Computer Security (COM-301)
Monday Live exercises
Malware

Carmela Troncoso
SPRING Lab
carmela.troncoso@epfl.ch

Winnie the Defender

You get hired as new security engineer at Pooh Technologies. On your first day they tell you that during the last week some of the employees laptops have been experiencing attacks, but a pattern has not been found yet.

What would you add to the network to help the team to stop the attack?

A Bastion host, a honeypot, or an Intrusion Detection System

The Bots are coming

Part 1. Agree or disagree with the following statement: *"Running an antivirus based on signatures on all machines within a company's internal network provides protection against a Botnet that attacks your company's network from the outside"*

Part 2. If you agree, provide a way for Botnets to bypass the defense. If you disagree, provide an alternative defense mechanism that would provide protection against Botnet attacks

Vaccine designer

After taking an entrepreneurship class, Alice registers a new start-up that designs and sells antivirus. In her first attempt to building an antivirus, Alice gathers a large data set of viruses and hashes their binary. Whenever the antivirus scans a program, it hashes the binary and checks whether this hash is a known virus.

Describe one method to bypass this antivirus, and a countermeasure

True of False

a) A star topology with one command and control station connected to all bots enables perfect control over the bots. Therefore it is a robust choice to configure a botnet.

b) Ransomware is a malware that threatens to destroy a computer's content unless the owner pays an economical compensation.

c) Eliminating buffer overflows would erradicate worms

d) Once a Trojan is installed in your laptop, it will automatically steal your data