AutoRun Logger Server

Process

The Windows client autorun data is sent via a HTTPS (TLS) service to the server. The client uses the **server.pem** file as a certificate pinning mechanism, this allows the use of a self signed TLS certificate.

The client connects to the HTTPS port and sends data to the server. The request URL takes the form of:

https://1.2.3.4:8000/domain/host/user

All data sent from the client is compressed using GZIP. When the server recieves a new client connection, it decompresses the data and sends the data to one of the worker threads. The number of worker threads can be set within the configuration file, or can be auto set by the server e.g. 1 thread per core. A good default value is the number of cores divided by 2.

When the processor thread recieves a new set of data, the XML data's header is corrected, as the **autorunsc.exe** binary produces UTF16 XML but the client converts the XML to UTF8, without changing the header. Once this is complete the XML can be marshalled into internal structs.

The database holds two sets of data per **domain/host** combination e.g. current and previous. When a new set of data is recieved, the data in the **current** table is moved to the **previous** table and the new data inserted.

Analysis

The server then iterates through the current data set and attempts to match the autoruns using the following:

- ItemName
- Location
- Profile
- FilePath
- Launch String
- Sha256

Using these parameters will permit the flagging of items that are:

- New
- Deleted
- Modified (including launch strings or files via hash)

If an autorun has been identifed as new/deleted/modified then a record is added to the **alert** table.

Summary

Every hour summaries are generated that provide unique lists of data. The summaries available are:

- SHA256
- MD5
- Domains
- Hosts
- Users

The data is written to a timestamped file that represents the most current data for a particular day and data type. Each time the file is overwritten, then once the date changes, a perminate record of the last data set for

that day will remain. An example of the file names used are detailed below:

- summary-domain-2016-06-16.csv
- summary-sha256-2016-06-16.csv
- summary-host-2016-06-16.csv
- summary-md5-2016-06-16.csv

The files can be downloaded from the user interface (UI) server.

Archive

The server has a configurable **archive** option that stores a compressed archive of the autorun data. The data is stored in the directory specified by the **archive_dir** configuration value. The archives are stored in sub-directories in the form "domain-host". Each time a new set of data is received, the XML is compressed as a zip file, using the timestamp as the file name.

The file is hashed and the hash compared to the last archive available, if the hash is different, then the file is kept. This method reduces the amount of archive data required. The archive files hash (MD5) is stored in a separate file with the same file name e.g. "/arl/archive/domain/host/2016-06-13T07:21:05Z.zip.md5"