e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
Volume:03/Issue:01/January-2021 Impact Factor- 5.354 www.irjmets.com

# TECHNIQUES TO AVOID WEBCAM HACKING

**Pallavi Suresh Poojary*1**

*1Student, Department of Msc-it Keraleeya Samajham Model College, Dombivli , India.

## ABSTRACT

Now a days many people are using laptops, phones tabs which have in build camera . But are we aware of the fact that there might be a chance that the webcam security has been compromised by some hacker and they might be covertly spying on us through webcam.

There are various cases where the victims webcam security was compromised and the hackers secretly spy on the victim by covertly activating the webcam without victims notice.

A webcam can be prone to attacker due to its vulnerability. Users might sometimes unknowingly download malware from email attachments, phishing websites or even from compromised website.

The purpose of this paper is to investigate which are the techniques which can help the user to prevent webcam hacking which is also known as camfecting.

By collecting and studying various research paper, journal, and websites, the techniques and methods for prevention of camfecting attack are been withdrawn.

**Keywords:** Webcam Hacking, Prevention, Techniques, User.

## I. INTRODUCTION

We live in an era where most of the people own a laptop, computer mobile phones etc. which has webcam . As technology evolved , the ways of hacking in to the users devices has also progressed.

Cyberattacks can happen in a various ways , one such technique is used by the attackers is called as "camfecting" which in simple words is webcam hacking .

This is a method where the attacker infects the users device by using virus that can provide access into the users device camera , to spy on them and then to use the collected video or image against the user.

So to avoid such attack every user of the devices with camera must be aware of the techniques which might help them in prevent camfecting attack

## II. BACKGROUND/LITERATURE REVIEW

A recent study made by Brocker and Checkoway in 2008 demonstrated that video and images can be captured from MacBook and iMac models produced prior to 2008 with the webcam indicator LED disabled.

PALO ALTO, Calif., July 17, 2019 (GLOBE NEWSWIRE) - HP Inc. had released an article ,the results of a unique study that works to better understand the level of awareness associated with webcam hacking and how users changed their behavior as a result.

HP commissioned a survey of approximately 3,000 individuals across North America, including 1,000 US consumers that own a laptop with an integrated webcam

The webcams face the user and have indicator LEDs to notify the user that the camera is on. , this is can alert the user to take defensive actions in the event that the webcam is recording without the their consent. Anecdotal evidence suggests that these assumptions are incorrect Remote Administration Tools (RATs) allow hackers to control an unsuspecting user's computers system and make changes in the LED system and can disable the LED when the webcam is turned on without the users consent.

## III. METHOD AND MATERIALS

- Journals , Newspaper, Case studies and Research papers all related to webcam hacking are been collected analyzed and compared to study what are the methods the attackers are using for hacking the users webcam and what are the methods which need to be followed by the users to avoid their webcam being hacked.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
Volume:03/Issue:01/January-2021 Impact Factor- 5.354 www.irjmets.com

- This research is based on Secondary data

## IV. DATA AND RESULTS

- After surveying through various Research papers , articles of news paper etc, it been noted that most common method used by the attacker for hacking the webcam is Remote Access Trojan (RAT) and Click jacking method .
- According to the cybersecurity expert Mr. Shivam Kapoor , As now a days most of the webcam are in built one it is difficult to analyse the risk . One must always be attentive as the actions could be watched through webcams.
- Most of the times a hidden files are saved in C drive and the hacker may have full access to the system through RAT.
- **Remote Administration Trojans (RATs)**
  It is a piece of code used to remotely access or control a computer. Most of the RATs are capable of camera capture, file access, code execution, registry management, password sniffing etc.
  Most of the time they are patched in email attachment . After infection they perform all unauthorized activities in the system .
  The attacker can remotely control the system by gaining the , webcam feeds, audio footage, screen captures, etc.
- **Clickjacking**
  Clickjacking, also known as a "UI redress attack", is when an attacker uses multiple transparent pages to trick a user into clicking into layered page.
  Thus, the attacker is hijacking clicks which are meant for their page and routing them to another page, most likely owned by another application, or both.
- And the other main thing is that sometimes user buy a second hand laptops or desktops which might contain malicious code , knowingly or unknowingly downloaded by the previous owner
  This might poses a threat to security on user's privacy .

❖ **Prevention method for webcam hacking**

After surveying through the news articles , journals and research paper written by a cyber security expert .

After comparing through these article , there are few common and important measures mentioned by them which might help the users to protect there device from webcam hacking.

- First to avoid as much as possible to click or visit suspicious websites.
- Not to click on the email messages with suspicious attachments .
- Always cover the webcam of the laptop with dark patch .
- If the camera is not in built in the computer then try disabling the cable between them when not in use.
- If have a second hand laptop make sure that the laptop disk is been cleaned properly.
- Always keep the software and the operating system of the system always up to date.
- Download legitimate antivirus software
- Always try shutting down your system when not in use.

## V. DISCUSSIONS

The main purpose of this paper was to determine what are main prevention methods which can be used by the users which can protect them from camfecting.

Most of the time attacker use simple and easy way of hacking the users webcam is by just sending malicious messages through email

Users who are unaware might access the email by just clicking the message.

After that the malicious code gets downloaded into the user system on its own without users knowing about it .

That malicious code which is known as Trojan helps the attacker to get access into the user system. And then the attacker start accessing the webcam and uses it against user privacy.

That's why it is suggested in article and research written by many cyber experts that the user must never access the email messages or websites which they feel might be suspicious and to always clear there spam inbox in their gmail account.

These kind of attacks can be avoided by installing firewalls in the system. These firewalls can keep the users system from being attacked by hackers.

Click jacking can be also prevented by the using the same techniques mentioned for RAT attack. The main thing is that users must be made aware of such attacks so that they can prevent such attacks and can be careful about it.

According to a study conducted by Kaspersky Lab and B2B International, 21 percent of users cover their webcams by a patch or tape because they are scared that the attacker might be spying on them through camera. In some other countries the rate is even higher than this. Chinese users are also aware of the webcam attack The study found that nearly a quarter of users (24 percent) are completely unaware that they could be watched via a webcam. Only 44 percent of respondents are aware of webcam attack and admit that the possibility of webcam hacks makes them feel uncomfortable. It's important to remember that hackers do not exclusively target public figures – anyone is potentially of interest.

## VI. CONCLUSION

First thing is that the users must be made aware about what webcam hacking is and what are its consequences so that the users would be always on alert while using there system and would not commit mistake which would be a positive point for the attacker.

And then they must be made aware of the prevention methods which will help them in keeping their system safe .

The methods for preventing such attacks are easy and simple to follow on daily basis .

- The most effective way to keep the webcam from covertly spying on the user is to patch the webcam with dark tape ,
- If the webcam is an independent one then the user can unplug the cable of the camera from the system , when not in use .
- Always keep the system up to date.
- Install a firewall which will help the system from being attacked.
- Always clear the spam messages in the gmail account.
- If the system is an second hand system then make sure to clean the system before using them and install an antivirus.
- Always shutdown the system when not in use .
- Avoid clicking suspicious websites and gmail attachments.

## ACKNOWLEDGEMENTS

I would like to express my special thanks of gratitude to all my teachers for their able guidance and support in completing my research

I also like to extend my gratitude to the Principal Sir "Dr. Vinay .G. Bhole" for helping me with all the facility that was required.

## VII. REFERENCES

[1] Abowd, G. D., and Mynatt, E. D. Charting past, present, and future research in ubiquitous computing. ACM Transactions on Computer-Human Interaction (TOCHI) 7, 1 (2000), 29–58.

[2] Anderson, N. Meet the Men Who Spy on Women through Their Webcams. http://arstechnica.com/tech-policy/2013/03/ratbreeders-meet-the-men-who-spy-on-womenthrough-their-webcams/, March 10 2013. Accessed: September 5, 2014.

[3] Jones, A. & Gagneja, Kanwalinder. (2016). Preventing Covert Webcam Hacking in the Civilian and Governmental Sectors. 993-998. 10.1109/CSCI.2016.0190.

[4] Rebecca S. Portnoff1 , Linda N. Lee1 , Serge Egelman1,2, Pratyush Mishra1 , Derek Leung1 , and David Wagner1 1University of California, Berkeley, CA {rsportnoff,lnl,egelman}@cs.berkeley.edu, {pratyushmishra,derek.leung}@berkeley.edu 2 International Computer Science Institute, Berkeley, CA, egelman@icsi.berkeley.edu

[5] Egelman, S., Cranor, L. F., and Hong, J. You've been warned: an empirical study of the effectiveness of web browser phishing warnings. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, ACM (2008), 1065–1074

[6] Rouse, R. A. Is someone watching you through your webcam? http://campatch.com/wpcontent/uploads/2012/05/CamPatch-AcademyStudy-on-Webcam-Hacking-Awareness-May2012.pdf, May 2012.

[7] Friedman, B., Hurley, D., Howe, D. C., Felten, E., and Nissenbaum, H. Users' conceptions of web security: A comparative study. In CHI '02 Extended Abstracts on Human Factors in Computing Systems, CHI EA '02, ACM (New York, NY, USA, 2002), 746–747.

[8] Check Point Software Technologies Ltd. Are You Being Watched Through Your Webcam? http://www.zonealarm.com/blog/2013/10/are-youbeing-watched-through-your-webcam/, October 2 2013. Accessed: September 6, 2014.

[9] Cannella, S., Polivy, D. J., Shin, M., Straub, C., and Tamassia, R. Secure Visualization of Authentication Information: A Case Study. In Visual Languages and Human Centric Computing, 2004 IEEE Symposium on, IEEE (2004), 35–37.

[10] One In Five Users Cover Their Webcams Due To Spying Fears. https://www.siliconindia.com/news/enterpriseit/one-in-five-users-cover-their-webcams-due-to-spying-fears-nid-173974-cid-7.html

[11] Top cybersecurity facts, figures and statistics for 2020 By Josh Fruhlinger https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html