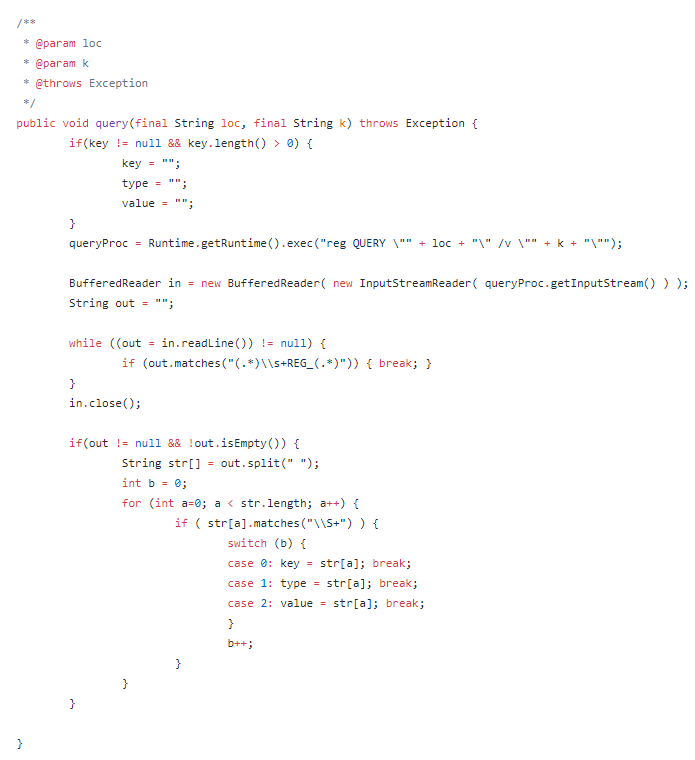
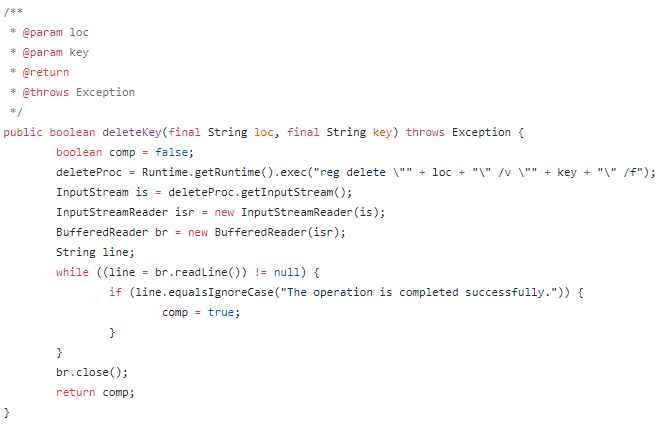
**VirusREM Implementation Details:**

1. **How to scan and detect a virus?**
2. A virus can be searched under all the registry keys using Registry Key Manager in a computer.
3. To search any virus, use “java.lang.Runtime” class & execute the command using “reg QUERY” (as explained in below code snippet) to search for a specified virus in all the registry locations.



1. If a virus is detected then, the corresponding key will be non-empty and a map is created to maintain all the detected viruses.
2. **How to attack & delete a virus if it’s found?**
3. A virus can be deleted using Registry Key Manager in a computer.
4. To delete any virus, use “java.lang.Runtime” class & execute the command using “reg delete” (as explained in below code snippet) to delete any virus in Registry Editor.



1. Once a virus is deleted, then corresponding virus map will be updated & threats count will be updated accordingly.
2. Number of threats is based on the size of virus map. If virus is not removed from the computer, then number of threats should be more than 0 and computer is potentially unprotected.
3. **How to check, if the detected virus is positive or not?**

We have implemented a virus cache where, all the different types of most common viruses are stored as given below.

Adware & Toolbars

CoolWebSearch

Toolbar

Potentially Unwanted App

Browser Hijacker

Macro Virus

Web Scripting Virus

Other types of viruses.., etc

We have defined a virus registry where all the registry locations are specified as given below.

HKEY\_LOCAL\_MACHINE

HKEY\_CURRENT\_USER

HKEY\_CLASSES\_ROOT

When a virus is detected in computer, it should be verified against the above cache. If it’s available in the cache then, it can be considered as a real virus & removed accordingly. Code Snippet is added here.



1. **What happens, if no virus is found?**

As part of scanning, if tool doesn’t find any virus then, virus map store should be updated accordingly. Number of threats is based on the size of virus map as code snippet is added here. In this case, number of threats should be 0 and computer has been scanned and potentially protected.



**Example:**

Based on the above detailed technical documentation, below is an example on virus details where it can be searched & delete it accordingly.

**Virus Name**: AdWare.Toolbar.EZ

**Search Registry**:

HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\RunOnce

HKLM\\SOFTWARE\\Clients\\StartMenu\\Internet\\INTEXPLORE.pif\\ToP

Scan the computer and virus called “AdWare.Toolbar.EZ” can be searched using query from Registry Key Manager (as given in step a) under the search registries as mentioned above. When this virus is found & can be validated against the virus cache as mentioned in step c. If it is well matched then, virus will be considered as malicious. Using deleteKey() from Registry Key Manager (as given in step b), this virus will be deleted or removed from the computer system. If the virus is removed successfully from the computer then, the system should be potentially protected. If the virus is not removed from the computer, then system should be potentially unprotected.

**Details of LOC (lines of code):**

Code can be found at Github repository. GitHub: <https://github.com/cgopi/VirusREM_AREnterprise>

|  |
| --- |
|  |
|  | Search Functionality:  -------------------------- |
|  | File Name: FXMLDocumentController.java |
|  | Method Name: createWorker() |
|  |  |
|  | Lines for scanning or searching the viruses: From 1200 to 1284 |
|  |  |
|  | Detect Functionality: |
|  | -------------------------- |
|  | File Name: FXMLDocumentController.java |
|  | Method Name: createWorker() |
|  |  |
|  | Lines for detecting the viruses: From 1286 to 1302 |
|  |  |
|  | Virus Signatures: |
|  | --------------------- |
|  | Adware & Toolbars |
|  | CoolWebSearch |
|  | Potentially Unwanted App |
|  | Other Types of Viruses |
|  |  |
|  | Viruses List: |
|  | --------------- |
|  | File Name: VirusCache.java |
|  | Method Name: getAllViruses() |
|  |  |
|  | Lines for list of viruses: From 24 to 1072 |
|  |  |
|  | Registry Keys: |
|  | ----------------- |
|  | File Name: VirusRegistry.java |
|  | Method Name: getVirusSearchList() |
|  |  |
|  | Lines for list of registry keys: From 84 to 131 |
|  |  |
|  | Virus Reporting Functionality: |
|  | -------------------------------------- |
|  | File Name: FXMLDocumentController.java |
|  | Method Name: createWorker() |
|  |  |
|  | Lines for viruses reporting to GUI: From 1376 to 1385 |