README | BSD-3-Clause license

BZAR (Bro/Zeek ATT&CK-based Analytics and Reporting)

1. Introduction

- **Zeek** 99.8%
- **Standard ML** 0.2%

The BZAR project uses the Bro/Zeek Network Security Monitor to detect ATT&CK-based adversarial activity.

MITRE ATT&CK is a publicly-available, curated knowledge base for cyber adversary behavior, reflecting the various phases of the adversary lifecycle and the platforms they are known to target. The ATT&CK model includes behaviors of numerous threats groups.

BZAR is a set of Bro/Zeek scripts utilizing the SMB and DCE-RPC protocol analyzers and the File Extraction Framework to detect ATT&CK-like activity, raise notices, and write to the Notice Log.

BZAR and CAR

BZAR is a component of the Cyber Analytics Repository. It was originally located within that library, but due to requirements for Zeek packages it was moved to its own repository. It's still managed as a component of CAR.

2. Tuning BZAR for Your Environment

BZAR must be tuned for your specific operational envrionment. For example, some of the ATT&CK-like activity that BZAR detects may be authorized and legitimate activity in your environment. Therefore, these detections would produce lots of unnecessary entries in the Notice Log. This can be tuned by the use of BZAR whitelists and by toggling on/off detection and/or reporting. See the CHANGES document for more information.

3. Complex Analytics for Detecting ATT&CK-like Activity

The BZAR analytics use the Bro/Zeek Summary Statistics (SumStats) Framework to combine two or more simple indicators in SMB and DCE-RPC traffic to detect ATT&CK-like

activity with a greater degree of confidence. Three (3) BZAR analytics are described below.

3.1. SumStats Analytics for ATT&CK Lateral Movement and Execution

Use SumStats to raise a Bro/Zeek Notice event if an SMB Lateral Movement indicator (e.g., SMB File Write to a Windows Admin File Share: ADMIN$ or C$ only) is observed together with a DCE-RPC Execution indicator against the same (targeted) host, within a specified period of time.

Relevant ATT&CK Techniques

- T1021.002 Remote Services: SMB/Windows Admin Shares (file shares only, not named pipes), and
- T1570 Lateral Tool Transfer, and
- One of the following:
  - T1569.002 System Services: Service Execution
  - T1047 Windows Management Instrumentation
  - T1053.002 Scheduled Task/Job: At (Windows)
  - T1053.005 Scheduled Task/Job: Scheduled Task

Relevant Indicators Detected by Bro/Zeek

- `smb1_write_andx_response::c$smb_state$path` contains `ADMIN$` or `C$`
- `smb2_write_request::c$smb_state$path**` contains `ADMIN$` or `C$`
- `dce_rpc_response::c$dce_rpc$endpoint + c$dce_rpc$operation` contains any of the following:
  - `svcctl::CreateServiceW`
  - `svcctl::CreateServiceA`
  - `svcctl::StartServiceW`
  - `svcctl::StartServiceA`
  - `IWbemServices::ExecMethod`
  - `IWbemServices::ExecMethodAsync`

- `atsvc::JobAdd`
- `ITaskSchedulerService::SchRpcRegisterTask`
- `ITaskSchedulerService::SchRpcRun`
- `ITaskSchedulerService::SchRpcEnableTask`

NOTE: Preference would be to detect smb2_write_response event (instead of smb2_write_request), because it would confirm the file was actually written to the remote destination. Unfortunately, Bro/Zeek does not have an event for that SMB message-type yet.

3.2. SumStats Analytics for ATT&CK Lateral Movement (Multiple Attempts)

Use SumStats to raise a Bro/Zeek Notice event if multiple SMB Lateral Movement indicators (e.g., multiple attempts to connect to a Windows Admin File Share: ADMIN$ or C$ only) are observed originating from the same host, regardless of write-attempts and regardless of whether or not any connection is successful --just connection attempts-- within a specified period of time.

Relevant ATT&CK Techniques

- T1021.002 Remote Services: SMB/Windows Admin Shares (file shares only, not named pipes)

Indicators detected by Bro/Zeek

- `smb1_tree_connect_andx_request::c$smb_state$path` contains `ADMIN$` or `C$`
- `smb2_tree_connect_request::c$smb_state$path` contains `ADMIN$` or `C$`

3.3. SumStats Analytics for ATT&CK Discovery

Use SumStats to raise a Bro/Zeek Notice event if multiple instances of DCE-RPC Discovery indicators are observed

originating from the same host, within a specified period of time.

Relevant ATT&CK Techniques

- T1016 System Network Configuration Discovery
- T1018 Remote System Discovery
- T1033 System Owner/User Discovery
- T1069 Permission Groups Discovery
- T1082 System Information Discovery
- T1083 File & Directory Discovery
- T1087 Account Discovery
- T1124 System Time Discovery
- T1135 Network Share Discovery

Relevant Indicator(s) Detected by Bro/Zeek

- `dce_rpc_response::c$dce_rpc$endpoint + c$dce_rpc$operation` contains any of the following:
  - `lsarpc::LsarEnumerateAccounts`
  - `lsarpc::LsarEnumerateAccountRights`
  - `lsarpc::LsarEnumerateAccountsWithUserRight`
  - `lsarpc::LsarEnumeratePrivileges`
  - `lsarpc::LsarEnumeratePrivilegesAccount`
  - `lsarpc::LsarEnumerateTrustedDomainsEx`
  - `lsarpc::LsarGetSystemAccessAccount`
  - `lsarpc::LsarGetUserName`
  - `lsarpc::LsarLookupNames`
  - `lsarpc::LsarLookupNames2`
  - `lsarpc::LsarLookupNames3`
  - `lsarpc::LsarLookupNames4`
  - `lsarpc::LsarLookupPrivilegeDisplayName`
  - `lsarpc::LsarLookupPrivilegeName`
  - `lsarpc::LsarLookupPrivilegeValue`
  - `lsarpc::LsarLookupSids`

- `lsarpc::LsarLookupSids2`
- `lsarpc::LsarLookupSids3`
- `lsarpc::LsarQueryDomainInformationPolicy`
- `lsarpc::LsarQueryInfoTrustedDomain`
- `lsarpc::LsarQueryInformationPolicy`
- `lsarpc::LsarQueryInformationPolicy2`
- `lsarpc::LsarQueryTrustedDomainInfo`
- `lsarpc::LsarQueryTrustedDomainInfoByName`
- `samr::SamrLookupNamesInDomain`
- `samr::SamrLookupIdsInDomain`
- `samr::SamrLookupDomainInSamServer`
- `samr::SamrGetGroupsForUser`
- `samr::SamrGetAliasMembership`
- `samr::SamrGetMembersInAlias`
- `samr::SamrGetMembersInGroup`
- `samr::SamrGetUserDomainPasswordInformation`
- `samr::SamrEnumerateAliasesInDomain`
- `samr::SamrEnumerateUsersInDomain`
- `samr::SamrEnumerateGroupsInDomain`
- `samr::SamrEnumerateDomainsInSamServer`
- `samr::SamrQueryInformationAlias`
- `samr::SamrQueryInformationDomain`
- `samr::SamrQueryInformationDomain2`
- `samr::SamrQueryInformationGroup`
- `samr::SamrQueryInformationUser`
- `samr::SamrQueryInformationUser2`
- `samr::SamrQueryDisplayInformation`
- `samr::SamrQueryDisplayInformation2`
- `samr::SamrQueryDisplayInformation3`
- `srvsvc::NetrConnectionEnum`
- `srvsvc::NetrFileEnum`
- `srvsvc::NetrRemoteTOD`

- `srvsvc::NetrServerAliasEnum`
- `srvsvc::NetrServerGetInfo`
- `srvsvc::NetrServerTransportEnum`
- `srvsvc::NetrSessionEnum`
- `srvsvc::NetrShareEnum`
- `srvsvc::NetrShareGetInfo`
- `wkssvc::NetrWkstaGetInfo`
- `wkssvc::NetrWkstaTransportEnum`
- `wkssvc::NetrWkstaUserEnum`

4. Simple Indicators for Detecting ATT&CK-like Activity

In addition to the analytics described above, BZAR uses simple indicators within SMB and DCE-RPC traffic to detect ATT&CK-like activity, although with a lesser degree of confidence than detection via the SumStats analytics. The BZAR indicators are grouped into six (6) categories, as described below.

4.1. Indicators for ATT&CK Lateral Movement

Raise a Bro/Zeek Notice event if a single instance of an SMB Lateral Movement indicator (e.g., SMB File Write to a Windows Admin File Share: ADMIN$ or C$ only) is observed, which indicates ATT&CK-like activity.

Relevant ATT&CK Techniques

- T1021.002 Remote Services: SMB/Windows Admin Shares (file shares only, not named pipes)
- T1570 Lateral Tool Transfer

Relevant Indicator(s) Detected by Bro/Zeek

- `smb1_write_andx_response::c$smb_state$path` contains `ADMIN$` or `C$`

- `smb2_write_request::c$smb_state$path**` contains `ADMIN$` or `C$`

NOTE: Preference would be to detect smb2_write_response event (instead of smb2_write_request), because it would confirm the file was actually written to the remote destination. Unfortunately, Bro/Zeek does not have an event for that SMB message-type yet.

4.2. Indicators for File Extraction Framework

Launch the Bro/Zeek File Extraction Framework to save a copy of the file associated with ATT&CK-like Lateral Movement onto a remote system. Raise a Bro Notice event for the Lateral Movement Extracted File.

Relevant ATT&CK Techniques

- T1021.002 Remote Services: SMB/Windows Admin Shares (file shares only, not named pipes)
- T1570 Lateral Tool Transfer

Relevant Indicator(s) Detected by Bro/Zeek

- `smb1_write_andx_response::c$smb_state$path` contains `ADMIN$` or `C$`
- `smb2_write_request::c$smb_state$path**` contains `ADMIN$` or `C$`

NOTE: Preference would be to detect smb2_write_response event (instead of smb2_write_request), because it would confirm the file was actually written to the remote destination. Unfortunately, Bro/Zeek does not have an event for that SMB message-type yet.

4.3. Indicators for ATT&CK Credential Access

Raise a Bro/Zeek Notice event if a single instance of any of the following Windows DCE-RPC functions (endpoint::operation) is

observed, which indicates ATT&CK-like Credential Access techniques on the remote system.

Relevant ATT&CK Technique(s)

- T1003.006 OS Credential Dumping: DCSync

Relevant Indicator(s) Detected by Bro/Zeek

- `dce_rpc_response::c$dce_rpc$endpoint + c$dce_rpc$operation` contains any of the following:
  - `drsuapi::DRSReplicaSync`
  - `drsuapi::DRSGetNCChanges`

4.4. Indicators for ATT&CK Defense Evasion

Raise a Bro/Zeek Notice event if a single instance of any of the following
Windows DCE-RPC functions (endpoint::operation) is observed, which indicates ATT&CK-like Defense Evasion techniques on the remote system.

Relevant ATT&CK Techniques

- T1070.001 Indicator Removal on Host: Clear Windows Event Logs

Relevant Indicator(s) Detected by Bro/Zeek

- `dce_rpc_response::c$dce_rpc$endpoint + c$dce_rpc$operation` contains any of the following:
  - `eventlog::ElfrClearELFW`
  - `eventlog::ElfrClearELFA`
  - `IEventService::EvtRpcClearLog`

4.5. Indicators for ATT&CK Execution

Raise a Bro/Zeek Notice event if a single instance of any of the following Windows DCE-RPC functions (endpoint::operation) is

observed, which indicates ATT&CK-like Execution techniques on the remote system.

Relevant ATT&CK Technique(s)

- T1569.002 System Services: Service Execution
- T1047 Windows Management Instrumentation
- T1053.002 Scheduled Task/Job: At (Windows)
- T1053.005 Scheduled Task/Job: Scheduled Task

Relevant Indicator(s) Detected by Bro/Zeek

- `dce_rpc_response::c$dce_rpc$endpoint + c$dce_rpc$operation` contains any of the following:
  - `svcctl::CreateServiceW`
  - `svcctl::CreateServiceA`
  - `svcctl::StartServiceW`
  - `svcctl::StartServiceA`
  - `IWbemServices::ExecMethod`
  - `IWbemServices::ExecMethodAsync`
  - `atsvc::JobAdd`
  - `ITaskSchedulerService::SchRpcRegisterTask`
  - `ITaskSchedulerService::SchRpcRun`
  - `ITaskSchedulerService::SchRpcEnableTask`

4.6. Indicators for ATT&CK Persistence

Raise a Bro/Zeek Notice event if a single instance of any of the following Windows DCE-RPC functions (endpoint::operation) is observed, which indicates ATT&CK-like Persistence techniques on the remote system.

Relevant ATT&CK Technique(s):

- T1547.004 Boot or Logon Autostart Execution: Winlogon Helper DLL

- T1547.010 Boot or Logon Autostart Execution: Port Monitors

Relevant Indicator(s) Detected by Bro/Zeek

- `dce_rpc_response::c$dce_rpc$endpoint + c$dce_rpc$operation` contains any of the following:
  - `ISecLogon::SeclCreateProcessWithLogonW`
  - `ISecLogon::SeclCreateProcessWithLogonExW`
  - `IRemoteWinspool::RpcAsyncAddMonitor`
  - `IRemoteWinspool::RpcAsyncAddPrintProcessor`
  - `spoolss::RpcAddMonitor` # a.k.a. winspool | spoolss
  - `spoolss::RpcAddPrintProcessor` # a.k.a. winspool | spoolss

4.7. Indicators for ATT&CK Impact

Raise a Bro/Zeek Notice event if a single instance of any of the following
Windows DCE-RPC functions (endpoint::operation) is observed, which indicates ATT&CK-like Impact techniques on the remote system.

Relevant ATT&CK Techniques

- T1529 System Shutdown/Reboot

Relevant Indicator(s) Detected by Bro/Zeek

- `dce_rpc_response::c$dce_rpc$endpoint + c$dce_rpc$operation` contains any of the following:
  - `InitShutdown::BaseInitiateShutdown`
  - `InitShutdown::BaseInitiateShutdownEx`
  - `WindowsShutdown::WsdrInitiateShutdown`
  - `winreg::BaseInitiateSystemShutdown`
  - `winreg::BaseInitiateSystemShutdownEx`
  - `winstation_rpc::RpcWinStationShutdownSystem`

- `samr::SamrShutdownSamServer` # MSDN says not used on the wire

5. Additional DCE-RPC Interfaces and Methods

The BZAR project adds 144 more Microsoft DCE-RPC Interface UUIDs (a.k.a. "endpoints") to the Bro/Zeek DCE_RPC::uuid_endpoint_map.

The BZAR project also adds 1,145 Microsoft DCE-RPC Interface Methods (a.k.a. "operations") to the Bro/Zeek DCE_RPC::operations.

See the Bro/Zeek script 'bzar_dce-rpc_consts' for more information.

Most of the DCE-RPC endpoints and operations defined in 'bzar_dce-rpc_consts' were merged into Zeek's main product line, version 3.2.0-dev.565 | 2020-05-26 21:55:54 +0000. Ref: https://github.com/zeek/zeek/blob/master/scripts/base/protocols/dce-rpc/consts.zeek#L92

6. References

1. Microsoft Developer Network (MSDN) Library. MSDN Library > Open Specifications > Protocols > Windows Protocols > Technical Documents. https://msdn.microsoft.com/en-us/library/jj712081.aspx
2. Marchand, "Windows Network Services Internals". 2006. http://index-of.es/Windows/win_net_srv.pdf

7. Contributing