sightlogix

Windows Defender Blocks SightMonitor with Trojan: Win32/Powessere.G Alert

Last Modified on 10/02/2018 3:01 pm EDT

Symptom: SightMonitor will not start. Windows Defender may falsely flag a component of SightMonitor as a Trojan Horse.

First, verify SHA1 checksum is valid

To verify that a virus has not been introduced, you can compare the SHA1 checksum from your installed rs.bat to the checksum for the original rs.bat in the SightLogix source code.

The expected SHA1 checksum for the file should be 2c9537dc157bdfb79e8886e70aa8ef63a7ea82f0

- Download and install Microsoft File Checksum Integrity Verifier (https://www.microsoft.com/enus/download/details.aspx?id=11533)
- Extract fciv.exe to a location you'll remember.
- Open a command prompt window, and enter the following command, replacing the first path with the location of where you saved fciv.exe:

C:\Users\user1\Documents>fciv.exe "C:\Program Files (x86)\SightLogix\CS\Tomcat\webapps\slcs\rs.bat" -sha1

The output should look like this:

//

11

// File Checksum Integrity Verifier version 2.05.

2c9537dc157bdfb79e8886e70aa8ef63a7ea82f0 c:\program files (x86)\sightlogix\cs\tomcat\webapps\slcs\rs.bat

• Verify that the checksum in the command prompt matches the correct value, 2c9537dc157bdfb79e8886e70aa8ef63a7ea82f0

Once you have verified that a virus has not been introduced, two solutions are suggested below.

Short-term Solution

Run SightMonitor as administrator. Right click on the application link in the start menu and select "run as administrator".

Permanent solution

Configure the SightMonitor shortcut to always run as administrator:

- Navigate to this file path: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\SightLogix
- There should be a shortcut to open SightMonitor in this folder. Right click the shortcut and click Properties.



- In the Shortcut tab, click Advanced towards the bottom.
- Check the box that enables Run as administrator.
- Click OK, Apply, then OK.



Next, make an exception to Windows Defender to ignore the component in regular virus scans: :

- Open Windows Defender Security Center.
- Click Virus & threat protection.
- Click Virus & threat protection settings, as shown



÷	Windows Defender Security Center	-	×
=	\bigcirc Virus & threat protection		
ଜ	View threat history, scan for viruses and other threats, specify protection		
0	settings, and get protection updates.		
R	1) Threat history		
എ	Last scan: 9/23/2018 (quick scan)		
	$0 \qquad 17264$		
_	0 17204		
~	Threats found Files scanned		
æ	Scan now		
~~	Run a new advanced scan		
	⁰⊗ Virus & threat protection settings		
	No action needed.		
	G Virus & threat protection updates		
	Last update: 9:25 AM Tuesday, September 25, 2018		
	Ransomware protection		
	Set up OneDrive for file recovery options in case of a ransomware attack.		
	Set up OneDrive		
	Dismiss		
03			

• Scroll to Exclusions, and click Add or remove exclusions.

←	Windows Defender Security Center	-	×
=	Privacy statement		
ŵ			
0	Automatic sample submission		
8	Send sample files to Microsoft to help protect you and others from potential threats. We'll prompt you if the file we need is likely to contain		
(p)	personal information.		
	On On		
д	Privacy statement		
ø	Submit a sample manually		
彘			
	Controlled folder access		
	Protect files, folders, and memory areas on your device from unauthorized changes by unfriendly applications.		
	Manage Controlled folder access		
	Exclusions		
(Windows Defender Antivirus won't scan items that you've excluded. Excluded items could contain threats that make your device vulnerable.		
	Add or remove exclusions		
	Notifications		
	Windows Defender Antivirus will send notifications with critical information about the health and security of your device. You can specify which non-critical notifications you would like.		
	Change notification settings		
٢			

• Click Add an exclusion > File, as shown

sightlogix



- Navigate to C:\Program Files (x86)\SightLogix\CS\Tomcat\webapps\slcs\rs.bat
- Windows may ask for your permission to make changes. Allow the changes.
- Reboot the PC for changes to be effective.
- SightMonitor should now start without Windows Defender detecting a threat.