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
  - 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

© 2019 The MITRE Corporation. All rights reserved. Approved for public release. Distribution unlimited. Case number 19-0379.
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
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](https://attack.mitre.org)
ATT&CK and Internal Network Monitoring

Techniques that necessarily generate network traffic

T1105: Remote File Copy

Desktop 1

Desktop 2

T1035: Service Execution

Techniques not normally executed over the network, but could be…
Bro / Zeek Protocol Analyzers

- **SMB Protocol Analyzer**
  - Message Types 145

- **DCE-RPC Protocol Analyzer**
  - 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

© 2019 The MITRE Corporation. All rights reserved. Approved for public release. Distribution unlimited. Case number 19-0379.

3 circa March 2018 (Bro v2.5.2 - v2.5.3)
Protocol Specifications (1 of 2)

- SMB Specifications
  - Microsoft Developer Network (MSDN) Documentation
    - 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:
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+**

\(^7\) [Index-of.es/Windows/win_net_srv.pdf](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

<table>
<thead>
<tr>
<th>Initial Access</th>
<th>Execution</th>
<th>Persistence</th>
<th>Privilege Escalation</th>
<th>Defense Evasion</th>
<th>Credential Access</th>
<th>Discovery</th>
<th>Lateral Movement</th>
<th>Collection</th>
<th>Command And Control</th>
<th>Exfiltration</th>
<th>Impact</th>
</tr>
</thead>
</table>

### Legend
- **White** = No Confidence of Detection
- **Orange** = Some Confidence of Detection

© 2019 The MITRE Corporation. All rights reserved. Approved for public release. Distribution unlimited. Case number 19-0379.
### ATT&CK Techniques Detected with BZAR

<table>
<thead>
<tr>
<th>Execution</th>
<th>Persistence</th>
<th>Lateral Movement</th>
</tr>
</thead>
<tbody>
<tr>
<td>T1035 Service Execution</td>
<td>Helper DLL</td>
<td>T1077 Windows Admin Shares</td>
</tr>
<tr>
<td>T1047 Windows Mgmt Instrumentation (WMI)</td>
<td>T1013 Port Monitors</td>
<td>T1077 Windows Admin Shares</td>
</tr>
<tr>
<td>T1053 Scheduled Task</td>
<td></td>
<td>T1105 Remote File Copy</td>
</tr>
<tr>
<td></td>
<td>Helper DLL</td>
<td>T1077 Windows Admin Shares</td>
</tr>
</tbody>
</table>

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

- **Indicators:** (*Four (4) RPC Functions*)
  - `svcclr :: CreateServiceA`
  - `svcclr :: CreateServiceW`
  - `svcclr :: StartServiceA`
  - `svcclr :: StartServiceW`

- **Analytics:** *Simple*
  - Detect *any* of the 4 RPC functions
  - Zeek event handlers
    - `dce_rpc_request()`
    - `dce_rpc_response()`
BZAR Example – 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

<table>
<thead>
<tr>
<th>Execution</th>
<th>Persistence</th>
<th>Defeat/Evasion</th>
<th>Lateral Movement</th>
</tr>
</thead>
<tbody>
<tr>
<td>T1035 Service Execution</td>
<td>T1004 Winlogon Helper DLL</td>
<td>T1006 Credential Dumping</td>
<td></td>
</tr>
<tr>
<td>T1047 Windows Mgmt Instrumentation (WMI)</td>
<td>T1013 Port Monitors</td>
<td>T1049 System Network Connections</td>
<td></td>
</tr>
<tr>
<td>T1053 Scheduled Task</td>
<td></td>
<td>T1105 Remote File Copy</td>
<td></td>
</tr>
</tbody>
</table>

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

© 2019 The MITRE Corporation. All rights reserved. Approved for public release. Distribution unlimited. Case number 18-03730-16.
**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...*
### BZAR Example – T1070 Indicator Removal on Host

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

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*
BZAR Example – 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

---

© 2019 The MITRE Corporation. All rights reserved. Approved for public release. Distribution unlimited. Case number 19-0379.

8 MSDN Library states not used on the wire
BZAR Example – 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 never see this in your environment, but if you DO…*

---

© 2019 The MITRE Corporation. All rights reserved. Approved for public release. Distribution unlimited. Case number 19-0379.
### BZAR Example – Lateral Movement

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*...

---

<table>
<thead>
<tr>
<th>Execution</th>
<th>Discovery</th>
<th>Persistence</th>
<th>Evasion</th>
<th>Credential Access</th>
<th>Lateral Movement</th>
</tr>
</thead>
<tbody>
<tr>
<td>T1035 Service Execution</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>T1077 Windows Admin Shares</td>
</tr>
<tr>
<td>T1047 Windows Mgmt Instrumentation (WMI)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>T1105 Remote File Copy</td>
</tr>
<tr>
<td>T1053 Scheduled Task</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>T1124 System Time</td>
</tr>
<tr>
<td>T1033 System Owner/User</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>T135 Network Share</td>
</tr>
<tr>
<td>T1082 System Info</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T1083 File &amp; Directory</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T1069 Permission Groups</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T1135 Network Share</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T1087 Account</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T1016 System Network Configuration</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T1070 Indicator Removal Host</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T1049 System Network Connections</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T1018 Remote System</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T1105 Remote File Copy</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T1047 Windows Mgmt Instrumentation (WMI)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T1035 Service Execution</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T1053 Scheduled Task</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

*Important: MUST be tuned for your environment!*

<table>
<thead>
<tr>
<th>Lateral Movement</th>
</tr>
</thead>
<tbody>
<tr>
<td>T1077 Windows Admin Shares</td>
</tr>
<tr>
<td>T1105 Remote File Copy</td>
</tr>
</tbody>
</table>
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. $T = 5\text{min}$
  - 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 \( \geq 1001 \)
    - Min Val = 1, Max Val = 1000
  - T-timeframe, e.g. \( T = 5\text{min} \)
  - 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](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
“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’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.