Taping over your webcam - paranoia or precaution? - blueAPACHE

Canonical: https://www.blueapache.com/blog/taping-over-your-webcam-paranoia-or-precaution

Details:

Summary

This blueAPACHE post reports: Should you be taping over your webcam and microphone? Facebook CEO, Mark Zuckerberg, recently posted a photo of himself celebrating Instagram’s 500 million monthly user milestone. It concerns emPOWER Security, Human Risk Management, Managed Detection & Response. Published in 2016. Figures, product names and event details reflect that time; for current information see the linked service pages.

Key facts

Label	Value
Publication year	2016
Services referenced	emPOWER Security, Human Risk Management, Managed Detection & Response
Topic	Taping over your webcam - paranoia or precaution?

Article

Should you be taping over your webcam and microphone? Facebook CEO, Mark Zuckerberg, recently posted a photo of himself celebrating Instagram’s 500 million monthly user milestone. The photo ended up revealing more than he may have intended, as the unforgiving eyes of social media users quickly picked up that Zuckerberg’s camera and microphone port on his Mac Book were both covered with tape. People were quick to point out the irony of the situation considering Facebook has been battling privacy issues and concerns from their users in recent years. Irony aside, the pertinent question was if the CEO of the world’s largest social media site, with an army of security and technology experts at his disposal, is resorting to a DIY security solution of taping his webcam, where does that leave us humble everyday users? Zuckerberg has now joined Federal Bureau of Investigation (FBI) Director James Comey and National Security Agency (NSA) whistleblower Edward Snowden who have been known to tape their webcams in hope of stopping hackers capturing video or photographs without their knowledge. Webcam hacking supposedly occurs frequently, both through hacking channels and government agencies. US Intelligence agencies including the FBI have admitted hacking computers to access webcams in order to spy on targets. Back in 2008, the Edward Snowden leaks revealed details on Optic Nerve – the NSA’s project to capture webcam images every five minutes from random Yahoo users. Remote hackers use malware like Remote Access Trojan (RAT) to access a computer, take control of the webcam and microphone to capture information and send it to remote location. Hackers can turn off the webcam and microphone indicator lights and notifications so that the user is never alerted that their device is now remotely spying on them. RAT malware is typically distributed through

phishing (click-on-this-link email) campaigns. It can also be installed directly onto a target computer where the physical address is known. Considering the extent of the hacks and ability to mask notifications, Zuckerberg’s taping of his webcam may not seem as paranoid as it initially sounded. According to a survey conducted by Kaspersky Lab, he is not alone. The survey showed near 35 percent of users cover their webcam with a band aid or post-it note and around 4 percent use duct tape. While this might prevent hackers from watching you or capturing live feeds, it will not protect your voice from being recorded. As with any other form of IT security, the fundamental form of protection is prevention through user awareness. It is good practice to scrutinise any links or suspicious emails you may receive and not be tricked into installing any software from dubious sources. To learn more about identifying security threats and educating staff on how to spot social engineering, whaling and phishing attacks, contact the blueAPACHE account team .

Related

emPOWER Security

emPOWER Security (pillar)

Human Risk Management

Managed Detection & Response

Frequently asked questions

Whose photo triggered the discussion in this article, and what did observers notice?

The article was triggered by a photo Mark Zuckerberg posted celebrating Instagram's 500 million monthly user milestone, in which social media users noticed his MacBook's camera and microphone port were both covered with tape.

What survey figures does the article cite on how many users cover their webcams?

The article cites a Kaspersky Lab survey finding around 35 percent of users cover their webcam with a band aid or post-it note, and around 4 percent use duct tape.

What NSA program does the article name in relation to webcam surveillance?

The article names Optic Nerve, the NSA project revealed by the Edward Snowden leaks that captured webcam images every five minutes from random Yahoo users.

What malware type does the article say is typically used for remote webcam hacking, and how is it distributed?

The article says Remote Access Trojan (RAT) malware is used to take control of a webcam and microphone remotely, and that it is typically distributed through phishing email campaigns or installed directly when the target's physical address is known.

Is the information in this post still current?

No. It reports a specific 2016 discussion prompted by a Mark Zuckerberg photo; for blueAPACHE's current security awareness guidance, see the emPOWER Security pillar page rather than this post.

Source

https://www.blueapache.com/blog/taping-over-your-webcam-paranoia-or-precaution/

Knowledge Base

What incident prompted the blueAPACHE article about taping over webcams?

Facebook CEO Mark Zuckerberg posted a photo celebrating Instagram's 500 million monthly user milestone, and social media users noticed that the camera and microphone port on his MacBook were both covered with tape.

Who else besides Mark Zuckerberg has been known to tape their webcams, ?

Federal Bureau of Investigation (FBI) Director James Comey and National Security Agency (NSA) whistleblower Edward Snowden have also been known to tape their webcams, in hope of stopping hackers from capturing video or photographs without their knowledge.

What did the Edward Snowden leaks reveal about webcam surveillance?

The Edward Snowden leaks, back in 2008, revealed details on Optic Nerve — the NSA's project to capture webcam images every five minutes from random Yahoo users.

How do remote hackers typically gain access to a computer's webcam and microphone?

Remote hackers use malware like Remote Access Trojan (RAT) to access a computer and take control of the webcam and microphone to capture information and send it to a remote location. RAT malware is typically distributed through phishing campaigns, or it can be installed directly onto a target computer where the physical address is known.

How do hackers avoid alerting users that their webcam is being remotely accessed?

Hackers can turn off the webcam and microphone indicator lights and notifications so that the user is never alerted that their device is remotely spying on them.

What did the Kaspersky Lab survey find about users covering their webcams?

According to a survey conducted by Kaspersky Lab, near 35 percent of users cover their webcam with a band aid or post-it note, and around 4 percent use duct tape.

Does covering a webcam protect against all forms of surveillance, ?

No — while covering a webcam might prevent hackers from watching you or capturing live feeds, it will not protect your voice from being recorded.

Who should you contact to learn more about identifying security threats like phishing and whaling, ?

The article recommends contacting our account team to learn more about identifying security threats and educating staff on how to spot social engineering, whaling and phishing attacks.