Quand les bleus se prennent pour des chercheurs de vulnérabilités

Recherche d'événements ETW (Event Tracing for Windows)



Sylvain Peyrefitte -- cert@airbus.com



Un problème de mesure

- Comment mesure-t-on l'état d'un système ?
- Avons-nous toutes les informations nécessaires?
- N'avons-nous pas trop d'informations?





AIRRI

2































L'état de notre sysadmin est à la fois content et pas content tant que nous ne pouvons mesurer



Théorie quantique de la mesure : L'école de Bohr



- Soit nous considérons que nous ne pouvons pas mesurer directement l'exploitation de la vulnérabilité, mais plutôt ses conséquences
 - Nous détectons les processus créés par le service
 - Nous détectons l'instabilité d'un processus via WER



Théorie quantique de la mesure : L'école d'Einstein

 Soit nous considérons qu'il existe une mesure qu'il faut découvrir et qui nous permettra de définir avec précision l' état de notre système







Que cherchons-nous à mesurer ?

- Bluekeep
 - Affecte le service TerminalServer
 - Se base sur le mélange entre les canaux statiques et dynamiques
 - En particulier le canal principal : ms_t120







Que peut-on mesurer ?

- Event Tracing for Windows
 - Provider, ceux qui vont émettre des événements
 - Session, afin de grouper les providers
 - Consumer, ceux qui vont consommer et manipuler les événements depuis une session

• Lister les providers émis par le service





• Lister les providers émis par le service logman query providers -pid 123

📧 Administrator: Command Prompt		-		\times
Microsoft Windows [Version 10.0.18362.77 (c) 2019 Microsoft Corporation. All righ	8] ts reserved.			^
C:\Windows\system32>logman query providers -pid 760				
Provider	GUID			
Microsoft-Windows-AppModel-Runtime	{F1EF270A-0D32-4352-BA52-DBAB41E1D859}			
Microsoft-Windows-ASN1	{D92EF8AC-99DD-4AB8-B91D-C6EBA85F3755}			
Microsoft-Windows-AsynchronousCausality	{19A4C69A-28EB-4D4B-8D94-5F19055A1B5C}			
Microsoft-Windows-COM-Perf	{B8D6861B-D20F-4EEC-BBAE-87E0DD80602B}			
Microsoft-Windows-COM-RundownInstrumentation {2957313D-FCAA-5D4A-2F69-32CE5F0AC44E}				
Microsoft-Windows-COMRuntime	{BF406804-6AFA-46E7-8A48-6C357E1D6D61}			
Microsoft-Windows-Crypto-BCrypt	{C7E089AC-BA2A-11E0-9AF7-68384824019B}			
Microsoft-Windows-Crypto-NCrypt	{E8ED09DC-100C-45E2-9FC8-B53399EC1F70}			
Microsoft-Windows-Diagnosis-PCW	{AABF8B86-7936-4FA2-ACB0-63127F879DBF}			
Microsoft-Windows-Direct3D11	{DB6F6DDB-AC77-4E88-8253-819DF9BBF140}			
Microsoft-Windows-DXGI	{CA11C036-0102-4A2D-A6AD-F03CFED5D3C9}			
Microsoft-Windows-Eventlog	{FC65DDD8-D6EF-4962-83D5-6E5CFE9CE148}			
Microsoft-Windows-Heap-Snapshot	{901D2AFA-4FF6-46D7-8D0E-53645E1A47F5}			
Microsoft-Windows-Networking-Correlatior	{83ED54F0-4D48-4E45-B16E-726FFD1FA4AF}			
Microsoft-Windows-PDC	{A6BF0DEB-3659-40AD-9F81-E25AF62CE3C7}			
Microsoft-Windows-RemoteDesktopServices-	RdpCoreTS {1139C61B-B549-4251-8ED3-27250A1EDEC8}			
Microsoft-Windows-RemoteDesktopServices-	RemoteFX-VM-User-Mode-Transport {741C6BE3-F74B-4E4D-88E7-5CE3A35F	AEB3}		
Microsoft-Windows-RPC	{6AD52B32-D609-4BE9-AE07-CE8DAE937E39}			
Microsoft-Windows-RPC-Events	{F4AED7C7-A898-4627-B053-44A7CAA12FCD}			
Microsoft-Windows-Services-Svchost	{06184C97-5201-480E-92AF-3A3626C5B140}			
Microsoft-Windows-Shell-Core	{30336ED4-E327-447C-9DE0-51B652C86108}			
Microsoft-Windows-TerminalServices-Remot	eConnectionManager {C76BAA63-AE81-421C-B425-340B4B24157F}			
Microsoft-Windows-User Profiles General	{DB00DFB6-29F9-4A9C-9B3B-1F4F9E7D9770}			~





- Lister les providers émis par le service
- Créer une session regroupant les providers qui nous semblent intéressants





- Lister les providers émis par le service
- Créer une session regroupant les providers qui nous semblent intéressants

logman start RDP -p Microsoft-Windows-RemoteDesktopServices-RdpCoreTS -ets -rt





- Lister les providers émis par le service
- Créer une session regroupant les providers qui nous semblent intéressants
- Visualiser les événements, les comparer, les analyser



- Lister les providers émis par le service
- Créer une session regroupant les providers qui nous semblent intéressants
- Visualiser les événements, les comparer, les analyser







Winshark

- Wireshark pour capturer des ETW
- Dissectors pour analyser les ETW
- **Provider** *Microsoft-Windows-NDIS-PacketCapture* (éviter d'installer un driver *NDIS* pour la capture réseau)
- Analyser les ETW de type Tracelogging
- Sauvegarder les ETW dans un fichier *pcap*





Winshark -- structure





Winshark : Demo détection bluekeep





Comprendre l'événement 148

- Attribuer cet événement seulement à la détection de l'exploit ?
- Sous quelle condition est-il émis ?
- Analyse statique et dynamique du module en charge de cet événement
- *HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WINEVT\Publishers*



Analyse avec ETWBreaker





Analyse avec ETWBreaker

ntdll!EtwEventWrite

rdpcorets!CRDPEventLogSessionBase::LogEvent+0xdd rdpcorets!CRDPEventLogSession::ChannelClose+0x47 RDPSERVERBASE!CRdpDynVC::OnClose+0x281 RDPSERVERBASE!CRdpDynVCMgr::CloseChannels+0x6a RDPSERVERBASE!CRdpDvnVCMgr::TerminateInstance+0x373 RDPSERVERBASE!CRDPWDUMXStack::TerminateInstance+0xf6 RDPSERVERBASE!CRDPENCConnection::Abort+0x77 RDPSERVERBASE!CRDPENCConnection::Terminate+0x1c RDPSERVERBASE/CRDPCoreConnection TerminateInstance+0x201 rdpcorets!CUMRDPConnection::TerminateInstance+0x210 rdpcorets!CUMRDPConnection::OnDisconnected+0x2b3 RDPSERVERBASE!CRDPCoreConnection::SMAPI Decoupled OnRDPStackDisconnected+0x241 RDPBASE!CTSMsq:::Invoke+0xfb RDPBASE!CTSThread::RunOueueEvent+0x130 RDPBASE!CTSThread::RunAllQueueEvents+0x111 RDPBASE!CTSThread::internalMsgPump+0xc9 RDPBASE!CTSThread::internalThreadMsgLoop+0xe9 RDPBASE!CTSThread::ThreadMsqLoop+0x1c RDPBASE!CRDPENCPlatformContext::STATIC_STAThreadProc+0x56





Comprendre l'événement 148

- RdpCoreTS_Event_ChannelClose
- ChannelName = ms_t120
- CRdpDynVC : Dynamic Virtual Channel





To be continued...

- Ajouter des providers
 - Exemple de l'AMSI
- Exploiter les WPP
- Winshark : <u>https://github.com/airbus-cert/Winshark</u>
- ETWBreaker : <u>https://github.com/airbus-cert/etwbreaker</u>

AIRBUS

Merci

On recrute !

Questions : cert@airbus.com

