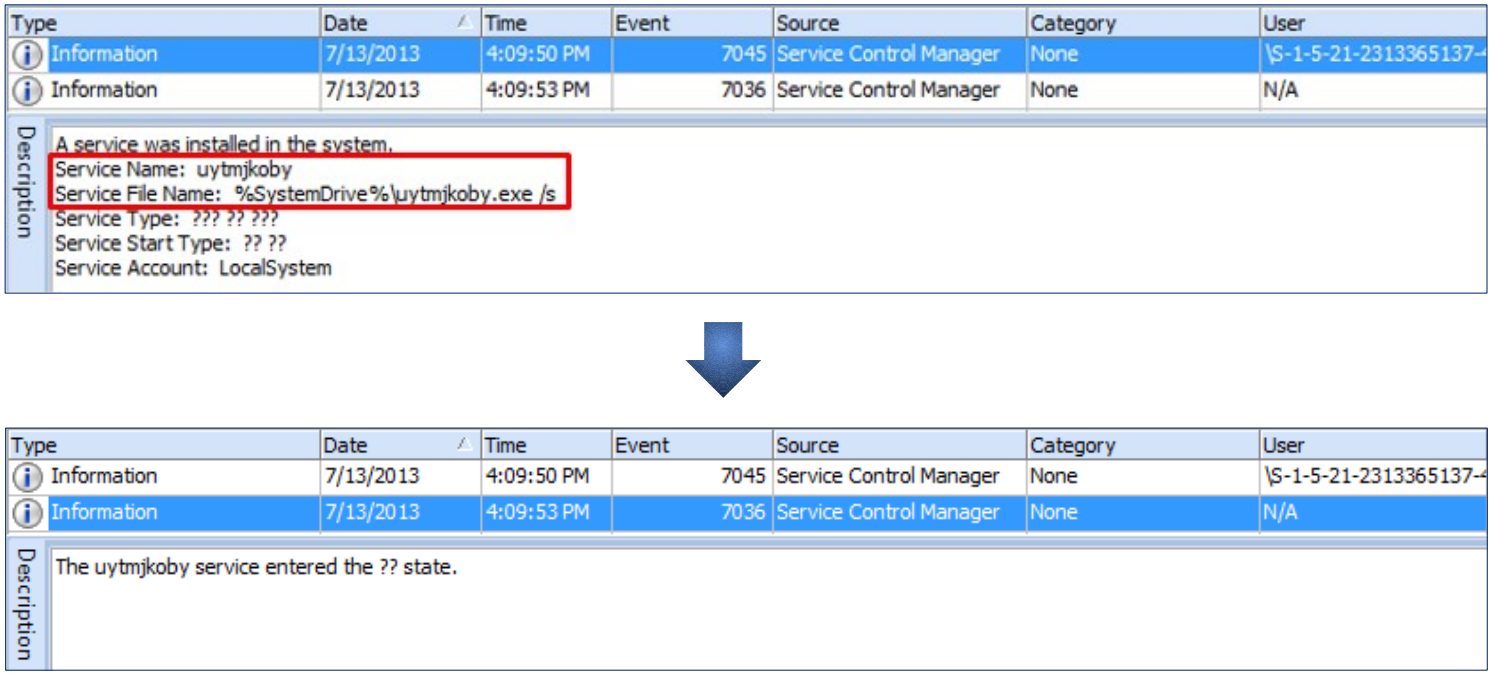
- Location : Victim System
- Artifact : Security Event Log
  - ✓ **Service Installation** ☒ **ID : 4697** (Not Default)
    - Information
      - Account Name, Domain
      - Service Name, Service File Name



Forensic Analysis

Remote service registration/execution

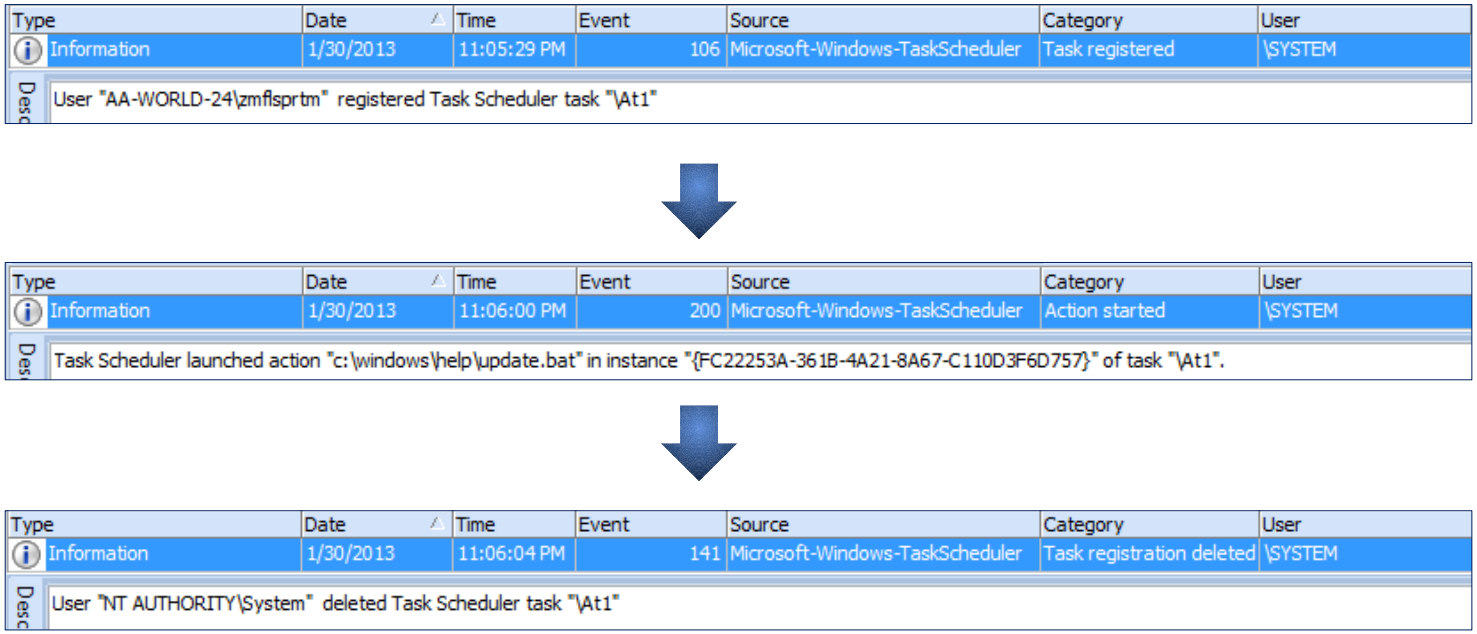
- Location : Victim System
- Artifact : SYSTEM Event Log
  - ✓ Service Installation ☒ ID : 7045
    - Information
      - Service Name
      - Service File Name
  - ✓ Changing Service State ☒ ID : 7036
    - Information
      - Whether backdoor is executed or not



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



Type	Date	Time	Event	Source	Category	User
Information	1/30/2013	11:05:29 PM	106	Microsoft-Windows-TaskScheduler	Task registered	\SYSTEM

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

Type	Date	Time	Event	Source	Category	User
Information	1/30/2013	11:06:00 PM	200	Microsoft-Windows-TaskScheduler	Action started	\SYSTEM

Task Scheduler launched action "c:\windows\help\update.bat" in instance "{FC22253A-361B-4A21-8A67-C110D3F6D757}" of task "\At1".

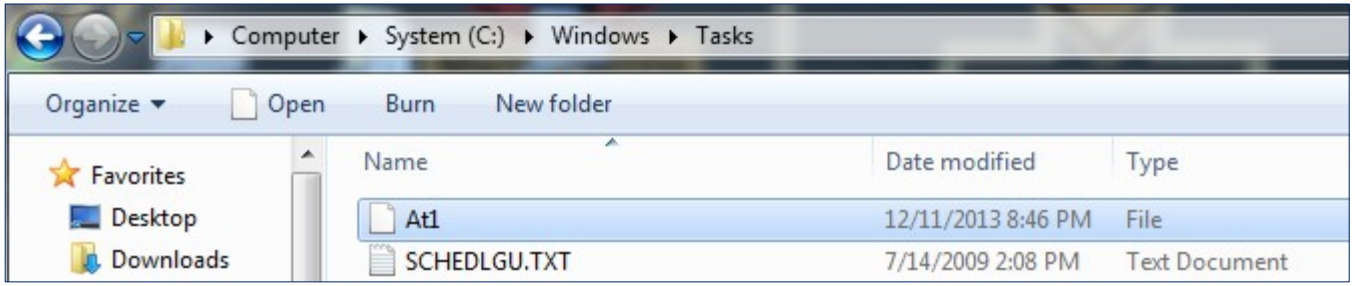
Type	Date	Time	Event	Source	Category	User
Information	1/30/2013	11:06:04 PM	141	Microsoft-Windows-TaskScheduler	Task registration deleted	\SYSTEM

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



✓

Name	File Created	Last Written	Last Accessed	Entry Modified
Tasks	2008-01-19 18:41:39	2013-07-24 21:27:32	2013-07-24 21:27:32	2013-07-24 21:27:32

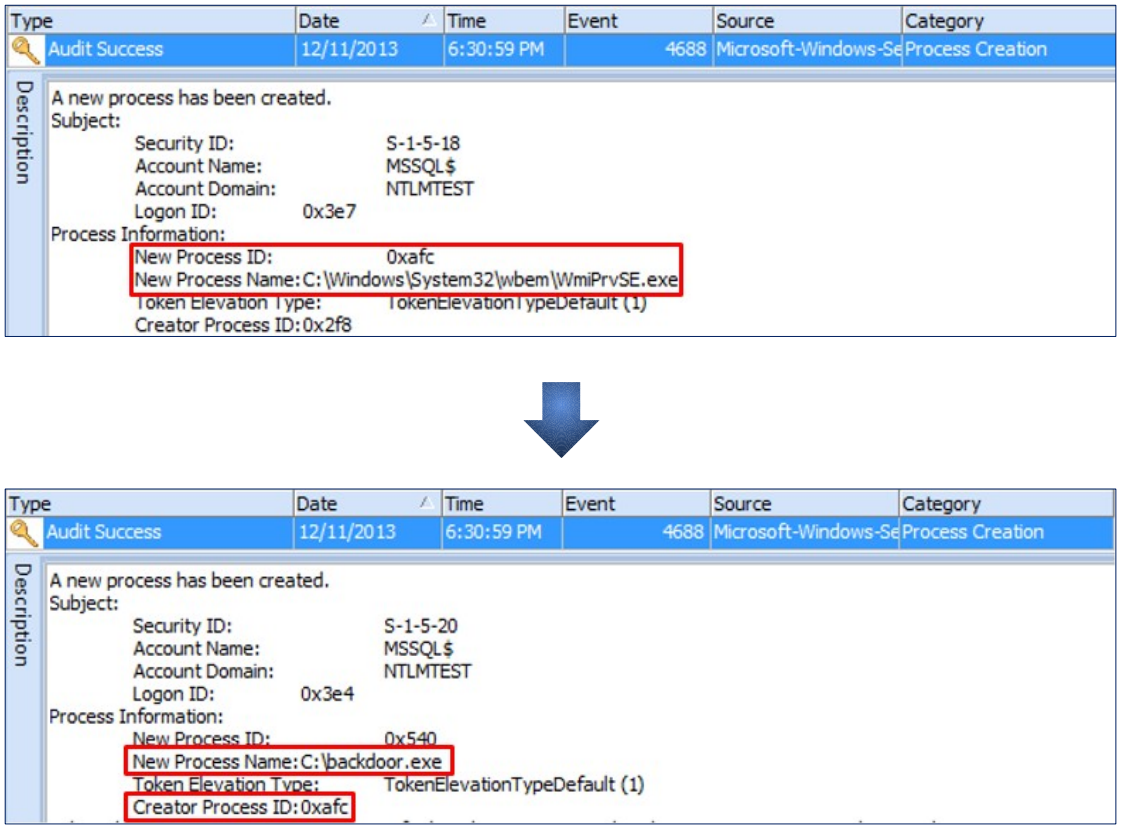
- ➢ Last Written
- ➢ Last Accessed
- ➢ MFT Entry Mdofied

Name	File Created	Last Written	Last Accessed	Entry Modified
Tasks	2008-01-19 18:41:39	2013-07-29 11:21:44	2013-07-29 11:21:44	2013-07-29 11:21:44

Forensic Analysis

Remote execution with wmic

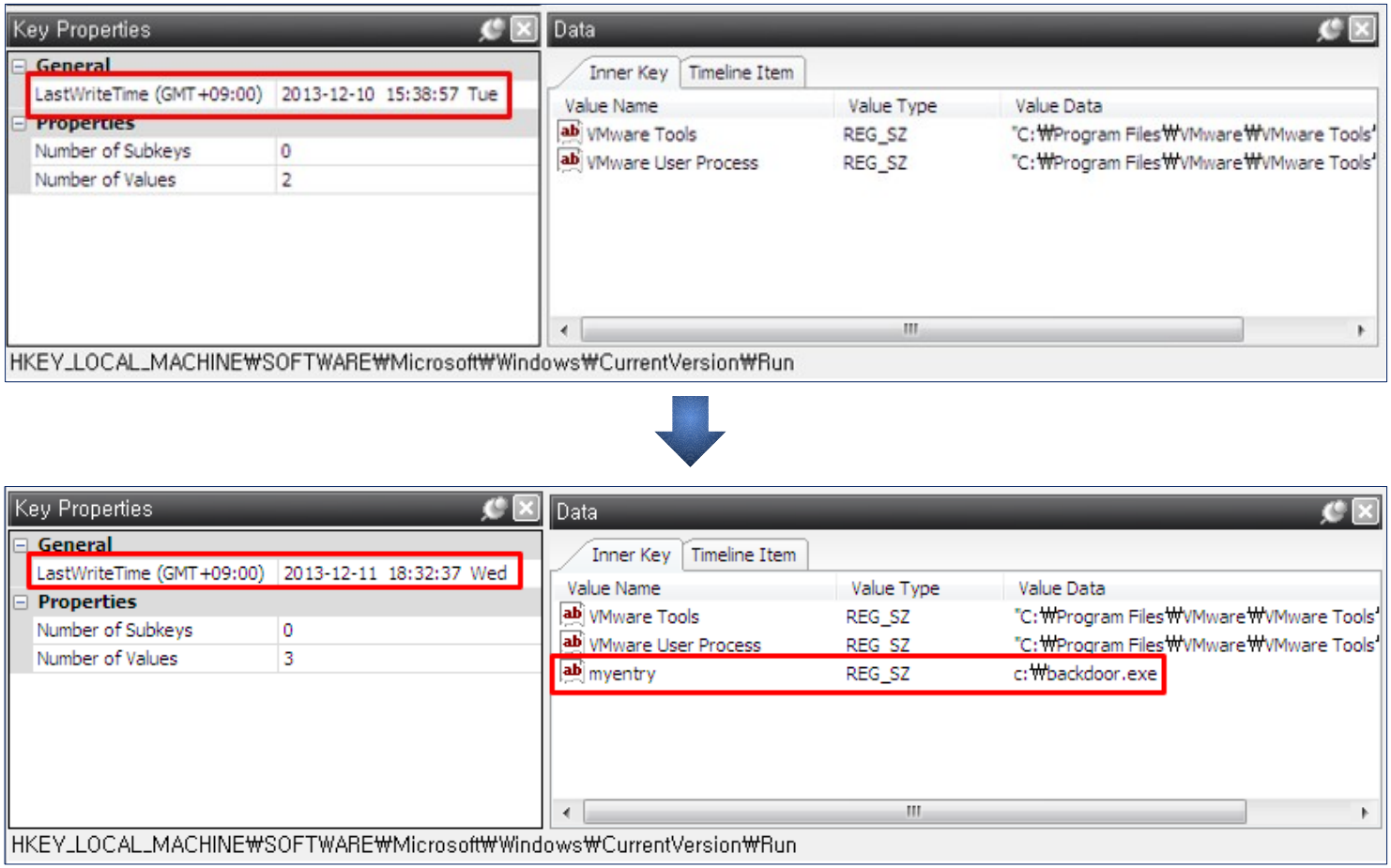
- Location : Victim System
- Artifact : Security Event Log
  - ✓ Creating Process ☒ **ID : 4688**(Not Default)
    - After creating **"WmiPrvSE.exe"** process, "**WmiPrvSE.exe**" creates backdoor process.



Forensic Analysis

Remote registry registration

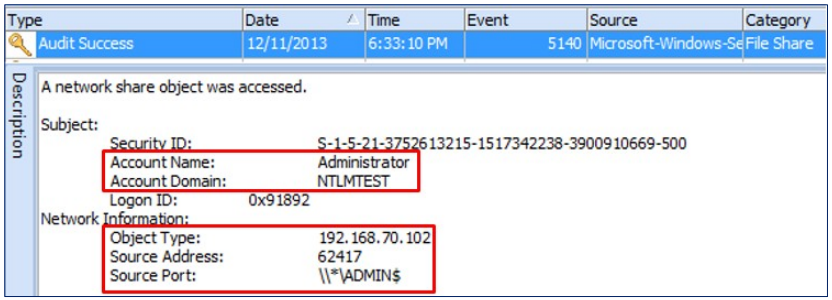
- **Location : Victim System**
- **Artifact : Registry**
  - ✓ Changing “Last Written Time” of relevant key

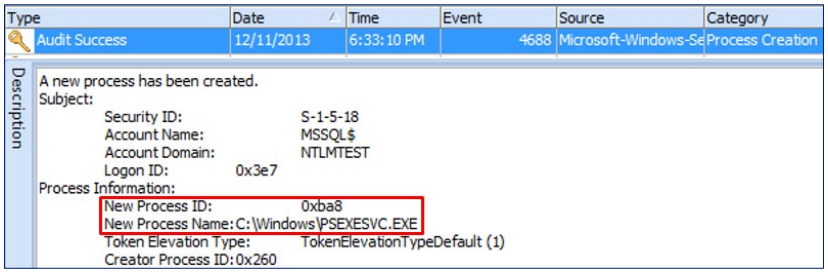


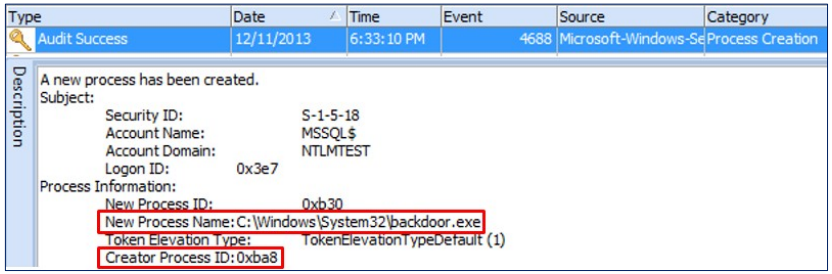
Forensic Analysis

Remote execution with psexec

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



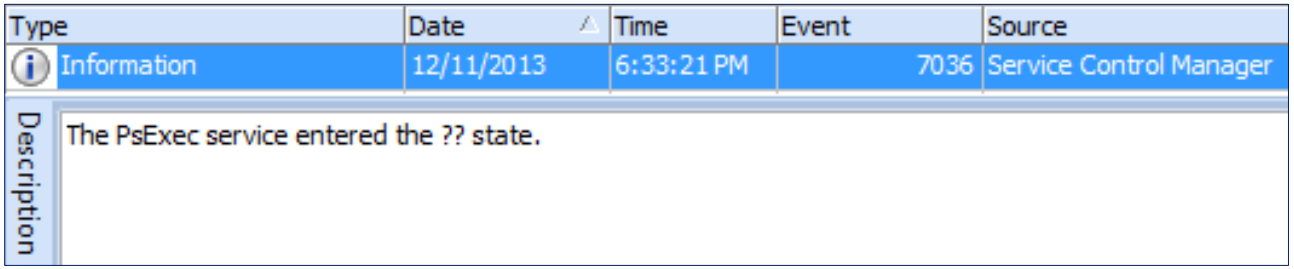




Forensic Analysis

Remote execution with psexec

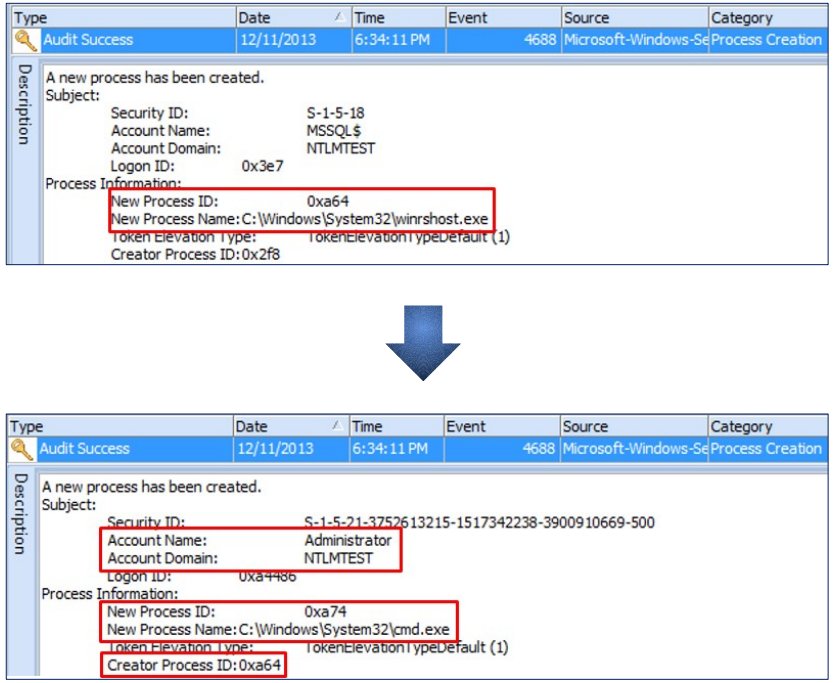
- **Location : Victim System**
- **Artifact : SYSTEM Event Log**
  - ✓ Changing Service State ☒ **ID : 7036**
    - Starting **PsExec** Service



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.



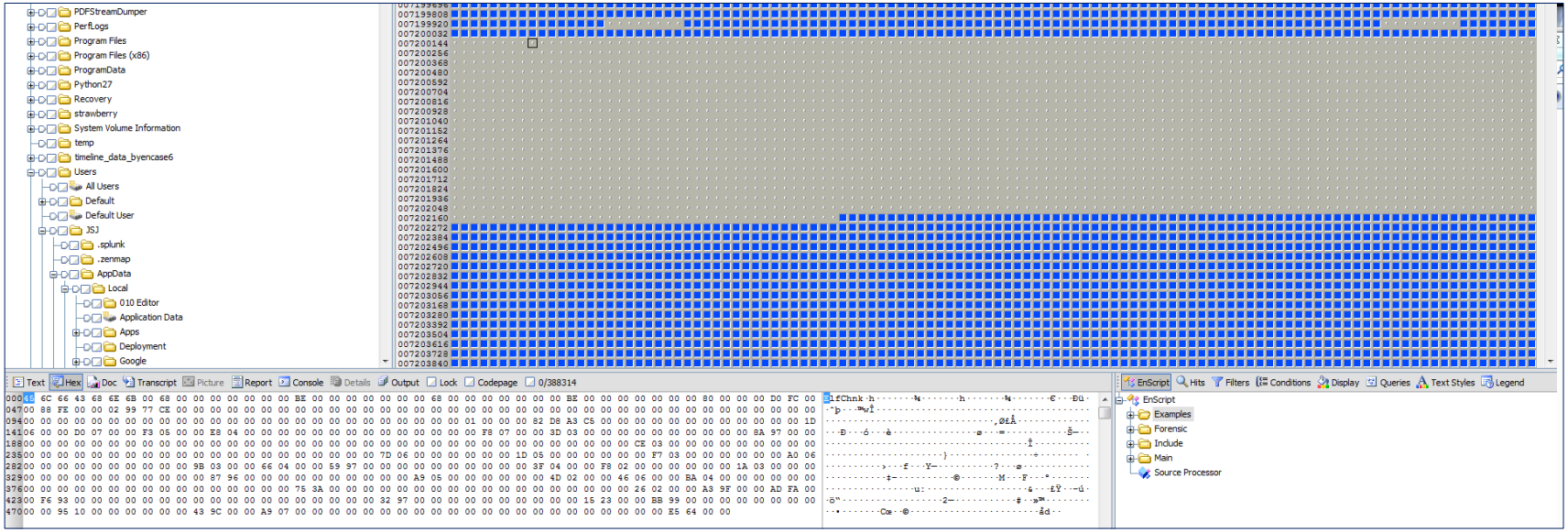
Forensic Analysis

Countermeasure for Anti Forensics

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

```
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
```

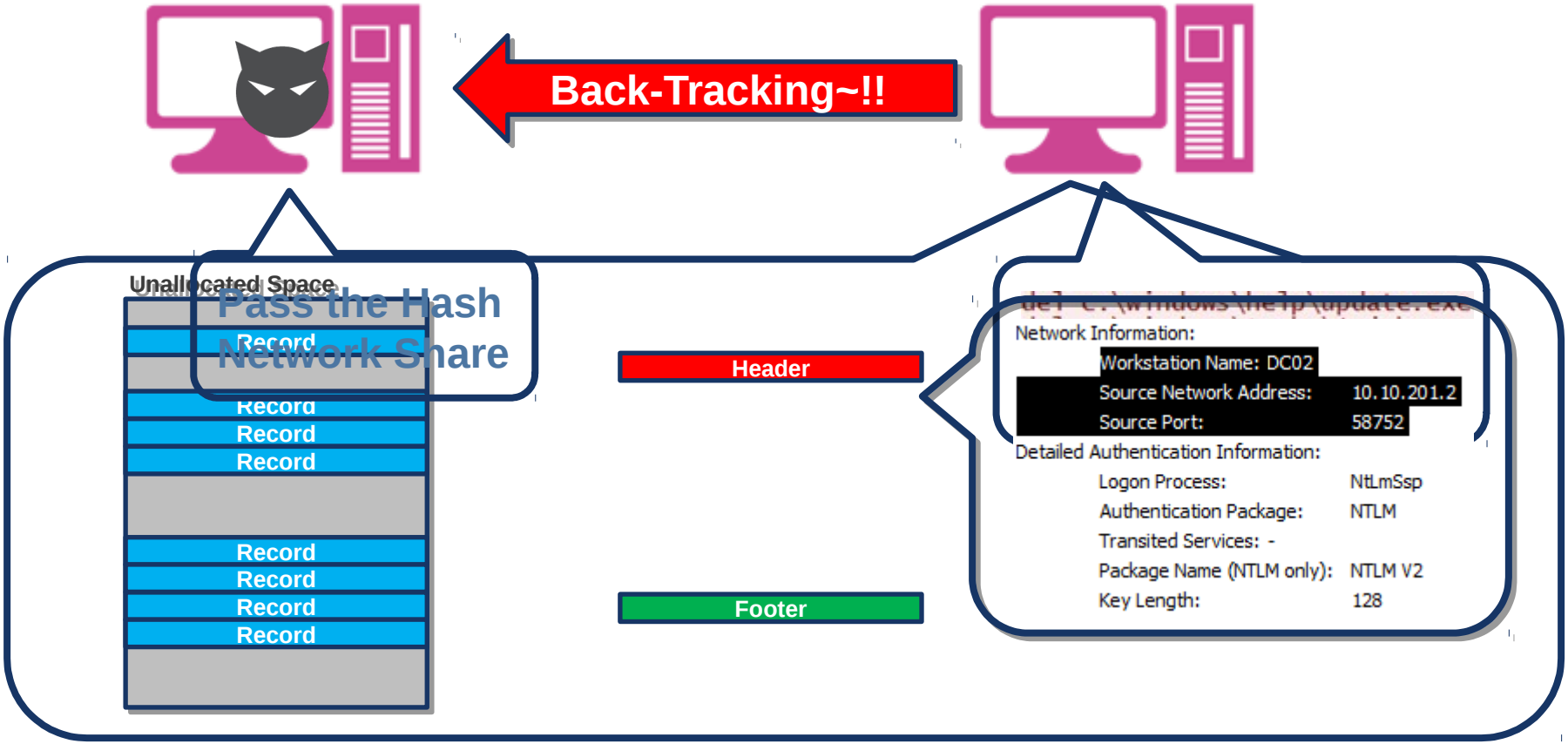
- **Countermeasure**



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

date_time	MACB	source	sourcetype	type	desc
2013-01-24 17:27:03	M...	LNK	Shortcut LNK	Modified	D:/04 SE Â±Â³ÃÂ° Â°Ã¼Â·Ã Â¹Â®Â¼Â-/04 2013 Â½ÃÃÃÂ»Ã§Â¿Ã¸SEÂ±Â³ÃÂ°Â±Â³Ã
2013-01-24 17:27:03	M..B	FILE	NTFS $MFT	$FN [M.CB] time	/System Volume Information/_restore{ACC8F1B1-F08E-4864-ACF1-9593F9388A97}/RP
2013-01-24 17:27:03	M..B	FILE	NTFS $MFT	$SI [M..B] time	/System Volume Information/_restore{ACC8F1B1-F08E-4864-ACF1-9593F9388A97}/RP
2013-01-24 17:28:00	M.C.	FILE	NTFS $MFT	$SI [M.C.] time	/WINDOWS/Tasks
2013-01-24 17:28:07	...B	FILE	NTFS $MFT	$FN [MACB] time	/WINDOWS/winhlp64
2013-01-24 17:28:07	...B	FILE	NTFS $MFT	$SI [...B] time	/WINDOWS/winhlp64
2013-01-24 17:28:29	...B	FILE	NTFS $MFT	$FN [...B] time	/RECYCLER/S-1-5-21-3297718615-3026638807-3313227778-13039/DC784~1.PPT
2013-01-24 17:28:29	...B	FILE	NTFS $MFT	$SI [...B] time	/RECYCLER/S-1-5-21-3297718615-3026638807-3313227778-13039/DC784~1.PPT

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

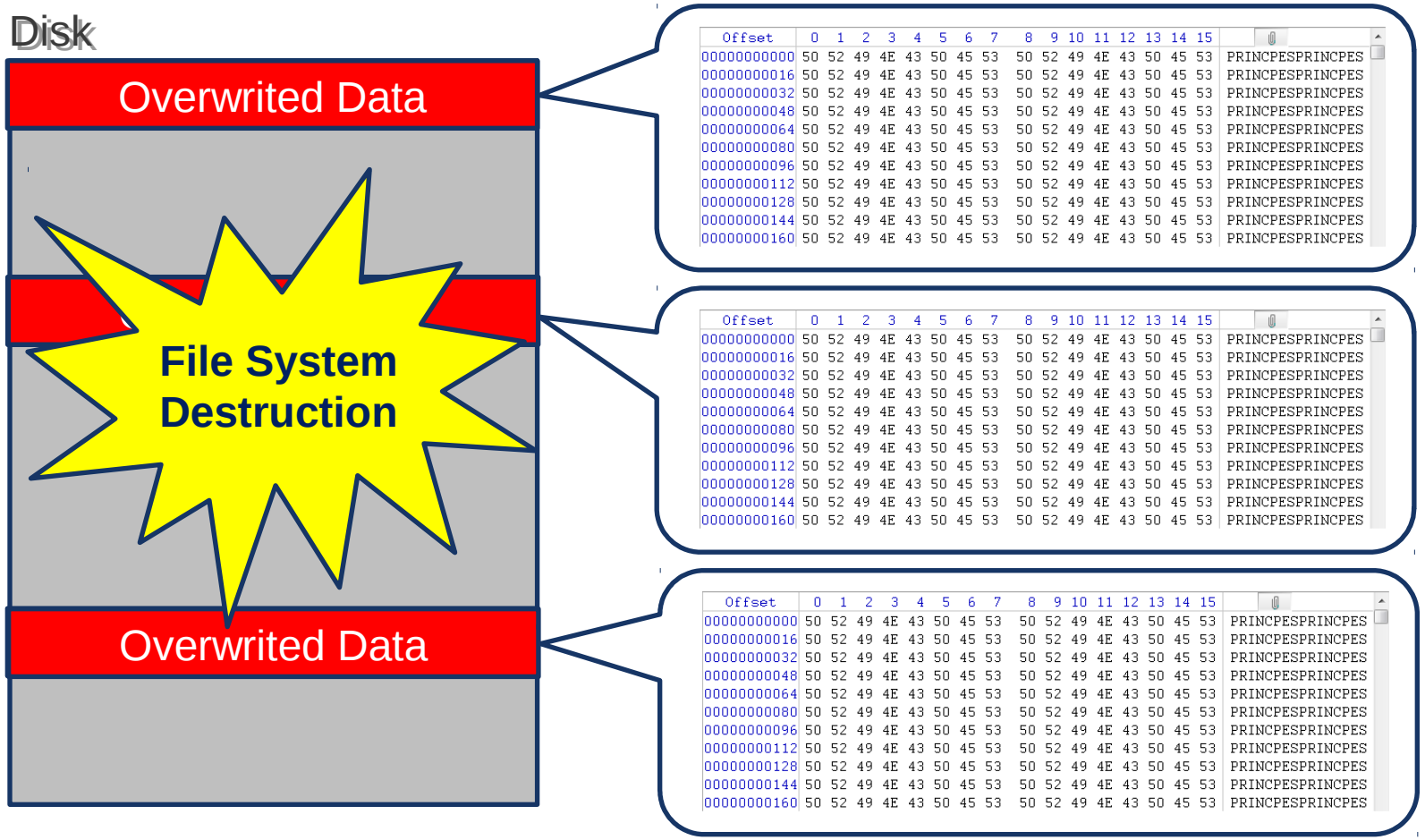
TimeStamp	USN	FileName	Full Path(from $MFT)	Event
2012-12-25 00:58:55	461968376	net6.bat	₩Windows₩IME₩net6.bat	File_Created
2012-12-25 00:58:55	461968456	net6.bat	₩Windows₩IME₩net6.bat	File_Created, File_Added
2012-12-25 00:58:55	461968536	net6.bat	₩Windows₩IME₩net6.bat	File_Created, File_Added, Data_Overwritten
2012-12-25 00:58:55	461968616	net6.bat	₩Windows₩IME₩net6.bat	File_Created, Attr_Changed, File_Added, Data_Overwritten
2012-12-25 00:58:55	461968696	net6.cpl	₩Windows₩IME₩net6.cpl	File_Created
2012-12-25 00:58:55	461968776	net6.cpl	₩Windows₩IME₩net6.cpl	File_Created, File_Added
2012-12-25 00:58:55	461968856	net6.cpl	₩Windows₩IME₩net6.cpl	File_Created, File_Added, Data_Overwritten
2012-12-25 00:58:55	461968936	net6.cpl	₩Windows₩IME₩net6.cpl	File_Created, Attr_Changed, File_Added, Data_Overwritten
2012-12-25 00:58:55	461969016	net6.exe	₩Windows₩IME₩net6.exe	File_Created
2012-12-25 00:58:55	461969096	net6.exe	₩Windows₩IME₩net6.exe	File_Created, File_Added
2012-12-25 00:58:55	461969176	net6.exe	₩Windows₩IME₩net6.exe	File_Created, File_Added, Data_Overwritten
2012-12-25 00:58:55	461969256	net6.exe	₩Windows₩IME₩net6.exe	File_Created, Attr_Changed, File_Added, Data_Overwritten
2012-12-25 00:59:07	461969336	net6.bat	₩Windows₩IME₩net6.bat	File_Created, Attr_Changed, File_Added, Data_Overwritten, File_Closed
2012-12-25 00:59:07	461969416	net6.cpl	₩Windows₩IME₩net6.cpl	File_Created, Attr_Changed, File_Added, Data_Overwritten, File_Closed
2012-12-25 00:59:07	461969496	net6.exe	₩Windows₩IME₩net6.exe	File_Created, Attr_Changed, File_Added, Data_Overwritten, File_Closed

TimeStamp	USN	FileName	Full Path(from $MFT)	Event
2012-12-25 01:59:12	462450008	net6.bat	₩Windows₩debug₩net6.bat	File_Closed, File_Deleted
2012-12-25 01:59:12	462450088	net6.cpl	₩Windows₩debug₩net6.cpl	File_Closed, File_Deleted
2012-12-25 01:59:12	462450168	net6.exe	₩Windows₩debug₩net6.exe	File_Closed, File_Deleted

Forensic Analysis

Countermeasure for Anti Forensics

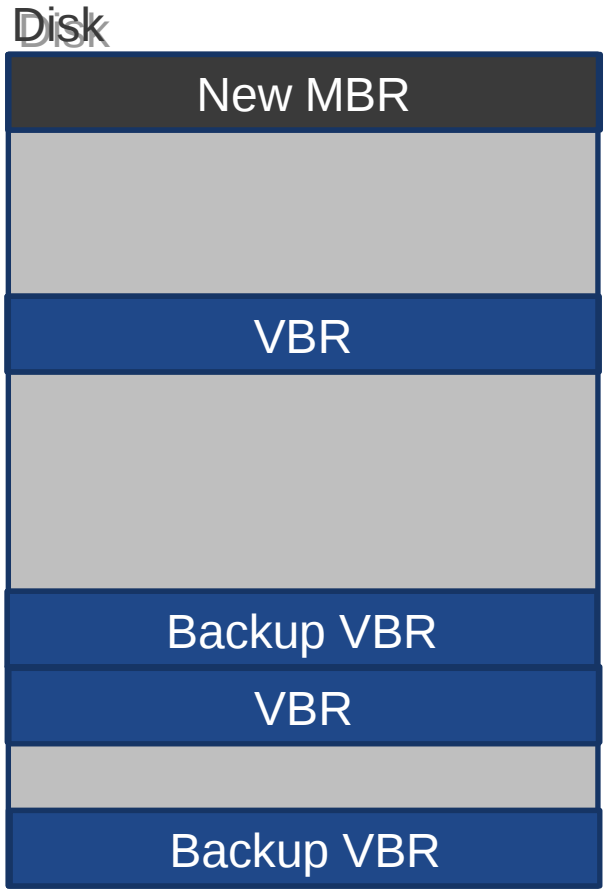
- **Disk Destruction(ex : 3.20 / 6.25 Cyber Attack in South Korea)**



Forensic Analysis

Countermeasure for Anti Forensics

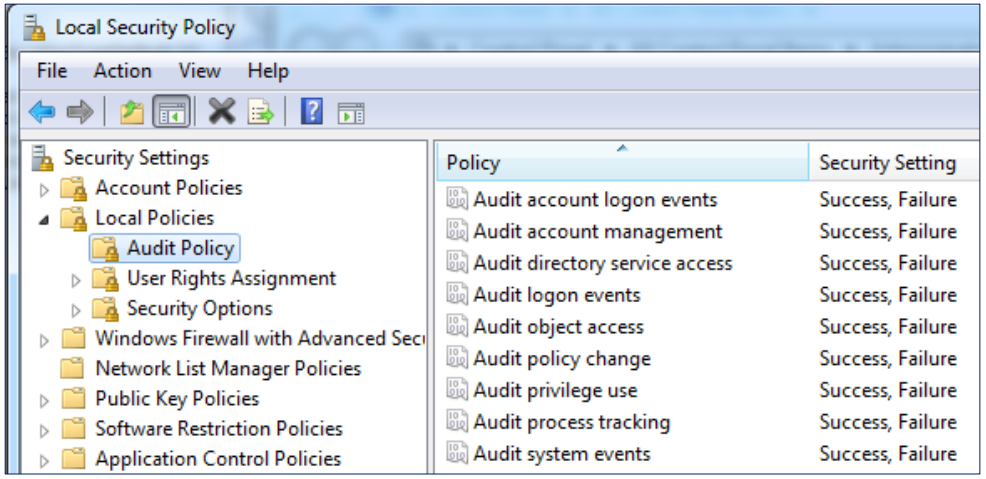
- **Countermeasure for Disk Destruction**
  - ✓ Recovering VBR by Backup VBT located in end of volume
  - ✓ Creating New MBR



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

```
C:₩>chkdsk /L:1048576
```

    - **$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.

```
C:₩>fsutil createjournal m=1073741824 a=107374182 C:
```

Forensic Analysis

Summary

- Attacker System

Behavior	Artifact	Detail
Escalation of Privileges	**Prefetch**	Program Execution
	Application Compatibility Cache	Program Execution
	RecentFileCache.bcf	Program Execution
	wceaux.dll	DLL of WCE
	sekurlsa.dll	DLL of Mimitakz
	Memory	String search
Attempting Logon	**Security Event Log**	Attempting Logon to another system with explicit credentials ID : **552(evt)** or **4648(evtx)**

Forensic Analysis

Summary

- Victim System

Behavior	Artifact	Detail
NTLM Authentication	**Security Event Log**	**Network Logon**(ID : **540** or **4624**) Logon Type : **3** Logon Process : **NtLmSsp** Package Name : **NTLM V2** or **NTLM**
	Network Traffic	Protocol : **SMB2** Characteristics 1. SessionSetup : NTLMSSP_NEGOTIATE 2. SessionSetup : NTLMSSP_AUTH, Domain, Username 3. TreeConnect : \\<IP or Host Name>**IPC$**
Copying Backdoor	**Security Event Log**	**File Share**(ID : **5140**)
	Network Traffic	Protocol : **SMB2** Characteristics 1. TreeConnect : \\<IP or Host Name>\<Share Point : **C$, D$** … > 2. Create 3. Write
Remote service registration/execution	**Security Event Log**	**Installing Service**(ID : **4697**)
	System Event Log	**Installing Service**(ID : **7045**) **Changing Service State**(ID : **7036**)
	Network Traffic	Protocol : **SVCCTL** Characteristics 1. OpenSCManager 2. CreateService or OpenService, StartService 3. CloseSeviceHandle

Forensic Analysis

Summary

- Victim System (continue…)

Behavior	Artifact	Detail
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 execution with wmic	**Security Event Log**	**Creating Process(** ID : **4688**) □ **WmiPrvSE.exe**
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…)

Behavior	Artifact	Detail
Remote execution with winrs	**Security Event Log**	**Creating Process**(ID : **4688**) → **winrshost.exe**
	Network Traffic	Protocol : **HTTP** Characteristics 1. NTLMSSSP_NEGOTIATE : **/wsman** 2. NTLMSSP_AUTH : Domain, Username

- Countermeasure for Anti Forensics

Behavior	Response	Detail
Deleting Event Log	Recovering Event Log	**Record Carving**
Deleting Job file	Keyword Search	Searching within $MFT
	Confirming **MFT Modified Time** of Tasks folder	Guessing creation and deletion time of job file
Deleting file	**Analyzing File System Log($LogFile, $UsnJrnl)**	**Using "NTFS Log Tracker"**

- Forensic Readiness

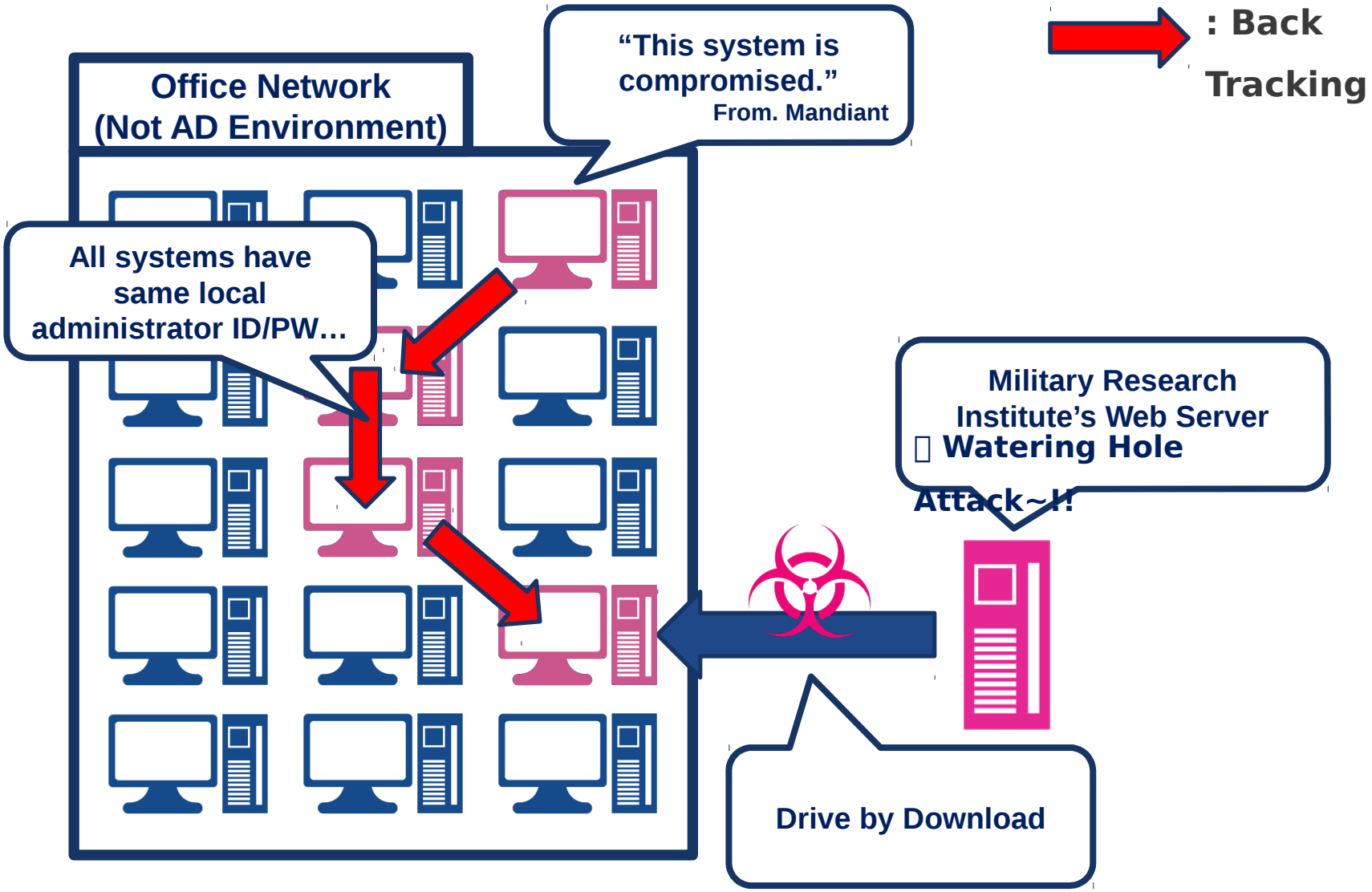
Target	Response	Detail
Event Log	Remote Backup Server	Real-time backup Backup server not included in domain
	Setting Audit Policy	Turn On all audits
	Changing size of event log file	wevtutil sl
$LogFile, $UsnJrnl	Changing size of log file	$LogFile → **chkdsk** $UsnJrnl → **fsutil**

Case Study

AhnLab

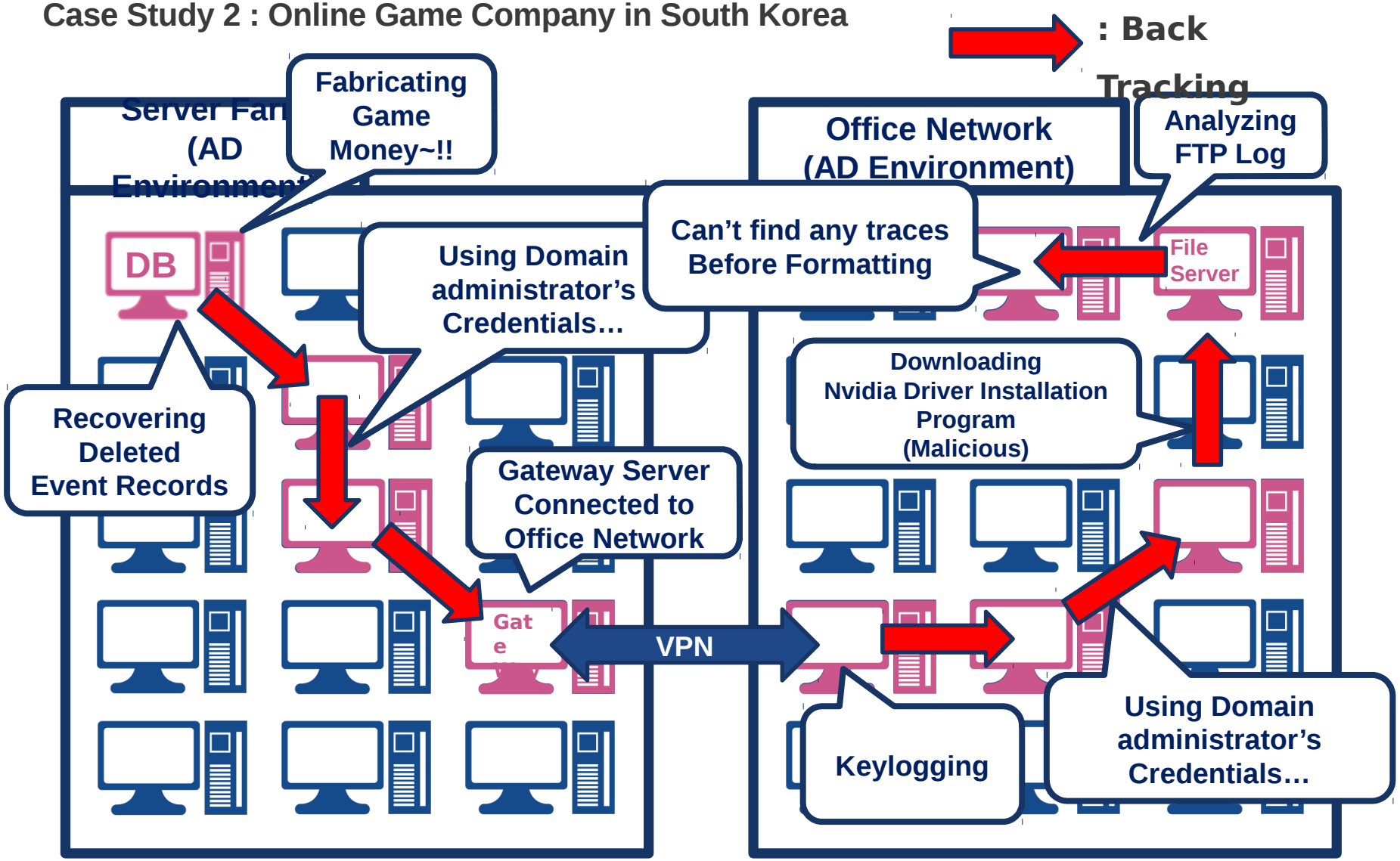
Case Study

Case Study 1 : Defense Contractor in South Korea



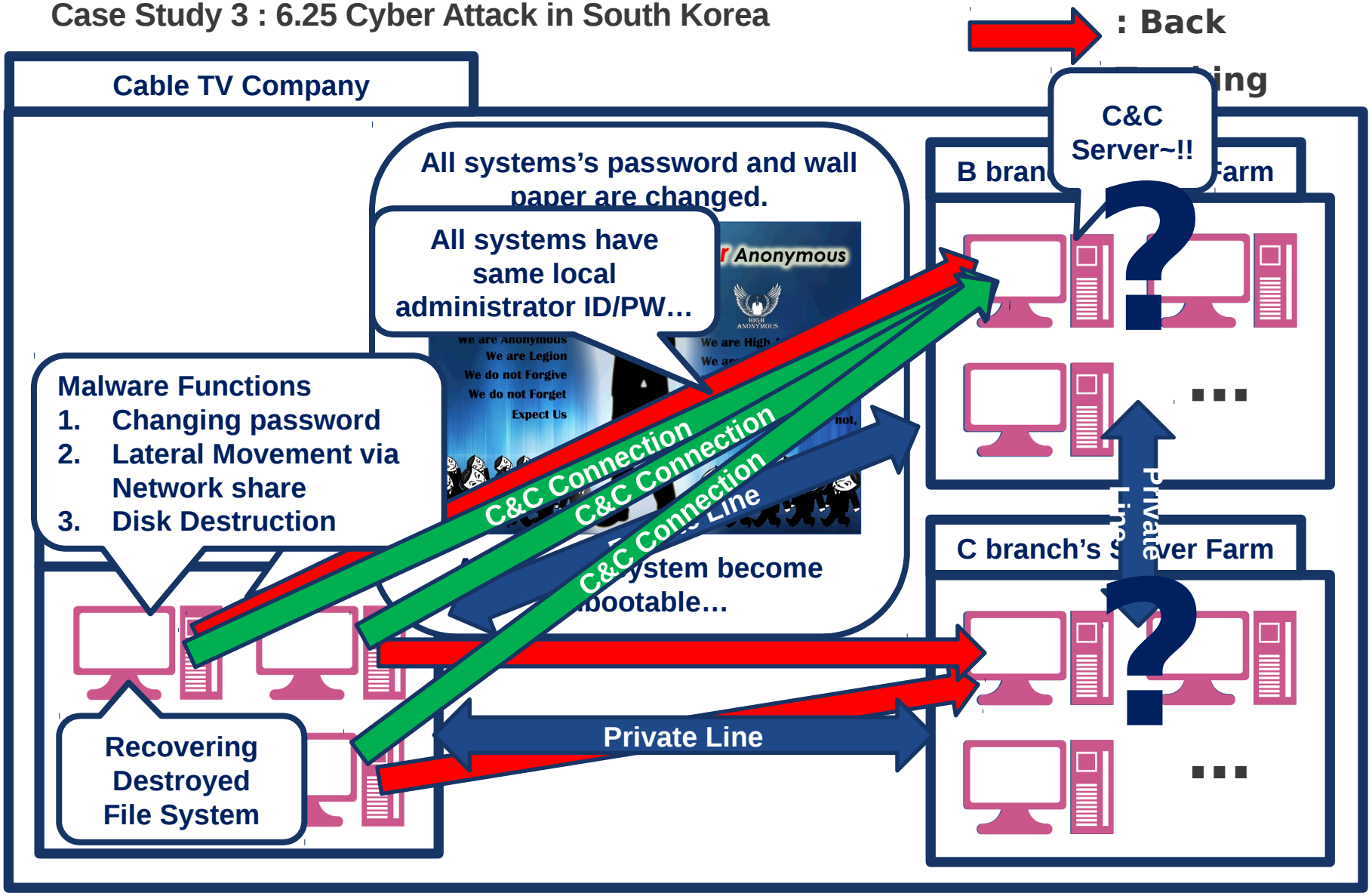
Case Study

Case Study 2 : Online Game Company in South Korea



Case Study

Case Study 3 : 6.25 Cyber Attack in South Korea



Conclusion

AhnLab

Conclusion

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

- **Forensic Analysis**
  - ✓ Malware Execution
  - ✓ Tracing NTLM Authentication
  - ✓ Countermeasure for Anti Forensics
  - ✓ Forensic Readiness

Thank you.

AhnLab

Reference

1. Mimikatz : http://blog.gentilkiwi.com/mimikatz
2. WCE : http://www.ampliasecurity.com/research/wcefaq.html
3. Authenticated Remote Code Execution Methods in Windows : http://www.scriptjunkie.us/2013/02/authenticated-remote-code-execution-methods-in-windows/
4. Mitigating Pass-the-Hash (PtH) Attacks and Other Credential Theft Techniques : http://www.microsoft.com/en-us/download/details.aspx?id=36036
5. Trust Technologies : http://technet.microsoft.com/en-us/library/cc759554(v=ws.10).aspx