

Countermeasures against camera vulnerabilities

Student Gheorghe Daniel Razoare
Supervisor Dr Kapilan Radhakrishnan

BACKGROUND

- Too little attention has been paid to this subject;
- In 2008, “Operation Optic Nerve”, a project launched by British Intelligence was used to capture and store millions of pictures captured through Yahoo Messenger;
- 2010, in United States, Pennsylvania, a remote monitoring software installed by school district on 2.300 Macbooks was used to capture images of students at home;
- 2013, Miss Teen USA, Cassidy Wolf was spied by one of her former classmates. He installed on her laptop Blackshades RAT malware;

WHAT IS “CAMFECTING”



Camfecting, in the field of computer security, is the process of attempting to hack into a person's webcam and activate it without the webcam owner's permission

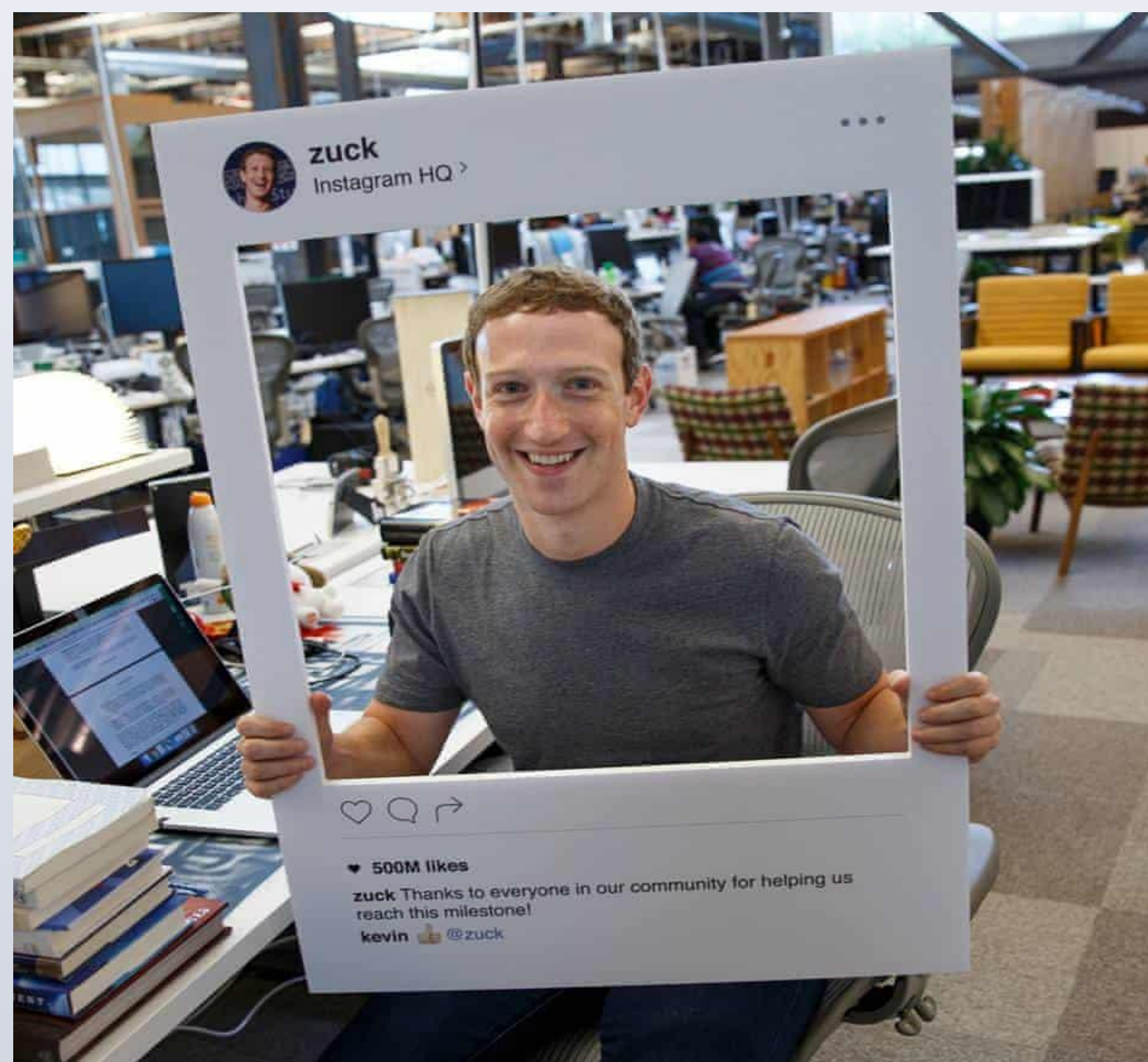
The most common webcam intrusion procedures can be made using Remote Administration Tool (RAT)

Examples of RAT Tools:

- » Luminosity Link
- » Nanocore
- » Black Shades,
- » Plasma
- » Dark Comet

KNOWN COUNTERMEASURES

- Webcam cover



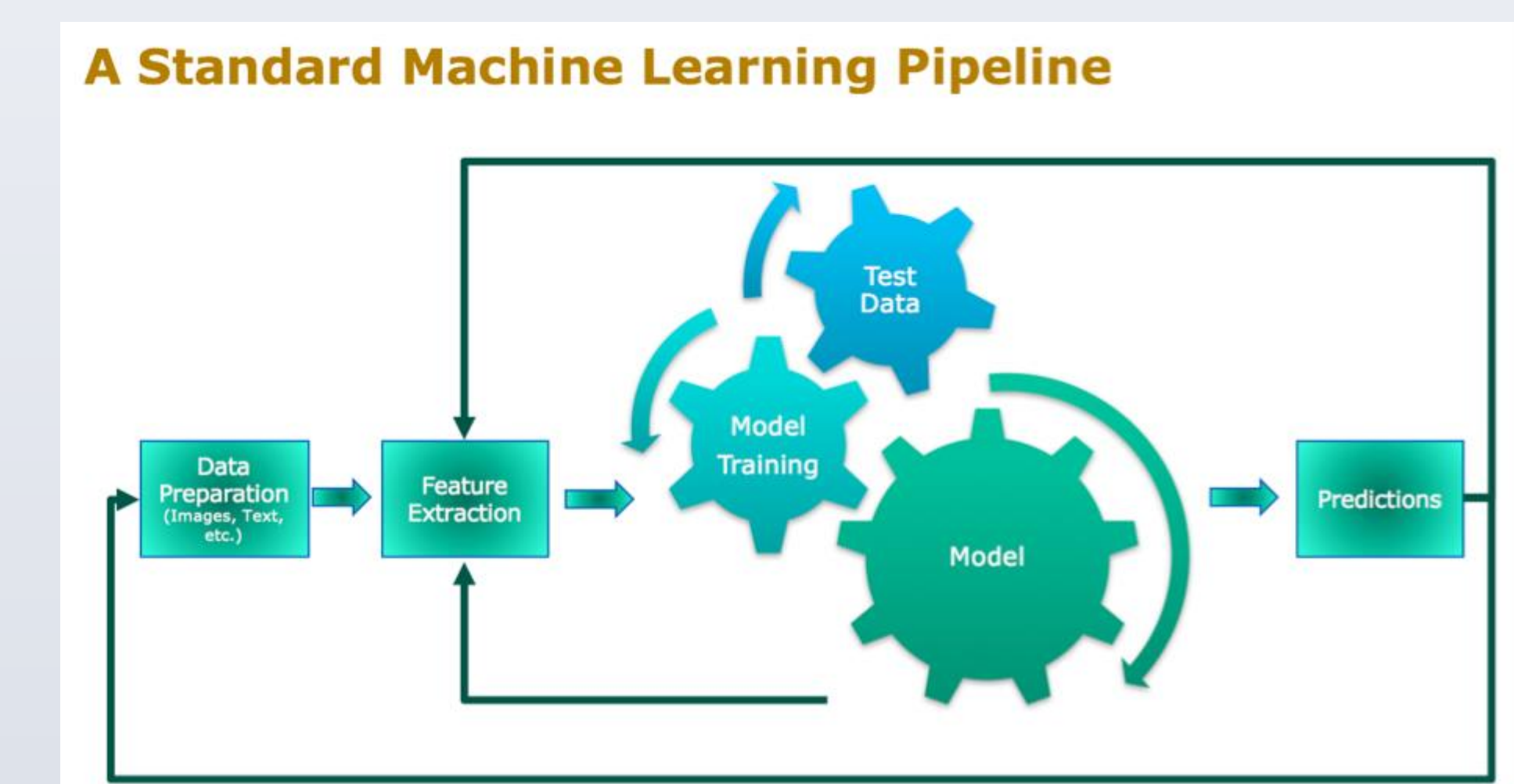
- Antivirus and antispyware
- Firewall
- Avoiding click on suspicious links or Opening E-mail Attachments From Unknown Sources
- VPN

ONS SURVEY

In the year ending in March 2018, the ONS UK Office for National Statistics ()estimates that around 4.5 million cybercrimes were committed in England and Wales during that twelve month period. Of those, around 3.24 million were fraud offences, and about 1.23 million were related to computer misuse (encompassing child pornography and hacking).

AIMS

- To investigate the use of machine learning algorithms in webcam traffic detection.



OBJECTIVES

Main objective: To produce open source software for unauthorised audio and video traffic detection

Secondary objective: To find new methods for detection and prevention along the research process

METHODOLOGY

- A lab environment will be created using virtual machines;
- Machine learning algorithms will be implemented to analyse traffic patterns;
- The outcome of virtual lab will be tested in real network environment;