

# ScadaBR event handle

To showcase the result, I set up an experiment.

When the state of red light changes twice (0 -> 1, 1 -> 0) in 10 seconds, activate emergency (send 1 to 803). When the conditional not met, deactivate emergency (send 0 to 803).

Click the orange box to show data point details.

The screenshot shows the ScadaBR 1.2 web application. At the top, there's a navigation bar with links like Home, Points, Reports, and Help. The main area has a green header bar with the title "ScadaBR" and a status message "Urgent". On the left, there's a sidebar titled "Points" with a tree view showing nodes like "OpenPLC\_Windows - GreenLight", "OpenPLC\_Windows - HMI\_EmergencyGreenPb", etc. On the right, there's a "Watch list" table with columns for "Point", "Value", and "Time". One row for "OpenPLC\_Windows - RedLight" has its "Edit" button highlighted with an orange box. Below the table is a date range selector from "From 2022 Oct 03 13:33:35" to "To 2022 Oct 04 13:33:35".

Click edit (orange box)

The screenshot shows the ScadaBR 1.2 web application on the "data\_point\_details.shtm?dpid=1" page. The left panel displays a data point named "RedLight" with its current value (0), time (13:33:42), and a "Set" input field containing "0". It also shows statistics: Starts (226), Runtime (97%), and Log entries (452). The right panel shows a "History" table with 10 recent records. Below these are "User notes" and a "Chart" section showing a red waveform over a timeline from October 3rd to 4th, 2022.

Configure event detector on the right hand side.

The screenshot shows the 'data\_point\_edit.shtm?dpid=1' page in a browser window titled 'ScadaBR 1.2'. The main area is divided into several sections:

- Point properties:** Data source is 'OpenPLC\_Windows', Point name is 'RedLight'.
- Logging properties:** Logging type is 'When point value changes', Purge after 1 year(s), Default cache size is 1.
- Purge now:** Purge data older than 1 year(s), Purge all data (checkbox), Purge now button.
- Text renderer properties:** Type is 'Plain', Suffix is empty.
- Chart renderer properties:** Type is 'None'.
- Event detectors:** Type is 'Change'.
  - Type: State change counter
  - Export ID (XID): PED\_177817
  - Alias: (empty)
  - Alarm level: None
  - State change count: 2
  - Duration: 10 second(s)

At the bottom, there are 'Save', 'Disable', 'Restart', and 'Cancel' buttons. A note says: 'Note: saving, disabling, or restarting a point causes all active events to be returned to normal.' The footer includes a copyright notice: '©2009-present Fundação Certi, MCA Sistemas, Unis Sistemas, Conitec. All rights reserved.'

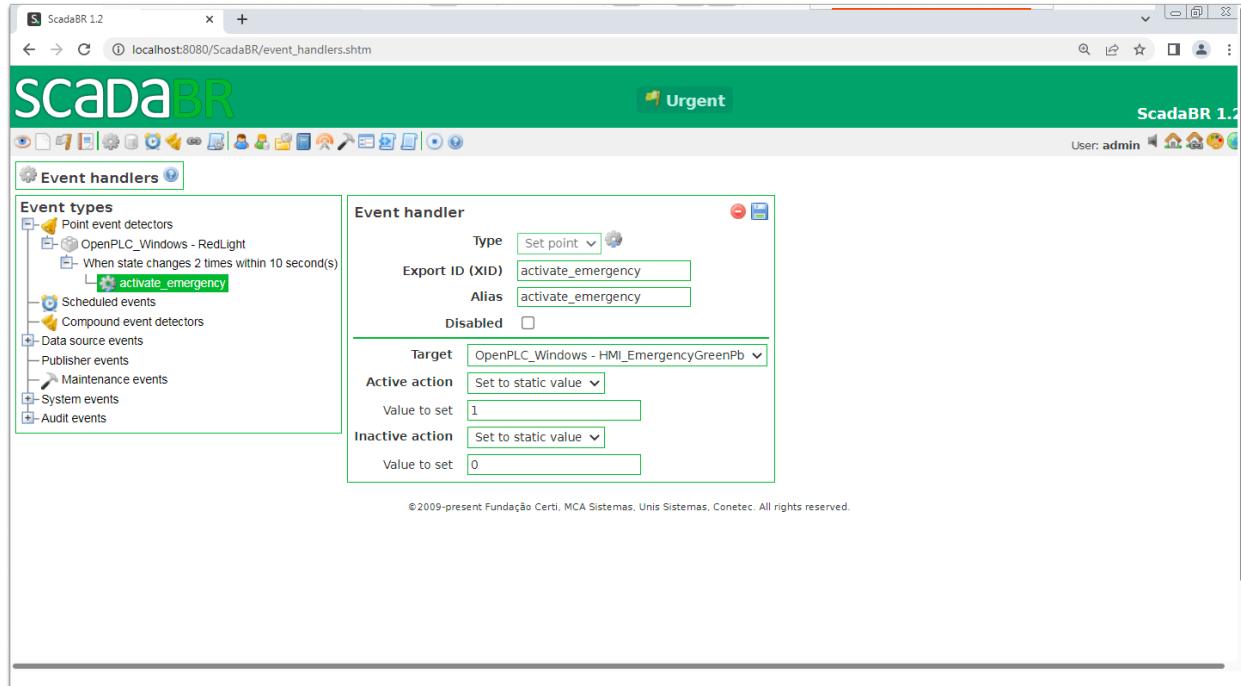
We can see alarm notification from the event on the watch list.

The screenshot shows the 'watch\_list.shtm' page in a browser window titled 'ScadaBR 1.2'. The left sidebar lists 'Points' with entries for 'OpenPLC\_Windows - GreenLight', 'OpenPLC\_Windows - HMI\_EmergencyGreenPb', 'OpenPLC\_Windows - OrangeLight', 'OpenPLC\_Windows - Pb\_Pedestrians', and 'OpenPLC\_Windows - RedLight'. The main area is titled 'Watch list' and shows the following log entries:

Event	Time	Details
OpenPLC_Windows - GreenLight	13:34:42	1
OpenPLC_Windows - OrangeLight	13:34:42	0
OpenPLC_Windows - RedLight	13:34:42	0
13:34:38 - Redlight has changed from "4" to "30 second(s)"	13:34:42	✓
OpenPLC_Windows - HMI_EmergencyGreenPb	13:34:42	0
OpenPLC_Windows - Pb_Pedestrians	13:34:42	0

At the bottom, there is a 'Chart' section and a time selection bar: 'From 2022 Oct 03 : 13 : 34 : 34' and 'Inception'.

Set up event handler to react to corresponding event. In this case, set HMI\_EmergencyGreenPb to 1 when active, set to 0 when inactive.



The pcap file is in google drive (event\_detect\_and\_handle.pcapng). With Wireshark filter “ip.addr == 192.168.204.133 && tcp.port == 502”, we can see the time and corresponding lights below, and it aligns with what we expect.

```
5.87 sec red
11.90 sec not red
11.96 sec write 1
15.97 sec write 0
20.90 sec red
20.96 sec write 1
30.92 sec write 0
```

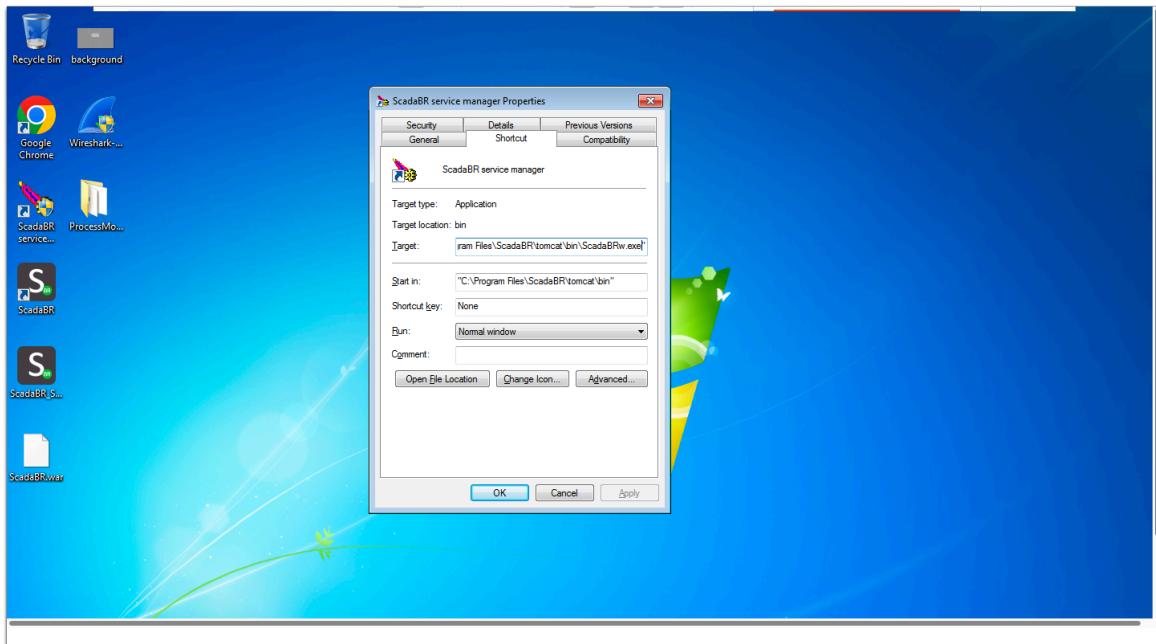
## Dynamic Analysis

I used Process Monitor to monitor processes. The version 3.84 works on Windows 7. (<https://web.archive.org/web/20210901132850/https://docs.microsoft.com/en-us/sysinternals/downloads/procmon>)

## Observation on starting ScadaBR

The log file is in google drive (StartScadaBRw.PML)

## ScadaBR service manager is the shortcut of ScadaBRw.exe



When we press “Start” in ScadaBRw, it creates a thread and call services.exe to start “ScadaBR.exe”, which runs the tomcat Web App.

The screenshot shows the Wireshark Process Tree window. The timeline covers the start of the 'services.exe (476)' process. This process then starts the 'ScadaBRw.exe' process (2880). Other processes listed in the timeline include 'svchost.exe (600)', 'wininit.exe (416)', 'vsmeter.exe (1576)', 'cryptui.dllhost.exe (2112)', 'cryptui.dllhost.exe (2260)', 'cryptui.dllhost.exe (2284)', 'cryptui.dllhost.exe (2304)', 'cryptui.dllhost.exe (2360)', and 'SearchIndexer.exe (2360)'. The window also displays details about the selected process, such as its description as 'Services and Controller app', company as Microsoft Corporation, path as 'C:\Windows\system32\services.exe', command as 'C:\Windows\system32\services.exe', user as 'NT AUTHORITY\SYSTEM', and PID as 476. The start time is listed as 10/5/2022 3:44:51 PM.

**Process Tree**

Only show processes still running at end of current trace

Timelines cover displayed events only

Process	Description	Image Path	Life Time	Company	Owner	Command	Start Time
sppsvc.exe (2884)	Microsoft Software... .NET Runtime Opt...	C:\Windows\system32\sppsvc.exe	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\system32\sppsvc.exe	10/5/2022 3:10:59 PM	
mscorsv.exe (2036)	.NET Runtime Opt...	C:\Windows\Microsoft.NET\Framework\v...	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorsv.exe	10/5/2022 3:10:59 PM	
taskhost.exe (2548)	Host Process for ...	C:\Windows\system32\taskhost.exe	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\system32\taskhost.exe	10/5/2022 3:10:59 PM	
SearchIndexer.exe (2360)	Microsoft Windows ...	C:\Windows\system32\SearchIndexer.exe	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\system32\SearchIndexer.exe /Embedding	10/5/2022 3:10:59 PM	
wmpnetwk.exe (3708)	Windows Media P...	C:\Program Files\Windows Media Player\...	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\wmpnetwk.exe	10/5/2022 3:10:59 PM	
svchost.exe (4000)	Host Process for ...	C:\Windows\System32\svchost.exe	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe -k LocalServicePeerNet	10/5/2022 3:10:59 PM	
svchost.exe (4824)	Host Process for ...	C:\Windows\System32\svchost.exe	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe -k seccavcs	10/5/2022 3:10:59 PM	
taskhost.exe (4260)	Host Process for ...	C:\Windows\System32\taskhost.exe	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\taskhost.exe	10/5/2022 4:00:00 AM	
svchost.exe (3660)	Host Process for ...	C:\Windows\System32\svchost.exe	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe /k WerSvGrp	10/5/2022 4:00:00 AM	
ScadaBR.exe (1036)	Apache Commons Daemon Service Runner	C:\Program Files\ScadaBR\tomcat\bin\ScadaBR.exe	Apache Software Foundation	NT AUTHORITY\SYSTEM	C:\Program Files\ScadaBR\tomcat\bin\ScadaBR.exe" /RS//ScadaBR	10/5/2022 4:00:00 AM	
lsass.exe (488)	Local Security Au...	C:\Windows\system32\lsass.exe	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\system32\lsass.exe	10/5/2022 3:10:59 PM	
lsm.exe (496)	Local Session Manager Service	C:\Windows\system32\lsm.exe	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\system32\lsm.exe	10/5/2022 3:10:59 PM	
csrss.exe (440)	Client Server Run...	C:\Windows\system32\cssrs.exe	Microsoft Corporation	NT AUTHORITY\SYSTEM	*SystemRoot*\system32\cssrs.exe ObjectDirectory=Windows SharedS...	10/5/2022 3:10:59 PM	
winlogon.exe (656)	Windows Logon A...	C:\Windows\system32\winlogon.exe	Microsoft Corporation	NT AUTHORITY\SYSTEM	winlogon.exe	10/5/2022 3:10:59 PM	
Explorer EXE (2792)	Windows Explorer	C:\Windows\Explorer.EXE	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\Explorer.EXE	10/5/2022 3:10:59 PM	
vmtold.exe (2975)	VMware Tools Con...	C:\Program Files\VMware\VMware Tools\...	VMware, Inc.	VMware, Inc.	lmgw-PC\lmgw1 "C:\Program Files\VMware\VMware Tools\vmtold.exe" -n vmar	10/5/2022 3:10:59 PM	
Procmon64.exe (1128)	Process Monitor	C:\Users\lmgw1\Desktop\ProcessMonit...	Sytematic Software	Sytematic Software	"C:\Users\lmgw1\Desktop\ProcessMonitor\Procmon64.exe"	10/5/2022 4:00:00 AM	
Procmon64.exe (4612)	Process Monitor	C:\Users\lmgw1\Desktop\ProcessMonit...	Sytematic Software	Sytematic Software	"C:\Users\lmgw1\Desktop\ProcessMonitor\Procmon64.exe"	10/5/2022 4:00:00 AM	
ScadaBR.exe (2624)	Apache Commons ...	C:\Program Files\ScadaBR\tomcat\bin\ScadaBR.exe	Apache Software Foundation	NT AUTHORITY\SYSTEM	C:\Program Files\ScadaBR\tomcat\bin\ScadaBR.exe	10/5/2022 4:00:00 AM	
Procmon64.exe (2052)	Process Monitor	C:\Users\lmgw1\Desktop\ProcessMonit...	Sytematic Software	Sytematic Software	"C:\Users\lmgw1\Desktop\ProcessMonitor\Procmon64.exe"	10/5/2022 4:00:00 AM	
GoogleCrashHandler.exe (1376)	Google Crash Han...	C:\Program Files\x86\Google\Update\1...	Google LLC	NT AUTHORITY\SYSTEM	C:\Program Files\x86\Google\Update\1.3.36.152\GoogleCrashHandler.exe	10/5/2022 3:10:59 PM	
GoogleCrashHandler64.exe (2728)	Google Crash Han...	C:\Program Files\x86\Google\Update\1...	Google LLC	NT AUTHORITY\SYSTEM	C:\Program Files\x86\Google\Update\1.3.36.152\GoogleCrashHandler64.exe	10/5/2022 3:10:59 PM	

Description: Apache Commons Daemon Service Runner  
 Company: Apache Software Foundation  
 Path: C:\Program Files\ScadaBR\tomcat\bin\ScadaBR.exe  
 Command: "C:\Program Files\ScadaBR\tomcat\bin\ScadaBR.exe" /RS//ScadaBR  
 User: NT AUTHORITY\LOCAL SERVICE  
 PID: 1036 Started: 10/5/2022 4:27:17 PM

[Go To Event](#) [Include Process](#) [Include Subtree](#)

Close

4:30 PM  
10/5/2022

**Process Monitor - Sysinternals: www.sysinternals.com**

[File](#) [Edit](#) [Eyer](#) [Filter](#) [Tools](#) [Options](#) [Help](#)

Time of Day	Process Name	PID	Operation	Path	Result	Detail
4/27/15 5436005 PM	svchost.exe	904	RegCloseKey	HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\Netlogon\Parameters\Expect...	SUCCESS	NAME NOT FOUND
4/27/15 5436159 PM	svchost.exe	904	RegQueryValue	HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\Netlogon\Parameters	SUCCESS	NAME NOT FOUND
4/27/15 5436277 PM	svchost.exe	904	RegCloseKey	HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\Netlogon\Parameters	SUCCESS	NAME NOT FOUND
4/27/15 16:39:396 PM	vmtold.exe	1652	CreateFile	C:\ProgramData\VMware\VMware Tools\tools\global.conf	NAME NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Options: 0x0
4/27/15 19:22:87 PM	vmtold.exe	1652	CreateFile	C:\ProgramData\VMware\VMware Tools\tools\global.conf	NAME NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Options: 0x0
4/27/15 20:44:462 PM	vmtold.exe	2976	CreateFile	C:\ProgramData\VMware\VMware Tools\tools\global.conf	NAME NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Options: 0x0
4/27/15 20:59:243 PM	vmtold.exe	2976	CreateFile	C:\ProgramData\VMware\VMware Tools\tools\global.conf	NAME NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Options: 0x0
4/27/15 20:59:370 PM	svchost.exe	904	Thread Exit		SUCCESS	Thread ID: 5008, User Time: 0.0780005, Kernel Time: 0
4/27/15 20:59:403 PM	svchost.exe	904	Thread Exit		SUCCESS	Thread ID: 4132, User Time: 0.0000000, Kernel Time: 0
4/27/15 20:59:434 PM	svchost.exe	1404	UDP Send	lmgw-PC\localdomain\61279 > 239.255.255.250 ssdp	SUCCESS	Length: 144
4/27/15 20:59:465 PM	svchost.exe	1404	UDP Receive	lmgw-PC\61280 > 239.255.255.250 ssdp	SUCCESS	Length: 133, seqnum: 0, connid: 0
4/27/15 20:59:502 PM	svchost.exe	1404	UDP Receive	lmgw-PC\61280 > 239.255.255.250 ssdp	SUCCESS	Length: 133, seqnum: 0, connid: 0
4/27/15 20:59:535 PM	ScadaBR.exe	2624	RegQueryKey	HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\CTF\KnownClasses	SUCCESS	Query: HandleTags, HandleTags: 0x0
4/27/15 20:59:572 PM	ScadaBR.exe	2624	RegQueryKey	HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\CTF\KnownClasses	SUCCESS	Query: Name
4/27/15 20:59:598 PM	ScadaBR.exe	2624	RegOpenKey	HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\CTF\KnownClasses	NAME NOT FOUND	Desired Access: Read
4/27/15 21:04:457 PM	ScadaBR.exe	2624	Thread Create		SUCCESS	Thread ID: 3115
4/27/15 21:08:077 PM	svchost.exe	1404	UDP Receive	f02c:ssdp > lmgw-PC\localdomain\61277	SUCCESS	Length: 146, seqnum: 0, connid: 0
4/27/15 21:08:124 PM	svchost.exe	1404	UDP Receive	f02c:ssdp > lmgw-PC\61278	SUCCESS	Length: 146, seqnum: 0, connid: 0
4/27/15 21:08:145 PM	svchost.exe	1404	UDP Receive	f02c:ssdp > lmgw-PC\61278	SUCCESS	Length: 146, seqnum: 0, connid: 0
4/27/15 21:08:391 PM	svchost.exe	476	RegQueryValue	HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\VAD\	NAME NOT FOUND	Desired Access: Read
4/27/15 21:08:562 PM	svchost.exe	476	RegQueryValue	HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\VAD\	NAME NOT FOUND	Desired Access: Read
4/27/15 21:09:084 PM	svchost.exe	476	RegQueryValue	HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\VAD\	NAME NOT FOUND	Desired Access: Read
4/27/15 21:09:395 PM	svchost.exe	476	RegQueryValue	HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\VAD\	NAME NOT FOUND	Desired Access: Read
4/27/15 21:10:227 PM	svchost.exe	476	RegQueryValue	HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\VAD\	NAME NOT FOUND	Desired Access: Read
4/27/15 21:10:502 PM	svchost.exe	476	RegCloseKey	HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\VAD\	SUCCESS	Desired Access: Read
4/27/15 21:10:585 PM	svchost.exe	476	RegQueryValue	HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\ScadaBR\ObjectName	SUCCESS	Desired Access: Read
4/27/15 21:11:022 PM	svchost.exe	476	RegCloseKey	HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\ScadaBR	SUCCESS	Desired Access: Read
4/27/15 21:11:086 PM	svchost.exe	476	RegQueryValue	HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\ScadaBR	SUCCESS	Desired Access: Read
4/27/15 21:11:332 PM	svchost.exe	476	RegQueryValue	HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\ScadaBR\ImagePath	SUCCESS	Desired Access: Read
4/27/15 21:11:462 PM	svchost.exe	476	RegQueryValue	HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\ScadaBR\WOW64	NAME NOT FOUND	Desired Access: Read
4/27/15 21:11:576 PM	svchost.exe	476	RegCloseKey	HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\ScadaBR	SUCCESS	Desired Access: Read
4/27/15 21:11:579 PM	svchost.exe	476	RegQueryValue	HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\ScadaBR\ObjectName	SUCCESS	Desired Access: Read
4/27/15 21:12:043 PM	svchost.exe	476	RegQueryValue	HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\ScadaBR\ObjectName	SUCCESS	Desired Access: Read
4/27/15 21:12:084 PM	svchost.exe	476	RegCloseKey	HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\ScadaBR	SUCCESS	Desired Access: Read
4/27/15 21:12:283 PM	svchost.exe	476	RegQueryValue	HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\ScadaBR\HKU	SUCCESS	Desired Access: Read
4/27/15 21:12:394 PM	svchost.exe	476	RegQueryValue	HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\ScadaBR\HKU\5-1-19	SUCCESS	Desired Access: Read
4/27/15 21:23:394 PM	svchost.exe	476	RegCloseKey	HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\ScadaBR\HKU\5-1-19	SUCCESS	Desired Access: Read/Write
4/27/15 21:24:105 PM	svchost.exe	476	RegQueryValue	HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\ScadaBR\HKU	SUCCESS	Query: HandleTags, HandleTags: 0x0
4/27/15 21:24:221 PM	svchost.exe	476	RegOpenKey	HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\ScadaBR\HKU\5-1-19	SUCCESS	Desired Access: Read/Write

Showing 121,180 of 204,439 events (50%) Backed by virtual memory

4:46 PM  
10/5/2022

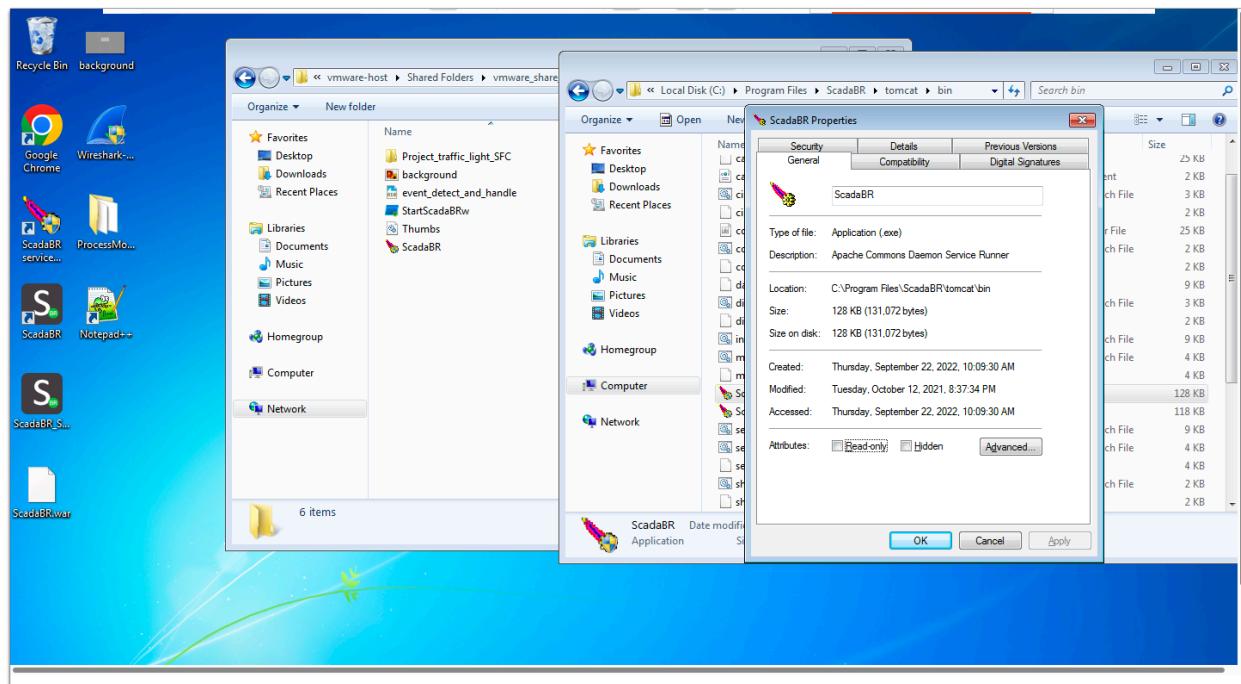
ScadaBR.exe starts

Time of Day	Process Name	PID	Operation	Path	Result	Detail
4/27/17 2148353 PM	services.exe	476	CreateFile	C:\Windows\ServiceProfiles	SUCCESS	Desired Access: Read Data/List Directory, Synchronize... FileInformationClass: FileBothDirectoryInformation, Filter...
4/27/17 2148614 PM	services.exe	476	QueryDirectory	C:\Windows\ServiceProfiles\LocalService	SUCCESS	
4/27/17 2148857 PM	services.exe	476	CloseFile	C:\Windows\ServiceProfiles	SUCCESS	
4/27/17 2149230 PM	services.exe	476	RegEnumValue	HKEYUS-15-Environment	SUCCESS	
4/27/17 2151139 PM	services.exe	476	CreateFile	C:\Windows\ServiceProfiles\LocalService\VppData\LocalTemp	SUCCESS	
4/27/17 2151434 PM	services.exe	476	QueryBasicInfor...	C:\Windows\ServiceProfiles\LocalService\VppData\LocalTemp	SUCCESS	
4/27/17 2152087 PM	services.exe	476	CreateFile	C:\Windows\ServiceProfiles\LocalService\VppData\LocalTemp	SUCCESS	
4/27/17 2152575 PM	services.exe	476	QueryDirectory	C:\Windows	SUCCESS	
4/27/17 2152869 PM	services.exe	476	QueryDirectory	C:\Windows\ServiceProfiles	SUCCESS	
4/27/17 2153374 PM	services.exe	476	CloseFile	C:\Windows	SUCCESS	
4/27/17 2154401 PM	services.exe	476	CreateFile	C:\Windows\ServiceProfiles	SUCCESS	
4/27/17 2154629 PM	services.exe	476	QueryDirectory	C:\Windows\ServiceProfiles\LocalService	SUCCESS	
4/27/17 2154845 PM	services.exe	476	CloseFile	C:\Windows\ServiceProfiles	SUCCESS	
4/27/17 2155260 PM	services.exe	476	RegCloseKey	HKEYUS-15-Environment	SUCCESS	
4/27/17 2155324 PM	services.exe	476	RegQueryKey	HKEYUS-15-19	SUCCESS	
4/27/17 2159453 PM	services.exe	476	RegOpenKey	HKEYUS-15-19\Volatile Environment	NAME NOT FOUND	Query: HandleTags, HandleTags: 0x0 Desired Access: Read
4/27/17 2159527 PM	services.exe	476	RegQueryKey	HKEYUS-15-19\Volatile Environment\0	NAME NOT FOUND	Query: HandleTags, HandleTags: 0x0 Desired Access: Read
4/27/17 2156168 PM	services.exe	476	RegCloseKey	HKEYUS-15-19	SUCCESS	
4/27/17 2157642 PM	services.exe	476	RegOpenKey	HKEYLM\System\CurrentControlSet\Services\ScadaBR	SUCCESS	Desired Access: Read
4/27/17 2157797 PM	services.exe	476	RegGetValue	HKEYLM\System\CurrentControlSet\Services\ScadaBR\Environment	NAME NOT FOUND	Length: 268
4/27/17 2157914 PM	services.exe	476	RegGetValue	HKEYLM\System\CurrentControlSet\Services\ScadaBR	SUCCESS	
4/27/17 2159730 PM	services.exe	476	CreateFile	C:\Program Files\ScadaBR\tomcat\bin\ScadaBR.exe	SUCCESS	
4/27/17 2159894 PM	services.exe	476	QueryBasicInfor...	C:\Program Files\ScadaBR\tomcat\bin\ScadaBR.exe	SUCCESS	
4/27/17 2160118 PM	services.exe	476	CloseFile	C:\Program Files\ScadaBR\tomcat\bin\ScadaBR.exe	SUCCESS	
4/27/17 2161722 PM	services.exe	476	CreateFile	C:\Program Files\ScadaBR\tomcat\bin\ScadaBR.exe	SUCCESS	
4/27/17 2161937 PM	services.exe	476	QueryBasicInfor...	C:\Program Files\ScadaBR\tomcat\bin\ScadaBR.exe	SUCCESS	
4/27/17 2163445 PM	services.exe	476	CreateFile	C:\Program Files\ScadaBR\tomcat\bin\ScadaBR.exe	SUCCESS	
4/27/17 2163142 PM	services.exe	476	QueryBasicInfor...	C:\Program Files\ScadaBR\tomcat\bin\ScadaBR.exe	SUCCESS	
4/27/17 2163414 PM	services.exe	476	CreateFileMap	C:\Program Files\ScadaBR\tomcat\bin\ScadaBR.exe	FILE LOCKED WITH ON...	Desired Access: Read Data/List Directory, Execute/Tra... Sync-Type: SyncTypeCreateSection, PageProtection:
4/27/17 2164519 PM	services.exe	476	CreateFileMap	C:\Program Files\ScadaBR\tomcat\bin\ScadaBR.exe	SUCCESS	Sync-Type: SyncTypeOther
4/27/17 2165429 PM	services.exe	476	RegOpenKey	HKEYLM\Software\Microsoft\Windows\NT\CurrentVersion\Image File Ex...	NAME NOT FOUND	Desired Access: Query Value, Enumerate Sub Keys
4/27/17 2166264 PM	services.exe	476	RegOpenKey	HKEYLM\System\CurrentControlSet\Control\SESSION MANAGER\Quota Sy...	NAME NOT FOUND	Desired Access: Query Value
4/27/17 2171426 PM	services.exe	476	QuerySecurityFile	C:\Program Files\ScadaBR\tomcat\bin\ScadaBR.exe	SUCCESS	Information: Label
4/27/17 2172031 PM	services.exe	476	QueryNameInfo	C:\Program Files\ScadaBR\tomcat\bin\ScadaBR.exe	SUCCESS	Name: "Program Files\ScadaBR\tomcat\bin\ScadaBR...
4/27/17 2172131 PM	ScadaBR.exe	1036	Process Create	C:\Program Files\ScadaBR\ScadaBR.exe	SUCCESS	PID: 1036, Command line: "C:\Program Files\ScadaBR\ScadaBR.exe"
4/27/17 2172205 PM	ScadaBR.exe	1036	Thread Create		SUCCESS	Parent PID: 476, Command line: "C:\Program Files\ScadaBR\ScadaBR.exe"
4/27/17 2172861 PM	services.exe	476	QuerySecurityFile	C:\Program Files\ScadaBR\tomcat\bin\ScadaBR.exe	SUCCESS	Information: Owner, Group, DACL, SACL, Label
4/27/17 2172864 PM	services.exe	476	QueryBasicInfor...	C:\Program Files\ScadaBR\tomcat\bin\ScadaBR.exe	SUCCESS	Creation Time: 3/22/2022 10:09:30 AM, LastAccessTim...

## Observation after starting ScadaBR

The log file is in google drive (ScadaBR\_Process.PML)

ScadaBR.exe is a service runner. Actions on ScadaBR are executed by jsp, jar, and java files.



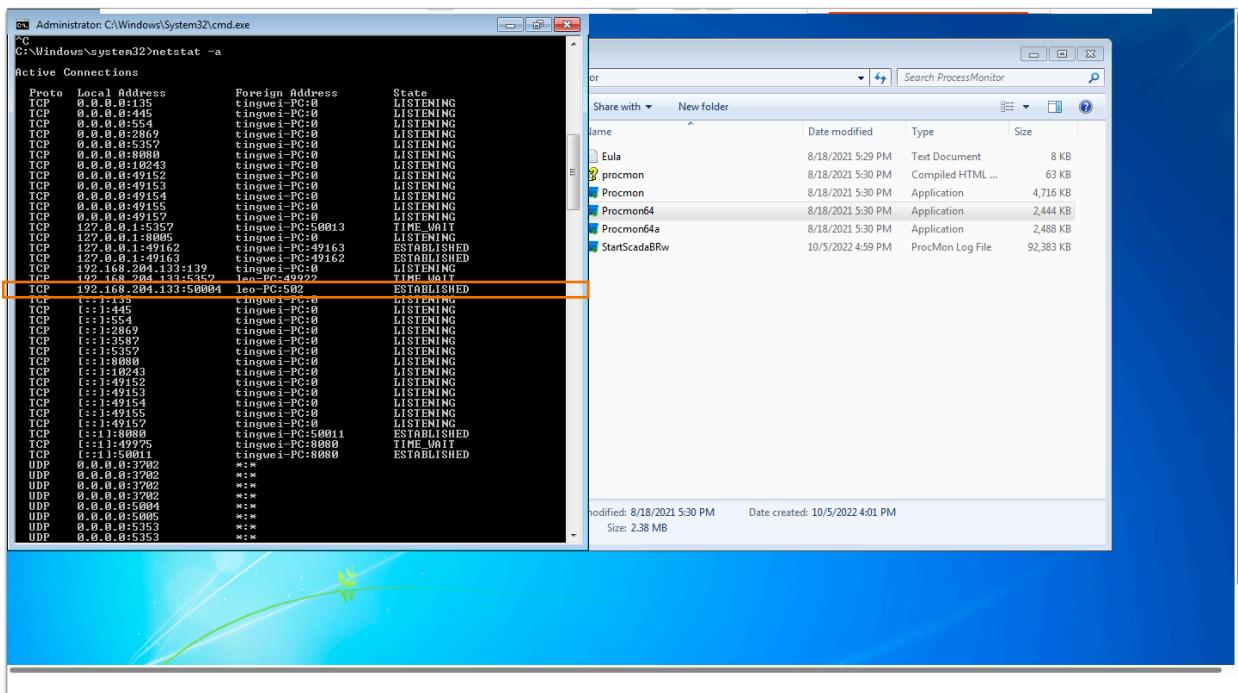
Access index.jsp when open <http://localhost:8080/ScadaBR>

Access login.jsp to perform login.

Time of Day	Process Name	PID	Operation	Path	Result	Detail
10:47:20 1048265 AM	ScadaBR.exe	1444	Close File	C:\Program Files\ScadaBR\tomcat\webapps\ScadaBR\index.jsp	SUCCESS	
10:47:20 1050175 AM	ScadaBR.exe	1444	Create File	C:\Program Files\ScadaBR\tomcat\webapps\ScadaBR\index.jsp	SUCCESS	Desired Access: Generic Read, Disp...
10:47:20 1050799 AM	ScadaBR.exe	1444	Read File	C:\Program Files\ScadaBR\tomcat\webapps\ScadaBR\index.jsp	SUCCESS	Offset: 0, Length: 1,816, Priority: Non...
10:47:20 1051185 AM	ScadaBR.exe	1444	Read File	C:\Program Files\ScadaBR\tomcat\webapps\ScadaBR\index.jsp	SUCCESS	Offset: 0, Length: 1,816, I/O Flags: N...
10:47:20 1076814 AM	ScadaBR.exe	1444	Close File	C:\Program Files\ScadaBR\tomcat\webapps\ScadaBR\index.jsp	SUCCESS	
10:47:20 1088995 AM	ScadaBR.exe	1444	Create File	C:\Program Files\ScadaBR\tomcat\work\Catalina\VirtualHost\ScadaBR\org.apache.jsp.viper.jsp	SUCCESS	Desired Access: Read Attributes, Dis...
10:47:20 1092330 AM	ScadaBR.exe	1444	QueryNetworkOpenInformationFile	C:\Program Files\ScadaBR\tomcat\work\Catalina\VirtualHost\ScadaBR\org.apache.jsp.viper.jsp	SUCCESS	Creation Time: 9/22/2022 4:44:33 PM
10:47:20 1100556 AM	ScadaBR.exe	1444	Create File	C:\Program Files\ScadaBR\tomcat\work\Catalina\VirtualHost\ScadaBR\org.apache.jsp.viper.jsp	SUCCESS	Desired Access: Generic Read, Disp...
10:47:20 1102660 AM	ScadaBR.exe	1444	Create File	C:\Program Files\ScadaBR\tomcat\work\Catalina\VirtualHost\ScadaBR\org.apache.jsp.viper.jsp	SUCCESS	Desired Access: Generic Read, Disp...
10:47:20 1103290 AM	ScadaBR.exe	1444	QueryNetworkOpenInformationFile	C:\Program Files\ScadaBR\tomcat\work\Catalina\VirtualHost\ScadaBR\org.apache.jsp.viper.jsp	SUCCESS	Desired Access: Read Attributes, Dis...
10:47:20 1103511 AM	ScadaBR.exe	1444	Close File	C:\Program Files\ScadaBR\tomcat\work\Catalina\VirtualHost\ScadaBR\org.apache.jsp.viper.jsp	SUCCESS	Desired Access: Read Attributes, Dis...
10:47:20 1104339 AM	ScadaBR.exe	1444	Read File	C:\Program Files\ScadaBR\tomcat\work\Catalina\VirtualHost\ScadaBR\org.apache.jsp.viper.jsp	SUCCESS	Offset: 0, Length: 1,024, Priority: Non...
10:47:20 1106250 AM	ScadaBR.exe	1444	Read File	C:\Program Files\ScadaBR\tomcat\work\Catalina\VirtualHost\ScadaBR\org.apache.jsp.viper.jsp	SUCCESS	Offset: 0, Length: 4,096, I/O Flags: N...
10:47:20 1106668 AM	ScadaBR.exe	1444	Read File	C:\Program Files\ScadaBR\tomcat\work\Catalina\VirtualHost\ScadaBR\org.apache.jsp.viper.jsp	SUCCESS	Offset: 1,024, Length: 2,048
10:47:20 1107170 AM	ScadaBR.exe	1444	Close File	C:\Program Files\ScadaBR\tomcat\work\Catalina\VirtualHost\ScadaBR\org.apache.jsp.viper.jsp	SUCCESS	Offset: 3,072, Length: 3,466
10:47:20 1107424 AM	ScadaBR.exe	1444	Create File	C:\Program Files\ScadaBR\tomcat\webapps\ScadaBR\WEB-INF\classes\javavet\service.jsp	NOT FOUND	
10:47:20 1109333 AM	ScadaBR.exe	1444	QueryDirectory	C:\Program Files\ScadaBR\tomcat\webapps\ScadaBR\WEB-INF\classes\javavet\service.jsp	NOT FOUND	Desired Access: Read Attributes, Dis...
10:47:20 1109906 AM	ScadaBR.exe	1444	QueryDirectory	C:\Program Files\ScadaBR\tomcat\webapps\ScadaBR\WEB-INF\jsp	SUCCESS	Desired Access: Read Attributes, Dis...
10:47:20 1109150 AM	ScadaBR.exe	1444	Create File	C:\Program Files\ScadaBR\tomcat\webapps\ScadaBR\WEB-INF\jsp	SUCCESS	Desired Access: Read Data (Load) File...
10:47:20 1109155 AM	ScadaBR.exe	1444	QueryDirectory	C:\Program Files\ScadaBR\tomcat\webapps\ScadaBR\WEB-INF\Login.jsp	SUCCESS	Desired Access: Read Data (Load) File...
10:47:20 1109227 AM	ScadaBR.exe	1444	Close File	C:\Program Files\ScadaBR\tomcat\webapps\ScadaBR\WEB-INF\Login.jsp	SUCCESS	FileInformationClass: FileBothDirector
10:47 20 14986-203 AM	ScadaBR.exe	1444	Create File	C:\Program Files\ScadaBR\tomcat\webapps\ScadaBR\WEB-INF\Login.jsp	SUCCESS	Desired Access: Read Attributes, Dis...
10:47 20 40989752 AM	ScadaBR.exe	1444	QueryNetworkOpenInformationFile	C:\Program Files\ScadaBR\tomcat\webapps\ScadaBR\WEB-INF\Login.jsp	SUCCESS	Creation Time: 9/22/2022 4:56:35 PM
10:47 20 40989984 AM	ScadaBR.exe	1444	Close File	C:\Program Files\ScadaBR\tomcat\webapps\ScadaBR\WEB-INF\Login.jsp	SUCCESS	
10:47 20 40992442 AM	ScadaBR.exe	1444	Create File	C:\Program Files\ScadaBR\tomcat\webapps\ScadaBR\WEB-INF\Login.jsp	SUCCESS	Desired Access: Read Attributes, Dis...
10:47 20 40993180 AM	ScadaBR.exe	1444	QueryNetworkOpenInformationFile	C:\Program Files\ScadaBR\tomcat\webapps\ScadaBR\WEB-INF\Login.jsp	SUCCESS	Creation Time: 9/22/2022 4:56:35 PM
10:47 20 40998859 AM	ScadaBR.exe	1444	Close File	C:\Program Files\ScadaBR\tomcat\webapps\ScadaBR\WEB-INF\Login.jsp	SUCCESS	
10:47 20 50002405 AM	ScadaBR.exe	1444	QueryNetworkOpenInformationFile	C:\Program Files\ScadaBR\tomcat\webapps\ScadaBR\WEB-INF\Login.jsp	SUCCESS	Desired Access: Read Attributes, Dis...
10:47 20 5000464 AM	ScadaBR.exe	1444	Close File	C:\Program Files\ScadaBR\tomcat\webapps\ScadaBR\WEB-INF\Login.jsp	SUCCESS	Creation Time: 9/22/2022 4:56:35 PM
10:47 20 5002340 AM	ScadaBR.exe	1444	Create File	C:\Program Files\ScadaBR\tomcat\webapps\ScadaBR\WEB-INF\Login.jsp	SUCCESS	Desired Access: Read Attributes, Sy...
10:47 20 5002717 AM	ScadaBR.exe	1444	QueryBasicInformationFile	C:\Program Files\ScadaBR\tomcat\webapps\ScadaBR\WEB-INF\Login.jsp	SUCCESS	Creation Time: 9/22/2022 4:56:35 PM
10:47 20 500281 AM	ScadaBR.exe	1444	Close File	C:\Program Files\ScadaBR\tomcat\webapps\ScadaBR\WEB-INF\Login.jsp	SUCCESS	
10:47 20 5006528 AM	ScadaBR.exe	1444	Create File	C:\Program Files\ScadaBR\tomcat\webapps\ScadaBR\WEB-INF\Login.jsp	SUCCESS	Desired Access: Read Attributes, Dis...
10:47 20 5007771 AM	ScadaBR.exe	1444	QueryNetworkOpenInformationFile	C:\Program Files\ScadaBR\tomcat\webapps\ScadaBR\WEB-INF\Login.jsp	SUCCESS	Creation Time: 9/22/2022 4:56:35 PM
10:47 20 5008093 AM	ScadaBR.exe	1444	Close File	C:\Program Files\ScadaBR\tomcat\webapps\ScadaBR\WEB-INF\Login.jsp	SUCCESS	
10:47 20 5012779 AM	ScadaBR.exe	1444	Create File	C:\Program Files\ScadaBR\tomcat\work\ehome\ScadaRR\WFR-INF\Login.jsp	SUCCESS	Desired Access: Read Attributes, Dis...

Also, there are watchList.jsp, dataSourceList.jsp, etc.

It only connects to modbus (port 502) on the other virtual machine running OpenPLC.



Port 502 is connected with PID 1444

```
C:\Windows\system32>netstat -o

Active Connections

Proto  Local Address          Foreign Address        State           PID
TCP    127.0.0.1:5357          tingwei-PC:50089      TIME_WAIT       0
TCP    127.0.0.1:5357          tingwei-PC:50119      TIME_WAIT       0
TCP    127.0.0.1:5357          tingwei-PC:50121      TIME_WAIT       0
TCP    127.0.0.1:49162         tingwei-PC:49163      ESTABLISHED    1444
TCP    127.0.0.1:49163         tingwei-PC:49162      ESTABLISHED    1444
TCP    192.168.204.133:5357   leo-PC:49942        TIME_WAIT       0
TCP    192.168.204.133:5357   leo-PC:49944        TIME_WAIT       0
TCP    192.168.204.133:50115  leo-PC:502          ESTABLISHED    1444
TCP    [::1]:8080              tingwei-PC:50120      ESTABLISHED    1444
TCP    [::1]:50088             tingwei-PC:8080       TIME_WAIT       0
TCP    [::1]:50120             tingwei-PC:8080       ESTABLISHED    1364
^C
```

And PID 1444 is ScadaBR.exe

```
C:\Windows\system32>tasklist | find "ScadaBR.exe"
ScadaBR.exe                   1444 Services                 0      281,908 K
C:\Windows\system32>
```

The source port of ScadaBR changes regularly. In this case, it changes from port 50154 to 50190.

The screenshot shows a Wireshark capture window titled "Local Area Connection". The packet list pane displays a series of Modbus TCP traffic between two hosts. The first host (192.168.204.133) initiates reads from the second host (192.168.204.136). The second host responds with the requested data. The details pane shows the structure of the Modbus frames, including function codes (0x03 for Read Discrete Inputs), starting addresses, and lengths. The bytes pane at the bottom shows the raw hex and ASCII data for each frame. A status bar at the bottom indicates the total number of packets (8000-8038) and the current packet number (10).

Frame 979: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF\_{7D4B0728-D8EF-4A5F-8E04-85A038E1A395}, id 0

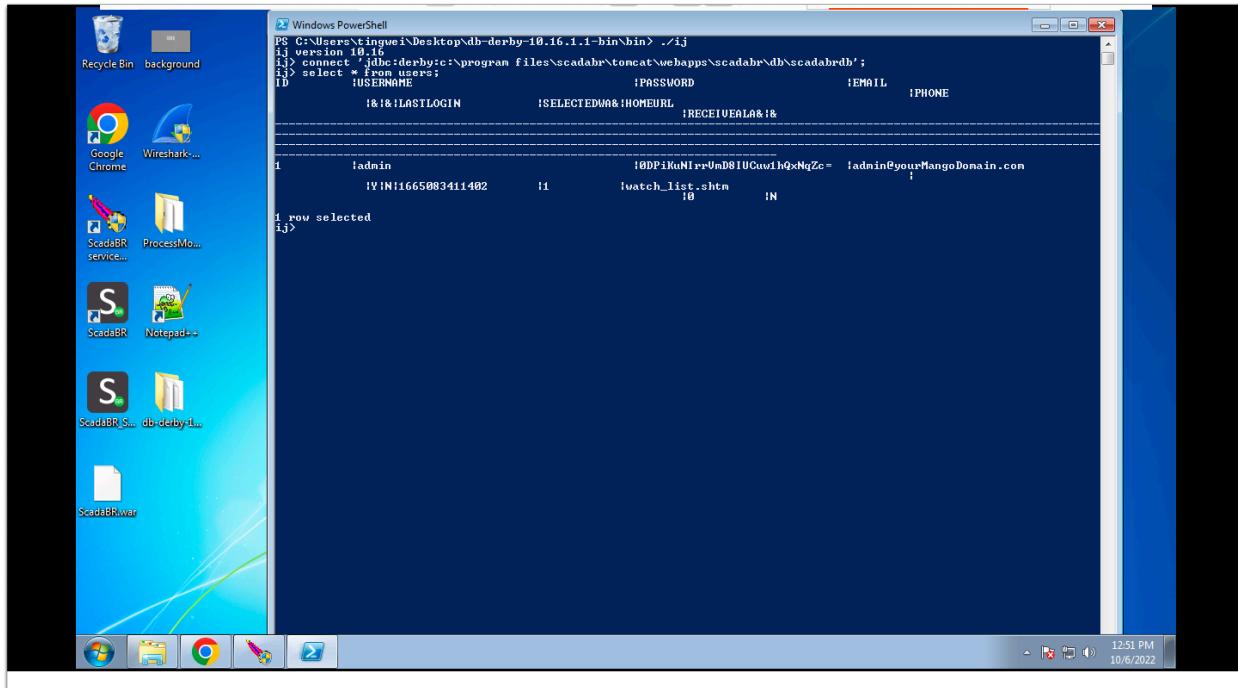
Ethernet II, Src: Vmware\_fde0:f0 (00:0c:29:fd:e0:f0), Dst: Vmware\_93:d3:96 (00:0c:29:03:d3:96)

Internet Protocol Version 4, Src: 192.168.204.133, Dst: 192.168.204.136

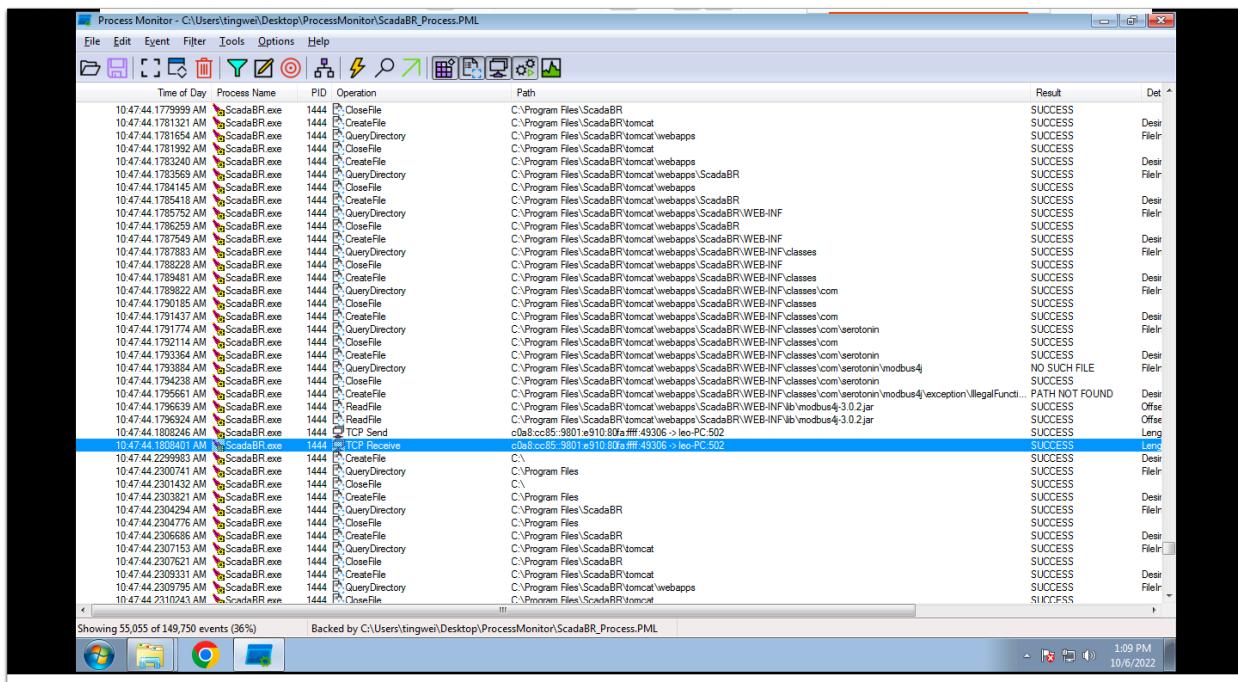
Transmission Control Protocol, Src Port: 50190, Dst Port: 502, Seq: 0, Len: 0

No.	Time	Source	Destination	Protocol	Length	Info
892	36.447966	192.168.204.136	192.168.204.133	Modbus...	64	Response: Trans: 2348; Unit: 1, Func: 2: Read Discrete Inputs
893	36.477244	192.168.204.133	192.168.204.136	Modbus...	66	Query: Trans: 2349; Unit: 1, Func: 1: Read Coils
894	36.477422	192.168.204.136	192.168.204.133	Modbus...	64	Response: Trans: 2349; Unit: 1, Func: 1: Read Coils
895	36.677083	192.168.204.133	192.168.204.136	TCP	60	50154 → 502 [ACK] Seq=1753 Ack=1460 Win=16392 Len=0
904	36.945874	192.168.204.133	192.168.204.136	Modbus...	66	Query: Trans: 2350; Unit: 1, Func: 2: Read Discrete Inputs
905	36.945875	192.168.204.136	192.168.204.133	Modbus...	64	Response: Trans: 2350; Unit: 1, Func: 2: Read Discrete Inputs
906	36.977132	192.168.204.133	192.168.204.136	Modbus...	66	Query: Trans: 2351; Unit: 1, Func: 1: Read Coils
907	36.977211	192.168.204.133	192.168.204.136	Modbus...	64	Response: Trans: 2351; Unit: 1, Func: 1: Read Coils
908	37.177086	192.168.204.133	192.168.204.136	TCP	60	50154 → 502 [ACK] Seq=1777 Ack=1481 Win=16387 Len=0
917	42.465935	192.168.204.133	192.168.204.136	TCP	66	50189 → 502 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
979	43.510233	192.168.204.133	192.168.204.136	TCP	66	50190 → 502 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
980	43.510394	192.168.204.136	192.168.204.133	TCP	66	502 → 50190 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
982	43.521731	192.168.204.133	192.168.204.136	TCP	60	50190 → 502 [ACK] Seq=1 Ack=1 Win=65704 Len=0
984	43.521732	192.168.204.133	192.168.204.136	Modbus...	66	Query: Trans: 2360; Unit: 1, Func: 2: Read Discrete Inputs
997	43.609758	192.168.204.136	192.168.204.133	Modbus...	64	Response: Trans: 2360; Unit: 1, Func: 2: Read Discrete Inputs
1000	43.663419	192.168.204.133	192.168.204.136	Modbus...	66	Query: Trans: 2361; Unit: 1, Func: 1: Read Coils
1001	43.663496	192.168.204.136	192.168.204.133	Modbus...	64	Response: Trans: 2361; Unit: 1, Func: 1: Read Coils
1003	43.663993	192.168.204.133	192.168.204.136	TCP	60	50190 → 502 [ACK] Seq=21 Ack=21 Win=65680 Len=0

It's using Apache Derby Database. Data source and point information are stored in here. Here's an example of accessing the database from "ij", which is a tool provided by Derby.



It shows that we are sending TCP Modbus traffic to OpenPLC, may be related to modbus4j-3.0.2.jar executed earlier.



There are different classes running inside that jar file, for message reading and writing purposes.

Time of Day	Process Name	PID	Operation	Path	Result	Detail
10/4744 1527653 AM	ScadaBR.exe	1444	ReadFile	C:\Program Files\ScadaBR\tomcat\webapps\ScadaBR\WEB-INF\lib\modbus4-3.0.2.jar	SUCCESS	Offset: 12
10/4744 1502209 AM	ScadaBR.exe	1444	QueryDirectory	C:\Program Files\ScadaBR\tomcat\webapps\ScadaBR\WEB-INF\classes\com\serotonin\modbus4\msg\WriteCoResponse.class	NO SUCH FILE	FileInfo
10/4744 1502209 AM	ScadaBR.exe	1444	CreateFile	C:\Program Files\ScadaBR\tomcat\webapps\ScadaBR\WEB-INF\classes\com\serotonin\modbus4\msg\WriteCoResponse.class	PATH NOT FOUND	Desired A
10/4744 1603497 AM	ScadaBR.exe	1444	ReadFile	C:\Program Files\ScadaBR\tomcat\webapps\ScadaBR\WEB-INF\lib\modbus4-3.0.2.jar	SUCCESS	Offset: 12
10/4744 1604030 AM	ScadaBR.exe	1444	ReadFile	C:\Program Files\ScadaBR\tomcat\webapps\ScadaBR\WEB-INF\lib\modbus4-3.0.2.jar	SUCCESS	Offset: 12
10/4744 1630537 AM	ScadaBR.exe	1444	QueryDirectory	C:\Program Files\ScadaBR\tomcat\webapps\ScadaBR\WEB-INF\classes\com\serotonin\modbus4	NO SUCH FILE	FileInfo
10/4744 1632745 AM	ScadaBR.exe	1444	CreateFile	C:\Program Files\ScadaBR\tomcat\webapps\ScadaBR\WEB-INF\classes\com\serotonin\modbus4\msg\WriteRegisterResponse.class	PATH NOT FOUND	Desired A
10/4744 1634170 AM	ScadaBR.exe	1444	ReadFile	C:\Program Files\ScadaBR\tomcat\webapps\ScadaBR\WEB-INF\lib\modbus4-3.0.2.jar	SUCCESS	Offset: 13
10/4744 1634402 AM	ScadaBR.exe	1444	ReadFile	C:\Program Files\ScadaBR\tomcat\webapps\ScadaBR\WEB-INF\lib\modbus4-3.0.2.jar	SUCCESS	Offset: 13
10/4744 1636540 AM	ScadaBR.exe	1444	QueryDirectory	C:\Program Files\ScadaBR\tomcat\webapps\ScadaBR\WEB-INF\classes\com\serotonin\modbus4	NO SUCH FILE	FileInfo
10/4744 1636593 AM	ScadaBR.exe	1444	CreateFile	C:\Program Files\ScadaBR\tomcat\webapps\ScadaBR\WEB-INF\classes\com\serotonin\modbus4\msg\ReadExceptionStatusResponse.class	PATH NOT FOUND	Desired A
10/4744 1636593 AM	ScadaBR.exe	1444	ReadFile	C:\Program Files\ScadaBR\tomcat\webapps\ScadaBR\WEB-INF\lib\modbus4-3.0.2.jar	SUCCESS	Offset: 11
10/4744 1636593 AM	ScadaBR.exe	1444	ReadFile	C:\Program Files\ScadaBR\tomcat\webapps\ScadaBR\WEB-INF\lib\modbus4-3.0.2.jar	SUCCESS	Offset: 11
10/4744 1636593 AM	ScadaBR.exe	1444	QueryDirectory	C:\Program Files\ScadaBR\tomcat\webapps\ScadaBR\WEB-INF\classes\com\serotonin\modbus4	NO SUCH FILE	FileInfo
10/4744 1636593 AM	ScadaBR.exe	1444	CreateFile	C:\Program Files\ScadaBR\tomcat\webapps\ScadaBR\WEB-INF\msg\WriteCellsResponse.class	PATH NOT FOUND	Desired A
10/4744 1636593 AM	ScadaBR.exe	1444	ReadFile	C:\Program Files\ScadaBR\tomcat\webapps\ScadaBR\WEB-INF\lib\modbus4-3.0.2.jar	SUCCESS	Offset: 12
10/4744 1636593 AM	ScadaBR.exe	1444	ReadFile	C:\Program Files\ScadaBR\tomcat\webapps\ScadaBR\WEB-INF\lib\modbus4-3.0.2.jar	SUCCESS	Offset: 12
10/4744 1720410 AM	ScadaBR.exe	1444	QueryDirectory	C:\Program Files\ScadaBR\tomcat\webapps\ScadaBR\WEB-INF\classes\com\serotonin\modbus4	NO SUCH FILE	FileInfo
10/4744 1722149 AM	ScadaBR.exe	1444	CreateFile	C:\Program Files\ScadaBR\tomcat\webapps\ScadaBR\WEB-INF\classes\com\serotonin\modbus4\msg\WriteRegistersResponse.class	PATH NOT FOUND	Desired A
10/4744 1722149 AM	ScadaBR.exe	1444	ReadFile	C:\Program Files\ScadaBR\tomcat\webapps\ScadaBR\WEB-INF\lib\modbus4-3.0.2.jar	SUCCESS	Offset: 13
10/4744 1723359 AM	ScadaBR.exe	1444	ReadFile	C:\Program Files\ScadaBR\tomcat\webapps\ScadaBR\WEB-INF\lib\modbus4-3.0.2.jar	SUCCESS	Offset: 13
10/4744 1744795 AM	ScadaBR.exe	1444	QueryDirectory	C:\Program Files\ScadaBR\tomcat\webapps\ScadaBR\WEB-INF\classes\com\serotonin\modbus4	NO SUCH FILE	FileInfo
10/4744 1747016 AM	ScadaBR.exe	1444	CreateFile	C:\Program Files\ScadaBR\tomcat\webapps\ScadaBR\WEB-INF\classes\com\serotonin\modbus4\msg\ReportSlaveResponse.class	PATH NOT FOUND	Desired A
10/4744 1749114 AM	ScadaBR.exe	1444	ReadFile	C:\Program Files\ScadaBR\tomcat\webapps\ScadaBR\WEB-INF\lib\modbus4-3.0.2.jar	SUCCESS	Offset: 12
10/4744 1749476 AM	ScadaBR.exe	1444	ReadFile	C:\Program Files\ScadaBR\tomcat\webapps\ScadaBR\WEB-INF\lib\modbus4-3.0.2.jar	SUCCESS	Offset: 12
10/4744 1759442 AM	ScadaBR.exe	1444	QueryDirectory	C:\Program Files\ScadaBR\tomcat\webapps\ScadaBR\WEB-INF\classes\com\serotonin\modbus4	NO SUCH FILE	FileInfo
10/4744 1771154 AM	ScadaBR.exe	1444	CreateFile	C:\Program Files\ScadaBR\tomcat\webapps\ScadaBR\WEB-INF\classes\com\serotonin\modbus4\msg\WriteMaskRegisterResponse.class	PATH NOT FOUND	Desired A
10/4744 1772068 AM	ScadaBR.exe	1444	ReadFile	C:\Program Files\ScadaBR\tomcat\webapps\ScadaBR\WEB-INF\lib\modbus4-3.0.2.jar	SUCCESS	Offset: 13
10/4744 1772350 AM	ScadaBR.exe	1444	ReadFile	C:\Program Files\ScadaBR\tomcat\webapps\ScadaBR\WEB-INF\lib\modbus4-3.0.2.jar	SUCCESS	Offset: 13
10/4744 1793884 AM	ScadaBR.exe	1444	QueryDirectory	C:\Program Files\ScadaBR\tomcat\webapps\ScadaBR\WEB-INF\classes\com\serotonin\modbus4	NO SUCH FILE	FileInfo
10/4744 1795661 AM	ScadaBR.exe	1444	CreateFile	C:\Program Files\ScadaBR\tomcat\webapps\ScadaBR\WEB-INF\classes\com\serotonin\modbus4\exception\IllegalFunctionException.class	PATH NOT FOUND	Desired A
10/4744 1795661 AM	ScadaBR.exe	1444	ReadFile	C:\Program Files\ScadaBR\tomcat\webapps\ScadaBR\WEB-INF\lib\modbus4-3.0.2.jar	SUCCESS	Offset: 35
10/4744 1795661 AM	ScadaBR.exe	1444	ReadFile	C:\Program Files\ScadaBR\tomcat\webapps\ScadaBR\WEB-INF\lib\modbus4-3.0.2.jar	SUCCESS	Offset: 35
10/4744 2229324 AM	ScadaBR.exe	1444	QueryDirectory	C:\Program Files\ScadaBR\tomcat\webapps\ScadaBR\WEB-INF\classes\com\serotonin\modbus4	NO SUCH FILE	FileInfo
10/4744 2229324 AM	ScadaBR.exe	1444	CreateFile	C:\Program Files\ScadaBR\tomcat\webapps\ScadaBR\WEB-INF\classes\com\serotonin\modbus4\ExceptionResult.class	PATH NOT FOUND	Desired A
10/4744 2229324 AM	ScadaBR.exe	1444	ReadFile	C:\Program Files\ScadaBR\tomcat\webapps\ScadaBR\WEB-INF\lib\modbus4-3.0.2.jar	SUCCESS	Offset: 8.8
10/4744 2229883 AM	ScadaBR.exe	1444	ReadFile	C:\Program Files\ScadaBR\tomcat\webapps\ScadaBR\WEB-INF\lib\modbus4-3.0.2.jar	SUCCESS	Offset: 8.8
10/4744 2230343 AM	ScadaBR.exe	1444	ReadFile	C:\Program Files\ScadaBR\tomcat\webapps\ScadaBR\WEB-INF\lib\modbus4-3.0.2.jar	SUCCESS	Offset: 8.8
10/4751 4676181 AM	ScadaBR.exe	1444	CloseFile	C:\Program Files\ScadaBR\tomcat\webapps\ScadaBR\WEB-INF\lib\modbus4-3.0.2.jar	SUCCESS	

Showing 434 of 149,750 events (0.28%)

Backed by C:\Users\tingwei\Desktop\ProcessMonitor\ScadaBR\_Process.PML

1:13 PM  
10/6/2022