Solution for Deceptive Download Buttons and Drive-By Installation

Amruth Nag[1]
Department of Information Science and Engineering
School of Engineering and Technology, Jain University
Bangalore Rural, India
amruthnaag1997@gmail.com

M S Sowmya[2]
Department of Information Science and Engineering
School of Engineering and Technology, Jain University
Bangalore Rural, India
ms.sowmya@jainuniversity.ac.in

***Abstract*- Deceptive download buttons are those on the internet which may look like it is meant to do an action but actually does something else which it is not intended by the user. Drive-by installations are those extra software which is installed in a user's device without him noticing it. This paper gives the information about the types of deceptive download buttons and the ways a common user can avoid clicking on such button while browsing the web. A few methods the advertiser may commonly use for making the end user a victim of the deceptive download buttons is discussed here. The methods by which someone can avoid these kinds of buttons are also given in this paper. An idea for the development of an extension to the user's browser, that runs in the background. This warns the user about those buttons prior to the button being clicked. This paper also includes information about drive-by installations of bloatware and the ways in which the end users are being affected by this, how the end user can avoid being a victim of drive-by installations and an idea to develop a tool which runs in the background as a small script in the operating system which will automatically warn the user about the drive-by installations.**

***Keywords*: - Deceptive buttons, web browsing, drive-by installations, software installations, bloatware, malware**

I. INTRODUCTION

Millions of people download millions of files from the Internet every day. People who do this are in range from beginners to experts. Not all the files you get on the internet are free. Some of them need you to complete some sort of survey. A few of them would need you to prove that you're a human and some of them offer those files for free and it is obvious to be suspicious.

There are lots of websites which offer malware and unwanted software in the name of offering them the files for free. Google is working on these sites which spread malware to the users. Google warns the user before entering such websites. There are some websites which offer the files but in a tricky way. If the user doesn't know how to overcome that, there are lot of chances for him/her to become a victim to the malware. The most widely used trick is to keep more than one download buttons (deceptive download buttons) so that the user who needs to download that file would be confused to click the inappropriate download button. When the user is unable to estimate the correct button, it's the best opportunity for the developers who spread malware and spyware.

Even after the user gets the needed file, there's no guarantee that he is safe from unwanted bloatware. There are millions of users struggling to remove the unwanted softwares and scripts from their PC's. Some users who have knowledge about the software architecture are able to remove it, but even after removing it there's a lot of chances for the bloatware to return to their machines without their notice. Though some intellectual users are able to remove it and are still getting affected by it. Users who are new to the internet and who don't know how to remove that unwanted bloatware from their machines would do nothing and those softwares would continue running in their machines.

II. DECEPTIVE BUTTONS

These are the buttons which look like they guide you to the content for which the user is searching for by blending themselves to look and feel as if they lead you to the correct and official content. They are often very hard to differentiate from the rest of the page.

A. Few examples of deceptive buttons

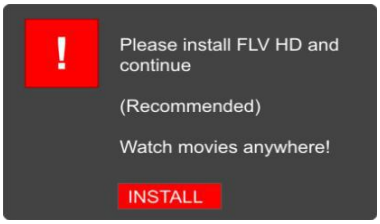


Fig-1.1

The above Fig-1.1 [3], pretends to lead us to the installation of some important official firmware but it doesn't. It can be identified that it is deceptive because there's no icon or logo of the official signed software anywhere.

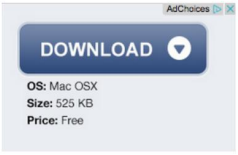


Fig-1.2

This is an open access article under the CC BY-SA 4.0 license (https://creativecommons.org/licenses/by-sa/4.0/)

The download button in Fig-1.2 [4] mimics to give us the MAC OS X. It really doesn't give us that. This can be identified by the user by looking at the details presented there. It clearly says that the file size is 525KB and it is a common sense that MAC OS can never be compressed to that small size. There's also a word saying "AdChoices" at the top right corner which is a clear indication for it to be an ad.

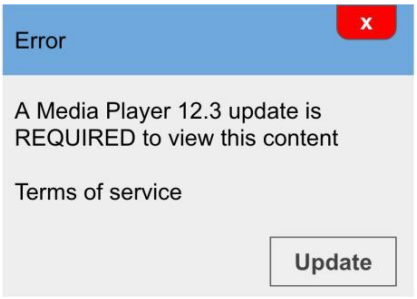


Fig-1.3

The above image (Fig-1.3 [5]) contains a popup which attracts the user to click on the update button but it never does what it tells us. This button can be identified as deceptive by noticing that the popup is titled as error which is clearly irrelevant to the content its displaying inside it.



Fig-1.4

The above image (Fig-1.4 [6]) contains the screenshot of a webpage consisting of many buttons labelled download and play now which obviously won't lead the user to the expected destination. These buttons are designed in such a way that they blend very good with the look of the webpage. All the buttons except the one in the middle of the page are deceptive.

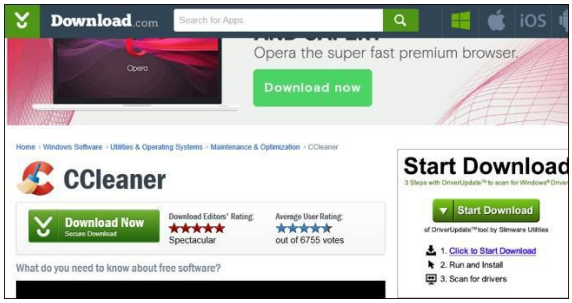


Fig-1.5

Fig-1.5 [7] is a screenshot of a webpage which gives us the file CCleaner.exe. The download button on the bottom left corner gives the required file to the user. All the other download buttons on the webpage are deceptive. The button located at the top middle portion of the page is situates in the middle of a promotion of opera browser. So it's clear that the user won't get the file he was looking for (CCleaner.exe) if he clicks that button. It can be noticed that this page also contains another download button located at the right side portion of the page which is also a deceptive download button. This can be identified by looking closely at the content around it. At a glance it can be noticed that the only thing this content highlights is terms like 'download now' and 'start download' but not any signs of an official developer or any useful software. Basically scan for drivers makes no sense. So, this is a deceptive button for sure.

B. Effects of deceptive buttons on users

Below are some problems faced by users because of deceptive buttons-

- The user might never get the file or information for what he was looking for.
- These buttons are the primary reason for the spreading of malware over the internet
- It is a major waste of time for all the users.
- There is also a very huge chance of the user getting attacked by spyware such as RAT. Such spyware would be coded as an autobot which will have the ability to multiply itself and spread to more number of users.
- The spyware with autobot in it would affect any storage device plugged into the already affected machine and it will also affect the machines to which it will be plugged thereafter.
- The unwanted softwares downloaded by this kind of links can keep running in the background and without the knowledge of the user, it slows down the machine's performance.

III. AVOID AND ELIMINATE DECEPTIVE BUTTONS

This can be achieved in two ways namely, just by using the common sense and the other way is to develop a script or an extension in such a way that it automatically scans the webpage and provides needed information for the user. The detailed information on how to execute the above methods is given below-

A. Use of Common sense

This is the easiest and the most convenient way to avoid deceptive buttons. To identify such buttons, the user must have a good experience browsing through the internet and should have some minimum knowledge about the ads on the internet and of course, "Common Sense".

IJSMS

This is an open access article under the CC BY-SA 4.0 license (https://creativecommons.org/licenses/by-sa/4.0/)

B. Development of a software

A software (maybe as an extension) can be developed to help the users who are new to the internet. It can be developed to guide the user to the correct link on the page. This can be done by highlighting the correct link or by giving some sort of rating on how safe is the link.

Google already does this by just blocking the access to the pages which contains deceptive buttons. Google also intelligently hides the option to continue to that page on user's risk. Even after the user enters the webpage, he is unable to decide where to click to get the information or the file he was looking for. So, despite blocking the whole webpage, this extension can be developed in such a way that it scans the whole page and detects the deceptive buttons by using some basic rules to identify them and using some algorithms based on phishing and data mining. The extension can be developed in such a way that it verifies the safety of the webpage when the mouse pointer is pointed at, so that it is easy for the user to decide which links he shouldn't click on and which are safe to visit. This verification process can be carried out in numerous ways out of which the one is discussed in the following paragraph.

Many websites like [8], [9] and [10] provide us a list of phishing sites and there are many which also provide the list of sites which are safe from phishing. Some pages like [11] help us to examine any link in realtime and provide its safety report. The extension may colour code all the hyperlinks present in a webpage to make it easy for the user. All the links which lead the user to phishing sites can be coloured red. All the safe links can be coloured green. Any sites which aren't listed on either lists can be coloured yellow. Even if the yellow coloured links seem like they make no sense or they are not helpful, these yellow links can be sent to the developer as a feedback and it will be his job to sort them to either one of the lists. [12] lists some online tools to lookup malicious websites.

IV. Drive-by installations

Drive-by installations can be defined as the extra softwares which will be installed with any other software by tricking the user to install it like most of them do or like a few of them, they just get installed without even the notice of the user. The problem of drive-by installations occur when the user gets the file needed for the installation of the software, many of the developers keep extra unwanted software (bloatware) which may also be called as an ad. When this extra software is installed, the developers earn some amount out of it and this amount is paid by the developers of those extra software. There is always a way to deselect the installation of these extra softwares at the time of installation itself but not all the users would know how to do it. This is because the option to disable the installation of these softwares will be presented in such a manner that it is so hard for the users to identify it at a glance.

Such extra softwares can ruin the user's machine sometimes. A few of them are also capable of leaking the user's personal information such as his key logs (A log of each and every key pressed on the keyboard), the information stored in cookies on the user's machine and other sensitive content too. Many of them are also capable of multiplying themselves and spreading to more and more devices automatically.

Few ways used to trick the user into drive-by installations-

- Modifying the name of the bloatware to be almost similar to that of some official software.
- A popup arises suddenly with the button to accept this which would be too noticeable and the button to disable this too small.
- As shown in Fig-4.1 [13], the check boxes for the installation of the extra software's is kept ticked initially even before the user notices it.

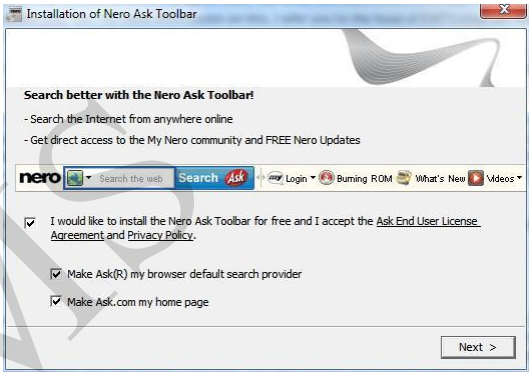


Fig-4.1

As shown in Fig-4.2 [14] , to keep the font colour of the option almost same as that of the background.

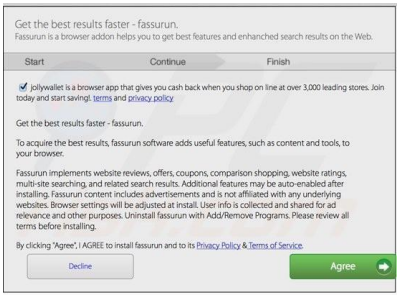


Fig-4.2

As shown in Fig-4.3 [15] , to trick the user by renaming the option to customize installation or quick installation from what it used to be named (disable installation).

To keep the option in some other installation page other than that which contains the description of those extra software's. As shown in Fig-4.4 [16], To keep the font of these options too small which is almost impossible to get noticed in a glance.

This is an open access article under the CC BY-SA 4.0 license (https://creativecommons.org/licenses/by-sa/4.0/)

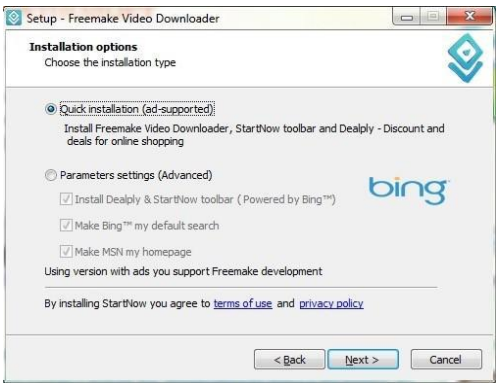


Fig-4.3

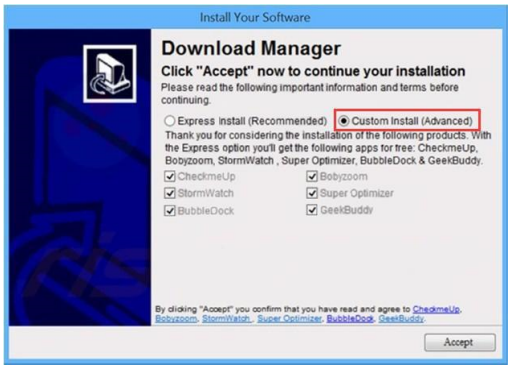


Fig-4.4

As shown in Fig-4.5, few developers keep the design of the unwanted application such that it should look and feel as some important or official software.



Fig-4.5

V. AVOID AND ELIMINATE DRIVE-BY INSTALLATIONS

A script can be developed to guide the users who are novices to the internet and computer. This software can run as a script in the background of the OS. It should be designed in such a way that it will highlight and guide the user for which options he must look while installing any software into his machine. This can be achieved by using some techniques of image to text conversion. When the image is converted to plain text, a system can be built in such a way that it looks for some pre-defined keywords and highlights them automatically when it is found on the screen. An example of this is shown. The below image Fig-5.1 shows a screenshot of the installation of a software. While the main software the user wants to be installed on his machine is FreeStudio, you notice that there are two more drive-by installations namely, ByteFence and Yahoo powered search happening side by side to the main software.

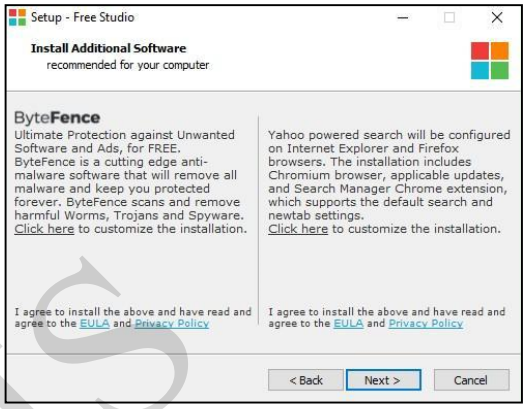


Fig-5.1

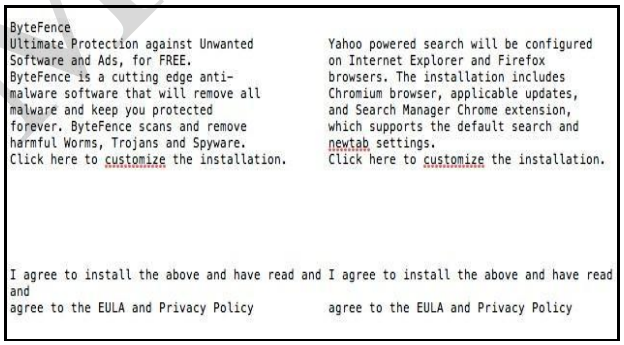


Fig-5.2

If notices properly, we can also find an option which says, “click here to customize the installation”. It takes us to a page where is an option to disable these drive-by installations. So here, “click here to customize the installation” can be taken as a keyword and guide the user to that option, the image can be converted to text as shown in Fig 5.2 for the easy analysis of what is there on the screen.

VI. CONCLUSION

To conclude the above paper, it can be said that deceptive download buttons and drive-by downloads are some of the problems faced by large scale of users browsing through the

IJSMS

This is an open access article under the CC BY-SA 4.0 license (https://creativecommons.org/licenses/by-sa/4.0/)

internet and users who download and install free software's from the web.

The methods suggested in this paper are easy to be implemented and they will be very helpful for the users who are novices. This also prevents the spread of malware to a major extent. This method helps all types of users around the world and the software's developed for these problems can be implemented globally

REFERENCES

[1] Giovanni Armano, Samuel Marchal, N. Asokan, *Real-Time Client-Side Phishing Prevention Add-on*, 2016 IEEE 36th International Conference on Distributed Computing Systems, Page no 777,778.
[2] Mohd. Mahmood Ali, Owais A.W. Siddiqui, Mohd. Nayeemuddin, Lakhsmi Rajamani, *An approach for Deceptive Phishing Detection and Prevention in Social Networking Sites Using Data Mining and WordNet Ontology*, International Conference on Electrical, Electronics, Signals, Communication and Optimization (EESCO) - 2015, 978-1-4799-7678-2/15/$31.00 ©2015 IEEE.
[3] https://3.bp.blogspot.com/
[4] http://www.makeuseof.com
[5] https://2.bp.blogspot.com
[6] https://pbs.twimg.com
[7] http://www.howtogeek.com
[8] https://www.phishtank.com
[9] http://www.malwaredomainlist.com
[10] http://app.webinspector.com
[11] http://www.avgthreatlabs.com
[12] https://zeltser.com/lookup-malicious- websites/
[13] http://blog.emsisoft.com/
[14] https://www.pcrisk.com
[15] http://dantri4.vcmedia.vn/
[16] http://guides.uufix.com

IJSMS

This is an open access article under the CC BY-SA 4.0 license (https://creativecommons.org/licenses/by-sa/4.0/)