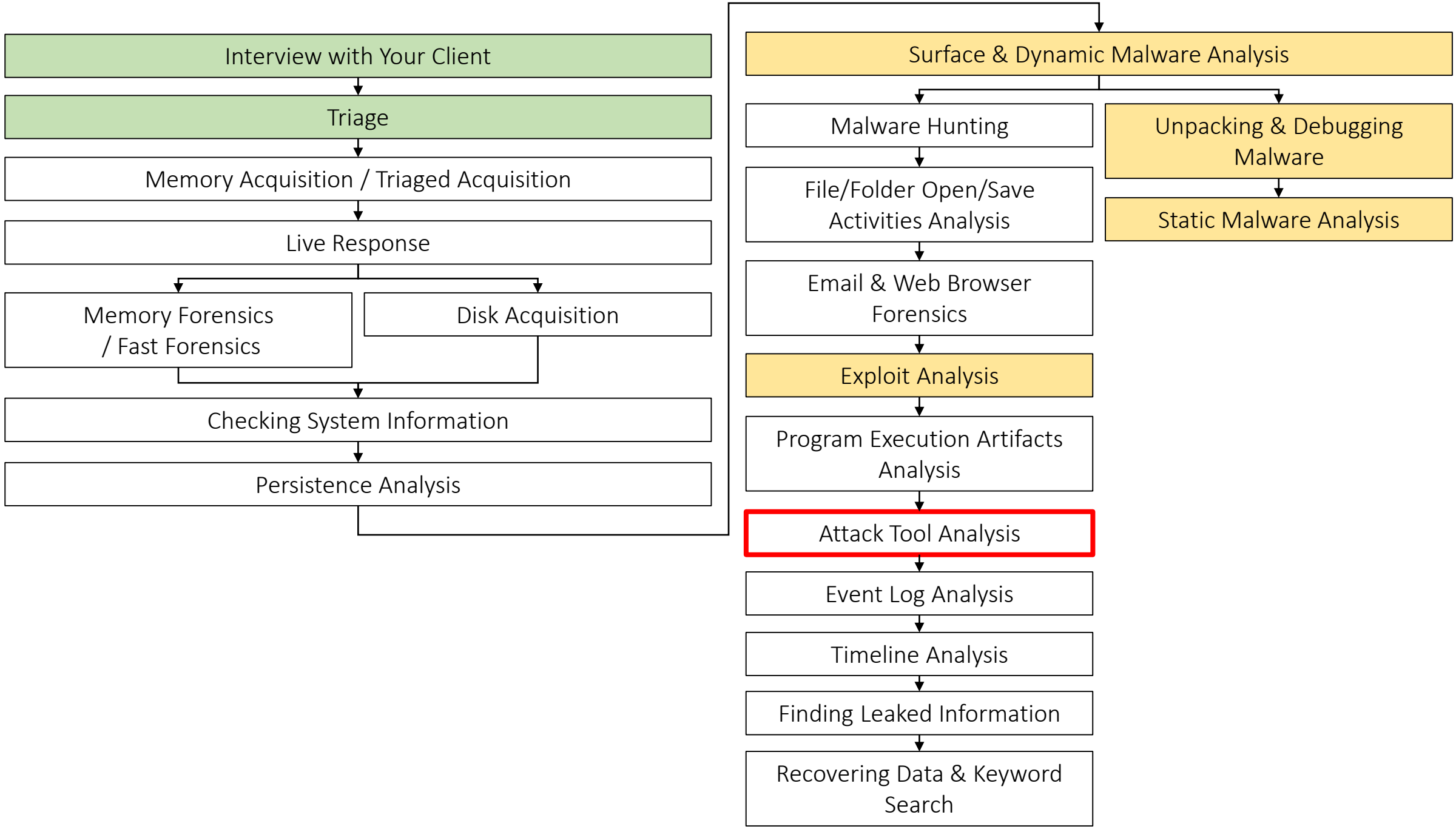
Attack Tool Analysis


Interview with Your Client
Triage
Memory Acquisition / Triaged Acquisition
Live Response
Memory Forensics / Fast Forensics
Disk Acquisition
Checking System Information
Persistence Analysis
Surface & Dynamic Malware Analysis
Malware Hunting
File/Folder Open/Save Activities Analysis
Email & Web Browser Forensics
Exploit Analysis
Program Execution Artifacts Analysis
Attack Tool Analysis
Event Log Analysis
Timeline Analysis
Finding Leaked Information
Recovering Data & Keyword Search
Unpacking & Debugging Malware
Static Malware Analysis

What is Attack Tool Analysis?

- It is to find and analyze tools that were used by attackers. It is similar to performing malware analysis and exploit analysis.
- By performing attack tool analysis, we could understand what attackers were planning to do. Moreover, it helps us to determine what they actually did.

Copyright Internet Initiative Japan Inc.

How We Perform Attack Tool Analysis

- We use both dynamic and static analysis during attack tool analysis.
- If a tool is an executable file, we typically try the dynamic analysis. Then, we perform the static analysis if necessary.
- If a tool is a bat or a script file, we just view it. Then, we execute it if necessary.

Copyright Internet Initiative Japan Inc.

Scenario 1 Labs: Lab 1

Analyzing Attacking Tools on client-win10-2

Scenario 1 Labs: Lab 1

Analyzing Attacking Tools on client-win10-2 (1)

- Conditions:
  - This is an investigation for scenario 1.
  - In Program Execution section, we found that the attacker executed some executable files such as "w10.exe" on client-win10-2.
  - These files are located under the folder "\ProgramData\s". It might be an attacker's working folder.
- Goal:
  - To find out tools placed under the folder.
  - To reveal the functions of those tools.
- Hint:
  - VSS snapshots might contain deleted files.

Copyright Internet Initiative Japan Inc.

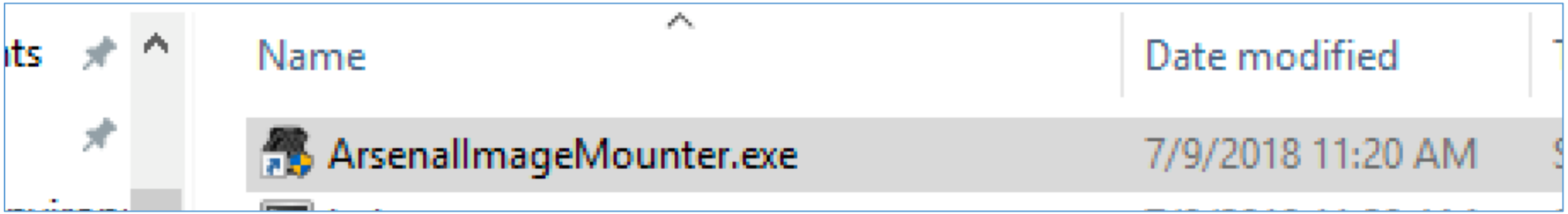
Scenario 1 Labs: Lab 1

Analyzing Attacking Tools on client-win10-2 (2)

- First of all, mount the following disk image with "Arsenal Image Mounter" in order to find the folder.
  - E:\Artifacts\scenario1_E01\Client-Win10-2_honda.E01

- Start "Arsenal Image Mounter" by double-clicking the icon in the shortcut folder.

Shortcuts\06_LateralMovementsInvestigation\0602_AttackToolsAnalysis

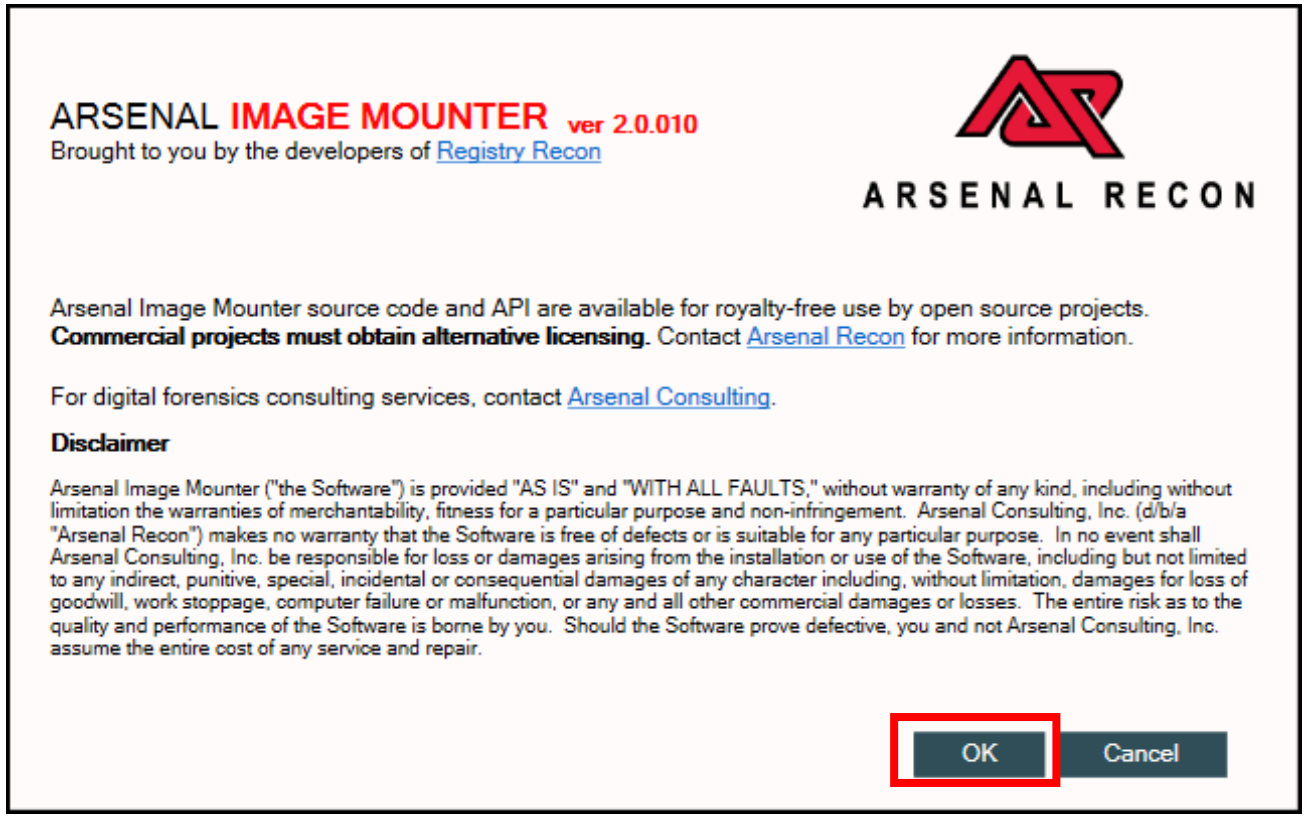


Copyright Internet Initiative Japan Inc.

Scenario 1 Labs: Lab 1

Analyzing Attacking Tools on client-win10-2 (3)

- On the license agreement window, press "OK" to continue.

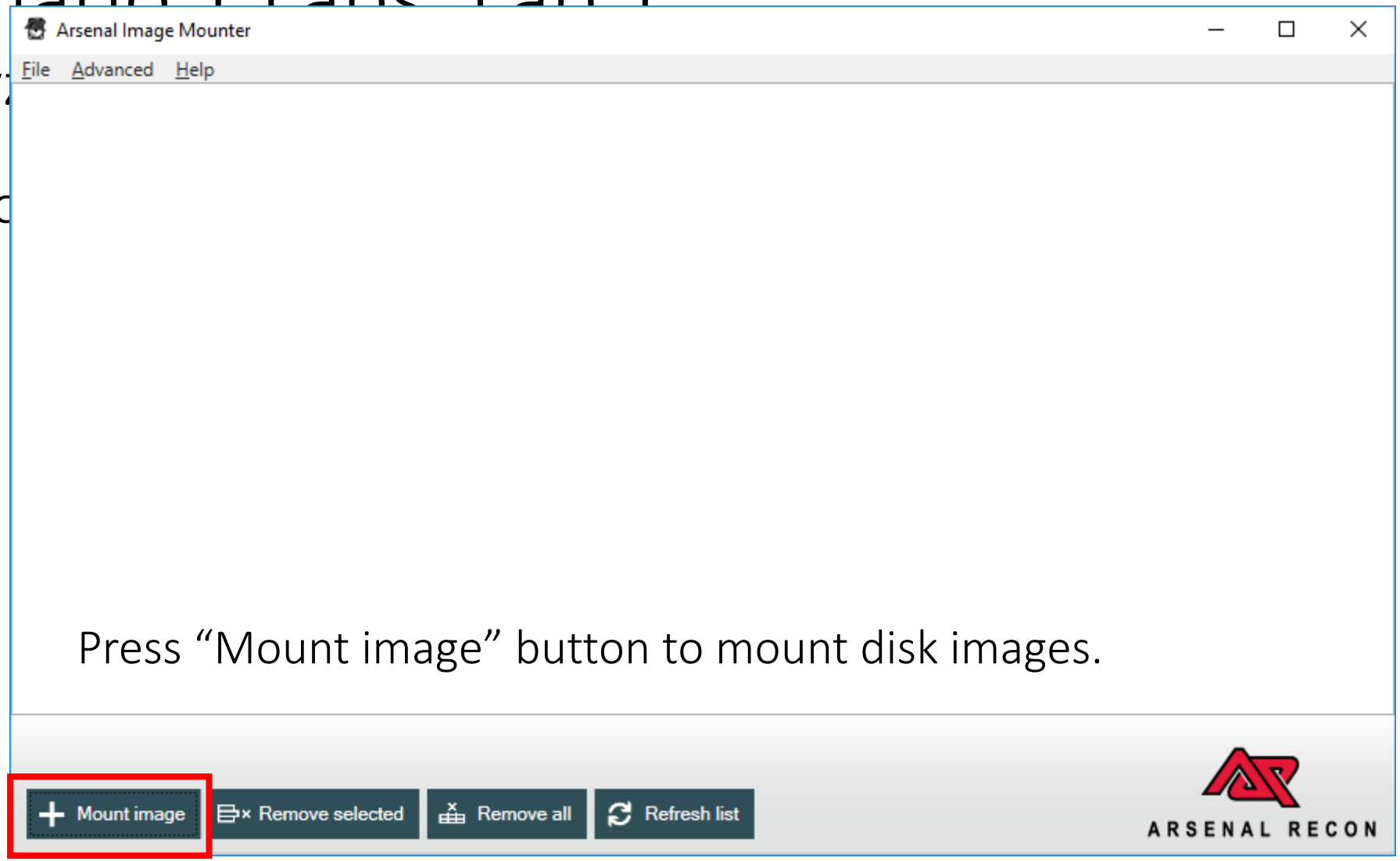


Copyright Internet Initiative Japan Inc.

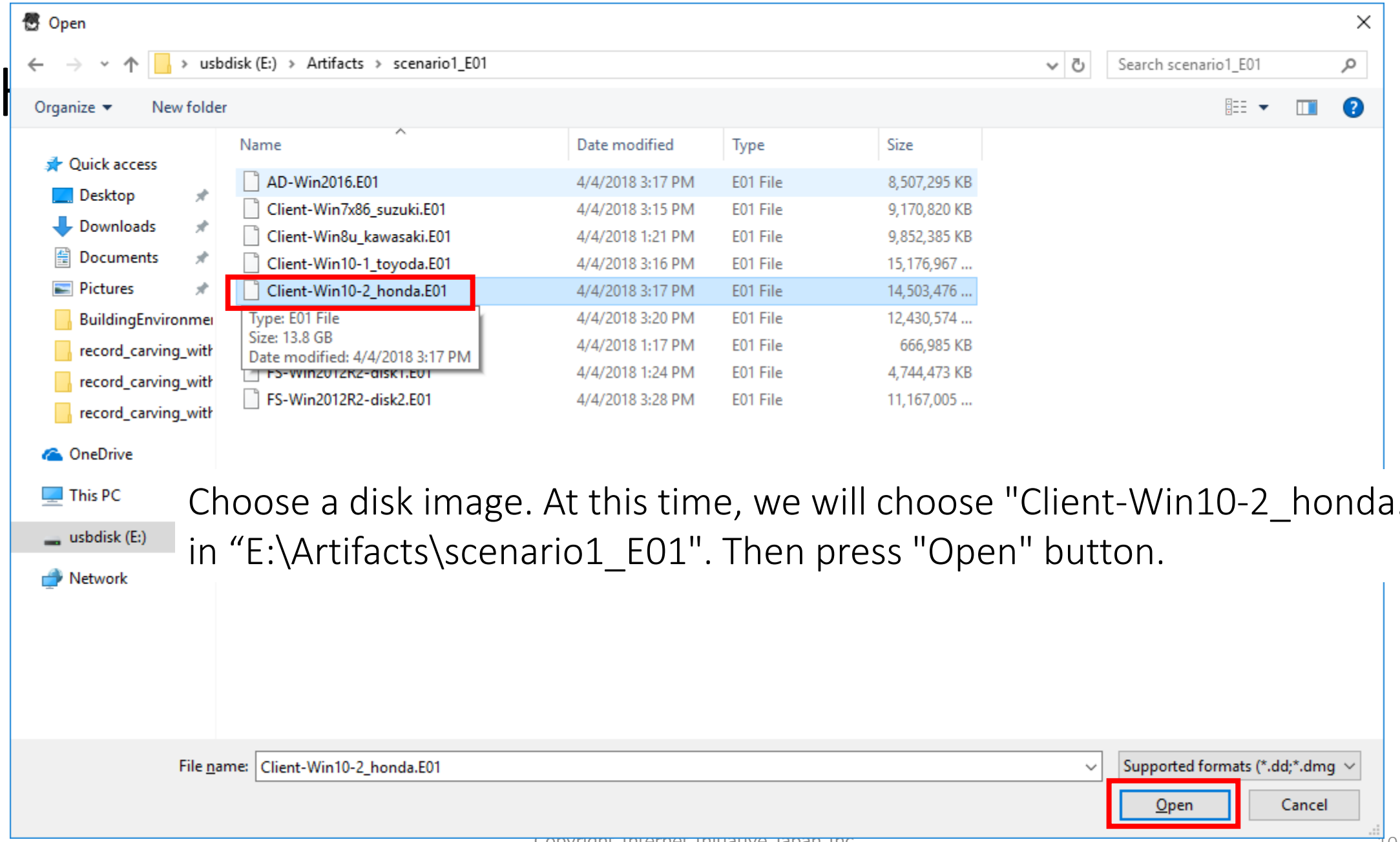
Scenario 1 Labs: Lab 1

Analy

- Resto



Copyright Internet Initiative Japan Inc.

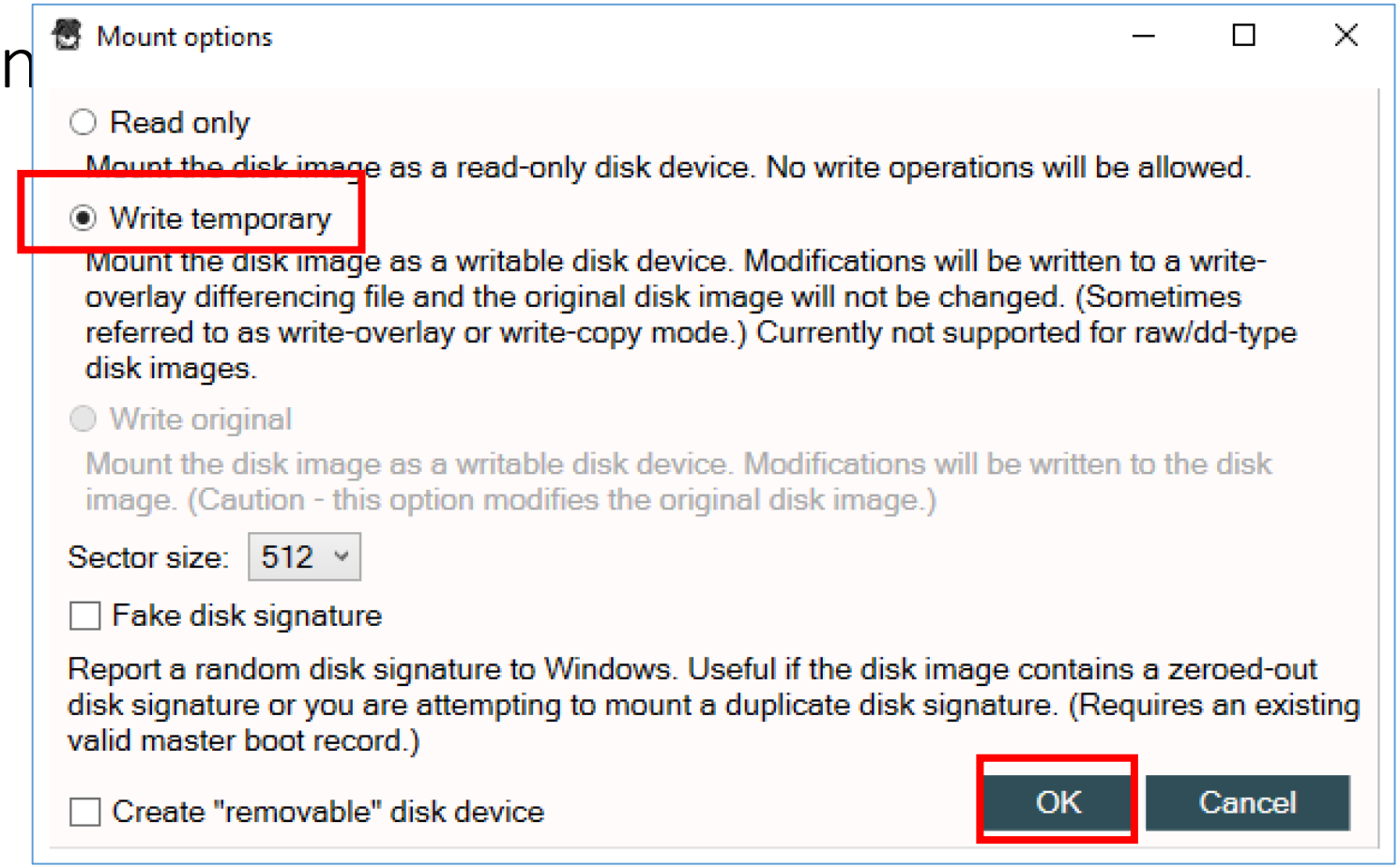


Choose a disk image. At this time, we will choose "Client-Win10-2_honda.E01“ in “E:\Artifacts\scenario1_E01". Then press "Open" button.

Copyright Internet Initiative Japan Inc.

Scenario 1 Labs: Lab 1

Analyzin

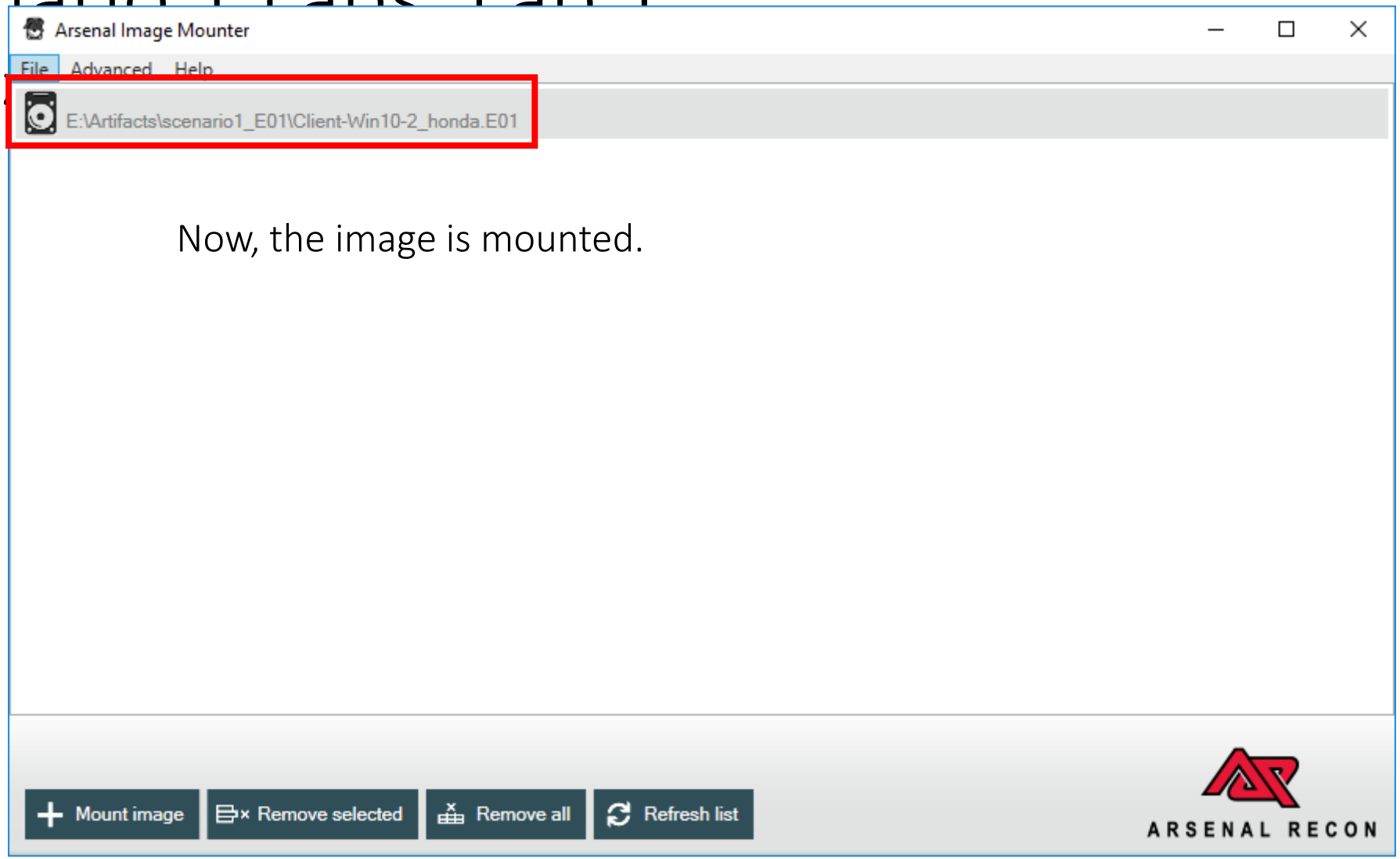


Select "Write temporary" option and press "OK" button.

Copyright Internet Initiative Japan Inc.

Scenario 1 Labs: Lab 1

Analy



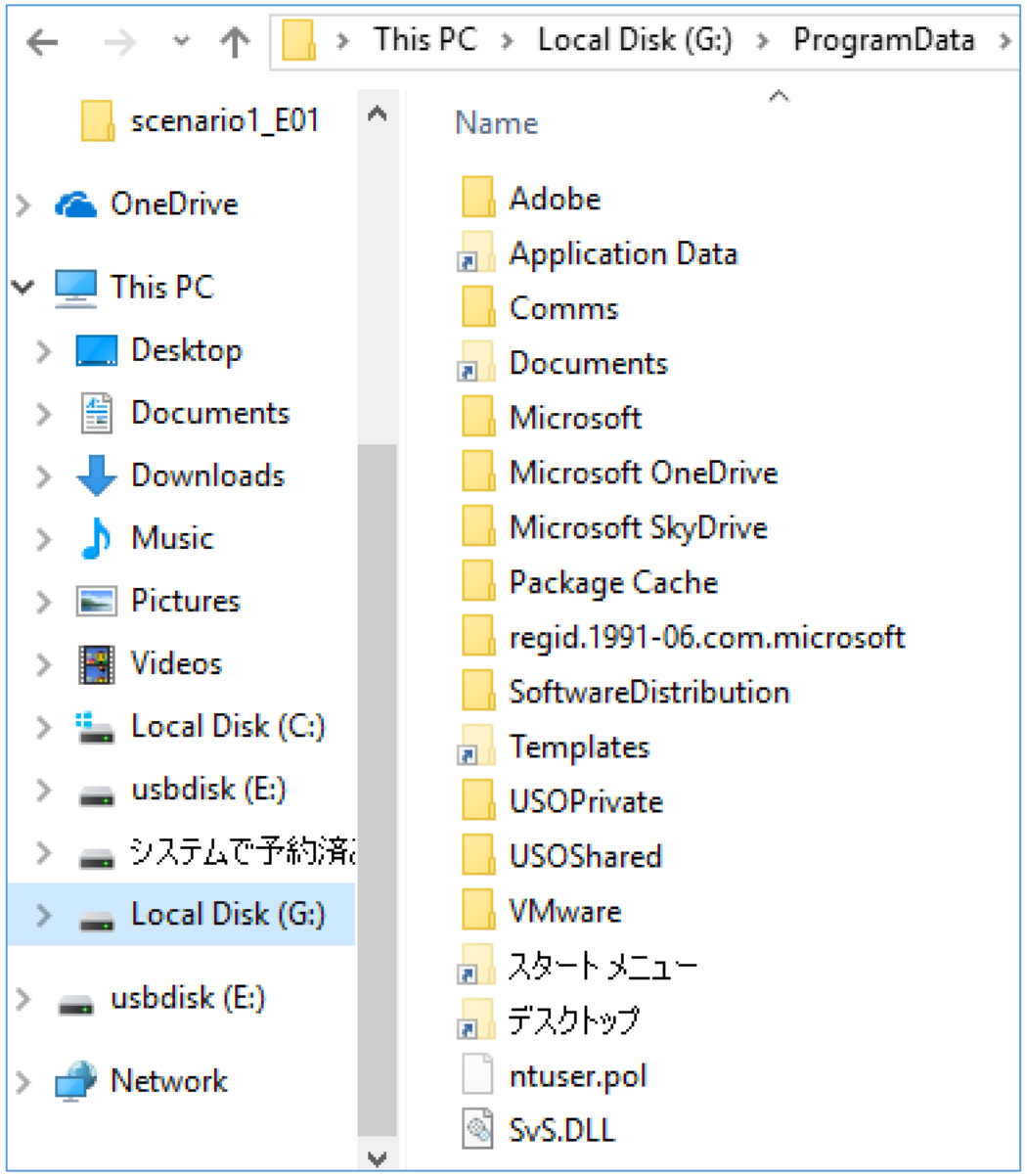
Copyright Internet Initiative Japan Inc.

Scenario 1 Labs: Lab 1

Analyzing Attacking Tools on client-wi

- Unfortunately, we cannot confirm the folder, even though the malware SvS.DLL exists.
  - \ProgramData\s

- The attacker could had deleted the folder. Let's try to recover it.

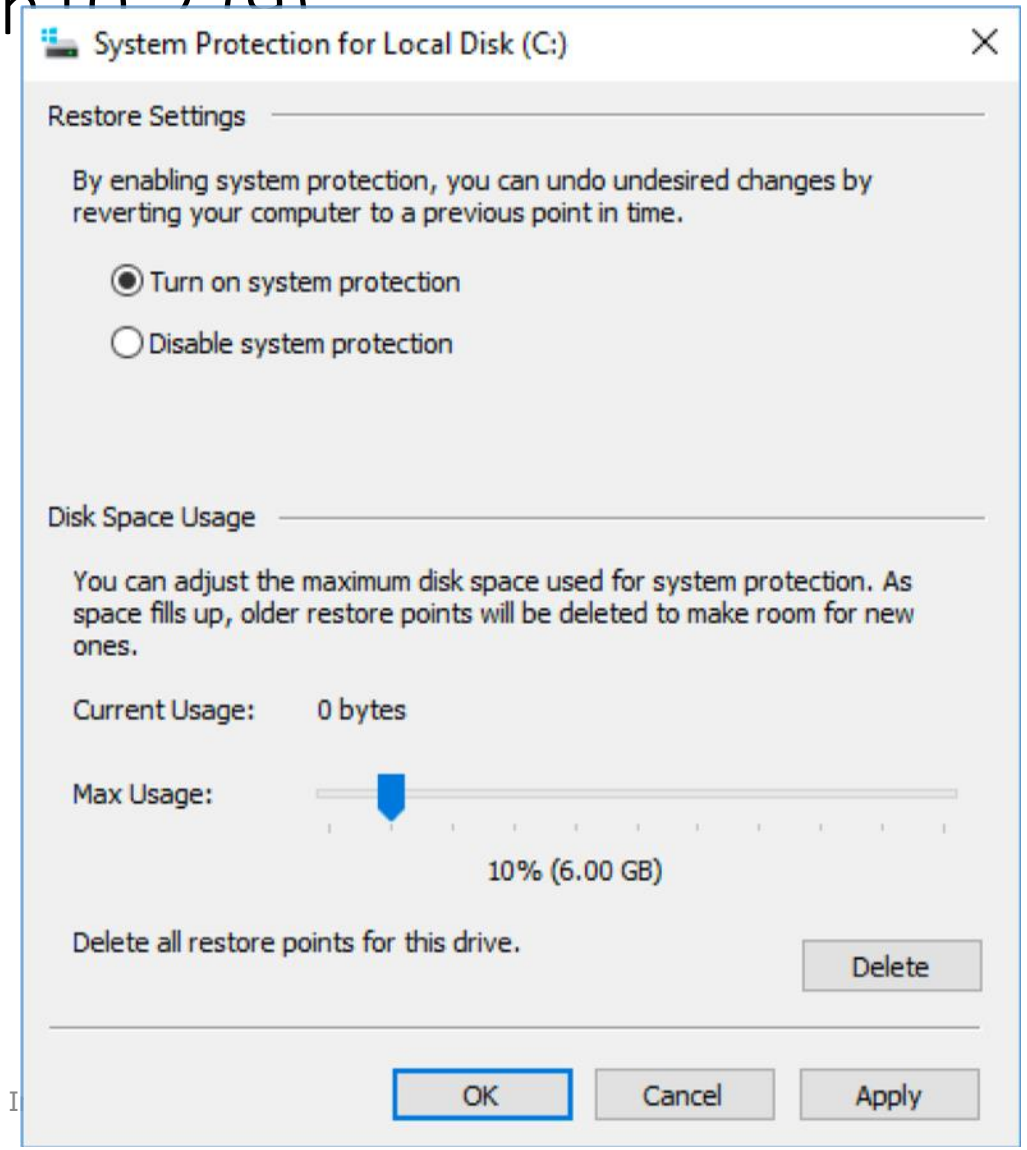


Copyright Internet Initiative Japan Inc.

Scenario 1 Labs: Lab 1

Analyzing Attacking Tools on client-win10-2 (9)

- Windows OS takes backups automatically with Volume Shadow Copy Service (VSS). It is for the "System Protection for Local Disk" function.
- We can restore system with VSS snapshots that were taken by this function.
- We can also extract files from VSS snapshots that are contained in disk images.
- We will learn VSS later, so you can use VSS with a rough understanding at this time.



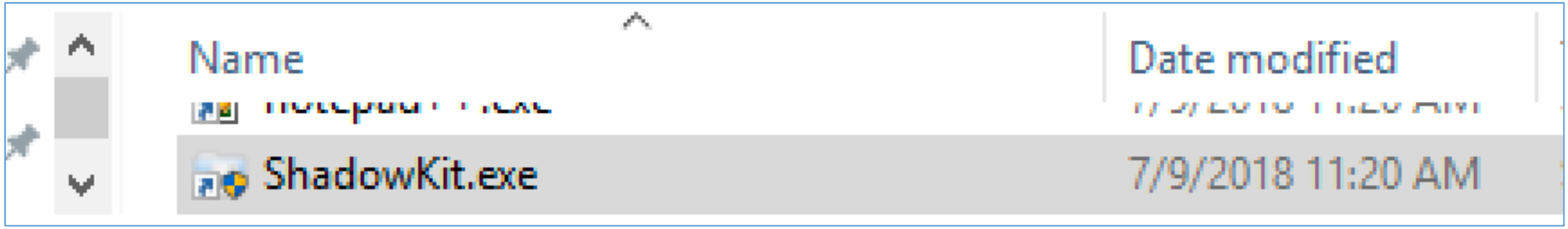
Copyright Internet Initiative Japan I

Scenario 1 Labs: Lab 1

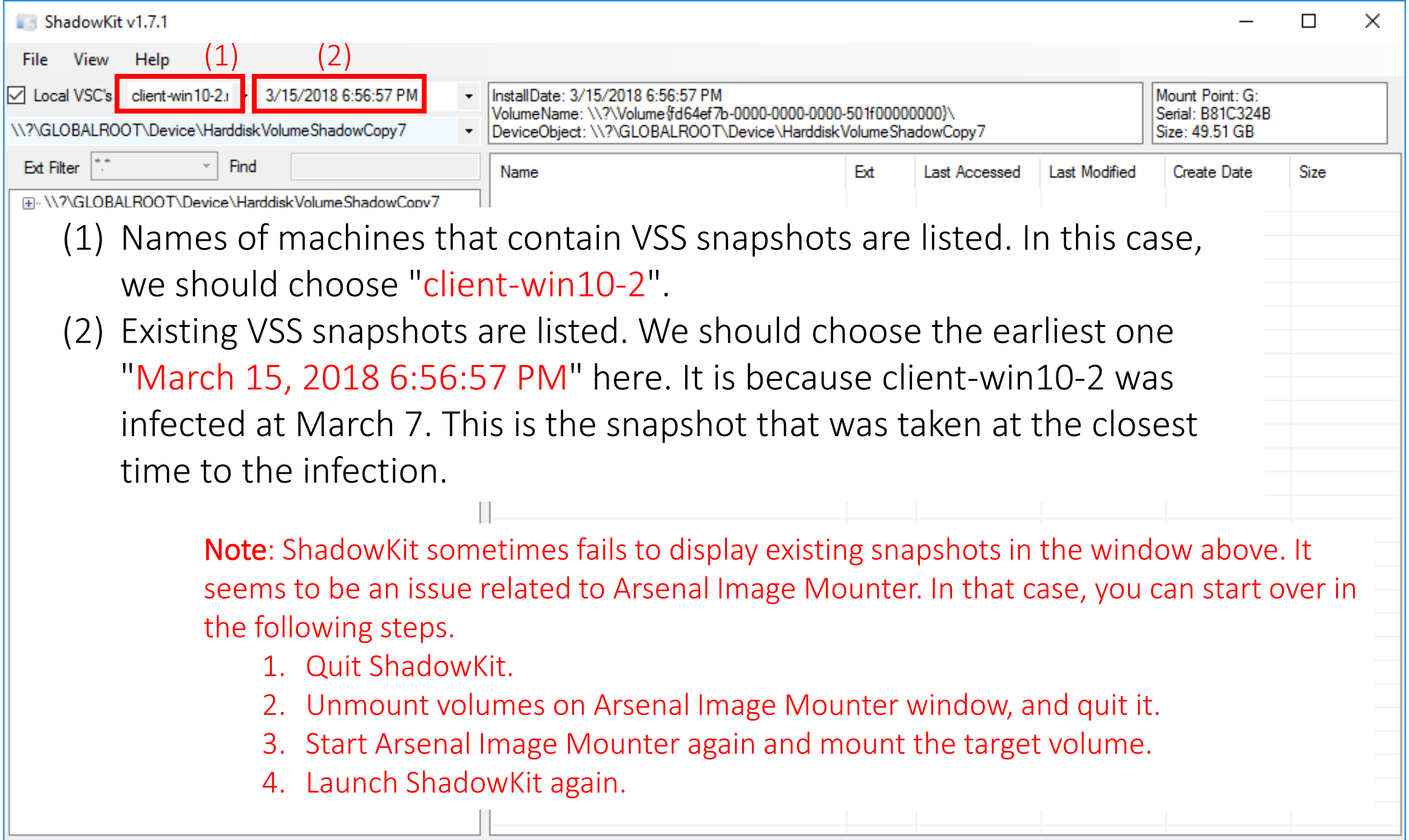
Analyzing Attacking Tools on client-win10-2 (10)

- In order to explore VSS snapshots, we will use ShadowKit.
- Launch ShadowKit by double-clicking its icon in the shortcut folder.

Shortcuts\06_LateralMovementsInvestigation\0602_AttackToolsAnalysis



Copyright Internet Initiative Japan Inc.



(1) Names of machines that contain VSS snapshots are listed. In this case, we should choose "client-win10-2".

(2) Existing VSS snapshots are listed. We should choose the earliest one "March 15, 2018 6:56:57 PM" here. It is because client-win10-2 was infected at March 7. This is the snapshot that was taken at the closest time to the infection.

Note: ShadowKit sometimes fails to display existing snapshots in the window above. It seems to be an issue related to Arsenal Image Mounter. In that case, you can start over in the following steps.

1. Quit ShadowKit.
2. Unmount volumes on Arsenal Image Mounter window, and quit it.
3. Start Arsenal Image Mounter again and mount the target volume.
4. Launch ShadowKit again.

Sc
Ar

ShadowKit v1.7.1

File View Help

Local VSC's client-win10-2.r 3/15/2018 6:56:57 PM

\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy20

InstallDate: 3/15/2018 6:56:57 PM
VolumeName: \\?\Volume{fd64ef7b-0000-0000-0000-501f00000000}\
DeviceObject: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy20

Ext Filter *.* Find

- \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy20
  - $Recycle.Bin
  - Documents and Settings
  - PerfLogs
  - Program Files
  - Program Files (x86)
  - ProgramData
    - Adobe
    - Application Data
    - Comms
    - Documents
    - Microsoft
    - Microsoft OneDrive
    - Microsoft SkyDrive
    - Package Cache
    - regid.1991-06.com.microsoft
    - s
      - Show All Dates
      - Close Nodes
      - Export
      - Clear List

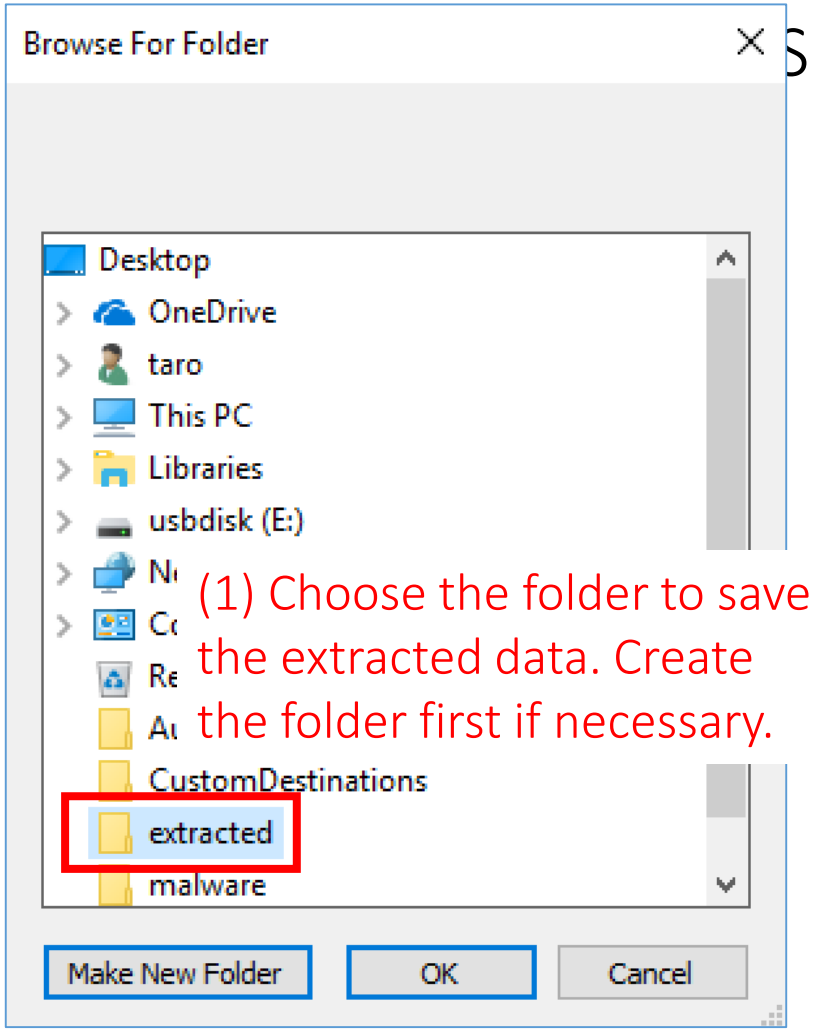
Name	Ext	Last Access
7.exe	.exe	10/5/2016
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA		3/12/2018
dq.exe	.exe	1/11/2018
g.bat	.bat	2/5/2018
g.log	.log	3/7/2018
l.exe	.exe	6/30/2017
m2.bat	.bat	2/28/2018
ms2.bat	.bat	2/28/2018
ms2s.bat	.bat	3/12/2018
o.bat	.bat	6/23/2017
output.tlb	.tlb	3/12/2018
p.bat	.bat	6/29/2017
run.sct	.sct	3/12/2018
w.vbs	.vbs	6/23/2017

Move to the target folder you are trying to extract files from. Then, you can recover files by right-clicking on the folder and choosing “Export”.

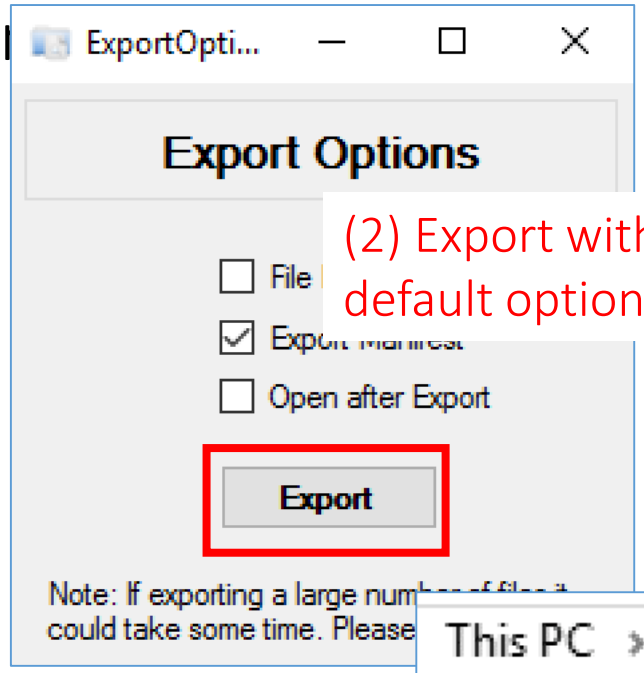
Copyright Internet Initiative Japan Inc.

Scenario 1 Labs: Lab 1

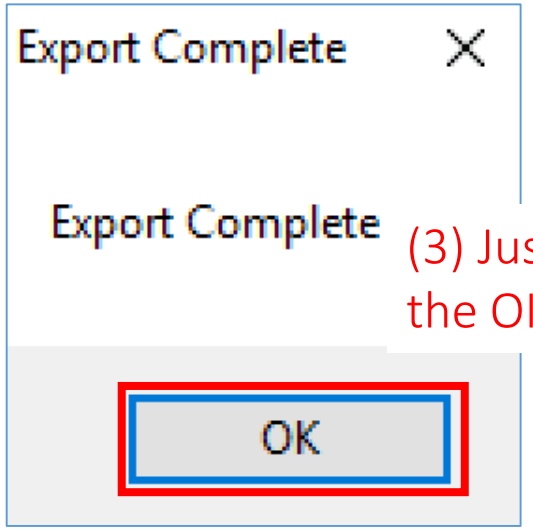
Analyzing Attacking Tools on client-win10-2 (13)



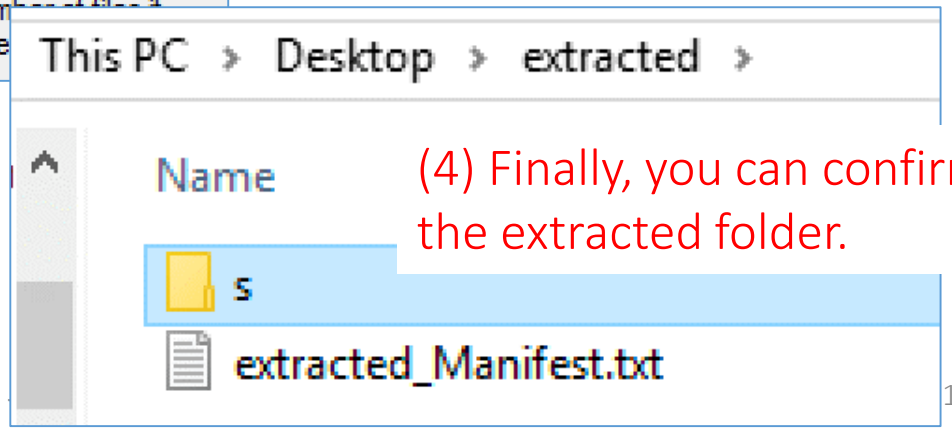
(1) Choose the folder to save the extracted data. Create the folder first if necessary.



(2) Export with the default option.



(3) Just press the OK button.



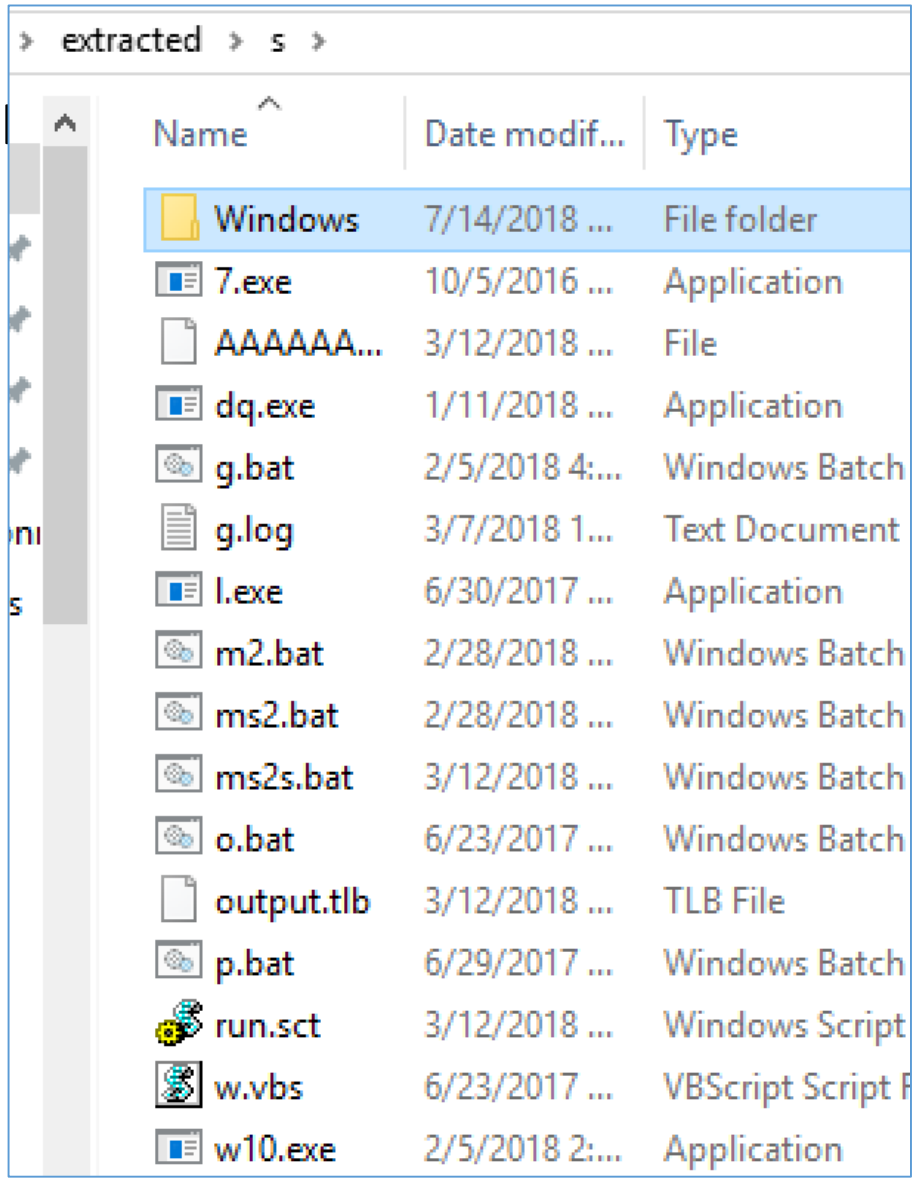
(4) Finally, you can confirm the extracted folder.

Copyright Internet Initiative

Scenario 1 Labs: Lab 1

Analyzing Attacking Tools on client-wi

- We have got some files under the folder. Let's check them one by one.
- The strategy:
  - We can presume the format of files by their extensions.
  - For executable files, execute them first. Then, perform static analysis if necessary.
  - For text files including batch and script files, view them first. Then, perform dynamic analysis if necessary.
  - In real cases, we must use a dedicated environment to perform the dynamic analysis.



Copyright Internet Initiative Japan Inc.

Scenario 1 Labs: Lab 1

Analyzing Attacking Tools on client-win10-2 (15)

- First, let's check text files.
- Open files named "g.bat" and "g.log" with Notepad++. Then, you can find that g.bat is a bat file to gather environment information and g.log is the result of "g.bat".

g.bat | g.log

```
@echo off
echo ----------------------------------------
echo Logon Server
echo %logonserver%

echo ----------------------------------------
echo SystemInfo
systeminfo

echo ----------------------------------------
echo Installed Softwares (via WMI)
powershell.exe -nologo "Get-WmiObject -Class Win32_Product"

echo ----------------------------------------
echo Installed Softwares (via Registry HKLM)
reg query "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Curre

echo ----------------------------------------
echo Installed Softwares (via Registry HKLM Wow64)
reg query "HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\W

```

g.bat | g.log

```
----------------------------------------
Logon Server
\\AD-WIN2016
----------------------------------------
SystemInfo

ホスト名:                  CLIENT-WIN10-2
OS 名:                     Microsoft Windows 10 Pro
OS バージョン:             10.0.14393 N/A ビルド 14393
OS 製造元:                 Microsoft Corporation
OS 構成:                   メンバー ワークステーション
OS ビルドの種類:           Multiprocessor Free
登録されている所有者:      Windows ユーザー
登録されている組織:
プロダクト ID:             00330-80116-33578-AA093
最初のインストール日付:    2018/01/26, 6:49:37
システム起動時間:          2018/03/07, 10:31:25
システム製造元:            VMware, Inc.
システム モデル:           VMware Virtual Platform
システムの種類:            x64-based PC
プロセッサ:                1 プロセッサインストール済みです。
                           [01]: Intel64 Family 6 Model 79 Stepping 1 Genuin
```

Scenario 1 Labs: Lab 1

Analyzing Attacking Tools on client-win10-2 (16)

- You can confirm other BAT files such as ms2.bat, ms2s.bat, o.bat and p.bat in the same way. Also you can find summary for their function in the later slide.
- A file named "w.vbs" provides other interesting information. Let's open it with a text editor.

```
15  Set objArgs = WScript.Arguments
16  intArgCount = objArgs.Count
17  If intArgCount < 2 Or intArgCount > 5 Then
18      WScript.Echo "WMI Remote Command Executor   By. Twi1ight@T00ls.Net"
19      WScript.Echo " Usage:" &
20                  vbTab & "wmiexec.vbs  /sh
21          vbNewLine & vbTab & "wmiexec.vbs  /shell  host  user  pass" & _
22          vbNewLine & vbTab & "wmiexec.vbs  /cmd  host  command" & _
23          vbNewLine & vbTab & "wmiexec.vbs  /cmd  host  user  pass  command" & vbNewLine & _
24          vbNewLine & vbTab & "  /shell"  & vbTab & "half-interactive shell mode" & _
```

What is wmiexec.vbs?

- By googling with the string "wmiexec.vbs", you could figure out that this script is a famous script file "wmiexec" itself. It is a kind of administration tools like psexec. In addition, attackers used it to move laterally in some real case.
  - https://github.com/Twi1ight/AD-Pentest-Script/blob/master/wmiexec.vbs

Scenario 1 Labs: Lab 1

Analyzing Attacking Tools on client-win10-2 (17)

w.vbs

```
1  On Error Resume Next
2  '################################
3  Const Path = "C:\windows\temp\"
4  Const FileName = "wmi.dll"
5  Const timeOut = 1200
6  '################################
7  file = Path & "\" & FileName
8  file = Replace(file,"\\","\")
9  Set fso = CreateObject("Scripting.
```

You can find a file path at the beginning of the file. And you can confirm that some commands in this script file redirect their output to the file. Therefore, it could be a path of the temporary output file. The temporary output file might be a text file, even though its extension is "dll".

```
69   WScript.Echo "WMIEXEC : Result File -> " & file
```

```
239      strExec = "cmd.exe /c " & cmd & " > " & file & " 2>&1"  '2>&1 err
```

Copyright Internet Initiative Japan Inc.

This PC › Local Disk (G:) › Windows › Temp

Name	Date modified
tem5BF6.tmp	1/26/2018 6:49 AM
temDDC1.tmp	1/29/2018 9:11 PM
vmware-vmsvc.log	4/2/2018 5:08 PM
vmware-vmusr.log	2/8/2018 4:52 PM
vmware-vmvss.log	3/20/2018 6:29 PM
wmi.dll	3/12/2018 9:40 PM

```
 .#####.   mimikatz 2.1.1 (x64) built on Feb  5 2018 2
.## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin
## \ / ##       > http://blog.gentilkiwi.com/mimikatz
'## v ##'       Vincent LE TOUX             ( vincent.
 '#####'       > http://pingcastle.com / http://mysma

mimikatz(commandline) # log C:\ProgramData\A8Lmsa3o.log
Using 'C:\ProgramData\A8Lmsa3o.log' for logfile : OK

mimikat
Privile

mimikatz(commandline) # sekurlsa::logonpasswords

Authentication Id : 0 ; 28151027 (00000000:01ad8cf3)
```

1. You can confirm that the temporary file exists in the current file system (drive G in this case). In addition, its timestamp could be the last execution time of WMIExec.

2. The temporary file contains logs for executing logonpasswords command of Mimikatz.

3. Mimikatz is a very famous tool to steal and forge credentials on Windows systems, and logonpasswords command is to dump credentials from the memory of the working system.

Scenario 1 Lab: Lab1

```
15  mimikatz(commandline) # sekurlsa::logonpasswords
16
17  Authentication Id : 0 ; 28151027 (00000000:01ad8cf3)
18  Session           : RemoteInteractive from 2
19  User Name         : ninja-rdp
20  Domain            : NINJA-MOTORS
21  Logon Server      : AD-WIN2016
22  Logon Time        : 2018/03/09 16:08:08
23  SID               : S-1-5-21-3671970501-3975728774-4289435121-3102
24      msv :
25       [00000003] Primary
26       * Username : ninja-rdp
27       * Domain   : NINJA-MOTORS
28       * NTLM     : 0fab10218d190412479512 8ca7cd8202
29       * SHA1     : 4a6adcc2d93d95c6439474b5ff9d9485364f2c2b
30       * DPAPI    : 81968b084ddeaadf24d55706694d6ff9
31      tspkg :
32      wdigest :
33       * Username : ninja-rdp
34       * Domain   : NINJA-MOTORS
```

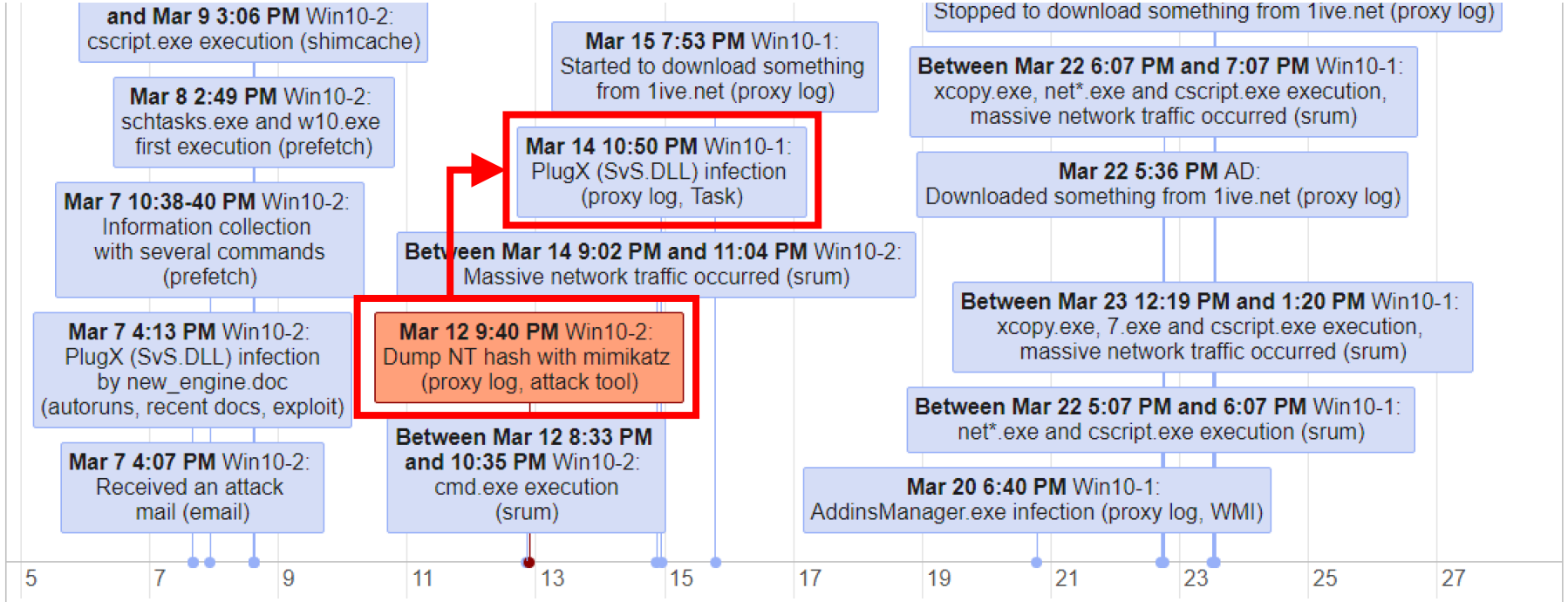
- The log shows that the NTLM hash of "ninja-rdp" account was dumped.

Copyright Internet Initiative Japan Inc.

Scenario 1 Labs: Lab 1

Analyzing Attacking Tools on client-win10-2 (20)

- In the victim environment, ninja-rdp is the dedicated account that is managed by administrator Toyoda to support and maintain computers via RDP. It is the only account that is allowed to access computers via RDP. Other employees did not have the credentials for the account.
- Thus, we can guess that the attacker penetrated from client-win10-2 to client-win10-1 with ninja-rdp's credentials.



Scenario 1 Labs: Lab 1

Analyzing Attacking Tools on client-win10-2 (21)

- Next, let's check the executable files.
- Start a file named "7.exe".
- Nothing happens when the file is double-clicked.
- Then, run the file from the Command Prompt.

cmd.exe

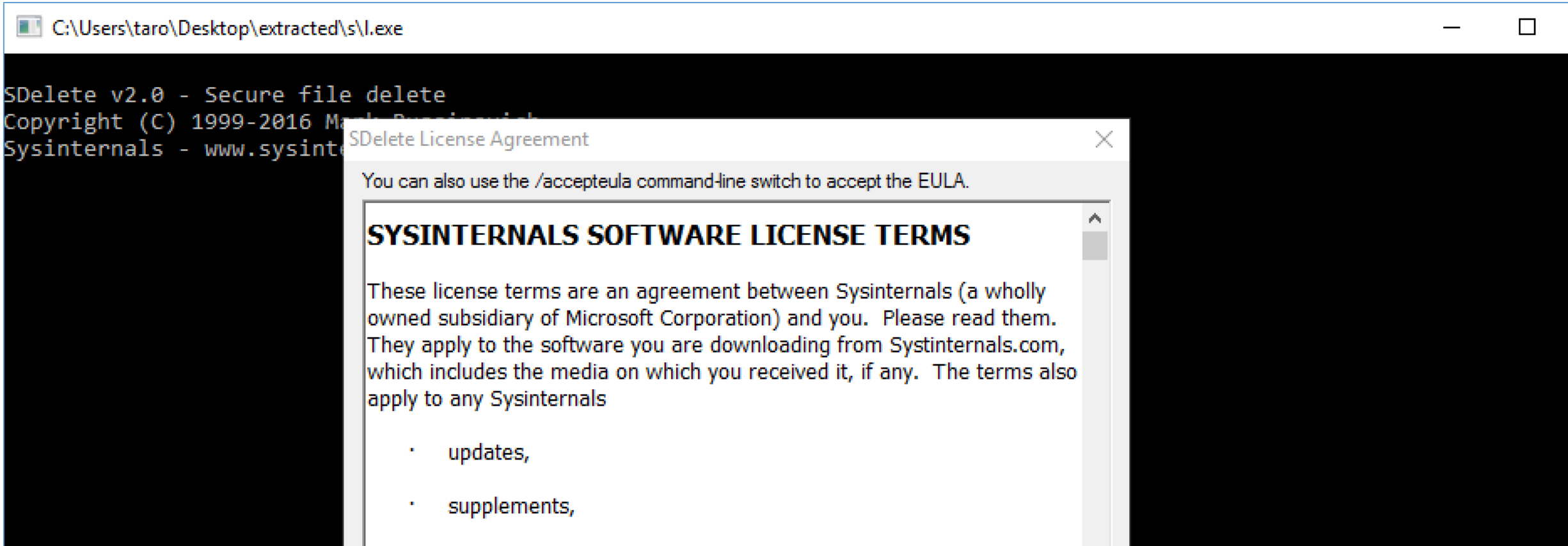
```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\shortcuts\09_LateralMovementsInvestigation\0902_AttackToolsAnalysis\tools>C:\Users\taro\Desktop\extracted\s\7.exe

7-Zip (a) [32] 16.04 : Copyright (c) 1999-2016 Igor Pavlov : 2016-10-04

Usage: 7za <command> [<switches>...] <archive_name> [<file_names>...]
       [<@listfiles...>]

<Commands>
  a : Add files to archive
  b : Benchmark
  d : Delete files from archive
```

Looks like an output from 7-zip command.

Scenario 1 Labs: Lab 1

Analyzing Attacking Tools on client-win10-2 (22)

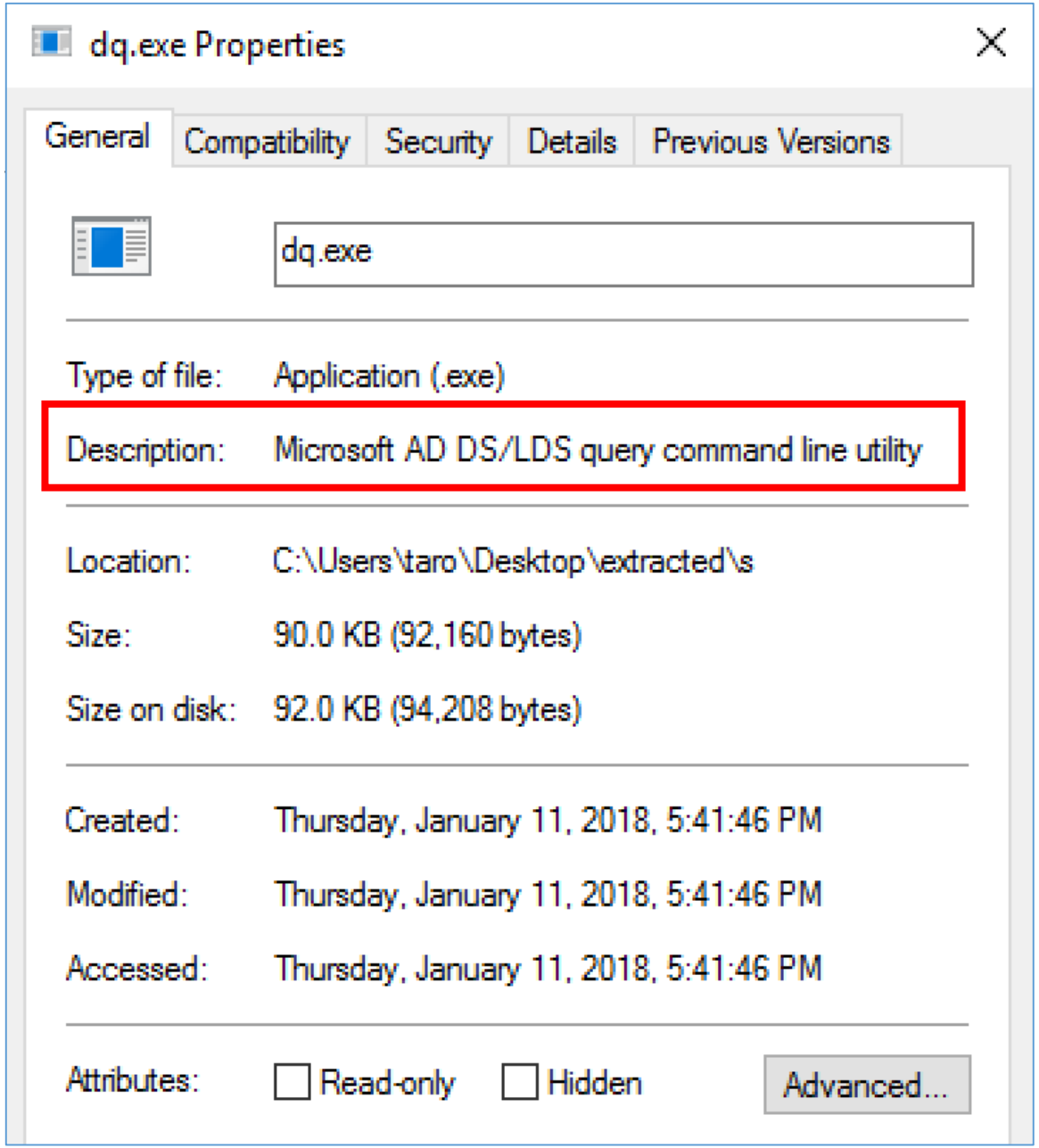
- You can use the same method for a file named "l.exe".
- It seems to be SDelete, a famous file deletion tool included in Sysinternals Suite.



Scenario 1 Labs: Lab 1

Analyzing Attacking Tools on client-

- A file "dq.exe" does not have any output.
- We can figure out what this file is from its properties.
- We can confirm that by comparing hash value with the legitimate binary of the same version of the program.



Copyright Internet Initiative Japan Inc.

Scenario 1 Labs: Lab 1

Analyzing Attacking Tools on client-win10-2 (24)

- An executable file named "w10.exe" is a little difficult to understand.
- By double-clicking it, you can confirm that it would drop the following files.
  - run.sct
    - It's a JScript to launch w10.exe with an argument.
  - AAAAAAAAAAAAAAA....
  - Output.tlb
  - .\Windows\System32\tapi3.dll
    - These two files looks like a kind of libraries by checking its magic.
- However, what is the purpose of the file?

Copyright Internet Initiative Japan Inc.

Scenario 1 Labs: Lab 1

Analyzing Attacking Tools on client-win10-2 (25)

- Let's perform surface analysis for w10.exe with cmd.exe.

- First, move to the "s" folder.

```
> cd C:\Users\taro\Desktop\extracted\s
```

- Then, run the following command in order to get strings in the executable file.

```
> strings -n 10 w10.exe > w10_strings.txt
```

Copyright Internet Initiative Japan Inc.

Scenario 1 Labs: Lab 1

Analyzing Attacking Tools on client-win10-2 (26)

- We extracted the strings that are contained in the executable file. Let's open the saved file with text editor.
- Are there any noticing strings?

These look like particular names of APIs or something . Actually, these are the names of COM object interfaces.

- Let's google with these names.

w10_strings.txt

```
QI - Marshaller: %ls %p
Queried Success: %p
AddRef: %d
Release: %d
Release object %p
Marshal Interface: %ls
Setting bad IID
Marshal Complete: %08X
Query for IUnknown
Query for IBackgroundCopyCallback2
Query for IBackgroundCopyCallback
Query for IPersist
Query for ITMediaControl
Unknown IID: %ls %p
JobTransferred
```

Copyright Internet Initia

Scenario 1 Labs: I

Analyzing Attacking Too

- You can find that the names are contained in the exploit code for CVE-2017-0213. In addition, you can also confirm that the other strings, such as "Marshal Interface: %ls" and so on, included in w10.exe are also contained in the exploit code.
- Thus, we can presume that w10.exe is the exploit code for CVE-2017-0213. It may have been built from the public code on GitHub.

Google

IUnknown IBackgroundCopyCallback2 IBackgroundCopyCallback IPersi

All Maps Images Videos News More Settings Tools

About 6 results (0.42 seconds)

Did you mean: ***Unknown*** IBackgroundCopyCallback2 ***IBackgroundCopy Callback*** IPersist ***IMediaControl***

IUnknown interface (COM) - MSDN - Microsoft
https://msdn.microsoft.com/en-us/library/windows/desktop/ms680509(v=vs.85).aspx
IPersist · **IPersistFile** ... All other COM interfaces are inherited, directly or indirectly, from **IUnknown**. ... You must implement **IUnknown** as part of every interface.
Missing: ~~ibackgroundcopycallback2~~ ~~ibackgroundcopycallback~~ ~~itmediacontrol~~

IPersist interface (COM) - MSDN - Microsoft
https://msdn.microsoft.com/en-us/library/windows/desktop/ms688695(v=vs.85).aspx
IPersist is the base interface for three other interfaces: **IPersistStorage**, IPersistStream, and ... The **IPersist** interface inherits from the **IUnknown** interface. **IPersist** ...
Missing: ~~ibackgroundcopycallback2~~ ~~ibackgroundcopycallback~~ ~~itmediacontrol~~

IUnknown - Wikipedia
https://en.wikipedia.org/wiki/IUnknown
In computer programming, the **IUnknown** (custom) interface is the fundamental interface in the Component Object Model (COM). The published COM ...
Missing: ~~ibackgroundcopycallback2~~ ~~ibackgroundcopycallback~~ ~~ipersist~~ ~~itmediacontrol~~

windows-kernel-exploits/CVE-2017-0213.cpp at master · SecWiki ...
https://github.com/SecWiki/windows-kernel-exploits/blob/.../CVE-2017-0213.cpp
~CMarshaller() {}. public: CMarshaller(**IUnknown*** unk) : _ref_count(1) .... class FakeObject : public **IBackgroundCopyCallback2**, public **IPersist** ... else if (riid == __uuidof(**IBackgroundCopyCallback**)) ... printf("Query for **ITMediaControl**\n");.

Free Automated Malware Analysis Service - powered by Falcon ...
https://www.reverse.it/.../0a4a0f0df5eea57f16a76bff6489dd95a7089afba8e9e5c8bca...

Scenario 1 Labs: Lab 1

Analyzing Attacking Tools on client-win10-2 (28)

- NIST NVD said:

> *Windows COM Aggregate Marshaler in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an elevation privilege vulnerability when an attacker runs a specially crafted application, aka "Windows COM Elevation of Privilege Vulnerability". This CVE ID is unique from CVE-2017-0214.*

https://nvd.nist.gov/vuln/detail/CVE-2017-0213#vulnCurrentDescriptionTitle

- client-win10-1 and client-win10-2 were running Windows 10 1703.
- The attacker could gain privileges by executing w10.exe. In other words, the attacker could had gained SYSTEM privilege after execution of this file.

Copyright Internet Initiative Japan Inc.

About CVE-2017-0213 and its exploit.

- CVE-2017-0213 is a type confusion vulnerability that occurs by using the IRemUnknown2 COM interface to access object-oriented programming (OOP) component object model (COM) object.
- To sum up, the exploit we found before use the vulnerability for a BITS callback interface and call LoadTypeLib with the same rights as BITS to execute arbitrary script. LoadTypeLib could be used for arbitrary execution with the condition that force to load forged type library by replacing the library path.
- For further information, you can get the full description, source code and executable binaries from its website.
  - https://github.com/WindowsExploits/Exploits/tree/master/CVE-2017-0213

Copyright Internet Initiative Japan Inc.

Scenario 1 Labs: Lab 1

Analyzing Attacking Tools on client-win10-2 (29)

- Summary of the files located in \ProgramData\s on client-win10-2:

Name	Content
7.exe	7-zip archiver
AAAAAAAA....	TLB file dropped by w10.exe
dq.exe	Microsoft AD DS/LDS query command line utility
g.bat	a bat to gather information about the environment
g.log	output of g.bat
l.exe	SDelete, a famous deletion tool
m2.bat	a bat to load "http://1ive.net/m1.ps1" via proxy server and execute it, avoiding script block logging.
ms2.bat	a bat to register m2.bat as a scheduled task named SyS
ms2s.bat	a bat to launch the task SyS
o.bat	a bat to get OS information from remote hosts

Scenario 1 Labs: Lab 1

Analyzing Attacking Tools on client-win10-2 (30)

- Summary of the files located in \ProgramData\s on client-win10-2 (Cont.) :

Name	Feature
output.tlb	TLB file dropped by w10.exe
p.bat	a bat to install the malware SvS.DLL and register it as a scheduled task for persistence
run.sct	a JScript file dropped by w10.exe
w.vbs	a remote/local administration tool, WMIExec
w10.exe	a local privilege escalation tool
.\Windows\System32\tapi3.dll	TLB file dropped by w10.exe

Copyright Internet Initiative Japan Inc.

Scenario 1 Labs: Lab 2

Analyzing Attacking Tools on client-win10-1

Scenario 1 Labs: Lab 2

Analyzing Attacking Tools on client-win10-1 (1)

- Condition:
  - This is an investigation for scenario 1.
  - We performed the attack tool analysis on client-win10-2 in the previous lab.
  - How about on client-win10-1?
- Goals:
  - To find out the attacker's working folder on client-win10-1.
  - To reveal the function of tools placed under the folder.
- Hint:
  - Attackers often use the same tools, locations and methods in the same campaign.

Copyright Internet Initiative Japan Inc.

Scenario 1 Labs: Lab 2

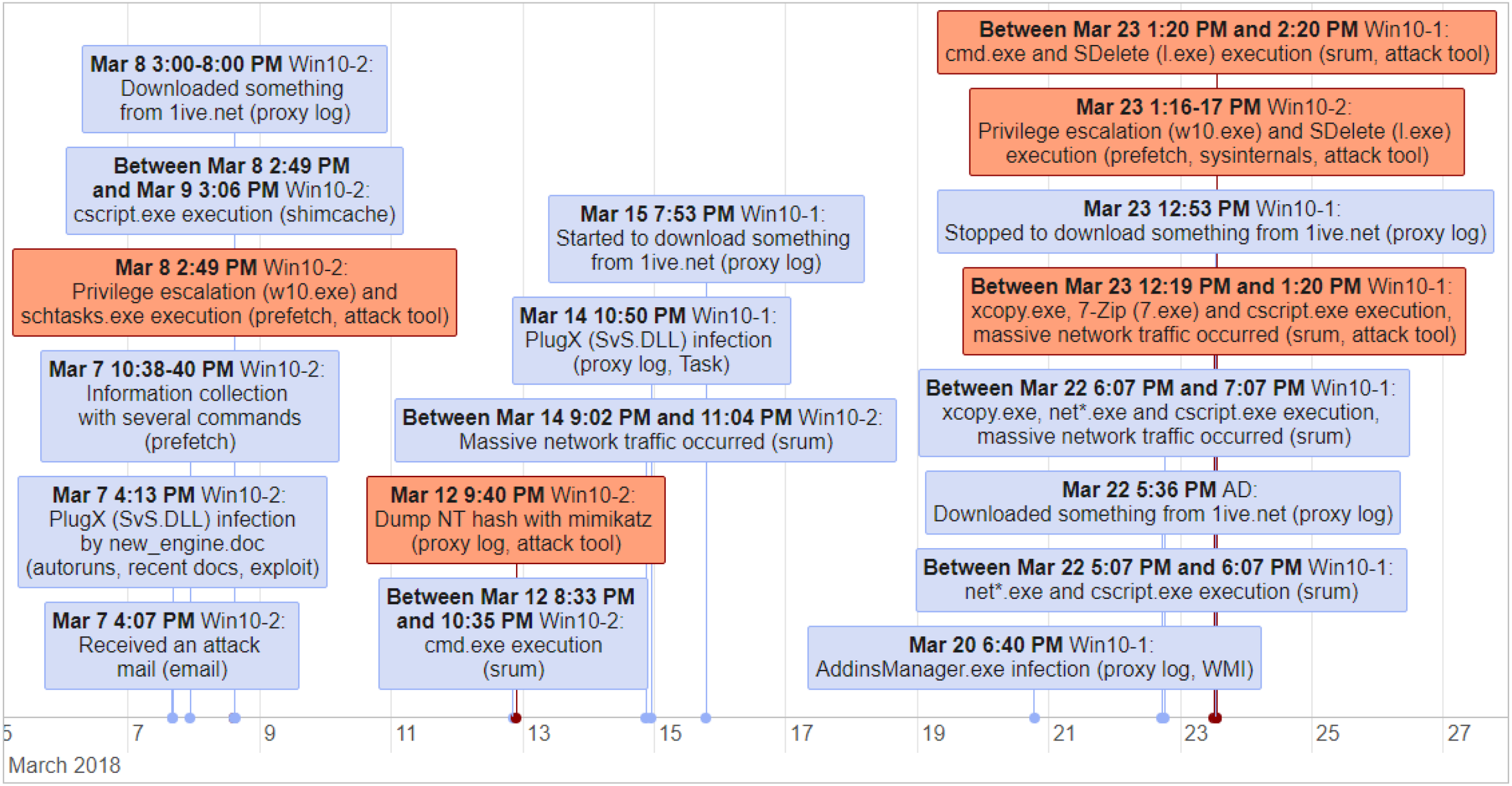
Analyzing Attacking Tools on client-win10-1 (2)

- Summary of the files located in \ProgramData\s on client-win10-1:

Name	Content
7.exe	7-zip archiver
g.bat	a bat to gather information about the environment
l.exe	SDelete, a famous deletion tool
m1.bat	a bat to load "http://1ive.net/m1.ps1" via proxy server and execute it, avoiding script block logging.
o.bat	a bat to get OS information from remote hosts
p.bat	a bat to install the malware SvS.DLL and register it as a scheduled task for persistence
w.vbs	a remote/local administration tool, WMIExec
w10.exe	an local privilege escalation tool

Copyright Internet Initiative Japan Inc.

Wrap Up


Mar 8 3:00-8:00 PM Win10-2: Downloaded something from 1ive.net (proxy log)
Between Mar 8 2:49 PM and Mar 9 3:06 PM Win10-2: cscript.exe execution (shimcache)
Mar 8 2:49 PM Win10-2: Privilege escalation (w10.exe) and schtasks.exe execution (prefetch, attack tool)
Mar 7 10:38-40 PM Win10-2: Information collection with several commands (prefetch)
Mar 7 4:13 PM Win10-2: PlugX (SvS.DLL) infection by new_engine.doc (autoruns, recent docs, exploit)
Mar 7 4:07 PM Win10-2: Received an attack mail (email)
Mar 15 7:53 PM Win10-1: Started to download something from 1ive.net (proxy log)
Mar 14 10:50 PM Win10-1: PlugX (SvS.DLL) infection (proxy log, Task)
Between Mar 14 9:02 PM and 11:04 PM Win10-2: Massive network traffic occurred (srum)
Mar 12 9:40 PM Win10-2: Dump NT hash with mimikatz (proxy log, attack tool)
Between Mar 12 8:33 PM and 10:35 PM Win10-2: cmd.exe execution (srum)
Between Mar 23 1:20 PM and 2:20 PM Win10-1: cmd.exe and SDelete (l.exe) execution (srum, attack tool)
Mar 23 1:16-17 PM Win10-2: Privilege escalation (w10.exe) and SDelete (l.exe) execution (prefetch, sysinternals, attack tool)
Mar 23 12:53 PM Win10-1: Stopped to download something from 1ive.net (proxy log)
Between Mar 23 12:19 PM and 1:20 PM Win10-1: xcopy.exe, 7-Zip (7.exe) and cscript.exe execution, massive network traffic occurred (srum, attack tool)
Between Mar 22 6:07 PM and 7:07 PM Win10-1: xcopy.exe, net*.exe and cscript.exe execution, massive network traffic occurred (srum)
Mar 22 5:36 PM AD: Downloaded something from 1ive.net (proxy log)
Between Mar 22 5:07 PM and 6:07 PM Win10-1: net*.exe and cscript.exe execution (srum)
Mar 20 6:40 PM Win10-1: AddinsManager.exe infection (proxy log, WMI)
5
7
9
11
13
15
17
19
21
23
25
27
March 2018

Conclusion

- Finding and analyzing tools that were used by attackers are useful to understand what attackers planned to do. Moreover, it helps us to determine what they actually did.
- We employ both static and dynamic analysis methods for it.
  - We must use a dedicated environment when we perform dynamic analysis.
- We should also be familiar with methods to recover deleted files.

Copyright Internet Initiative Japan Inc.