Software Vulnerabilities: Exploitation and Mitigation
Video 5: Cyber Arms Race

Artem Kaliahin
artem.kaliahin.001@student.uni.lu

April 2019

Question 1.1 Who is Mikko Hypponen?

Mikko Hypponen is CRO working in FSecure in Finland. He's been analyzing the first virus in the history "Brain" back to 1986.

Question 1.2 Who did he visit in 2011?

He visited brothers Basit and Amjad Alvi in Pakistan. They created the world's first computer virus.

Question 1.3 For which operating system was the virus written?

Virus was written for DOS.

Question 1.4 How did the virus propagate?

"Brain" was distributed with help of the people travelling around the world in possession of infected floppy disks.

Question 1.5 Why did they write a virus?

They wanted to explore security rules of the DOS in comparison with UNIX OS. They wanted to know how vulnerable the new operating system (DOS) was.

Question 2.1 What is Stuxnet?

Stuxnet is a large and complex piece of malware spreading on USB-sticks that was supposed to attack particular industrial control system.

Question 2.2 Why is there a before and an after Stuxnet?

Because it was massively complex piece of malware and it was unique and first of kind that days.

Question 2.3 When was Stuxnet discovered and analyzed?

It was discovered and analyzed in summer 2010.

Question 2.4 How many zero-days did Stuxnet contain?

According to the video, there were 3 zero-days vulnerabilities. According to Wikipedia - 4 vulnerabilities.

Question 2.5 How did Stuxnet know it's running in the "target" environment?

Stuxnet had a fingerprint it was searching for. It's been looking for a specific configuration of factory's power converters. This configuration has leaked simply through the Iran's government website.

Question 2.6 Why are governments, intelligent agencies and the militaries interested in offensive use of cyber power?

It is cheaper than alternatives (affordable), it gets the job done (effective) and IAs can deny that they used it (deniable).

Question 2.7 How could one know the configuration of the nuclear power plant?

Configuration of nuclear power plants aren't get distributed over the internet usually. It simply leaked from the website with pictures of Iran's president visit to power plant and configuration accidentally got on the picture so attackers could reconstruct it.

Question 2.8 Is using a Stuxnet a cyber-war? Why or why not?

No, it's not. At that time there was no war between supposed attackers (US and Israel) and a target (Iran). Instead of cyber-war, Stuxnet was a cyber-sabotage.

Question 2.9 How was Petya propagated to infect computers?

Attackers used and update server of medoc.ua website to ship an update to every customer running this company's software. That update was Petya and it started distributing all over the network.

Question 2.10 Why have non-ukrainian companies also been affected by Petya?

Because all the companies that had branches or were registered in Ukraine had to file taxes in Ukraine and they used this software which had Petya in the patch.

Question 2.11 How did Maersk recover from the lost of the authentication servers?

There was only one Maersk server that was offline (so it wasn't affected by Petya) on June 29th (date of Petya patching) that had back-up. It was in Ghana and it was turned off due to power outage.

Question 2.12 What is the most expensive computer accident in history?

Petya virus was the most expensive computer incident in history.

Question 2.13 What is the average time for a company to detect it has been breached?

200 days is the average time for company to detect data leakage or itself being hacked.

Question 2.14 What to do when the network (the safe) has been breached?

It would be nice to have security information and event management software (e.g. Qradar) that allows you to prevent or at least detect breach (equivalent to motion radar in safe).

Question 2.15 What is the Hypponen's Law?

Whenever and appliance is described as "smart", it's vulnerable.

Question 2.16 How did the attackers get access to the credit card terminals?

Attackers got access to the network through ventilation system controlling linux-servers first. Then they gained access to financial network of the company hence to the CC-terminals.

Question 2.17 Why do recent botnets such as Mirai infect IoT devices?

Because IoT devices have enough power and bandwidth to perform any kind of attack (e.g. denial-of-service attack).

Question 2.18 We know how to patch computer systems. But do we know how to "patch" people?

No. People don't usually learn on theirs mistakes, so they are completely "unpatchable".

Question 2.19 Why is there a job security in security?

It's hard to explain to some people how to be "secure" and why security matters in a modern world so these people become the weakest link in the security chain. That's why security professionals are in high demand and have low chances to lose their job if they do it well.

Question 2.20 Do you agree with the pessimistic view that all smart devices are vulnerable?

Actually, yes. Because everything in this world is vulnerable, it depends on the context in which we define this notion. There are no invulnerable systems in general. These systems can be protected only from certain kinds of attack.