1. Introduction To Your Malware Type (**Trojans, Rootkits, Botnets**) . You should have at least one quality resource for each topic.

Trojans: It must be done by the victim in order to work. They look like actual programs but instead they contain certain instructions that makes you to run a certain program on your pc. Example: fake antiviruses programs that instruct you to run a program to clean the pc.

Rootkits: modifies the operating system to take total control of a computer using a stealth program which is made to control computers without being detected by security programs or the users themselves

Botnets: These are infected computers which become part of many hostile networks and then become under control by a botnet master.

a) What it does to an infected computer / user

Trojans: <https://blog.malwarebytes.com/cybercrime/2013/06/what-are-trojans/>, <https://youtu.be/jkoMYFOkozw>

Rootkits: <https://www.veracode.com/security/rootkit>

Botnets: <https://us.norton.com/internetsecurity-malware-what-is-a-botnet.html>

b) How it infects a computer

Trojans: <https://itstillworks.com/do-trojan-horses-computer-6526732.html>

Rootkits: <https://www.guidingtech.com/4467/what-is-a-rootkit/>

Botnets: <https://www.jolera.com/how-botnets-infect-your-computers/>

c) How it spreads

Trojans: <https://enterprise.comodo.com/how-are-trojan-horses-spread.php>

Rootkits: <https://www.youtube.com/watch?v=0LvF0KtBWxY>

Botnets: <https://www.youtube.com/watch?v=s0sgiY93w9c>

d) How it is different from other types of malware

<https://tools.cisco.com/security/center/resources/virus_differences#:~:targetText=Trojans,Greeks%20used%20to%20infiltrate%20Troy.&targetText=Trojans%20are%20also%20known%20to,nor%20do%20they%20self%2Dreplicate.>

e) How to detect this type of malware

Trojans: <https://enterprise.comodo.com/forensic-analysis/how-to-detect-trojan-virus-on-computer.php>

Rootkits: <https://www.varonis.com/blog/rootkit/#:~:targetText=A%20surefire%20way%20to%20find,reliable%20methods%20of%20detecting%20rootkits.>

Botnets: <https://www.alienvault.com/blogs/security-essentials/botnet-detection-and-removal-methods-best-practices>

f) How to remove this type of malware

Trojans: <https://www.youtube.com/watch?v=gC1m0ADkdWA>

Rootkits: <https://www.mcafee.com/enterprise/en-ca/downloads/free-tools/how-to-use-rootkitremover.html>

Botnets: <https://www.youtube.com/watch?v=PVWEv9eE6ds>

2. News report(s) of specific case/outbreak of your malware

<http://news.bbc.co.uk/2/hi/technology/7701227.stm>

a) Summarize what happened

The details of around 500000 online bank accounts information, credit and debit card information have been stolen by a trojan virus. The effect was near global as over 200 domains were damaged.

b) When and where it happened

This occured in 2008. Took place globally as many computers worldwide were affected. Although the information was taken specifically from US, UK, Australia, Poland.

c) Its affects: computers infected / countries attacked / financial damage

It caused financial damage as almost 270000 banking accounts were compromised as well as 240000 credit and debit cards from financial institutions. It also massively affected computers because the group made sure to put in a lot of infrastructure because the return and potential return was so great. Also they stayed ahead of detection as they periodically released new variants to keep a grip on the infected computers

d) Who was responsible (if available)

The sinowal trojan was tracked down by the The RSA which helped secure networks for 500 companies. There was not anyone who was found involved but it was said that no Russian accounts were hit by the sinowal trojan. Most of the evidence was leading to Russia and eastern Europe because there were connections from the past with online gangs to the russian buisness network.