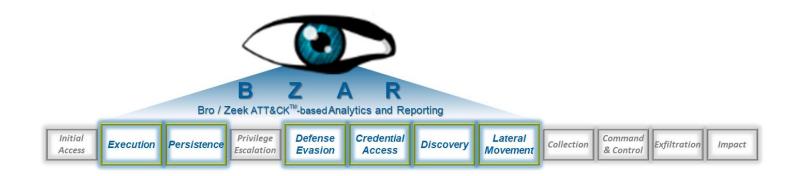
B Z A R – Bro/Zeek ATT&CK[™]-based Analytics and Reporting

Detecting Adversary Behaviors via Internal Network Monitoring

M.I. Fernandez | The MITRE Corporation



Presentation for



Seattle, WA | 09 Oct 2019



Motivation

- Objective: Detect Adversary Behaviors via Internal Network Monitoring
 - Execution

Discovery

Persistence

Credential Access

- Lateral Movement
 - 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

BZAR

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



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 Knowledge¹

- 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 Analytics²

Step 1: *Identify Behaviors* Steps 4-5: Develop Scenario & Emulate Threat

Step 2: *Acquire Data*Step 6: Investigate Attack

Step 3: *Develop Analytics* Step 7: Evaluate Performance

¹ https://attack.mitre.org

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



Initial Access Drive-by Com

External Remo Hardware Add

Replication Removable

Spearphishing

Spearphishing

Speamhishing

Supply Chain Trusted Releti

Valid Account

Tactics: the adversary's technical goals

Services Common Survive Interior. Accessability Position. Accessabili	SS	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And	Exfiltration	Impact
No Secretion Account Merigation Applical III. See Commission Marith Risk Applicate III.1. See Commission Marith Risk Applicate III.1. Application III.1. Application Service Marith Risk Application III.1. Application Service Marith Risk Application Service	npromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulati	Access Token Manipulation	Account Manipulation		AppleScript	Audio Capture		Automated Exfiltration	Data Destruction
Compaled HTML File Applicat DLLs. Applicat DLLs. Application Sharmon and Companies of Management DLLs. Application Sha	ic-Facing	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery		Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Imp
Corporal Fellows Application Streaming Appli	note Services	Command-Line Interface	Account Manipulation	AppCert DLLs		Brute Force	Browser Bookmark Discovery	Distributed Component Object Model			Data Encrypted	Defacement
Content of the process of the content of the process of the process of the content of the process of the proc	ditions	Compiled HTML File	AppCert DLLs	Applnit DLLs	Bypass User Account Control	Credential Dumping		Exploitation of Remote Services	Data from Information Repositories			Disk Content Wipe
Design New Processor Part	Through Media	Control Panel Items	Applnit DLLs		Clear Command History	Credentials in Files	File and Directory Discovery	Logon Scripts		Custom Cryptographic Protocol	PIOLOCOI	Disk Structure Wipe
No Secret Designation from Good 18 153 Jobs Composed Processing Pr	ng Attachmer	Dynamic Deta Exchange	Application Shimming		CMSTP		Network Service Scanning	Pass the Hash	Driva	Data Encoding	Exfiltration Over Commar and Control Channel	Endpoint Denial of Se
Compound	ng Link	Execution through API	thentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credentia Access	Network Share Discovery	Pass the Ticket	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Firmware Corruption
Installible Charge Debata First The System Permission Comported Debata First Comported Debata	ng via Service		BITS Jobs -		Compile After Delivery	Forced Authentication	Network Sniffing	Remote Desktop Protoco	Data Staged		Exfiltration Over Physical Medium	Inhibit System Recov
Installul Space Default File Trip System Permissions County and Learnful Component Firmware In Housing a Control Panel Interest Referenceshifty Process Society Shartwideboots Shartwideboots Panel Interest Process Street Control Panel Interest Referenceshifty Process Shartwideboots Panel Interest Process Street Process Panel Interest Panel Inter	n Compromis	Exploitation for Client Execution	Dootkit	Exploitation for Privilege Escalation	Compiled HTML File	Hooking		Remote File Copy	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Network Denial of Ser
Launched Component Firmware Local Job Scheduling Loss and Scheduli	tionship	Graphical User Interface		I injection		Input Capture	Peripheral Device Discovery		Input Capture	Fallback Channels		Resource Hijacking
Local Job Scheduling Local Job	its	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 Manipu
Lisads Driver Contal Accode Lisanch Dearmon Deadline cash Decoder Plant Lisanch Dearmon Deadline cash Decoder Plant Lisanch Dearmon Dear		Launchctl			Control Panel Items	Kerberoasting	Process Discovery	Shared Webroot	Screen Capture	Multi-Stage Channels		Service Stop
Death Public Part Death De		Local Job Scheduling	Component Object Model Hijacking	Image File Execution Options Injection			Query Registry	SSH Hijacking	Video Capture	Multiband Communication		Stored Data Manipula
Regave/Agegame Kutamal Remote Service Platat Scripting Street Floring Scripting Service Secution Segret Secution Segret Separation Service Secution Segret Strap Plany Surviva Segret Plany Surviva Segret Strap Plany Surviva Segret Strap Plany Surviva Segret Strap Service Segret Plany Surviva Segret Strap Service Segret Plany Surviva Segret Strap Service Segret Plany Surviva Segret Plany Surviva Segret		LSASS Driver		Launch Daemon	Deebfuscate/Decode Files or Information	LLMNR/NBT-NS Poisonir and Relav		Taint Shared Content		Multilayer Encryption		Transmitted Data Manipulation
Regard R		Mshta	DLL Search Order Hijacking	New Service		Network Sniffing		Third-party Software		Port Knocking		
Regavi22 Fig. Styleam Permissions Proceedures: Specific technique implementation Proceedures: Specific technique implementation Scheduled Task Proceedures: Specific technique implementation Scheduled Task Proceedures: Specific technique implementation Scheduled Task Proceedures: Specific technique implementation Specific technique i		PowerShell	Dylib Hijacking	nterception	DLL Search Order	Password Filter DLL	System Information	Windows Admin Shares		Remote Access Tools		
Scheduled Task Hooking Schelled Task Hooking Service Execution Hypervisor Service Execution Supred Binary Proxy Signed Binary Proxy Service Hoodules and Sub- Sub- Sub- Signed Binary Proxy Service Hoodules and Sub- Sub- Sub- Sub- Sub- Sub- Sub- Sub-		RegsvcVRegasm										
Scheduled Task Hooking Schelled Task Hooking Service Execution Hypervisor Service Execution Supred Binary Proxy Signed Binary Proxy Service Hoodules and Sub- Sub- Sub- Signed Binary Proxy Service Hoodules and Sub- Sub- Sub- Sub- Sub- Sub- Sub- Sub-		Regsvr32	File System Permissions Weakness	Port Proc	edures: S	pecific te	chniaue i	mplemer	ntation	Standard Application Lay Protocol	er .	
Scripting Hypervisor Service Execution Migner File Expectation State Support Service S		Rundll32	Hidden Files and Directories	Proce						Standard Cryptographic Protocol		
Service Secution Signed Script Proxy Signed Script Proxy Signed Script Proxy Laurch Agent Source Launch Service Space after Filename Launchctt Trap Local Job Scheduleg Trusted Developer Utilitie Login Item User Execution User Execution User Schedules Windows Management Los ASS Driver Windows Management Nets hitelepe DLL New Service Office Application Startup Plat Interception Plat Modification Port Knooking Port Monitos Re-opened Applications Redundant Access Registry Rim Key / Stiffuln Folder Respective Management Respective Mana		Scheduled Task	Hooking	Sche	I . I	1				Standard Non-Application Laver Protocol		
Service Secution Signed Script Proxy Signed Script Proxy Signed Script Proxy Laurch Agent Source Launch Service Space after Filename Launchctt Trap Local Job Scheduleg Trusted Developer Utilitie Login Item User Execution User Execution User Schedules Windows Management Los ASS Driver Windows Management Nets hitelepe DLL New Service Office Application Startup Plat Interception Plat Modification Port Knooking Port Monitos Re-opened Applications Redundant Access Registry Rim Key / Stiffuln Folder Respective Management Respective Mana		Scripting		Speart Speart	ohishina A	ttachmen [,]	į			Uncommonly Used Port		
Source Launch Baemon Sude Space after Fliename Launchell Sude Space after Fliename Launchell Sude Third-party Software LC_LOAD_DYISE Addition Value Local Job Scheduling Trap Local Job Scheduling Trusted Developer Utilities Login Item Logon Scripts Windows Management Instrumentation: Windows Management Instrumentation: New Service XSL Script Processing Neth Helper DLL New Service Office Application Statup Path Interception Plat Modification Port Knocking Port Monitors Re-common Redundant Access Registry Report Port Common Redundant Access Registry Report Scheduled Task Scheduled Task Scheduled Task Development Scheduled Task Developmen				Setul	_		-			Web Service		
Source Launch Baemon Sude Space after Fliename Launchell Sude Space after Fliename Launchell Sude Third-party Software LC_LOAD_DYISE Addition Value Local Job Scheduling Trap Local Job Scheduling Trusted Developer Utilities Login Item Logon Scripts Windows Management Instrumentation: Windows Management Instrumentation: New Service XSL Script Processing Neth Helper DLL New Service Office Application Statup Path Interception Plat Modification Port Knocking Port Monitors Re-common Redundant Access Registry Report Port Common Redundant Access Registry Report Scheduled Task Scheduled Task Scheduled Task Development Scheduled Task Developmen		Signed Binary Proxy Execution	Temel Modules and Extensions	side Examn	es							
Space after Filename Launchctt Sudd Third-party Software LC_LOAD_DYTM_Addition Valid Trap Local Job Scheduling Trusted Developer Utilities User Execution Logon Scripts Windows Management Instrumentation: Management Instrumentation: Ministrumentation: Modify Existing Service XSL Script Processing New Service Office Application Startup Path Interception Pilist Modification Port Knocking Port Monitors R. c. common Redundant Access Segistry Run Keys / Scription Tolding / Scription April Applications Redundant Access Registry Run Keys / Scription Tolding / Scription April Applications Redundant Access Registry Run Keys / Scription Tolding / Scription April Applications Redundant Access Registry Run Keys / Scription Tolding / Scription April Applications Redundant Access Registry Run Keys / Scription Tolding / Scription Applications Redundant Access Registry Run Keys / Scription Tolding / Scription Applications Redundant Access Registry Run Keys / Scription Tolding / Scription Applications Redundant Access Registry Run Keys / Scription Tolding / Scription Applications Redundant Access Registry Run Keys / Scription Tolding / Scription Applications Redundant Access Registry Run Keys / Scription Tolding / Scription Applications Redundant Run		Signed Script Proxy Execution	Launch Agent	Starti								
Space after Filename Launchctt Sudo Third-party Software LC_LOAD_PYTER_Addition Valid Trap Local Job Scheduling Web Trusted Developer Utilities Light Item User Execution Logon Scripts Windows Management ILSASS Driver Windows Management ILSASS Driver Windows Remote Modify Existing Service XSL Script Processing Netsh Heliper DLL New Service Office Application Startup Path Interception Pilist Modification Port Knocking Port Monitons Rc common Re-opened Applications Redundant Access Segistry Kun Keys / Script File Attributes Scheduled Task New Service North Management ILSASS Driver Management ILSASS Driver Management ILSASS Driver Management ILSASS Driver Modify Existing Service New Service Office Application Startup Path Interception Port Knocking Port Monitors Rc common Redundant Access Segistry Kun Keys / Script File Attributes Opticacted Files or Indicator Command New Service North Management ILSASS Driver New Service North Management ILSASS Driver North Management ILSASS Drive		Source	Launch Naemon	Sudo	Description							
Trap Local Job Scheduling Web Trusted Developer Utilities Login Item User Execution User Execution Windows Management Instrumentation Windows Remote Modify Existing Service XSL Script Processing Nets Helper DLL New Service Office Application Startup Path Interception Pirist Modification Port Knocking Port Monitors Re-opened Applications Re-opened Applications Redundant Access Registry Run Keys / Spitulus Folder Scheduled Task New Service Response Registry Run Keys / Spitulus Folder Scheduled Task New Service Response Registry Run Keys / Spitulus Folder Scheduled Task New Service Defined Removal on Host Processing Modify Registry Mesta Response Response Run		Space after Filename	Launchetl 📏	Sudo	Description							
Trusted Developer Utilities Login Item User Execution Logon Scripts Windows Management LSASS Driver Windows Region Web Helper DLL New Service Office Application Startup Path Interception Plist Modification Port Knocking Port Monitors Re-opened Applications Re-opened Applications Redundant Access Registry Run Keys / Sighun Folder Scheduled Task Resorting		Third-party Software	LC_LOAD_DYL® Addition	Valid	ADT10t			-l VI ON 4 f + - + - - -				
User Execution Windows Management UsASS Driver Windows Remote Modify Existing Service XSL Script Processing New Service Office Application Startup Path Interception Pits Modification Port Knocking Port Monitors Re-opened Applications Recommon Re-opened Applications Redundant Access Registry, Run Keys / Schemic Foliate Scheduled Task Results APT28 sent spearphishing emails containing malicious Microsoft Office attachments. [2][3][4][5][6] APT28 sent spearphishing emails containing malicious Microsoft Office attachments. [2][3][4][5][6] APT28 sent spearphishing emails containing malicious Microsoft Office attachments. [2][3][4][5][6] Holicator Removal on Host Indicator Removal Indicator Removal Indicator Removal Indicator Removal Indi		Trap	Local Job Scheduling	Web APT19	APT 19 sent spearpnish	ing emails with maliciou	is attachments in RTF an	d XLSIVI formats to deliv	er initial exploits. ¹¹¹			
Windows Management Instrumentation Windows Remote 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 / Sighth Profiler Scheduled Task Redundant Access Registry Run Keys / Sighth Profiler Scheduled Task AP128 Sent spearphishing emails containing malicious Microsoft Office attachments. Path Interception Indicator Removal on Host Indicator Removal on Hos		Trusted Developer Utilities	Login Item									
Windows Remote Modify Existing Service XSL Script Processing Netsh Helper DLL New Service Office Application Startup Path Interception Plist Modification Port Knocking Port Monitors Recommon Re-opened Applications Redundant Access Registry Run Keys / Scheduled Task Redundant Access Registry Run Keys / Scheduled Task			Logon Scripts	ΔPT28	ΔPT28 sent snearnhish	ing emails containing m	alicious Microsoft Office	attachments [2][3][4][5][6]				
XSL Script Processing Netsh Helper DLL Indicator Removal on Host Indicator Removal on Host Indicator Removal on Host Indicator Startup Path Interception Path Interception Port Monitors Install Root Certificate Install Root Removal on Host Install Root Certificate Install		Windows Management Instrumentation	LSASS Driver	Al 120	Ai 120 dent opeurphion	ing critails containing in	ancious whoresort office	attachments.				
New Service Office Application Startup Path Interception Pist Modification Port Knocking Port Monitors Rc.common Re-opened Applications Redundant Access Registry, Run Keys / Sightly, Fun Keys / Scheduled Task Indirect Command Indirect Command Install Root Certificate In	[Windows Remote Management	Modify Existing Service		Tools							
Office Application Startup Path Interception Install Root Certificate Install Util Plist Modification Launchotl Port Knocking Port Monitors Re.common Re.common Reopened Applications Redundant Access Redundant Access Registry, Run Keys / Startun Folder Scheduled Task Install Root Certificate Inst		XSL Script Processing	Netsh Helper DLL			t						
Path Interception Plist Modification Launchctl Port Knocking Port Monitors Recommon Recommon Re-opened Applications Redundant Access Registry, Run Keys / Staffun Folder Scheduled Task Redundard Scheduled Task Redundant Access Registry Run Keys / Scheduled Task Redundant Access Registry Run Keys / Scheduled Task Redundant Access Registry Run Keys / Scheduled Task Redundant Run			New Service]	Indirect Command Execution							
Plist Modification Port Knocking LC_MAIN Hijacking Port Monitors Masquerading Rc.common Modify Registry Re-opened Applications Redundant Access Registry Run Keys / Stattub Folder Scheduled Task Optus cated Files or information			Office Application Startup		Install Root Certificate							
Port Knocking Port Monitors Masquerading Rc.common Modify Registry Re-opened Applications Redundant Access Redundant Access Registry Run Keys / Stattub Folder Scheduled Task Diffus cated Files or information			Path Interception		InstallUtil							
Port Monitors Rc.common Modify Registry Re-opened Applications Redundant Access Redundant Access Registry Run Keys / Statiub Folder Scheduled Task Obfuscated Files or information			Plist Modification		Launchctl							
Rc.common Modify Registry Re-opened Applications Mshta Redundant Access Registry Run Keys / Staffun Folder Staffun Folder Scheduled Task Objuscated Files or information			Port Knocking		LC_MAIN Hijacking							
Re-opened Applications Redundant Access Registry, Run Keys / Startung Connection Removal Startung Folder Scheduled Task Scheduled Task Mshta Mshta Metwork Share Connection Removal Removal NTFS File Attributes Obfuscated Files or Information			Port Monitors	1	Masquerading							
Redundant Access Registry, Run Keys / Statutor Folder Scheduled Task Registry and Reys / Scheduled Task Registry and Reys / Scheduled Task Removal Rem			Rc.common	1	Modify Registry							
Redundant Access Registry, Run Keys / Startun Folder Scheduled Task Optuscated Files or Information			Re-opened Applications	1	, , ,							
Registry Run Keys / Statuto-Folder Scheduled Task Opfuscated Files or Information				1		,						
Scheduled Task Obfuscated Files or Information				1								
			Charles Folder	1								
			Screensaver	1	Information Plist Modification							

Service Registry

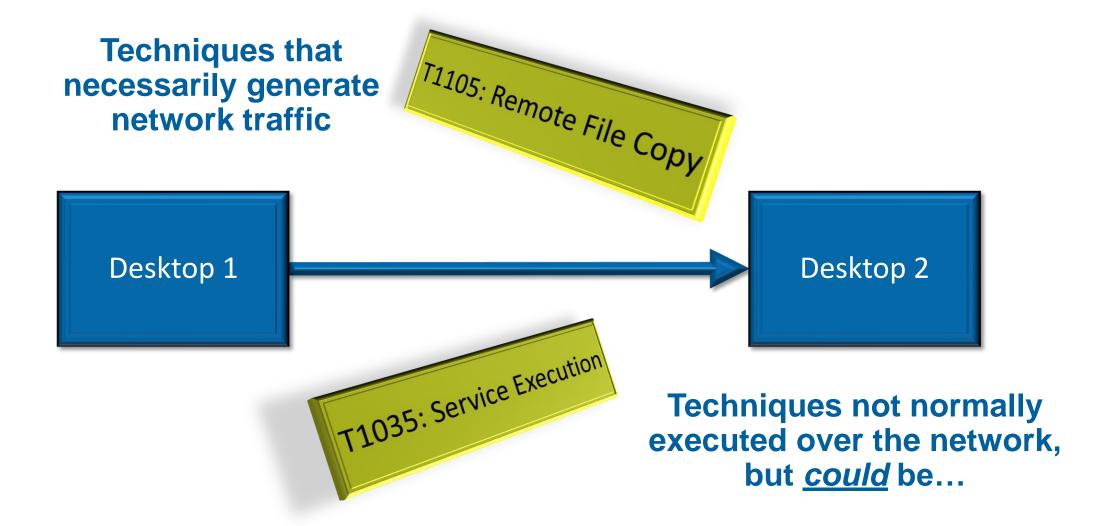
Security Support Provider

Port Knocking

Process Hollowing

Process Doppelgänging

ATT&CK and Internal Network Monitoring





Bro / Zeek Protocol Analyzers

- SMB Protocol Analyzer³
 - Message Types145

How Many Exist in Windows?

- DCE-RPC Protocol Analyzer³
 - Interface Definitions 81
 - Method Definitions 1,471

How Many Exist in Windows?

- Authentication Protocol Analyzers
 - Used in SMB and RPC Authentication

File Extraction Analyzer

- Extract Files from Network Traffic
- Lateral Movement

Bonus!

Bonus!

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



Protocol Specifications (1 of 2)

SMB Specifications

- Microsoft Developer Network (MSDN) Documentation⁴
 - 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

us/library/jj/12081.uspx

Protocol Specifications (2 of 2)

RPC Specifications

- The Open Group, Technical Standard C706⁵
 - Distributed Computing Environment (DCE) 1.1: Remote Procedure Call (RPC) [1997]
 - Nineteen (19) Basic Message Types
- MSDN Documentation⁶
 - Eighty (80) Protocol Documents Contained RPC Interface Definitions
 - Some Documents Defined More Than One RPC Interface
- Other Documentation
 - J.B. Marchand, Windows Network Services Internals⁷
- Total RPC Interfaces: <u>379</u>

Methods: <u>2,572+</u>

http://pubs.opengroup.org/onlinepubs/9629399/toc.pdf
 https://msdn.microsoft.com/en-us/library/jj712081.aspx
 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 <u>145</u> as Indicators of <u>Potential</u> ATT&CK Techniques

RPC Protocol Summary

- Reviewed 165 (out of 379) Interfaces
- Mapped <u>1,480</u> (out of 2,572) Methods to <u>Potential</u> ATT&CK Techniques

BZAR

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



Impact

Data Destruction

Data Encrypted for Impact

Defacement

Disk Content Wipe

Disk Structure Wipe

Endpoint Denial of Service

Firmware Corruption

Inhibit System Recovery

Network Denial of Service Resource Hijacking Runtime Data Manipulation Service Stop Stored Data Manipulation Transmitted Data Manipulation

ΔΤΤ&CK Techniques Detected with BZAR – Heatmap

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	
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	
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	Г
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	\perp
plication 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	
Spearphishing Attachment	Control Panel Items	Applnit 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	
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	, E
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	
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	+-
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	
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		<u> </u>
	InstallUtil	Change Default File Association	File System Permissions Weakness	Control Panel Items	Input Prompt	Process Discovery	Replication Through Removable Media		Multi-hop Proxy		R
	Launchetl	Component Firmware	Hooking	DCShadow	Kerberoasting	Query Registry	Shared Webroot	Screen Capture	Multilayer Encryption		-
	Local Job Scheduling	Component Object Model Hijacking	Image File Execution Options Injection	· · · · · · · · · · · · · · · · · · ·		Remote System Discovery	SSH Hijacking	Video Capture	Multi-Stage Channels		
	LSASS Driver	Create Account	Launch Daemon	Disabling Security Tools	LLMNR/NBT-NS Poisoning	Security Software Discovery	Taint Shared Content	-	Port Knocking		Tra
	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 External Remote Services	Path Interception	DLL Side-Loading	Password Filter DLL	System Network Configuration Discover	y Windows Admin Shares		Remote File Copy		
	Regsvcs/Regasm	File System Permissions Weakness	Plist Modification	Exploitation for Defense Evasion Extra Window Memory Injection	Private Keys Securityd Memory	System Network Connections Discovery	/ Windows Remote Management		Standard Application Layer Protocol		
	Regsvr32 Rundll32	Hidden Files and Directories	Port Monitors Process Injection	File Deletion	Two-Factor Authentication Interception	System Owner/User Discovery System Service Discovery			Standard Cryptographic Protocol Standard Non-Application Layer Protocol		
	Scheduled Task	Hooking Hooking	Scheduled Task	File Permissions Modification	Two-ractor Authentication interception	System Time Discovery			Uncommonly Used Port		
	Scripting	Hypervisor	Service Registry Permissions Weakness	File System Logical Offsets	-	system time discovery			Web Service		
	Service Execution	Image File Execution Options Injection	Setuid and Setgid	Gatekeeper Bypass	-				Web service	I	
	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	Launchetl	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							
	L	Re-opened Applications		Port Knocking							
		Scheduled Task		Process Doppelgänging	_						
	-	Screensaver	_	Process Hollowing							
	-	Security Support Provider	_	Process Injection							
	-	Service Registry Permissions Weakness	<u> </u>	Redundant Access	4						
	-	Setuid and Setgid	<u> </u>	Regsvcs/Regasm	\dashv						
	-	Shortcut Modification	-	Regsvr32	\dashv						
	-	SIP and Trust Provider Hijacking	-	Rootkit	4						
	-	Startup Items	-	Rundll32	\dashv						
	-	System Firmware	-	Scripting	-						
	-	Time Providers	-	Signed Binary Proxy Execution	\dashv						
	-	Trap	- 	Signed Script Proxy Execution	-						
	-	Valid Accounts	-	SIP and Trust Provider Hijacking	-						
		Web Shell		Software Packing						Legend	

Space after Filename

Template Injection Timestomp Trusted Developer Utilities Valid Accounts Web Service XSL Script Processing

egend

White = No Confidence of Detection

Orange = Some Confidence of Detection



Windows Management Instrumentation Event Subscription

Winlogon Helper DLL

ATT&CK Techniques Detected with BZAR

Execution Persist T1035 Service Execution Helper DLL T1047 Windows Mgmt T1013 Port Instrumentation (WMI) Monitors T1053 Scheduled Task

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...

T1087 Account

T1124 System Time

T1135 Network Share

Lateral Movement

T1077 Windows Admin Shares

T1105 Remote File Copy

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

<u>Execution</u>	<u>Persistence</u>	<u>Defe</u> <u>Eva</u>	A port monitor can be set through the API call to set a DLL to be loaded at	<u>vement</u>
T1035 Service Execution	T1004 Winlogon Helper DLL	T10	startup loaded by the <i>print spooler</i>	/s Admin
T1047 Windows Mgmt Instrumentation (WMI)	T1013 Port Monitors		service	File Copy
T1053 Scheduled Task			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 T1135 Network Share	



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

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

Persistence

T1013 Port Monitors

BZAR Example – T1070 Indicator Removal on Host

<u>Execution</u>	<u>Persistence</u>	<u>Defense</u> <u>Evasion</u>	
T1035 Service Execution	T1004 Winlogon Helper DLL	T1070 Indicator Removal Host	
T1047 Windows Mgmt Instrumentation (WMI)	T1013 Port Monitors		
T1053 Scheduled Task			

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

T1135 Network Share



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 :: SamrShutdownSamServer⁸

⁸ MSDN Library states not used on the wire



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

May no Important: MUST be tuned for your environment!



BZAR Example – Lateral Movement

Execution

T1035 Service Execution

T1047 Windows Mgmt Instrumentation (WMI)

T1053 Scheduled Task

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

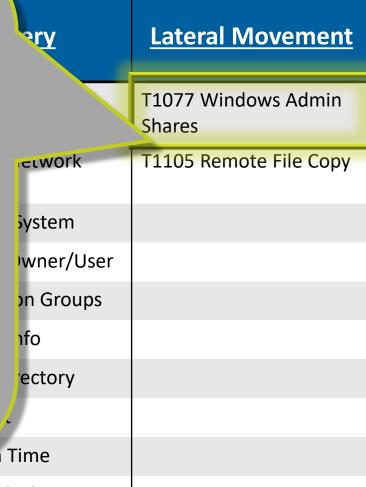
Adversaries may use this technique... to remotely access a networked system over server message block (SMB) to... transfer files, and run transferred binaries through remote Execution...

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

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

em Time,

T1135 Network Share





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!



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

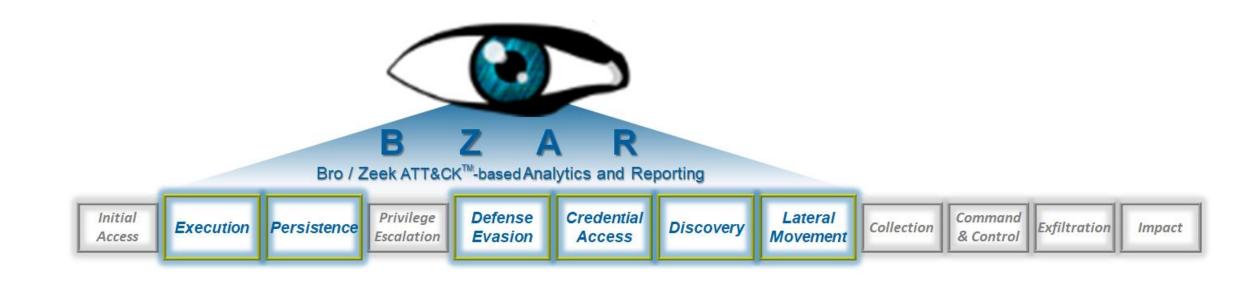


Future Work

- 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'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.









