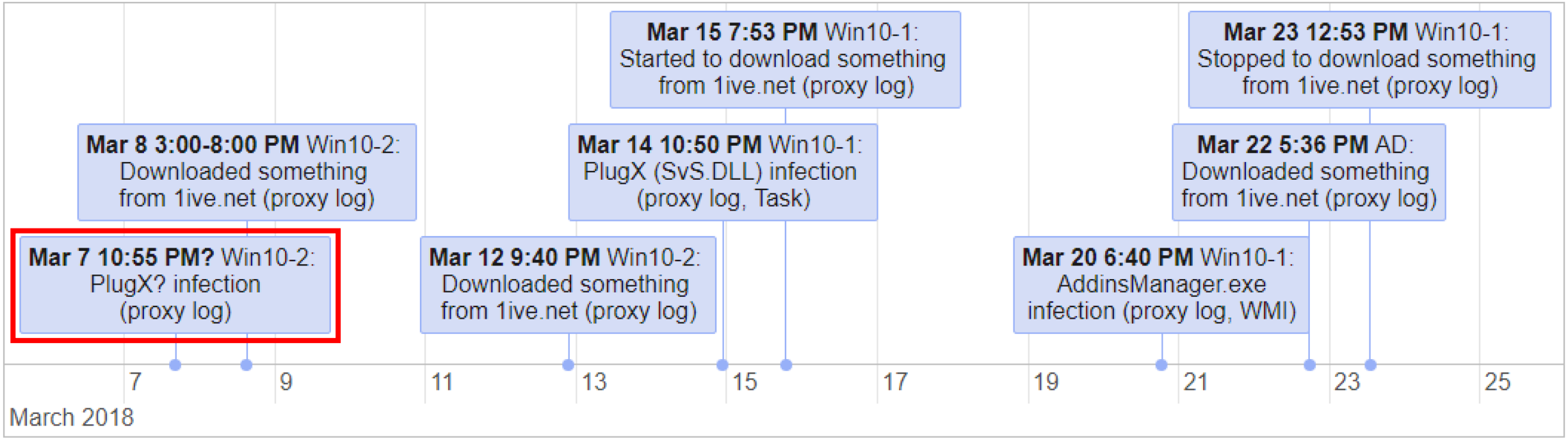
Persistence Analysis 2

What We Will Investigate in This Section

- We found C2 traffics from client-win10-2 in proxy log analysis. It started at one week before the infection of client-win10-1.
- Therefore, we should perform persistence analysis on client-win10-2 in order to confirm the infection on the host.



Scenario 1 Labs: Lab 3

Investigating persistence on client-win10-2

Scenario 1 Labs: Lab 3

Investigating persistence on client-win10-2 (1)

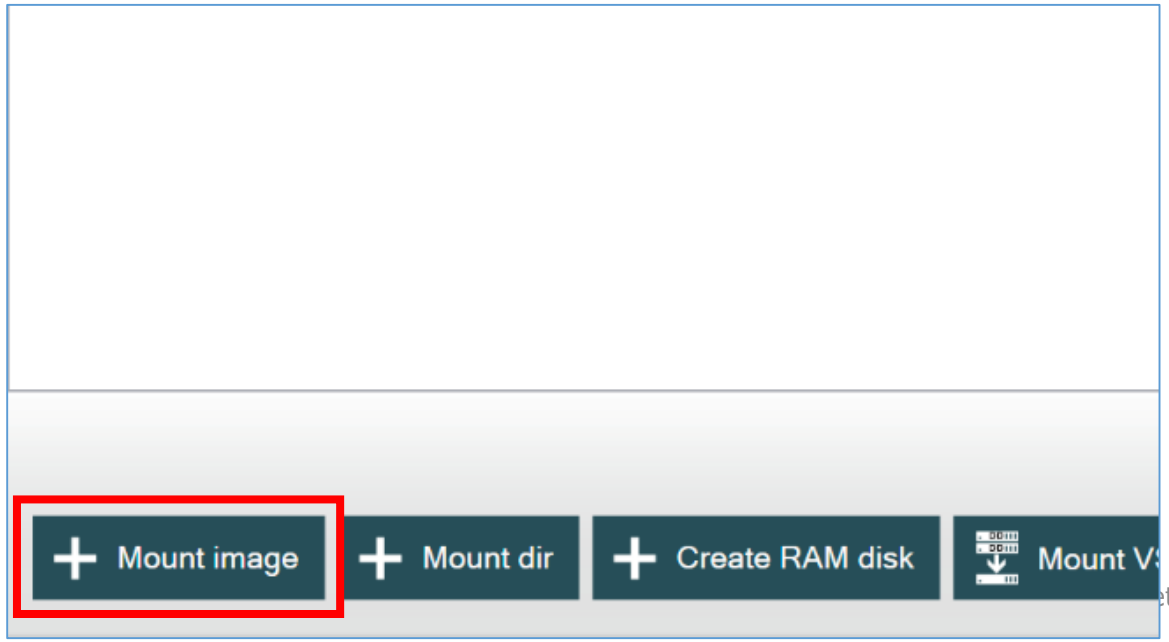
- This is an investigation for scenario 1.

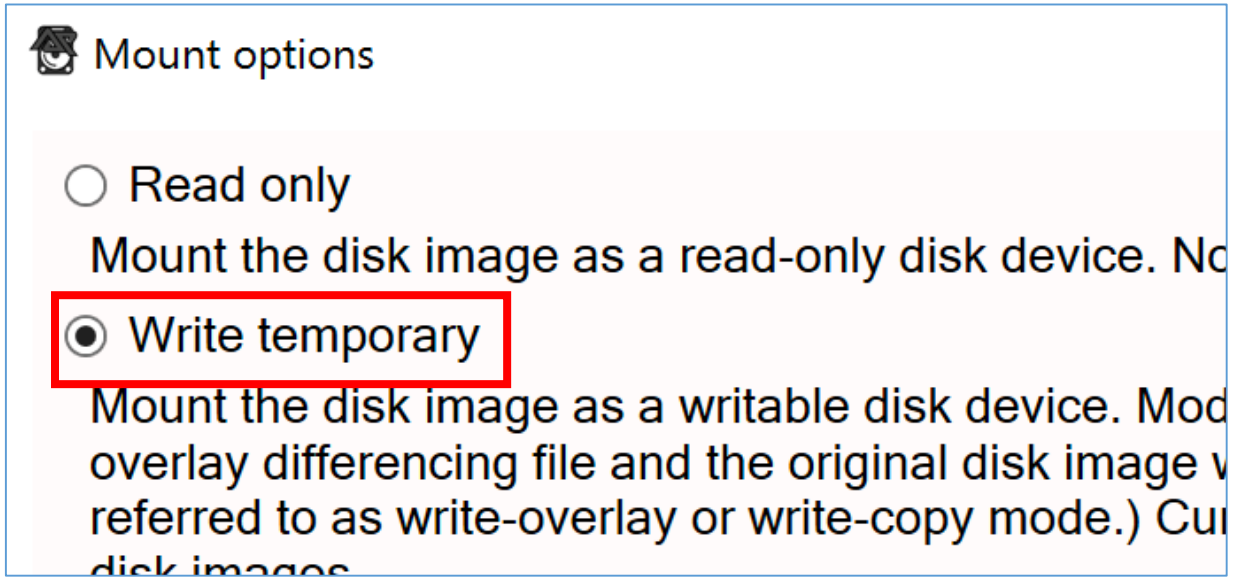
- Goal:
  - To find out the persistence of malware on the client-win10-2.
- Hints:
  - You should focus on the Autoruns' result in this exercise.
  - The main user of client-win10-2 is honda.
  - Attacker often use the same kind of malware in the same campaign. In other words, it is possible that client-win10-2 was infected by the same malware as client-win10-1.

Scenario 1 Labs: Lab 3

Investigating persistence on client-win10-2 (2)

- First of all, we should restart analysis machine because of Autoruns offline analysis limitation. It requires system restart for each analysis.
- Then, mount the disk image below with Arsenal Image Mounter.
  - E:\Artifacts\scenario1_E01\Client-Win10-2_honda.E01

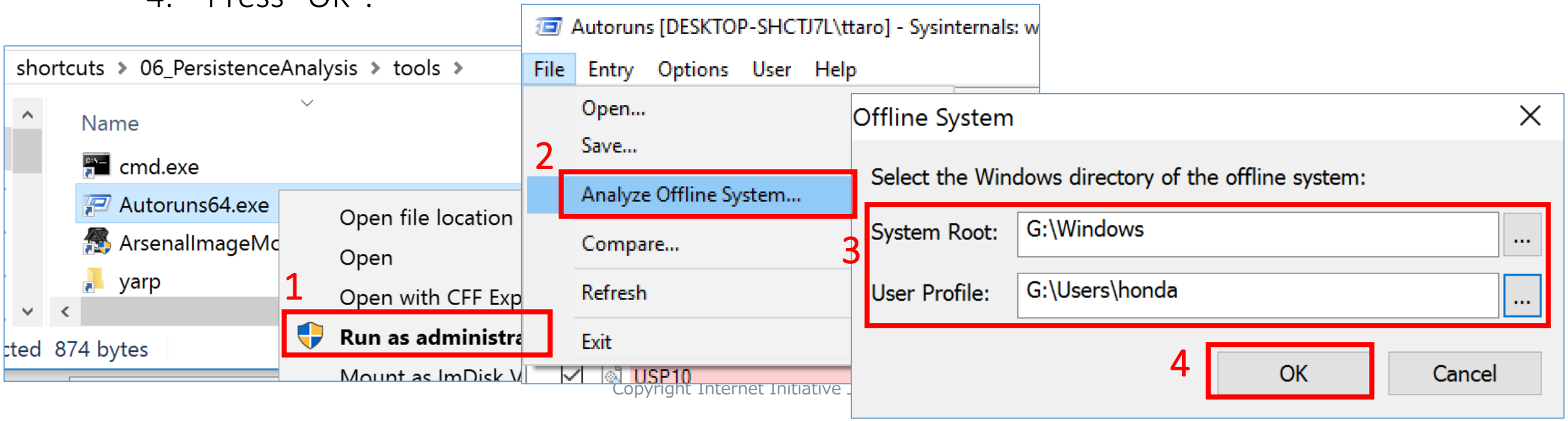




Scenario 1 Labs: Lab 3

Investigating persistence on client-win10-2 (3)

1. Launch Autoruns as Administrator. Then, **press ESC key immediately** to stop the scan.
2. Select "Analyze Offline System..." from File menu.
3. Input "System Root" and "User Profile".
   - System Root: **G:\Windows**
   - User Profile: **G:\Users\honda**
4. Press "OK".



Scenario 1 Labs: Lab 3

Investigating persistence on client-win10-2 (4)

- As we mentioned before, Autoruns seems to have issues related to memory handling or something.
- In spite of you did the workaround that we recommended, it might freeze when it starts or stops scanning. Also, it might not display a correct result.
- In these cases, you can start over the offline analysis in the following steps.
  1. Unmount volumes on Arsenal Image Mounter's window.
  2. Quit Autoruns. And mount the target image again with Arsenal Image Mounter.
  3. Start Autoruns without stopping scan. (Do not press ESC key.)
  4. Wait for the scan to complete.
  5. Quit Autoruns again.
  6. Start Autoruns again and press ESC key immediately. Then, start offline analysis with setting target folders.

Scenario 1 Labs: Lab 3

Investigating persistence on client-win10-2 (5)

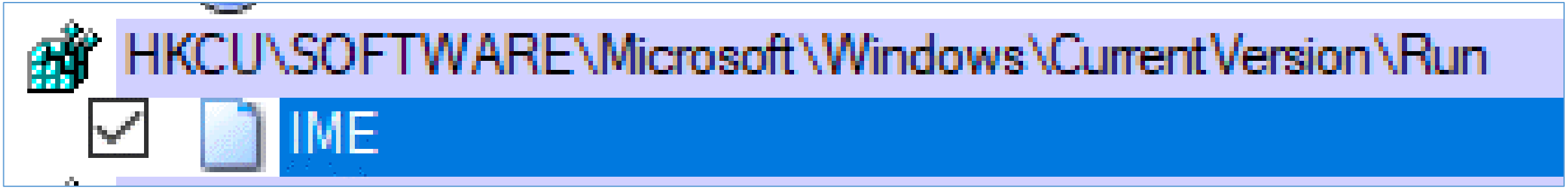
- Here is the reminder for performing persistence analysis efficiently.

- In short, we recommend you to check Autoruns in the following order.
  - First, check entries that contain following paths in their image path.
    - \Users\
    - \ProgramData\
    - Recycle.bin
    - \Windows\Temp\
  - Second, check the registry entries containing the prefix "HKCU".
  - Third, check the following six tabs.
    - Winsock Providers
    - Print Monitors
    - LSA Providers
    - Network Providers
    - Boot Execute
    - Winlogon
  - If you cannot find one with the methods above, you should check Scheduled Tasks and WMI.

Scenario 1 Labs: Lab 3

Investigating persistence on client-win10-2 (6)

- You might find two entries like the figure by checking registry keys that have a prefix "HKCU".



Scenario 1 Labs: Lab 3

Investigating persistence on client-win10-2 (7)

- You might find a suspicious entry like the figure by checking registry keys that have a prefix "HKCU".

Autorun Entry	Description	Publisher	Image Path	Timestamp
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell				7/16/2016 8:48 PM
cmd.exe	Windows Command Proc...	(Ve	cmd.exe	7/16/2016 11:23 AM
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				1/26/2018 3:55 PM
VMware User Process	VMware Tools Core Servi...	(Verified) VMware, Inc.	c:\program files\vmware\vmware tool...	2/17/2016 8:27 AM
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run				2/8/2018 5:58 PM
KeePass 2 PreLoad	KeePass	(Verified) Open Source Devel...	c:\program files (x86)\keepass passw...	1/9/2018 7:49 PM
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				3/7/2018 4:13 PM
IME	Windows host process (R...	(Verified) Microsoft Windows	c:\windows\system32\rundll32.exe	7/16/2016 11:18 AM
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components				2/8/2018 5:59 PM
Google Chrome	Google Chrome Installer	(Verified) Google Inc	c:\program files (x86)\google\chrome...	3/20/2018 12:31 PM
Microsoft Windows	Windows Mail	(Not verified) Microsoft Corpo...	c:\program files\windows mail\winmail...	7/16/2016 11:25 AM

This is the time the key was registered. It is shown in JST(+9).

rundll32.exe — Size: 68 K
Windows host process (Rundll32) — Time: 7/16/2016 11:18 AM
Microsoft Corporation — Version: 10.0.14393.0
RUNDLL32.EXE C:\ProgramData\SvS.DLL,GnrkQr

This is the image path with arguments. It has the same arguments as it is in the host client-win10-1!
Since the executable image's name is just RUNDLL32.EXE, it would not be listed if your apply a filter with the path "ProgramData".

Scenario 1 Labs: Lab 3

Investigating persistence on client-win10-2 (8)

- Next, check the other entry that have the prefix "HKCU".
- First, let's confirm the file that would be loaded by the entry.

Autorun Entry	Description	Publisher	Image Path	Timestamp
HKCU\Software\Microsoft\Internet Explorer\Extensions				2/8/2018 5:57 PM
@C:\Users\honda\AppData\Local\Apps\Evemo...			c:\users\honda\appdata\local\apps\evemote\evemote\evemoteieres\addnote.html	12/12/2017 9:00 PM

G:\Users\honda\AppData\Local\Apps\Evernote\Evernote\EvernoteIERes

Name	Date modified
css	2/8/2018 5:57 PM
html	2/8/2018 5:57 PM
images	2/8/2018 5:57 PM
oldclipper	2/8/2018 5:57 PM
scripts	2/8/2018 5:57 PM
AddNote.html	12/12/2017 9:00 PM

```
<html>
    <head>
        <script type="text/javascript" src="scripts/Evernote.js"></script>
        <script type="text/javascript" src="scripts/addin/AddinCreator.js"></script>
        <script type="text/javascript" src="scripts/Messages.js"></script>
        <script type="text/javascript" src="scripts/EvernoteAsyncEngine.js"></script>
        <script type="text/javascript" src="scripts/EvernoteAddin.js"></script>
        <script type="text/javascript" src="scripts/Injector.js"></script>
        <script type="text/javascript" src="scripts/Constants.js"></script>
        <script type="text/javascript" src="scripts/loggers/FileLogger.js"></script>
        <script type="text/javascript" src="scripts/loggers/ConsoleLogger.js"></script>
        <script type="text/javascript" src="scripts/loggers/AlertLogger.js"></script>
        <script type="text/javascript" src="scripts/loggers/LoggerConfigurator.js"></scr
        <script type="text/javascript" src="scripts/addin/EvernoteExternal.js"></script>
        <script type="text/javascript" src="scripts/BrowserDetection.js"></script>
        <script type="text/javascript" src="scripts/IEVersion.js"></script>
        <script type="text/javascript" src="scripts/addin/DocumentFinder.js"></script>
        <script type="text/javascript" src="scripts/InjectPhase.js"></script>
```

The file loads multiple script files. If you would like to confirm whether these script files are legitimate or not, you can download legitimate files from the official service and compare these scripts with the downloaded ones.

```
        }
        catch ( e ) {
            alert(e);
```

Scenario 1 Labs: Lab 3

Investigating persistence on client-win10-2 (10)

- Also we should check some special tabs (1).
  - This tab contains drivers made by VMware or Microsoft. Although you cannot verify the code signatures of these Microsoft drivers with Autoruns, you can confirm if they are legitimate or not by checking their hash values or tweaking patch status of your VM.
  - In this case, we will put them into a cold stage as we did in an exercise before.

Winsock Providers | Print Monitors | LSA Providers | Network Providers | WMI | Office

orun Entry	Description	Publisher	Image Path
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries			
vSockets DGRAM	VSockets Library	(Verified) VMware, Inc.	c:\windows\system3
vSockets STREAM	VSockets Library	(Verified) VMware, Inc.	c:\windows\system3
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries			
E-mail Naming Shim Provider	E-mail Naming Shim Provider	(Not verified) Microsoft Corporation	c:\windows\system3
Network Location Awareness Legacy (NLAv1) ...	Network Location Awareness 2	(Not verified) Microsoft Corporation	c:\windows\system3
NTDS	LDAP RnR Provider DLL	(Not verified) Microsoft Corporation	c:\windows\system3
PNRP Cloud Namespace Provider	PNRP Name Space Provider	(Not verified) Microsoft Corporation	c:\windows\system3
PNRP Name Namespace Provider	PNRP Name Space Provider	(Not Verified) Microsoft Corporation	c:\windows\system3
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries64			

Scenario 1 Labs: Lab 3

Investigating persistence on client-win10-2 (11)

- Also we should check some special tabs (2).
  - This tab contains drivers made by Microsoft. Here, we will put them into a cold stage as we did so far.

Winsock Providers | Print Monitors | LSA Providers | Network Providers | WMI | Office

orun Entry	Description	Publisher	Image Path
HKLM\SYSTEM\CurrentControlSet\Control\Print\Monitors			
Local Port	Local Spooler DLL	(Not Verified) Microsoft Corporation	c:\windows\system3
Microsoft Shared Fax Monitor	Microsoft Fax Print Monitor	(Not Verified) Microsoft Corporation	c:\windows\system3
Standard TCP/IP Port	Standard TCP/IP Port Monitor DLL	(Not Verified) Microsoft Corporation	c:\windows\system3
USB Monitor	Standard Dynamic Printing Port Moni...	(Not Verified) Microsoft Corporation	c:\windows\system3
WSD Port	WSD Printer Port Monitor	(Not Verified) Microsoft Corporation	c:\windows\system3
HKLM\SYSTEM\CurrentControlSet\Control\Print\Providers			
Internet Print Provider	Internet Print Provider DLL	(Not Verified) Microsoft Corporation	c:\windows\system3
LanMan Print Services	Client Side Rendering Print Provider	(Not Verified) Microsoft Corporation	c:\windows\system3

Scenario 1 Labs: Lab 3

Investigating persistence on client-win10-2 (12)

- Also we should check some special tabs (3).
  - These tabs contain drivers made by Microsoft. Here, we will put them into a cold stage as we did so far.

Winsock Providers | Print Monitors | LSA Providers | Network Providers | WMI | Office

Autorun Entry	Description	Publisher	Image Path
HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Authentication Packages			
msv1_0	Microsoft Authentication Package v1.0	(Not verified) Microsoft Corporation	c:\windows\system3
HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Notification Packages			
scecli	Windows Security Configuration Edit...	(Not verified) Microsoft Corporation	c:\windows\system3
HKLM\SYSTEM\CurrentControlSet\Control\Lsa\OSConfig\Security Packages			
cloudAP	Cloud AP Security Package	(Not verified) Microsoft Corporation	c:\windows\system3
kerberos	Kerberos Security Package	(Not verified) Microsoft Corporation	c:\windows\system3
msv1_0	Microsoft Authentication Package v1.0	(Not Verified) Microsoft Corporation	c:\windows\system3
		Microsoft Corporation	c:\windows\system3
		Microsoft Corporation	c:\windows\system3
		Microsoft Corporation	c:\windows\system3
		Microsoft Corporation	c:\windows\system3
		Microsoft Corporation	c:\windows\system3

Winsock Providers | Print Monitors | LSA Providers | Network Providers | WMI | Office

Autorun Entry	Description	Publisher	Image Path
HKLM\SYSTEM\CurrentControlSet\Control\NetworkProvider\Order			
LanmanWorkstation	Microsoft Windows Network	(Not verified) Microsoft Corporation	c:\windows\system3
RDPNP	Microsoft Terminal Services	(Not verified) Microsoft Corporation	c:\windows\system3
webclient	Web Client Network	(Not verified) Microsoft Corporation	c:\windows\system3

Scenario 1 Labs: Lab 3

Investigating persistence on client-win10-2 (13)

- Also we should check some special tabs (4).
  - This tab contains drivers made by Microsoft. Here, we will put them into a cold stage as we did so far.

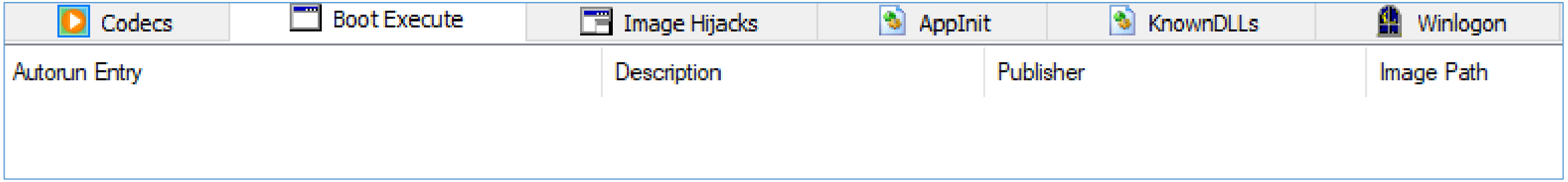
Codecs | Boot Execute | Image Hijacks | AppInit | KnownDLLs | Winlogon

orun Entry	Description	Publisher	Image Path
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers			
CCertProvider	Cert Credential Provider	(Not Verified) Microsoft Corporation	c:\windows\syst
CngCredUICredentialProvider	Microsoft CNG CredUI Provider	(Not Verified) Microsoft Corporation	c:\windows\syst
FaceCredentialProvider	Face Credential Provider	(Not Verified) Microsoft Corporation	c:\windows\syst
GenericProvider	Credential Providers	(Not Verified) Microsoft Corporation	c:\windows\syst
IrisCredentialProvider	Face Credential Provider	(Not Verified) Microsoft Corporation	c:\windows\syst
NGC Credential Provider	Microsoft Passport Credential Provider	(Not Verified) Microsoft Corporation	c:\windows\syst
NPProvider	Credential Providers	(Not Verified) Microsoft Corporation	c:\windows\syst
PasswordProvider	Credential Providers	(Not Verified) Microsoft Corporation	c:\windows\syst
PicturePasswordLogonProvider	Credential Providers Legacy	(Not Verified) Microsoft Corporation	c:\windows\syst
PINLogonProvider	Credential Providers Legacy	(Not Verified) Microsoft Corporation	c:\windows\syst
Remote NGC Credential Provider	Microsoft Passport Credential Provider	(Not Verified) Microsoft Corporation	c:\windows\syst

Scenario 1 Labs: Lab 3

Investigating persistence on client-win10-2 (14)

- Also we should check some special tabs (5).
  - This tab contains no drivers.



Scenario 1 Labs: Lab 3

Investigating persistence on client-win10-2 (15)

- In conclusion, we found a persistence mechanism on client-win10-2.

	Persistence Type	Name	File to Execute	Registered Date	Access Rights
Persistence C	Run key under HKCU	IME	C:\ProgramData\SvS.DLL,GnrkQr	2018-03-07 16:13	Non-admin

- The SHA1 hash value of the DLL file is below. It is the same value as the malware that was found on client-win10-1.
  - SvS.DLL: A93BDAD07871D0B25E02EBEEF5C99E315A89473E
- In addition, the registered time is earlier than the infection of client-win10-1. Therefore, client-win10-2 may be the first host that was infected by the attack.
- In a real case, you should check WMI and Scheduled tasks, too.

Scenario 1 Labs: Lab 3

Investigating persistence on client-win10-2 (16)

- We have confirmed the malware binary and its infection time on client-win10-2.