Computing

Lesson 4: Rise of the Bots

Cybersecurity

Ben Garside

Task 1: Malware quick read

Your local cybersecurity police force want you to make a quick read fact sheet to help educate the public on malware.

Pick one of the following to research:

- Viruses
- Worms
- Ransomware
- Trojans

You will need to:

1. Research the malware to give information as to what is it.
2. Describe how it would break the Computer Misuse Act (see notes from the previous lesson).
3. Find a case study about where the malware was used and what impact it had.

Task 1 - Malware quick read

The websites on the next two slides will help you with this task.

Please ask a parent or carer for permission before attempting this task.
Oak National Academy are not responsible for any third party content.

Task 1 - Malware quick read

Viruses

- oaknat.uk/comp-virus-wiki
- oaknat.uk/comp-virus-example-wiki
- oaknat.uk/comp-norton-virus

Worms

- oaknat.uk/comp-worm-wiki
- oaknat.uk/comp-norton-worm
- oaknat.uk/comp-comodo-worm

Task 1 - Malware quick read

Ransomware

- oaknat.uk/comp-ransomware-wiki
- oaknat.uk/comp-ransomware-mb
- oaknat.uk/comp-norton-malware

Trojans

- oaknat.uk/comp-trojan-wiki
- oaknat.uk/comp-norton-trojan
- oaknat.uk/comp-kaspersky-trojan

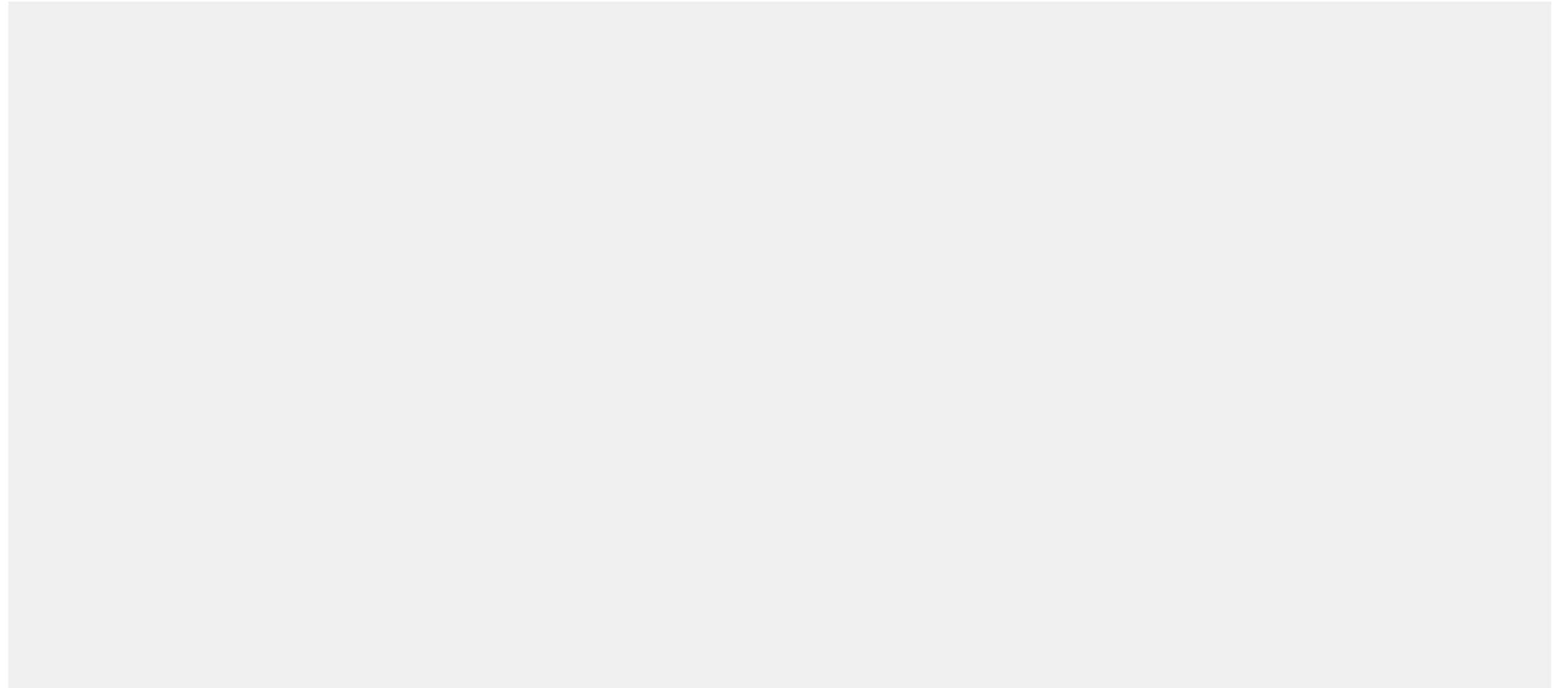# Malware: [insert malware type here]

What is [insert malware here]?

What the law says

Malware: [insert malware type here]

Case study

[Malware] in the real world (Explorer task)

Task 2: Botnet

"We have identified a total of 50,258 automated accounts that we identified as Russian-linked and tweeting election-related content during the election period."

Source: blog.twitter.com/official/en_us/topics/company/2018/2016-election-update.html

What are the potential consequences of 50,258 automated accounts (non-human users) posting election-based content?