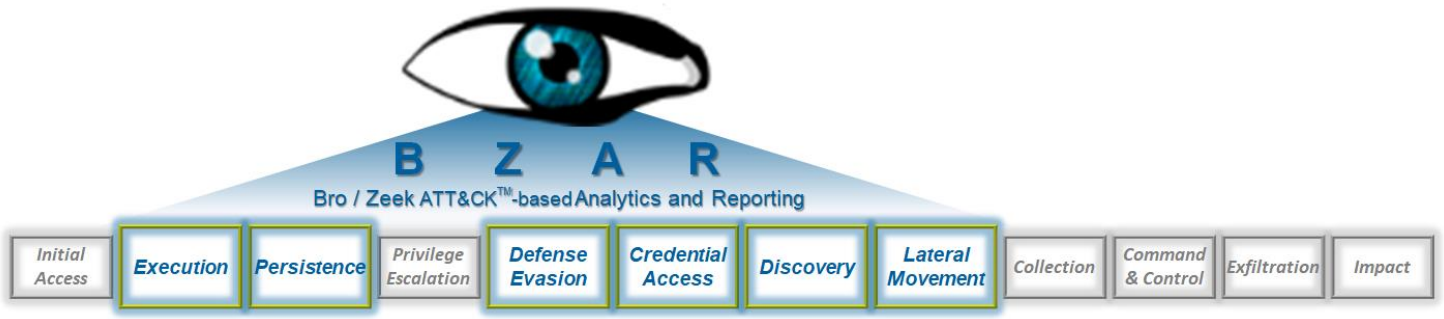
B Z A R – Bro/Zeek ATT&CK™-based Analytics and Reporting

Detecting Adversary Behaviors via Internal Network Monitoring

M.I. Fernandez | The MITRE Corporation



Presentation for

zeek week

Seattle, WA | 09 Oct 2019

MITRE

Motivation

- **Objective:** ***Detect Adversary Behaviors via Internal Network Monitoring***
  - Execution
  - Credential Access
  - Discovery
  - Lateral Movement
  - Persistence
  - Defense Evasion
- **Problem:** ***Internal Network Traffic Can be Very Noisy***
  - Server Message Block (SMB) Protocol
  - Remote Procedure Call (RPC) Protocol
- **Technology:** ***Bro / Zeek Network Security Monitor***
  - Open Source
  - Deep Packet Inspection

Result

B Z A R

Bro / Zeek ATT&CK-based Analytics and Reporting

Bizarre: very strange or unusual

BZAR: open-source Bro/Zeek scripts

https://github.com/mitre-attack/bzar

MITRE

Outline

- **Quick Background**
  - MITRE ATT&CK Model
- **Relevant Network Protocols**
  - Server Message Block (SMB)
  - Remote Procedure Call (RPC)
- **ATT&CK Detection with BZAR**
  - SMB & RPC Indicators, Analytics & Reporting
  - Examples
- **Key Takeaways**

ATT&CK for Enterprise

- **Adversarial Tactics, Techniques, & Common Knowledge**[1]
  - Globally-accessible knowledge base of adversary tactics and techniques [i.e., behaviors] based on real-world observations
  - Reflects various phases of an adversary's lifecycle and the platforms they are known to target

- **MITRE Technical Report: *Finding Cyber Threats with ATT&CK-Based Analytics***[2]

Step 1: *Identify Behaviors*

Step 2: *Acquire Data*

Step 3: *Develop Analytics*

Steps 4-5: Develop Scenario & Emulate Threat

Step 6: Investigate Attack

Step 7: Evaluate Performance

[1] *https://attack.mitre.org*

[2] *https://www.mitre.org/publications/technical-papers/finding-cyber-threats-with-attck-based-analytics*

MITRE

Tactics: the adversary's technical goals

Techniques: how the goals are achieved

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulati	Access Token Manipulati	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternativ Protocol	Disk Structure Wipe
Spearphishing Attachmen	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Network Shared Drive	Data Encoding	Exfiltration Over Comman and Control Channel	Endpoint Denial of Service
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Firmware Corruption
Spearphishing via Service	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compile After Delivery	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Inhibit System Recovery
Supply Chain Compromis	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Compiled HTML File	Hooking	Password Policy Discove	Remote File Copy	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Network Denial of Service
Trusted Relationship	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Firmware	Input Capture	Peripheral Device Discovery	Remote Services	Input Capture	Fallback Channels		Resource Hijacking
Valid Accounts	InstallUtil	Change Default File Association	File System Permissions Weakness	Component Object Model Hijacking	Input Prompt	Permission Groups Discovery	Replication Through Removable Media	Man in the Browser	Multi-hop Proxy		Runtime Data Manipulation
	Launchctl	Component Firmware	Hooking	Control Panel Items	Kerberoasting	Process Discovery	Shared Webroot	Screen Capture	Multi-Stage Channels		Service Stop
	Local Job Scheduling	Component Object Model Hijacking	Image File Execution Options Injection	DCShadow	Keychain	Query Registry	SSH Hijacking	Video Capture	Multiband Communicatior		Stored Data Manipulation
	LSASS Driver	Create Account	Launch Daemon	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisonin and Relay	Remote System Discover	Taint Shared Content		Multilayer Encryption		Transmitted Data Manipulation
	Mshta	DLL Search Order Hijacking	New Service	Disabling Security Tools	Network Sniffing	Security Software Discovery	Third-party Software		Port Knocking		
	PowerShell	Dylib Hijacking	Path Interception	DLL Search Order Hijacking	Password Filter DLL	System Information Discovery	Windows Admin Shares		Remote Access Tools		
	Regsvcs/Regasm	External Remote Services	Plist						Remote File Copy		
	Regsvr32	File System Permissions Weakness	Port						Standard Application Layer Protocol		
	Rundll32	Hidden Files and Directories	Proce						Standard Cryptographic Protocol		
	Scheduled Task	Hooking	Sche						Standard Non-Application Layer Protocol		
	Scripting	Hypervisor	Servi Perm						Uncommonly Used Port		
	Service Execution	Image File Execution Options Injection	Setui						Web Service		
	Signed Binary Proxy Execution	Kernel Modules and Extensions	SID-H								
	Signed Script Proxy Execution	Launch Agent	Start								
	Source	Launch Daemon	Sudo								
	Space after Filename	Launchctl	Sudo								
	Third-party Software	LC_LOAD_DYLIB Addition	Valid								
	Trap	Local Job Scheduling	Web								
	Trusted Developer Utilities	Login Item									
	User Execution	Logon Scripts									
	Windows Management Instrumentation	LSASS Driver									
	Windows Remote Management	Modify Existing Service									
	XSL Script Processing	Netsh Helper DLL									
		New Service									
		Office Application Startup									
		Path Interception									
		Plist Modification									
		Port Knocking									
		Port Monitors									
		Rc.common									
		Re-opened Applications									
		Redundant Access									
		Registry Run Keys / Startup Folder									
		Scheduled Task									
		Screensaver									
		Security Support Provider									
		Service Registry Permissions Weakness									
		Setuid and Setgid									
				Indicator Removal from Tools							
				Indicator Removal on Host							
				Indirect Command Execution							
				Install Root Certificate							
				InstallUtil							
				Launchctl							
				LC_MAIN Hijacking							
				Masquerading							
				Modify Registry							
				Mshta							
				Network Share Connection Removal							
				NTFS File Attributes							
				Obfuscated Files or Information							
				Plist Modification							
				Port Knocking							
				Process Doppelgänging							
				Process Hollowing							

Procedures: Specific technique implementation

Spearphishing Attachment

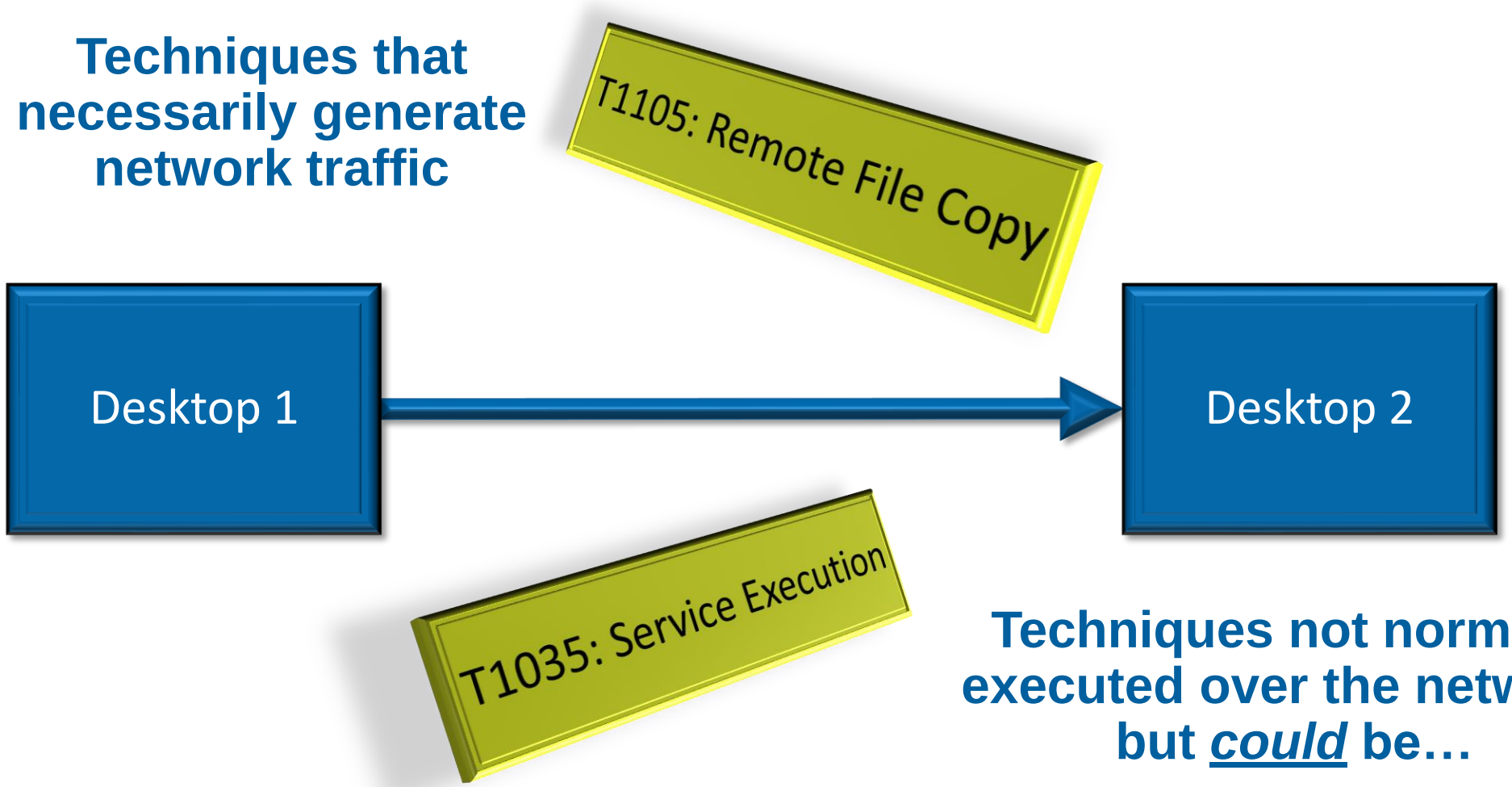
Examples

Name	Description
APT19	APT19 sent spearphishing emails with malicious attachments in RTF and XLSM formats to deliver initial exploits.[1]
APT28	APT28 sent spearphishing emails containing malicious Microsoft Office attachments.[2][3][4][5][6]

MITRE

ATT&CK and Internal Network Monitoring

Techniques that necessarily generate network traffic



Techniques not normally executed over the network, but *could* be…

MITRE

Bro / Zeek Protocol Analyzers

- **SMB Protocol Analyzer**[3]
  - Message Types 145
- **DCE-RPC Protocol Analyzer**[3]
  - Interface Definitions 81
  - Method Definitions 1,471
- **Authentication Protocol Analyzers**
  - Used in SMB and RPC Authentication
- **File Extraction Analyzer**
  - Extract Files from Network Traffic
  - Lateral Movement

How Many Exist in Windows?

How Many Exist in Windows?

Bonus!

Bonus!

[3] *circa March 2018 (Bro v2.5.2 - v2.5.3)*

MITRE

Protocol Specifications *(1 of 2)*

- **SMB Specifications**
  - Microsoft Developer Network (MSDN) Documentation[4]
    - ms-brws Common Internet File System (CIFS) Browser Protocol
    - ms-cifs Common Internet File System (CIFS) Protocol
    - ms-mail Remote Mailslot Protocol
    - ms-msrp Messenger Service Remote Protocol
    - ms-rap Remote Administration Protocol
    - ms-smb Server Message Block (SMB) Protocol
    - ms-smb2 Server Message Block (SMB) Protocol Versions 2 and 3
    - ms-smbd SMB2 Remote Direct Memory Access (RDMA) Transport Protocol
  - Total SMB Commands & Sub-Commands: ***332***

[4] *MSDN Library > Open Specifications > Protocols > Windows Protocols > Technical Documents: https://msdn.microsoft.com/en-us/library/jj712081.aspx*

Protocol Specifications *(2 of 2)*

- **RPC Specifications**
  - The Open Group, Technical Standard C706[5]
    - Distributed Computing Environment (DCE) 1.1: Remote Procedure Call (RPC) [1997]
    - Nineteen (19) Basic Message Types
  - MSDN Documentation[6]
    - Eighty (80) Protocol Documents Contained RPC Interface Definitions
    - Some Documents Defined More Than One RPC Interface
  - Other Documentation
    - J.B. Marchand, *Windows Network Services Internals*[7]
  - Total RPC Interfaces: ***379***

    Methods: ***2,572+***

[5] *http://pubs.opengroup.org/onlinepubs/9629399/toc.pdf*

[6] *https://msdn.microsoft.com/en-us/library/jj712081.aspx*

[7] *http://index-of.es/Windows/win_net_srv.pdf*

Map Protocols to ATT&CK Techniques

- **SMB Protocol Summary**
  - Reviewed all 332 Commands & Sub-Commands
  - Mapped ***145*** as Indicators of *Potential* ATT&CK Techniques

- **RPC Protocol Summary**
  - Reviewed 165 (out of 379) Interfaces
  - Mapped ***1,480*** (out of 2,572) Methods to *Potential* ATT&CK Techniques

- **BZAR**
  - Eight (8) SMB Indicators
  - Ninety-three (93) RPC Indicators

ATT&CK Techniques Detected with BZAR – *Heatmap*

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
Hardware Additions	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Replication Through Removable Media	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Spearphishing Attachment	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe
Spearphishing Link	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Endpoint Denial of Service
Spearphishing via Service	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Firmware Corruption
Supply Chain Compromise	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Inhibit System Recovery
Trusted Relationship	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Component Firmware	Hooking	Peripheral Device Discovery	Remote File Copy	Email Collection	Fallback Channels	Scheduled Transfer	Network Denial of Service
Valid Accounts	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Object Model Hijacking	Input Capture	Permission Groups Discovery	Remote Services	Input Capture	Multiband Communication		Resource Hijacking
	InstallUtil	Change Default File Association	File System Permissions Weakness	Control Panel Items	Input Prompt	Process Discovery	Replication Through Removable Media	Man in the Browser	Multi-hop Proxy		Runtime Data Manipulation
	Launchctl	Component Firmware	Hooking	DCShadow	Kerberoasting	Query Registry	Shared Webroot	Screen Capture	Multilayer Encryption		Service Stop
	Local Job Scheduling	Component Object Model Hijacking	Image File Execution Options Injection	Deobfuscate/Decode Files or Information	Keychain	Remote System Discovery	SSH Hijacking	Video Capture	Multi-Stage Channels		Stored Data Manipulation
	LSASS Driver	Create Account	Launch Daemon	Disabling Security Tools	LLMNR/NBT-NS Poisoning	Security Software Discovery	Taint Shared Content		Port Knocking		Transmitted Data Manipulation
	Mshta	DLL Search Order Hijacking	New Service	DLL Search Order Hijacking	Network Sniffing	System Information Discovery	Third-party Software		Remote Access Tools		
	PowerShell	Dylib Hijacking	Path Interception	DLL Side-Loading	Password Filter DLL	System Network Configuration Discovery	Windows Admin Shares		Remote File Copy		
	Regsvcs/Regasm	External Remote Services	Plist Modification	Exploitation for Defense Evasion	Private Keys	System Network Connections Discovery	Windows Remote Management		Standard Application Layer Protocol		
	Regsvr32	File System Permissions Weakness	Port Monitors	Extra Window Memory Injection	Securityd Memory	System Owner/User Discovery			Standard Cryptographic Protocol		
	Rundll32	Hidden Files and Directories	Process Injection	File Deletion	Two-Factor Authentication Interception	System Service Discovery			Standard Non-Application Layer Protocol		
	Scheduled Task	Hooking	Scheduled Task	File Permissions Modification		System Time Discovery			Uncommonly Used Port		
	Scripting	Hypervisor	Service Registry Permissions Weakness	File System Logical Offsets					Web Service		
	Service Execution	Image File Execution Options Injection	Setuid and Setgid	Gatekeeper Bypass							
	Signed Binary Proxy Execution	Kernel Modules and Extensions	SID-History Injection	Hidden Files and Directories							
	Signed Script Proxy Execution	Launch Agent	Startup Items	Hidden Users							
	Source	Launch Daemon	Sudo	Hidden Window							
	Space after Filename	Launchctl	Sudo Caching	HISTCONTROL							
	Third-party Software	LC_LOAD_DYLIB Addition	Valid Accounts	Image File Execution Options Injection							
	Trap	Local Job Scheduling	Web Shell	Indicator Blocking							
	Trusted Developer Utilities	Login Item		Indicator Removal from Tools							
	User Execution	Logon Scripts		Indicator Removal on Host							
	Windows Management Instrumentation	LSASS Driver		Indirect Command Execution							
	Windows Remote Management	Modify Existing Service		Install Root Certificate							
	XSL Script Processing	Netsh Helper DLL		InstallUtil							
		New Service		Launchctl							
		Office Application Startup		LC_MAIN Hijacking							
		Path Interception		Masquerading							
		Plist Modification		Modify Registry							
		Port Knocking		Mshta							
		Port Monitors		Network Share Connection Removal							
		Rc.common		NTFS File Attributes							
		Redundant Access		Obfuscated Files or Information							
		Registry Run Keys / Startup Folder		Plist Modification							
		Re-opened Applications		Port Knocking							
		Scheduled Task		Process Doppelgänging							
		Screensaver		Process Hollowing							
		Security Support Provider		Process Injection							
		Service Registry Permissions Weakness		Redundant Access							
		Setuid and Setgid		Regsvcs/Regasm							
		Shortcut Modification		Regsvr32							
		SIP and Trust Provider Hijacking		Rootkit							
		Startup Items		Rundll32							
		System Firmware		Scripting							
		Time Providers		Signed Binary Proxy Execution							
		Trap		Signed Script Proxy Execution							
		Valid Accounts		SIP and Trust Provider Hijacking							
		Web Shell		Software Packing							
		Windows Management Instrumentation Event Subscription		Space after Filename							
		Winlogon Helper DLL		Template Injection							
				Timestomp							
				Trusted Developer Utilities							
				Valid Accounts							
				Web Service							
				XSL Script Processing							

Legend
White = No Confidence of Detection
Orange = Some Confidence of Detection

MITRE

ATT&CK Techniques Detected with BZAR

Execution	Persist				Lateral Movement
T1035 Service Execution	Helper DLL				T1077 Windows Admin Shares
T1047 Windows Mgmt Instrumentation (WMI)	T1013 Port Monitors				T1105 Remote File Copy
T1053 Scheduled Task					
				T1087 Account	
				T1124 System Time	
				T1135 Network Share	

Adversaries may execute a binary, command, or script that interacts with Windows services, such as the *Service Control Manager*. This can be done by either *creating a new service or modifying an existing service*…

Examples: ***APT32, BBSRAT, Cobalt Strike, Empire, FIN6, Honeybee…***

Excerpt from – https://attack.mitre.org/techniques/T1035

BZAR Example – T1035 Service Execution

Execution
T1035 Service Execution

- **Indicators:** ***Four (4) RPC Functions***
  - svcctl :: CreateServiceA
  - svcctl :: CreateServiceW
  - svcctl :: StartServiceA
  - svcctl :: StartServiceW
- **Analytics:** ***Simple***
  - Detect ***any*** of the 4 RPC functions
  - Zeek event handlers
    - dce_rpc_request()
    - *dce_rpc_response()*

BZAR Example – T1035 Service Execution

Execution
T1035 Service Execution

- **Reporting:** ***Write to Zeek Notice Log***
  - "ATTACK::Execution"
  - "svcctl::StartServiceW"
  - IP addresses & TCP/UDP ports
  - Zeek connection ID

Important: MUST be tuned for your environment!

BZAR Example – T1013 Port Monitors

Execution	Persistence	Defe… Eva…	…ovement
T1035 Service Execution	T1004 Winlogon Helper DLL	T10…	…s Admin
T1047 Windows Mgmt Instrumentation (WMI)	T1013 Port Monitors		File Copy
T1053 Scheduled Task			
		T1135 Network Share	

A port monitor can be set *through the API call* to set a DLL to be loaded at startup… loaded by the *print spooler service*…

Adversaries can use this technique to *load malicious code* at startup that will *persist on system reboot and execute as SYSTEM*.

Example: *APT38*

Excerpt from – https://attack.mitre.org/techniques/T1013

MITRE

BZAR Example – T1013 Port Monitors

- **Indicators:** ***Four (4) RPC Functions***
  - spoolss :: RpcAddMonitor # aka winspool | spoolss
  - spoolss :: RpcAddPrintProcessor # aka winspool | spoolss
  - IRemoteWinspool :: RpcAsyncAddMonitor
  - IRemoteWinspool :: RpcAsyncAddPrintProcessor
- **Analytics:** ***Simple***
  - Detect ***any*** of the 4 RPC functions
- **Reporting:** ***Write to Zeek Notice Log***
  - "ATTACK::Persistence"
  - <rpc_interface_name>::<rpc_method_name>
  - IP addresses & TCP/UDP ports
  - Zeek connection ID

Persistence
T1013 Port Monitors

May never see this in your environment, but if you DO…

MITRE

BZAR Example – T1070 Indicator Removal on Host

Execution	Persistence	Defense Evasion			
T1035 Service Execution	T1004 Winlogon Helper DLL	T1070 Indicator Removal Host			
T1047 Windows Mgmt Instrumentation (WMI)	T1013 Port Monitors				
T1053 Scheduled Task					
				T1124 System Time	
				T1135 Network Share	

Adversaries may delete or alter generated artifacts on a host system... ***make forensic analysis and incident response more difficult*****...**

Clear Windows Event Logs**…**
Adversaries... may choose to clear the events in order to hide their activities.

Example: ***APT23, APT29, APT32, APT38, BankShot, BlackEnergy…***

Excerpt from – https://attack.mitre.org/techniques/T1070

MITRE

BZAR Example – T1070 Indicator Removal on Host

Defense Evasion
T1070 Indicator Removal on Host

- **Indicators:** ***Ten (10) RPC Functions***
  - eventlog :: ElfrClearELFA
  - eventlog :: ElfrClearELFW
  - IEventService :: EvtRpcClearLog
  - winreg :: BaseInitiateSystemShutdown
  - winreg :: BaseInitiateSystemShutdownEx
  - InitShutdown :: BaseInitiateShutdown
  - InitShutdown :: BaseInitiateShutdownEx
  - WindowsShutdown :: WsdrInitiateShutdown
  - winstation_rpc :: RpcWinStationShutdownSystem
  - samr :: SamrShutdownSamServer[8]

[8] *MSDN Library states not used on the wire*

MITRE

BZAR Example – T1070 Indicator Removal on Host

Defense Evasion
T1070 Indicator Removal on Host

- **Analytics:** ***Simple***
  - Detect ***any*** of the 10 RPC functions
- **Reporting:** ***Write to Zeek Notice Log***
  - "ATTACK::Defense_Evasion"
  - <rpc_interface_name>::<rpc_method_name>
  - IP addresses & TCP/UDP ports
  - Zeek connection ID

Important: MUST be tuned for your environment!

BZAR Example – Lateral Movement

Execution				ery	Lateral Movement
T1035 Service Execution					T1077 Windows Admin Shares
T1047 Windows Mgmt Instrumentation (WMI)				etwork	T1105 Remote File Copy
T1053 Scheduled Task				System	
				wner/User	
				n Groups	
				nfo	
				ectory	
				stem Time	
			T1135 Network Share		

Windows systems have hidden network shares... Example network shares include *C$, ADMIN$, and IPC$*.

Adversaries may use this technique... to *remotely access a networked system over server message block (SMB)* to… transfer files, and run transferred binaries through remote Execution...

Examples: *APT3, APT32, BlackEnergy, Cobalt Strike, DeepPanda...*

Excerpt from – https://attack.mitre.org/techniques/T1077

MITRE

BZAR Example – Lateral Movement

- **Indicators:** ***Two (2) SMB Commands***
  - SMBv1 Write
  - SMBv2 Write
- **Analytics:** ***Complex***
  - Detect SMB Write to Windows Admin Shares
    - ADMIN$ or C$ ***only***
    - Ignore IPC$ (e.g., names pipes)
  - Zeek event handlers
    - smb1_write_andx_response()
    - smb2_write_request()

Lateral Movement
T1077 Windows Admin Shares
T1105 Remote File Copy

BZAR Example – Lateral Movement

- **Reporting:** ***Write to Zeek Notice Log***
  - "ATTACK::Lateral_Movement"
  - "SMB::FILE_WRITE to admin file share"
  - IP addresses & TCP/UDP ports
  - Zeek connection ID
  - Full Universal Naming Convention (UNC) path and file name

Lateral Movement
T1077 Windows Admin Shares
T1105 Remote File Copy

Important: MUST be tuned for your environment!

BZAR Example – Lateral Movement Extracted File

- **Using the File Extraction Analyzer**
  - Detect SMB file write to admin file share
  - Copy the file to Bro/Zeek storage
- **Reporting: *Write to Zeek Notice Log***
  - “ATTACK::Lateral_Movement_Extracted_File”
  - “Saved a copy of the file written to admin file share <file>”
  - IP addresses & TCP/UDP ports
  - Zeek connection ID
  - Zeek file ID
  - UNC Path & File Name

BZAR Example – Lateral Movement Multiple Attempts

- **Detect Multiple SMB Admin File Share Indicators**
  - T1077 Windows Admin Shares (ADMIN$ or C$ only)
  - From the Same Host
- **Bro/Zeek Summary Statistics Thresholds**
  - N-occurrences, e.g. *N = 5*
  - T-timeframe, e.g. *T = 5min*
  - H-host, where H = same *originating* IP address
- **Reporting: *Write to Zeek Notice Log***
  - “ATTACK::Lateral_Movement”
  - “Detected T1077 Admin File Share activity from host <H>, total attempts <N> within timeframe <T>”

BZAR Example – Lateral Movement and Execution

- **Detect One Occurrence of Each**
  - SMB Write to Admin File Share
  - RPC Execution
- **Bro/Zeek Summary Statistics Thresholds**
  - S-score, where *S = 1 for SMB Write and S = 1000 for RPC Execution*
    - *Total Score >= 1001*
    - *Min Val == 1, Max Val == 1000*
  - T-timeframe, e.g. *T = 5min*
  - H-host, where H = same *target* IP address
- **Reporting: *Write to Zeek Notice Log***
  - “ATTACK::Lateral_Movement_and_Execution”
  - “Detected activity against host <H>, total score <S> within timeframe <T>”

Prototype Testing

- **MITRE CALDERA: Automated Red Team Agent**
  - Emulates Adversary Behaviors, based on ATT&CK Model
    - https://github.com/mitre/caldera

- **Successful Detection of CALDERA Activity**
  - CALDERA Exercise on Lab Network

Conclusion

Important: MUST be tuned for your environment!

MITRE

BZAR Summary *(1 of 2)*

- **“ATTACK::Execution”**
  - Detect *Any* of the 10 RPC Functions
- **“ATTACK::Persistence”**
  - Detect *Any* of the 6 RPC Indicators
- **“ATTACK::Defense_Evasion”**
  - Detect *Any* of the 10 RPC Indicators
- **“ATTACK::Credential_Access”**
  - Detect *Any* of the 2 RPC Indicators
- **“ATTACK::Discovery”**
  - Detect *Any* of the 57 RPC Indicators
  - Specified Number of *Occurrences* within Specified *Timeframe* from the Same *Originating* IP Address

BZAR Summary *(2 of 2)*

- **“ATTACK::Lateral_Movement”**
  - Detect SMB File Write to Windows Admin File Share
- **“ATTACK::Lateral_Movement_Multiple_Attempts”**
  - Specified Number of *Occurrences* within Specified *Timeframe* from the Same *Originating* IP Address
- **“ATTACK::Lateral_Movement_And_Execution”**
  - Detect One Occurrence of *Each* within Specified *Timeframe* to the Same *Target* IP Address
- **“ATTACK::Lateral_Movement_Extracted_File”**
  - Make a Copy of File Written to Windows Admin File Share

Other BZAR Contributions to Bro/Zeek

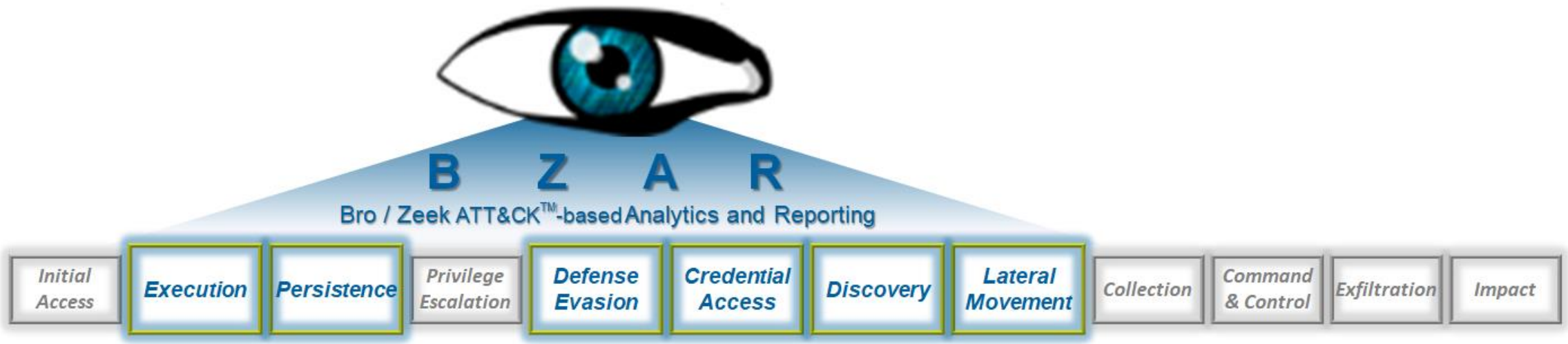
- **DCE-RPC Protocol Analyzer – *Bug Report & Fix***
  - Discovered Bug in AlterContext and AlterContext_Resp Message Parsers
  - ***Fixed in Bro v2.6***

- **DCE-RPC Additions**
  - 144 more RPC Interface Definitions
  - 1,145 more RPC Method Definitions

Future Work

- **New Feature: *Improved Whitelisting***
  - IP Address, IP Subnet, and/or Host Name
  - per ATT&CK Technique
- **New Feature: *Disable Detection and Disable Reporting***
  - Disable Detection (and thereby Reporting, too)
  - Enable Detection, but Disable Reporting
  - per ATT&CK Technique
- **Opportunities for New Detections**
  - So Many SMB Commands...
  - So Many RPC Methods...

Questions?



https://github.com/mitre-attack/bzar

MITRE

MITRE

MITRE's mission-driven teams are dedicated to solving problems for a safer world. Through our federally funded R&D centers and public-private partnerships, we work across government to tackle challenges to the safety, stability, and well-being of our nation.

Learn more at www.mitre.org.