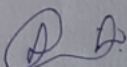


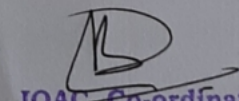
BLDE Association's  
S B Arts and KCP Science College, Vijayapur  
Re-accredited at 'A' by NAAC  
Department of BCA

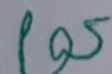
Date:20/09/2016

## NOTICE

It is here by informed to all the BCA students to attend the "Ted Talk" on 21/09/2016 at 3.15 pm in M.Sc class room . All the students should be present on time.

  
**Co-ordinator**  
BCA Programme  
S.B.Arts & K.C.P.Science College,  
Vijayapur.

  
**IOAC, Co-ordinator**  
S.B.Arts & K.C.P.Science College,  
Vijayapur.

  
**Principal**  
S.B.Arts & K.C.P.Science College,  
Vijayapur.

Contd..

B.L.D.E.Association's  
S.B.Arts and K.C.P Science College,Vijayapur  
Department of BCA

**TED-TALK REPORT**



***Mikko Hypponen - Fighting viruses defending the net***

No. of student's attd: **45 (UG/BCA)**

Date of Webinar: **21/09/2016**

Webinar conducted at **M.Sc.-Classroom**

Conducted by: **Prof. Smt. S D Patil**

Time: **03:15 PM**

Duration: **18 min**

*contd. -*

## TED-TALK REPORT

### *Mikko Hyppönen - Fighting viruses defending the net*

No. of student's attd: 45 (UG/BCA)

Conducted by: Prof. Smt. S D Patil

Date of Webinar: 21/09/2016

Time: 03:15 PM

Webinar conducted at M.Sc.-Classroom

Duration: 18 min

*Link* : [https://www.ted.com/talks/mikko\\_hypponen\\_fighting\\_viruses\\_defending\\_the\\_net?language=en](https://www.ted.com/talks/mikko_hypponen_fighting_viruses_defending_the_net?language=en)

#### **About:**

It's been 25 years since the first PC virus (Brain A) hit the net, and what was once an annoyance has become a sophisticated tool for crime and espionage. Computer security expert Mikko Hyppönen tells us how we can stop these new viruses from threatening the internet as we know it.

#### **Subtitles and Transcript:**

<u>Time</u>	<u>Content</u>
1:07	So let me show you something. This here is Brain. This is a floppy disk -- five and a quarter-inch floppy disk infected by Brain.A. It's the first virus we ever found for PC computers. And we actually know where Brain came from. We know because it says so inside the code. Let's take a look. All right. That's the boot sector of an infected floppy, and if we take a closer look inside, we'll see that right there, it says, "Welcome to the dungeon." And then it continues, saying, 1986, Basit and Amjad. And Basit and Amjad are first names, Pakistani first names. In fact, there's a phone number and an address in Pakistan.
2:14	Now, 1986. Now it's 2011. That's 25 years ago. The PC virus problem is 25 years old now. So half a year ago, I decided to go to Pakistan myself. So let's see, here's a couple of photos I took while I was in Pakistan. This is from the city of Lahore, which is around 300 kilometers south from Abbottabad, where Bin Laden was caught. Here's a typical street view. And here's the street or road leading to this building, which is 730 Nizam block at Allama Iqbal Town. And I knocked on the door. (Laughter) You want to guess who opened the door? Basit and Amjad; they are still there. (Laughter) (Applause) So here standing up is Basit. Sitting down is his brother Amjad. These are the guys who wrote the first PC virus. Now of course, we had a very interesting discussion. I asked them why. I asked them how they feel about what they started. And I got some sort of satisfaction from learning that both Basit and Amjad had had their computers infected dozens of times by completely unrelated other viruses over these years. So there is some sort of justice in the world after all.

BLDEA's S B Arts and K C P Science college, Vijayapur.

Contd..

4:07 For example, let's go with the Centipede virus first. And you can see at the top of the screen, there's a centipede scrolling across your computer when you get infected by this one. You know that you're infected because it actually shows up. Here's another one. This is the virus called Crash, invented in Russia in 1992. Let me show you one which actually makes some sound. (Siren noise) And the last example, guess what the Walker virus does? Yes, there's a guy walking across your screen once you get infected. So it used to be fairly easy to know that you're infected by a virus, when the viruses were written by hobbyists and teenagers.

5:50 So where are all these coming from then? Well today, it's the organized criminal gangs writing these viruses because they make money with their viruses. It's gangs like -- let's go to GangstaBucks.com. This is a website operating in Moscow where these guys are buying infected computers. So if you are a virus writer and you're capable of infecting Windows computers, but you don't know what to do with them, you can sell those infected computers -- somebody else's computers -- to these guys. And they'll actually pay you money for those computers. So how do these guys then monetize those infected computers? Well there's multiple different ways, such as banking trojans, which will steal money from your online banking accounts when you do online banking, or keyloggers. Keyloggers silently sit on your computer, hidden from view, and they record everything you type. So you're sitting on your computer and you're doing Google searches. Every single Google search you type is saved and sent to the criminals. Every single email you write is saved and sent to the criminals. Same thing with every single password and so on.

7:50 One example of how these guys actually are capable of monetizing their operations: we go and have a look at the pages of INTERPOL and search for wanted persons. We find guys like Bjorn Sundin, originally from Sweden, and his partner in crime, also listed on the INTERPOL wanted pages, Mr. Shaileshkumar Jain, a U.S. citizen. These guys were running an operation called I.M.U., a cybercrime operation through which they netted millions. They are both right now on the run. Nobody knows where they are. U.S. officials, just a couple of weeks ago, froze a Swiss bank account belonging to Mr. Jain, and that bank account had 14.9 million U.S. dollars on it.

8:32 So the amount of money online crime generates is significant. And that means that the online criminals can actually afford to invest into their attacks. We know that online criminals are hiring programmers, hiring testing people, testing their code, having back-end systems with SQL databases. And they can afford to watch how we work -- like how security people work -- and try to work their way around any security precautions we can build. They also use the global nature of Internet to their advantage. I mean, the Internet is international. That's why we call it the Internet.

9:10 And if you just go and take a look at what's happening in the online world, here's a video built by Clarified Networks, which illustrates how one single malware family is able to move around the world. This operation, believed to be originally from Estonia, moves around from one country to another as soon as the website is tried to shut down. So you just can't shut these guys down. They will switch from one country to another, from one jurisdiction to another -- moving around the world, using the fact that we don't have the capability to globally police operations like this. So the Internet is as if someone would have given free plane tickets to all the online criminals of the world. Now, criminals who weren't capable of reaching us before can reach us.

9:54 So how do you actually go around finding online criminals? How do you actually track them down? Let me give you an example. What we have here is one exploit file. Here, I'm looking at the Hex dump of an image file, which contains an exploit. And that basically means, if you're trying to view this image file on your Windows computer, it actually takes over your computer and runs code.

10:16 Now, if you'll take a look at this image file -- well there's the image header, and there the actual code of the attack starts. And that code has been encrypted, so let's decrypt it. It has been encrypted with XOR function 97. You just have to believe me, it is, it is. And we can go here and actually start decrypting it. Well the yellow part of the code is now decrypted. And I know, it doesn't really look much different from the original. But just keep staring at it. You'll actually see that down here you can see a Web address: [unionseek.com/d/i00.exe](http://unionseek.com/d/i00.exe) And when you view this image on your computer it actually is going to download and run that program. And that's a backdoor which will take over your computer.

11:02 But even more interestingly, if we continue decrypting, we'll find this mysterious string, which says O600KO78RUS. That code is there underneath the encryption as some sort of a signature. It's not used for anything. And I was looking at that, trying to figure out what it means. So obviously I Googled for it. I got zero hits; wasn't there. So I spoke with the guys at the lab. And we have a couple of Russian guys in our labs, and one of them mentioned, well, it ends in RUS like Russia. And 78 is the city code for the city of St. Petersburg. For example, you can find it from some phone numbers and car license plates and stuff like that. So I went looking for contacts in St. Petersburg, and through a long road, we eventually found this one particular website.

11:52 Here's this Russian guy who's been operating online for a number of years who runs his own website, and he runs a blog under the popular Live Journal. And on this blog, he blogs about his life, about his life in St. Petersburg -- he's in his early 20s -- about his cat, about his girlfriend. And he drives a very nice car. In fact, this guy drives a Mercedes-Benz S600 V12 with a six-liter engine with more than 400 horsepower. Now that's a nice car for a 20-something year-old kid in St. Petersburg.

12:27 How do I know about this car? Because he blogged about the car. He actually had a car accident. In downtown St. Petersburg, he actually crashed his car into another car. And he put blogged images about the car accident -- that's his Mercedes -- right here is the Lada Samara he crashed into. And you can actually see that the license plate of the Samara ends in 78RUS. And if you actually take a look at the scene picture, you can see that the plate of the Mercedes is O600KO78RUS. Now I'm not a lawyer, but if I would be, this is where I would say, "I rest my case."

13:10 So what happens when online criminals are caught? Well in most cases it never gets this far. The vast majority of the online crime cases, we don't even know which continent the attacks are coming from. And even if we are able to find online criminals, quite often there is no outcome. The local police don't act, or if they do, there's not enough evidence, or for some reason we can't take them down. I wish it would be easier; unfortunately it isn't.

13:35 But things are also changing at a very rapid pace. You've all heard about things like Stuxnet. So if you look at what Stuxnet did is that it infected these. That's a Siemens S7-400 PLC, programmable

logic [controller]. And this is what runs our infrastructure. This is what runs everything around us. PLC's, these small boxes which have no display, no keyboard, which are programmed, are put in place, and they do their job. For example, the elevators in this building most likely are controlled by one of these. And when Stuxnet infects one of these, that's a massive revolution on the kinds of risks we have to worry about. Because everything around us is being run by these. I mean, we have critical infrastructure. You go to any factory, any power plant, any chemical plant, any food processing plant, you look around --everything is being run by computers.

14:35 Everything is being run by computers. Everything is reliant on these computers working. We have become very reliant on Internet, on basic things like electricity, obviously, on computers working. And this really is something which creates completely new problems for us. We must have some way of continuing to work even if computers fail.

15:20 So preparedness means that we can do stuff even when the things we take for granted aren't there. It's actually very basic stuff -- thinking about continuity, thinking about backups, thinking about the things that actually matter.

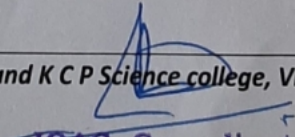
15:35 I do. Think about all the services we have online. Think about if they are taken away from you, if one day you don't actually have them for some reason or another. I see beauty in the future of the Internet, but I'm worried that we might not see that. I'm worried that we are running into problems because of online crime. Online crime is the one thing that might take these things away from us.

16:12 I've spent my life defending the Net, and I do feel that if we don't fight online crime, we are running a risk of losing it all. We have to do this globally, and we have to do it right now. What we need is more global, international law enforcement work to find online criminal gangs -- these organized gangs that are making millions out of their attacks. That's much more important than running anti-viruses or running firewalls. What actually matters is actually finding the people behind these attacks, and even more importantly, we have to find the people who are about to become part of this online world of crime, but haven't yet done it. We have to find the people with the skills, but without the opportunities and give them the opportunities to use their skills for good.

BLDEA's S B Arts and K C P Science college, Vijayapur.

  
Co-ordinator

BCA Programme  
S.B.Arts & K.C.P.Science College  
Vijayapur.

  
IQAC, Co-ordinator

S.B.Arts & K.C.P.Science College, S.B.Arts & K.C.P.Science College,  
Vijayapur.

  
Principal

S.B.Arts & K.C.P.Science College,  
Vijayapur.