CITIZENLAB Deep Packet Inspection SCAM

When I start writing, I want to mention about myself. I started my academic career as a research assistant at Gazi University after completing my undergraduate studies in Computer Engineering in 2005. This career was supposed to end until I completed my PHD Studies in 2014, but I had to work as a research assistant 4 more years. In this process, I carried out post-doctoral research on Data Mining in USA. After returning home, while making applications for staff, I began to work as an instructor although I got the assistant professor title before 2 months. I know that there is a difficult process of being associated professor while keeping a balance in the difficult and easy sides of the academic life. In this process, my aim is not only publishing articles but also publishing high quality articles.

While searching for a topic as such, I found a site relating to my study area which is cyber security. I decided to create a blog by focusing on the first topic to be more beneficial to humanity. The idea of reaching everybody having internet connections is more attractive while Academic publications reach only to the university community.

In my first blog post, I will touch on an institution called Citizen Lab (https://citizenlab.ca) which I have encountered while doing academic research on my topic. Although the name seems to be more like a Project to improve the quality of life in Europe, in fact it is a laboratory based in Canada and it publishes articles consisting of slanders about Turkey in a way that I cannot understand. The slanders are so exaggerated that there is an internet site fulfilled with the rules that are non-existent and a baseless report consisting of output obtained within so-called technical possibilities to put Turkey in danger.

Let us start by giving information about the staff. The founder of the Citizen Lab, Ronald J.DEIBERT is unfortunately not a computer scientist. The person claimed to be the founder of a research group controlling and monitoring the network traffic of the countries and having nearly 40.000 followers in Twitter, believe it or not is a Professor of Political Science. The head of the Laboratory which carries out research regarding internet, cyber space, switching, call routing equipment, OSI layers, analyzing SSL and encrypted TCP packages and also claims incredible arguments relating to Turkey is the person who will not go beyond opening four transaction calculator in terms of numerical operation. All of these show how these declarations are full of politics and completely a smear campaign against Turkey.

Although these assertions have been made by people non-computer scientists, the aim of this blog is not to deny them but to add another perspective to the alleged declarations. In general, the scientific research does not consist of alleged statements. These statements should be open to discussion unlike here. The weaknesses of the study should be stated as well. However, in this report, this kind of perspective is avoided. It seems that this report has been prepared by someone else but signed by others. Now I want to explain the reason why I got this idea. There are many names under the titles of Staff and Research Fellows except Ronald J. DEIBERT who is the head of the research. In that section, you can also see the names of the Senior Researchers whereas Staff consists of only administrative personnel in Turkish. Especially Jakub DALEK, Ivy LO, Sarah MCKUNE, Irene POETRANTO and Adam SENFT having @utoronto.ca e-mail addresses are written under Staff section. When you look at the distribution of tasks of these people, although being specified as a senior researcher in the site, you cannot reach Jakub DALEK through internet search regarding Toronto University. Moreover Ivy LO specified as a Business Officer, Sarah MCKANE having a Ph.D. degree in Ecology and being specified as Senior Researcher and also Adam SENFT specified as Operations Manager are the names written in the same section. Nonetheless, in the Faculty section which should include the names of the people carrying out the actual research, you can only see the name of Ronald J. DEIBERT. Despite of the fact that the names of the people who are assigned by the Faculty members to conduct the research are written in the Research Fellows (2017-2018)section, those 20 research fellows do not have any link to Toronto University. Furthermore, only 3 of the research fellows have an e-mail address. I believe that you have noticed the irony here. There is no real researcher working in this Laboratory which claims numerous arguments relating to Turkey and having nearly 40.000 followers in Twitter. The people working as a manager or a staff do not have any idea about computer.

Maybe, these evidences are enough to release the games played on our country. However as I have mentioned above, the aim of this blog is to respond to their slanders by giving technical and scientific facts, adding a point of view and shedding a light on the truth.

The title of the report consisting of the slanders against Turkey is Bad Traffic. Maybe you will not believe but the writers of the report are Bill MARCZAK, Jacub DALEK, Sarah MCKUNE, Adam SENFT, John SCOTT-RAILTON, and Ron DEIBERT. I have mentioned before about Jakub DALEK, Sarah MCKUNE, Adam SENFT. It seems that these people working related to the administrative matters have got promoted as a researcher in Computer Sciences in one night. Although the information about Bill MARCZAK is being accessed, you need to go deeper for

John SCOTT-RAILTON, and Ron DEIBERT. Ron DIEBERT is supposed to be the short name of the Professor of Political Science and when you search about John SCOTT-RAILTON, it is found in LinkedIn that he has a Ph.D. degree in Public Administration. Bill MARCZAK is the only Computer Scientist in this Laboratory. On the other hand most of the people stated above still live in USA at least according to their LinkedIn accounts. It is not easy to understand why these people have created such a research group in Canada and have been writing technical reports on computer sciences although they are qualified in politics, public administration, etc. Certainly, disciplinary studies can be carried out but it is difficult to understand why 1 computer scientist and 5 social based people have come together for a report including technical data and specific libelous expressions. It cannot be accepted as a disciplinary research under no circumstances.

The technical report prepared by non-technical people starts with this sentence: “This report describes how we used Internet scanning to uncover the apparent use of Sandvine/Procera Networks Deep Packet Inspection (DPI) devices (i.e. middleboxes) for malicious or dubious ends, likely by nation-states or ISPs in two countries”. The first question that comes to mind is how they could follow the network in Turkey from Canada since they support their claims by saying “Through internet scanning, we found deep packet inspection (DPI) middleboxes on Turk Telekom’s network.” They have monitored Turk Telekom network from Canada. Maybe the readers of this blog are not capable of technical data but you are reading the most nonsense and meaningless sentence that I have encountered in my life. For an ordinary person, internet is a topology consists of virtual gateways and physical wired devices providing access from A point to B point. Nevertheless, it is not technically possible to follow the traffic or make a packet analysis even in your 3 computer network that you created at home. For 20 years Switch devices which we call smart switching have been used rather than HUB switching devices. So if I cannot examine incoming and outgoing network packages of my neighbor or follow the network traffic of my wife’s laptop from my desktop computer, it is not reasonable for a Canadian political scientist to follow the network packages in my country. Thus, Deep Packet Inspection and Packet Injection Device cannot go beyond being a very splendent name. DPI is a technology that cannot go beyond packet analyzer Wireshark software used on your personal computers. To understand the reasons of this, we need to examine how the internet is originated.

The first internet came into use as a result of a network called ARPANET developed by Darpa in 1983. In time, countless systems and devices like firewalls (FW), intrusion detection systems (IDS), intrusion prevention systems (IPS), wired/wireless/optical smart devices, Layer 3

Switches, Routers have entered into our lives. All these software and hardware devices have played an important role in making the internet safer and accessible as they make our life easier. In the technical report, a series of middleboxes are said to be found in Turk Telekom's network and are used to get users' data and monitor them by adding malware into the legitimate Windows applications. This is a claim that does not fit into the mind. First of all, middlebox is a common name. The firewalls and NAT devices used in big institutions like the university where I work are middlebox devices. Network Address Translator (NAT) is a technology used by all over the world when IPv4 is not efficient enough. Its goal is to combine the local IP address of the device on the local network with the other IP address of it which will be required in the outside world. Hence, a single IP address can connect to the internet smoothly from a single gateway. middleboxes are the devices used by thousands of service providers (ISP) and millions of different users all over the world. They are used in Turk Telekom, Gazi University or Toronto University due to compelling reasons. Calling Deep Packet Inspection (DPI) devices at the beginning of the report can be accepted; however, calling middleboxes is not reasonable. I am not a psychologist, but an unknown device having a beautiful name and abbreviation and a known actual device's name appear at the same time, a voice from inside tells me that the first device should be right too. When I look at the academic qualifications of the people preparing the report, it appears that they talk pedantically. The Deep Packet Inspection devices are used for prevention, routing the internet traffic to the appropriate context, but not for installing spyware by injecting into the package. This is ridiculous and a non-scientific/non-technical argument.

Nevertheless, to be skeptical, let us imagine that there are middlebox devices in Turk Telekom that can be detected by DPI from Canada since the claim or slander is that those devices enable Turkish Government to use Spyware in Turkey, Egypt and Syria triangle. It is alleged that when I attempt to download free Windows applications including Avast Antivirus, CCleaner, Opera and 7-Zip from official vendor websites, I am redirected to malicious versions by way of injected http redirects.

There are 4 problems with this allegation. The first one is no one connects to the 7-Zip by knowing its address. Everybody connects to this kind of sites by searching them from Google. Google operates with HTTPS, not with HTTP. In other words, all the words that are searched are encrypted from the internet. The encryption technique is ECDSA P256. Even if the algorithms like Brute force that do not operate at internet speed are used, the Turkish Government needs to find the RSA encryption technique. Therefore it is not technically possible

to reach the documents protected by RSA in today's world. While this operation takes months/years for an individual even with a Brute Force attack, analyzing the network traffic package of thousands of people takes time for ever and ever. It requires a processor that even Google or Microsoft does not have.

The second problem is that the producers publish the hash values on the internet against this and similar attacks. Hash functions are the algorithms used for both verification and encryption techniques producing fixed length mathematical outputs (varying from null to terabyte values) in computer science.

The most prominent feature of its intended purpose is that even if a bite changes in software, the generated output differs. For instance; the MD5 output of Uraz written with big U is "fbc8bf9b15985fc6701ef99e19c7f3e4", but the MD5 output of uraz with small u is "b4dca2685b4ed253636ad48638a6baff". Hence if we go through the 7-Zip example, in the sourceforge.net in 28.03.2018 (the date of this post is written) the MD5 hash value for 7z1803.exe (the latest version of 7-Zip Software) is published as "db573e490e0c5145282aaaf6e2dc34df" but SHA1 hash value which is more secure is published as "1f28fd6afb36e97649d7e534907b13624ed8a645". When users download the files to their computers and test them with the software for hash value, they will see the same value since it is impossible for Turkish government or another government to download spyware into these setup files and to forward these files to their own or other citizens. The person claiming this should say that these hashes are different. There is no such an incredible claim or a slander to show middlebox as an evidence of spy. The claims should be supported. This claim is more nonsense than saying 2+2 equals to 7. The person thinking this post is insufficient need to download the software and "file md5 calculator" and to compare the hashes of them with the ones in the original site. You can also test it and see nobody could add even a byte to that setup file.

Additionally, the third problem is the Cyber Terrorist Action being one of the biggest cyber issues in global world. Of course the subject that I have implied is revealing the secrets of the governments with hacking like WikiLeaks and Anonymous. Here someone should ask the following question; if the countries really spied by means of DPI, would not the cyber terrorists reveal the fact rather than the political scientists. Actually even this hypothesis is enough to understand that our country has been libeled. The libelers are good at writing in Turkish, since there is an abstract in Turkish in that site. It says "The official websites for these programs even

though they might have supported HTTPS, directed users ton on-HTTPS downloads by default". Unfortunately, the address of the 7-Zip Program starts with HTTPS https://www.7-zip.org/ and the address of the downloaded site starts with HTTPS "https://sourceforge.net/projects/sevenzip/files/7-zip/18.03/.

I try to tell, the facts do not match with the given examples. The readers of this report are tried to be convinced that the findings of the report are true. Scientific and technical point of view comes into play here. Science means experiment and observation. The important point is not having blind confidence in something, but coming to a conclusion as a result of experiment and observation. In a modern society, if 40 thousand people follow a non-scientific site and a Twitter account, what percentage of the followers are real person or troll and who are these guys being good at Turkish? That is the question I want to ask.

The fourth problem is virus protection and firewall software. Everyone with some awareness uses this software at home and/or at work. In the above mentioned report it says "Before switching to the StrongPity spyware, the operators of the Turkey injection used the FinFisher 'lawful intercept' spyware". It can be understood from this statement that spyware is not developed by Turkish government but it is widely known and used by all over the world. In other words, all the virus protection software has the ability to detect this spyware, since they have not been popped up. Leave aside installing such a spyware on a PC, even when you download a spyware integrated application on a computer you will see the notification of virus alert. However if you add all security software companies like McAfee, Eset, Kaspersky, BitDefender, etc. to this conspiracy theory and say all the security software companies from Russia to Israel and from USA to China are controlled by the Turkish government, it is something else. The other concern of this issue is by means of the firewalls, it is likely to know how your computer communicates in the outside world and also you can allow or prevent the traffic. I mean, when a spyware intends to transfer your data to the outside world since the same gateway that is Ethernet or Wi-Fi interface will be used during this transfer, you will be warned by the firewalls. In order to understand how ridiculous this report is just search "FinFisher Eset" or "FinFisher Kaspersky" on Google and see the protection bulletins prepared by anti-virus companies a year before the report was published.

The most striking aspect of the following sections of the technical report is its lack of references. If you are preparing a technical report in the academic world, you will have some arguments. Before these arguments, you will give quotations from academic sources called literature to

support your arguments and evaluate the process of your thinking. For instance; you can create a bibliography from IEEE, ACM, Internet, News sites, etc. and refer to these sources in your writing. In this report it says “The apparent use of Sandvine devices to surreptitiously inject malicious and dubious redirects for users in Turkey, Syria, and Egypt raises significant human rights concerns.”, “After an extensive investigation, we matched characteristics of the middleboxes in Turkey and Egypt to Sandvine PacketLogic devices”. As you can see there have been numerous claims and research results in the report; however no single source has been published on how they have been obtained or published. It gives the impression of imagination. It is an entirely non-scientific report and I am sad to believe that there are foreigners of Turkish-oriented in the background of this report. As an academician in Turkey, I give someone else’s thoughts in quotes and I feel sorry to see that the writers of this report seeming to have high ability in the academic field miss seven such a simple rule.

As having a skeptical point of view I believe to examine the report as a whole and I want to deal with Sandvine PacketLogic devices. It is asserted in the report that Turkey has bought a large number of these devices. According to what they say the company that makes these devices constitutes of two firms based in USA and Canada. Perhaps the most shocking statement of this report is that “in Egypt and Turkey, we also found that devices matching our Sandvine PacketLogic fingerprint were being used to block dozens of human rights, political and news websites”. To analyze this sentence, what fingerprint means should be clear. It can be defined as the addition of information belonging to the device which passes through to that device. The area of my study is not network devices but I am interested in network devices in terms of cyber security. That’s why after examining the books related to network devices I can point out that if TCP packages kept all the information regarding fingerprints of numerous network devices, there would be no space to keep the actual communication data. For instance; you have an e-mail account from G-mail, the TCP package which transfers e-mail account to you comes from USA and visits 20-30 network devices. When you imagine all the fingerprint information being added to your TCP package, you will notice that it is not technically possible. To exemplify this, you can also try to display the TCP packages with the programs like WireShark.

It is not possible to get the modified results by Citizen Lab. The most significant component of science is that others can reach the result you have achieved by using your method, data set and logic. The results of this scenario remain only as outputs of Citizen Lab working group. As it is easily understood the ones who create the problem, generate the data set unpublished

explicitly and solve the problem are the same people after all. Also to support their scenario, Citizen Lab bought a second-hand Sandvine Packet Logic device and used its picture in the report. They allege that they have got fingerprint from a device and it is not clear how this device has been obtained or whether it has been intervened. In other words, while leading the people to dead end and creating a public opinion by using expressions far from science and technology against Turkey, they are adding one more brick to the smearing campaign against Turkey.

This report continues with numerous baseless libels and slanders.

Lastly, I want to touch on the subject that Bill MARCZAK who is the only person being a computer scientist among the writers not using any academic or technical format and paying attention to any rules while writing this report received a B.S. degree from Pennsylvania University in the years 2005-2009.

Uraz YAVANOĞLU, PhD