1. INTRODUCTION

Malvertising is a pretty new term. It was first coined in 2007. It is extracted from two words malware and advertising. The first malvertising attack was done in 2008. Vulnerability in Adobe Flash was the major cause which affected many platforms like MySpace, and Excite. So, by the meaning definition can be advertising malware is called malvertising. “Malvertising is the use of online advertising to spread malware” [1]. “It typically involves injecting malicious or malware-laden advertisements into legitimate online advertising networks and webpages” [2]. Malware is a term for small pieces of software that aim to do harm to the computer. “There are Three types of malware: viruses, worms and Trojans [3]. They can modify, delete or send files and reduce computer performance. 1 million malware software were created daily in 2014. Through malvertising malwares can be injected to the system just while looking at a website.

Online publishers sell ads through ad networks and exchangers. Utilizing a security flaw ‘flash program’ that is used to display ads cyber criminals use add networks to place infected ads. When viewed by a regular internet user, malware can automatically infect the user system even if they don't click anything. So, the solution to it is use of html5 instead of flash program. Major flaw of advertising is it is unstoppable due to some of the reasons. “Malvertising is attractive to attackers because they 'can be easily spread across a large number of legitimate websites without directly compromising those websites'” [4].

In July 2015 Microsoft first launched windows 10. Which had many new functionalities and many critical updates like Microsoft edge. Windows 10 package also included Cortana an AI based intelligent bot to help the user with internal and external searches and queries. Later on, Microsoft introduced it in my systems.

In malvertising some very known trustworthy companies are also involved. In the beginning they just spread and advertised clean advertisement for the sake of good reputation and when they have gained enough trust of people, they started their job by inserting the malwares behind the advertisements. After fulfilling their purpose, when enough malware got spread and they captured information or spy
of all the users they simply removed the malware from behind for no clue against them in future. That is why their identity is nearly impossible to trace. The other reason of tracing the identity of those is advertisement network is much complex because many links can be related to a single advertisement link [5].

2. EXAMPLES OF MALVERTISING

In this example geekseek.com website is visited that is for the gold prices around the World.

![Fig 1: screen shot of goldseek.com](image)

It can be seen that there are many advertisements on the page. There is nothing with the advertisements. Actually, these advertisements are pointing to an invisible iframe on the page which is point to a shadow gate which is redirecting the user to an Operating system which is compromising the user security [7]. It will evoke a ransom ware which pop ups the message to insert a CD to burn in CD driver. This error is popped up again and again on screen.

![Fig 2: Pop Up Error](image)

It is usually seen during surfing on cell phone suddenly phone displays a pop up. Which might have a message like your phone is seriously damaged or Your battery is badly damaged and phone vibrates badly. At the end of message there is a button displayed with caption, 'Remove the Virus Now' [13]. User gets scared by sudden pop up and vibration scares him more. So as a result, he presses the button and hardware gets damaged or OS vanishes or data is compromised or any sort of problem can occur according to the query in the backend of that button. This is usually done with pirated or suspicious websites but legit websites can also cause this malvertising [6].

![Fig 3: Warnings](image)

3. ANALYSIS

This pie chart is designed by Kaspersky.com. It is seen that in the past malvertising attack was performed using Adobe Flash player but in 2018 its ratio is only 2.4% because most of the websites are using html5 or other methods instead of Adobe flash player. But unfortunately, malvertising hackers have also changed their priorities and methods. They are targeting the advertisements run in browsers as the ratio for browser malware attacks is 23.47% [11]. By considering this chart, it can be seen that ratio for office attacks is alarming. Its ratio is 47.15% which nearly the half of attacks are being done with any sort of tool or technique.
Not only phones and laptop devices but embedded systems and IoT systems are also not safe. This statistic was also taken from Kaspersky.com. It can be clearly seen in the graph that ratio for IoT successful malware attacks in the first half of 2018 is much higher than 2017 [15]. These are three times more done in whole year of 2017. The turnover between 2016 and 2017 was also much higher as it was 10 times the amount targeted in 2016. It is dangerous because people are more relying and focusing to automate their homes, offices, institutes and workplaces also [12].

4. METHODOLOGY

There are many methods and cases of office malwares but most common and most used malware is cortana.exe. So now the question rises that what Cortana.exe actually is. Cortana.exe is not that AI based bot introduced by Microsoft. That Cortana has nothing to do with anything with this. Hackers use the name of Cortana to mask their virus that usually use the resources of the host system for cryptocurrency mining purpose without the knowing of owner of device. Attackers can get access to users' system without logging in using Cortana voice command. Many other illegal tasks can be performed also by using Cortana.exe [14].

The owner will even not know that they have committed a crime. Even if it uses the resources of host only for mining purpose even than it can be very dangerous for device. It takes lots of resources so the devices can be damaged. User should be aware of malvertising issue. Need to pay clear attention to the processes of their system by looking into performance of the system.

5. COUNTERMEASURES

The worst thing is user have nearly nothing to do if it is infected. Although if system is not effected, some counter measures can be imposed.

1. Always pay attention while updating or installing operating system and software’s [3].
2. Always read pop ups and warnings.
3. Always be conscious while surfing over the internet.
4. Try to download programs from official platforms only.
5. Do not use freeware and shareware software’s.
6. Always update installed anti viruses and applications.
7. Do not open the attachments of emails without scanning if not trusted [15].
8. If suspicious that the device is infected use the tools to detect and eliminate the malwares [9].

6. RESULTS

After successful implementation of Countermeasures user can prevent himself from malware-based viruses. Results for that can be seen by using windows task manager which will directly highlight processes against the usage.
7. CONCLUSION

In the digital World full of hackers and scammers, data security is what everyone needs the most. Hackers and scammers invent the new ways of stealing the information on daily basis. A comparatively modern concept in the World of hacking is malvertising.

The worst thing about malvertising is its starting point is just surfing the internet. Surfing can be via browser, any app, Cortana or any other way. User don't need to click on anything. Just opened the page that contains malvertising and user's security will get compromised. There must be a ban on malvertising and strong countermeasures should be taken by international organizations for cyber security enforcement.

8. REFERENCES


