QGIS Application - Bug report #19670
McAfee reporting "ransomware - HTA file creation" - False positive?

2018-08-22 07:16 PM - Kaz Shimamura

Status:	Closed		
Priority:	Normal		
Assignee:			
Category:	Build/Install		
Affected QGIS version:	3.2.2	**Regression?:**	No
Operating System:	Windows 10	**Easy fix?:**	No
Pull Request or Patch supplied:	No	**Resolution:**	invalid
Crashes QGIS or corrupts data:	No	**Copied to github as #:**	27495

Description

Hello,

At work my McAfee Endpoint Security has reported the following when I tried to install QGIS 3.2.2:

QGIS-OSGEO4W-3.2.2-1-SETUP-X86_64.EXE, which tried to access C:\PROGRAM FILES\QGIS 3.2\APPS\RBATCHFILES\FIND-MIKTEX.HTA, violating the rule "Ransomware - HTA file creation", and was blocked.

I'm wondering if this is a false positive or if it needs closer inspection? McAfee rated the severity as "critical" and has blocked "FIND-MIKTEX.HTA".

all the best,
Kaz

History

#1 - 2018-08-23 08:52 AM - Alessandro Pasotti

Can you check if the md5sum of your downloaded package matches?
https://download.osgeo.org/qgis/windows/QGIS-OSGeo4W-3.2.2-1-Setup-x86_64.exe.md5sum

#2 - 2018-08-23 09:22 AM - Jürgen Fischer

- Resolution set to invalid

- Status changed from Open to Closed

False positive. Find-MicTex.HTA contains:

```
<!-- (c) 2013 GKX Associates Inc. -->
<!-- License: GPL 2.0 -->
<head>
<STYLE TYPE="text/css">
.highlight {background:#ff00ff}
.text {color:#ff00ff}
.both {color:white;background:black}
</STYLE>
<title>find-miktex</title>
</head>
<body onLoad="window.resizeTo(650,250);">
```

```
<h1>Find MiKTeX</h1>
<script type="text/jscript">

fso = new ActiveXObject("Scripting.FileSystemObject");
mik = new ActiveXObject("MiKTeX.Session");

i = 0;
while (true) {
	try {
		rt = mik.GetRootDirectory(i);
		if (fso.FileExists(rt + "\\miktex\\bin\\latex.exe")) {
			document.write(rt + "\\miktex\\bin<br>");
		}
		i++;
	} catch(e) {break};
}

</script>
</body>
</html>
```

#3 - 2018-08-23 12:09 PM - Jürgen Fischer

The hta was removed from rbatchfiles in OSGeo4W.