

# Persistence Analysis Appendix

# Extra Exercise:

Checking auto-start locations on an infected disk C

# Extra Exercise:

## Checking auto-start locations on an infected disk C (1)

- Conditions:
  - We are investigating a compromised client's disk image, which is saved as the file below.
    - "E:\Artifacts\other\_E01\infected\_drive\_c.E01"
  - The client seemed to be infected with malware.
  - The account name of the client's main user is "ttaro".
- Goal:
  - To find out the persistence of malware in the image.

# Extra Exercise:

## Checking auto-start locations on an infected disk C (2)

- Mount the disk image "infected\_drive\_c.E01" with Arsenal Image Mounter and view the auto-start locations with Autoruns. In this case, since we are focusing on the user "ttaro", we should use ttaro's home folder as "User Profile".
- Then, apply the filter with a part of the path like exercises we have done.


Autoruns [DESKTOP-P4HMK0S\taro] - Sysinternals: [www.sysinternals.com](http://www.sysinternals.com)

File Entry Options User Help

Filter: users

KnownDLLs Winlogon Winsock Providers Print Monitors LSA Providers

Everything Logon Explorer Internet Explorer Scheduled Tasks Services Dri

Autorun Entry	Description	Publisher	Image Path	Timestamp	VirusTotal
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				4/23/2018 11:06 AM	
<input checked="" type="checkbox"/>  Devic...	Symantec 802.1x...	(Verified) Symant...	c:\users\ttaro\appdata\roaming\symant...	2/2/2009 2:38 PM	

# Extra Exercise:

## Checking auto-start locations on an infected disk C (3)

- Check the entry.
  - At the first glance, the file seems to be legitimate because it has a valid code-sign, but the file is located in a temporary folder. It looks so strange because those entries listed by Autoruns are related to persistence.


Autoruns [DESKTOP-P4HMK0S\taro] - Sysinternals: www.sysinternals.com

File Entry Options User Help

Filter: users

KnownDLLs Wi Code-sign is valid, but... Providers

Everything Logon Explorer Internet Explorer LSA Providers Services Drivers

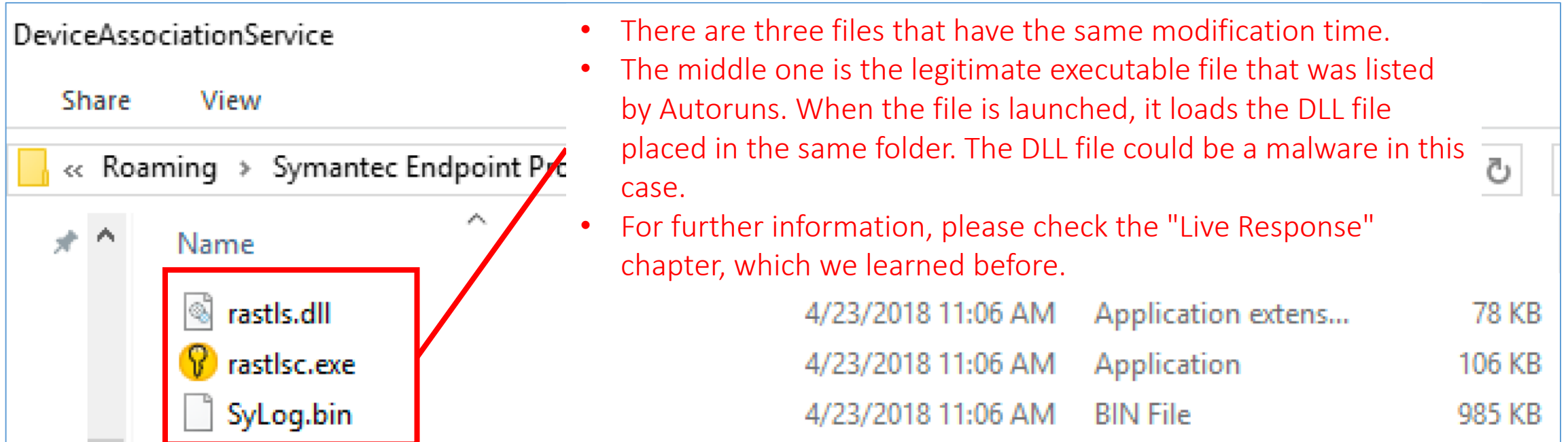
Autorun Entry	Description	Publisher	Image Path	Timestamp	VirusTotal
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				4/23/2018 11:06 AM	
<input checked="" type="checkbox"/>  Devic... Symantec 802.1x...		(Verified) Symantec	c:\users\taro\appdata\roaming\symantec...	2/2/2009 2:38 PM	

Although this executable is persistent, the file is located in a temporary folder!

# Extra Exercise:

## Checking auto-start locations on an infected disk C (4)

- It seems that this is one of the anti-Autoruns techniques such as DLL side loading that we learned in "Live Response" chapter.
- Let's open the folder that contains the executable file.



DeviceAssociationService

Share View

<< Roaming > Symantec Endpoint Protection > DeviceAssociationService

Name	Modified	Type	Size
rastls.dll	4/23/2018 11:06 AM	Application extension...	78 KB
rastlsc.exe	4/23/2018 11:06 AM	Application	106 KB
SyLog.bin	4/23/2018 11:06 AM	BIN File	985 KB

- There are three files that have the same modification time.
- The middle one is the legitimate executable file that was listed by Autoruns. When the file is launched, it loads the DLL file placed in the same folder. The DLL file could be a malware in this case.
- For further information, please check the "Live Response" chapter, which we learned before.

# Extra Exercise:

## Checking auto-start locations on an infected disk C (5)

- In a real case, you should get all files in the temporary folder (at least rastlsc.exe, rastls.dll and SyLog.bin), and execute it on your dynamic analysis environment.