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

Detecting Adversary Behaviors via Internal Network Monitoring

M.I. Fernandez

19 May 2020

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD™

APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED. CASE NUMBER 19-03281-5.

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

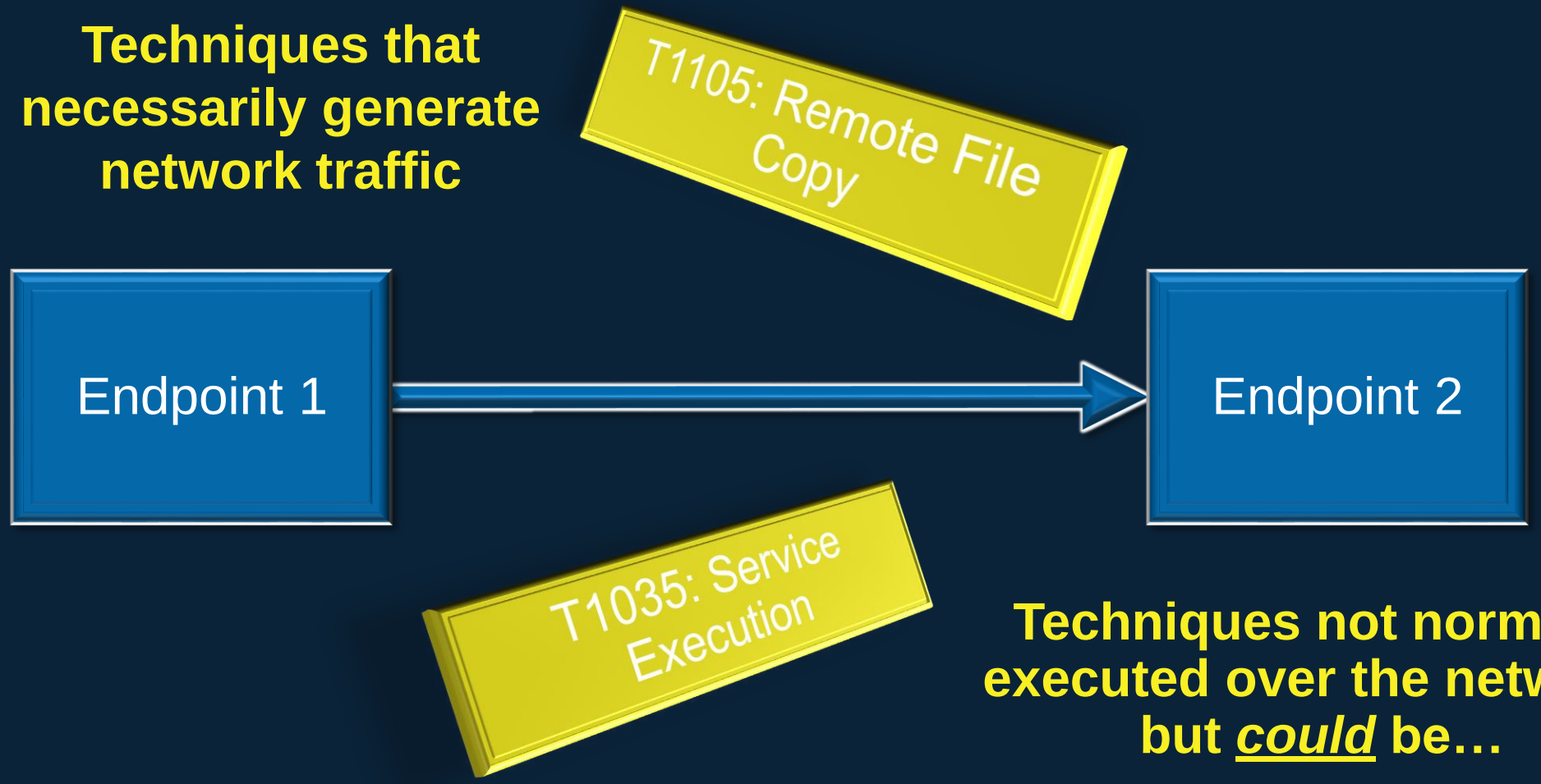
Bizarre: very strange or unusual

BZAR: open-source Bro/Zeek scripts

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

ATT&CK and Internal Network Monitoring

Techniques that necessarily generate network traffic



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

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							
		Re.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

ATT&CK Techniques Detected with BZAR

Execution	Persistence	Defense Evasion	Credential Access	Discovery	Lateral Movement
T1035 Service Execution	T1004 Winlogon Helper DLL	T1070 Indicator Removal Host	T1003 Credential Dumping	T1016 System Network Configuration	T1077 Windows Admin Shares
T1047 Windows Mgmt Instrumentation (WMI)	T1013 Port Monitors			T1049 System Network Connections	T1105 Remote File Copy
T1053 Scheduled Task				T1018 Remote System	
				T1033 System Owner/User	
				T1069 Permission Groups	
				T1082 System Info	
				T1083 File & Directory	
				T1087 Account	
				T1124 System Time	
				T1135 Network Share	

ATT&CK Techniques Detected with BZAR

Execution	Persistence	Defense Evasion	Credential Access	Discovery	Lateral Movement
T1035 Service Execution	T1004 Winlogon Helper DLL	T1070 Indicator Removal Host	T1003 Credential Dumping	T1016 System Network Configuration	T1077 Windows Admin Shares
T1047 Windows Mgmt Instrumentation (WMI)	T1013 Port Monitors			T1049 System Network Connections	T1105 Remote File Copy
T1053 Scheduled Task				T1018 Remote System	
				T1033 System Owner/User	
				T1069 Permission Groups	
				T1082 System Info	
				T1083 File & Directory	
				T1135 Network Share	

Important: MUST be tuned for your environment!

BZAR Tuning

- **Whitelist**
  - IP Address, IP Subnet, and/or *Host Name*
  - per ATT&CK Technique
- **Toggle Switch: Disable Detection and Disable Reporting**
  - Disable Detection (and thereby Reporting, too)
  - *Enable Detection, but Disable Reporting*
  - per ATT&CK Technique

Analytics and Reporting with BZAR *(1 of 2)*

- **“ATTACK::Execution”**
  - Detect *Any* of the 10 RPC Indicators
- **“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 same *Originating* IP address

Analytics and Reporting with BZAR *(2 of 2)*

- **“ATTACK::Lateral_Movement”**
  - Detect SMB File Write to Windows Admin *File* Share (e.g., ADMIN$ or C$)
- **“ATTACK::Lateral_Movement_Multiple_Attempts”**
  - Specified Number of *Occurrences* Specified *Timeframe* from Same *Originating* IP Address
- **“ATTACK::Lateral_Movement_And_Execution”**
  - Detect One Occurrence of *Each* Specified *Timeframe* to Same *Target* IP Address
- **“ATTACK::Lateral_Movement_Extracted_File”**
  - Make a Copy of File Written to Windows Admin *File* Share

Possible Future Work

- **New Detections**
  - T1080 Taint Shared Content
  - T1129 Execution through Module Load
  - T1023 Shortcut Modifications
  - T1137 Office Application Startup
  - T1027 Obfuscate Files or Information
  - T1158 Hidden Files and Directories
  - T1096 NTFS File Attributes
  - T1107 File Deletion
- **BZAR and ATT&CK Sub-Techniques**
- **Network Protocols and ATT&CK**

Questions?

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

M.I. Fernandez

mfernandez@mitre.org

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD™