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

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

Possible answer:
The pattern is not known. Therefore, one needs to either:

- learn the pattern: by using a honeypot to learn how the attack works; or
- detect patterns that are not legitimate by using an anomaly-based Intrusion Detection System

A bastion host would not be a first thing to add, as if you don't know what the attack pattern is you cannot configure/defend the bastion host against it.

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

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"*

Possible answer:
Disagree. Botnets are external machines. Antivirus within the network will not remove the malware from the bots. (partial points were given for saying that it reduces the damage from the bots)

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

Possible answer:
An Intrusion Detection System (detect anomalous behaviour from the botnet)
Or a Honeypot, to learn how the botnet works, find the C&C and dismantle it

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

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

Possible answer:
Alice's antivirus is based on a hard check of equality (the hash function provides a deterministic unique representation of the code). Any change in the code will result on a change in the hash and therefore bypass the antivirus.

A countermeasure would be to, instead of focus on the code, focus on the operation of the virus, creating a heuristic-based antivirus.
Saying that the antivirus creates signatures or regexp of particular parts of the virus that cannot change (e.g., because the functionality is key to the malicious activity) would also be accepted.

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

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.

False. While it is convenient and efficient, having only one C&C is not robust. It is a single point of failure. If that computer is taken down, the botnet cannot be managed anymore.

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

True. Ransomware is a malware that encrypts your hard drive, effectively destroying the content from your point of view
False because it does not threaten to destroy, it destroys directly (by encrypting)
False because it does not necessarily request economic compensation

c) Eliminating buffer overflows would erradicate worms

False. Buffer overflow is just one of the multiple security vulnerabilities worms can exploit.

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

False. It will not automatically steal the data, it needs the program to run
True. The trojan can start stealing during installation (there is no evidence that any real Trojan has ever worked like that, but it is a valid answer given the specification)