Installation

The client is implemented as a Windows service. The service uses the SysInternals Autoruns tool to extract the autorun data. The Autoruns tool is provided in two forms, GUI and console.

The console version of the Autoruns tool (autorunsc.exe) must be downloaded separately and put into the same directory as the rest of the AutoRuns client files.

The service uses the configuration details within the **AutoRunLogger.xml** file. The file contains two settings:

- CertificateFileName: The file name of the servers TLS certificate
- RemoteServer: The IP/hostName and port of the remote analysis server e.g. **192.168.0.100:8000**

The service uses the analysis servers TLS certificate file (server.pem) to perform certificate pinning. The file should be copied into the same directory as the rest of the AutoRuns client files.

The AutoRuns client files need to be copied to the target host. The required files are:

```
AutoRunLogger.exe
AutoRunLogger.xml
server.pem
autorunsc.exe
```

Once the files have been copied to the host, the file permissions should be modified to prevent other users from modifying the files, in particular the **autorunsc** binary as this is executed by the service, which has **SYSTEM** permissions.

Autorunsc

This version has been tested with **Autoruns v13.62**. Ensure that this version only is used.

Service

The **AutoRunLogger.exe** has automatic Windows service installation code which means that the use of **sc.exe** or **InstallUtil.exe** is not required.

To install the service, use the following command from an elevated command prompt:

```
AutoRunLogger.exe -install
```

To uninstall the service, use the following command from an elevated command prompt:

```
AutoRunLogger.exe -uninstall
```