Analysis onto the Evolving Cyber-Attack Trends during COVID-19 Pandemic

Senthuran Nallainathan

No.25, 3/1, 8th Lane, Colombo – 03, Sri Lanka
Email: *senthurannallainathan[at]gmail.com*

Abstract: ***This report aims to study today's different types of cyber threats faced during COVID-19 Pandemic. Search terms such as "face masks", "corona virus" information sky rocketed during the last few months. This proof the target of Coronavirus related anxiety among users due to the pandemic which could be taken advantage by hackers in order to exploit their machines. It could also be seen 70% of organizations increased their cyber security spending, in an attempt to prevent, narrow down their vulnerabilities, shows the significance of this issue to be studied. Cyber threats during pandemic placed organizations in a financial stress, to their already affected cash flows. DDoS, Ransomware, Malware, Malicious domains were the most common attacks seen during this pandemic. Challenges faced by organizations due to cyber threats and factors (new technological applications such as video conferencing) contributing to increased vulnerability are critical issues. Importance of Cyber security consultations when implementing new applications to support WFH are essential.***

Keywords: cyber security, covid-19, cyber-attack trends, cyber security during covid-19, cyber security and WFH practices

1. Introduction

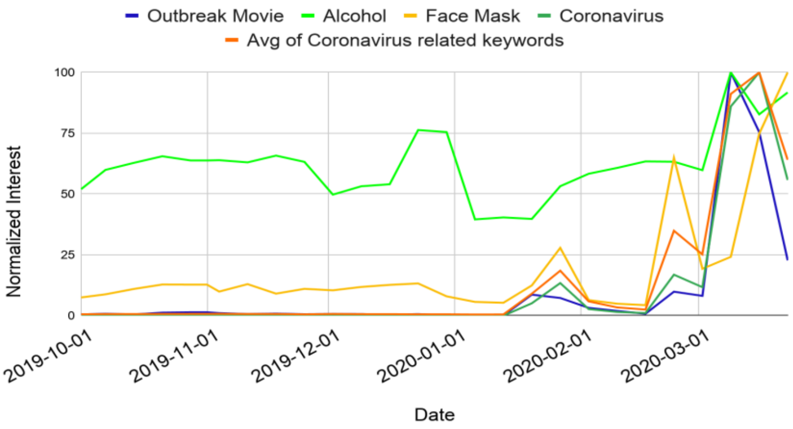
1.1 Background

Today's world has changed to a greater extend of the bad sides, where people tend to work in inhuman ways. Current situation has led to public outcry where many people's lives were lost and many have been hospitalized and suffering from a deadly disease where friends and families are worrying all day. This was taken as an opportunity by the hackers to use such a vulnerable situation to take advantage of them by cyber attacking individuals and especially organizations (including healthcare organizations) and this was seen a fivefold increase than normal during the COVID-19 time. (WHO, 2020)(DEKRA, n.d.) This could be compared to how people robbed from people affected, lost their lives (The Sydney Morning Herald, 2005)(BBC, 2005) and even raped women in such times (Irish Examiner, 2005)during Tsunami 2004 December 24th in Sri Lanka. These both activities are totally unacceptable and intolerable. The actual reason behind this is you can never win and create a safer, good society by having an arms race with the unlawful residents, thieves. It is only possible by educating the good values and creating/shaping a society which would lead to good and safer society.

1.2 Current Issue

These unlawful activities, the fruits of undisciplined society resulted in cyber-attacks, cybercrimes took place during this COVID-19 pandemic which is a great disaster because even healthcare organizations were victims of these attacks, which itself explains the importance and significance of this issue to be studied. The increase in such cyber-attacks which was nearly fivefold during these COVID-19 pandemic (WHO, 2020) of nearly five months is the topic of study of the current issue in question.
COVID – 19 Cyber Crime Associated Issues
COVID-19 Trends of Internet

The below figure explains the internet search trends by analysing the keywords, while explanation provided below the image.



(Janos Szurdi, 2020)

The internet user's trend and interests were analysed where it was seen that there is a huge spike in search engine searches and website visits related to corona virus information later part of February and followed with a huge spike afterwards in March and thereon.

It was also noted that the trend moved towards searching of Face masks had a huge spike in middle of February, while it is worth noting the searches for face masks were increased weeks before searches regarding corona virus information increase.
Financial Implications

There were several financial implications such as additional cyber security spending and financial losses during this pandemic due to increased cyber threats. It was seen than more than 70% of the organizations seen to have increased cyber security spending (SECURITY Magazine, 2020) shows the prevalence of the issue and explains the additional financial stress placed on companies, even at such difficult times.

Cyber Vulnerability
Cyber vulnerability is where the security layer of the organization is reduced either by reduced security measures, or not present which leads to loop holes which could be exploited by the hacker to gain advantage, access into the system. It is worth noting that even during the pandemic there is no reason for increased cyber security vulnerability in the organizations because the existing security protocols and policies are in force leading to security, so additional vulnerability due to pandemic cannot be present in the infrastructure but the anxiety of corona virus could lead to employees clicking on suspicious emails which titles something related to corona virus could be possible.

2. Types of Cyber Attacks

Denial of Service (DoS) Attack
DoS or DDoS attack is a common form of cyber-attack which targets a specific server or a cluster of servers/networks with an aim of making it inaccessible/slow down to the original, needful users using the services provided by such servers. (Alam, 2012) Distributed Denial of Service attack is a new, advanced form of DoS attack which uses distributed resources from various sites in order to create and divert a large volumetric flooding of requests to the victim servers.

The first DDoS attack was performed 20 years ago, but still DDoS attacks are one of the most feared attacks by organizations, obviously because of technology advancement, cyber attacking methods such as DDoS are also evolving. But in order to perform this attack, resources should be available in order to create a flood the host server with unnecessary requests. But the services could be obtained from the dark web as low as $400 to takedown a server for 24 hours. (page, 2019)

Volumetric based DDoS attacks past 1.2Gbps leads to network disruptions, and slips past available and present defence mechanisms making this attack still a viable one for attacks, as the ability of it to bypass and penetrate past defences present. (NEWMAN, 2018)

This was one of the attacks targeted towards the corona virus period towards COVID-19 information websites and helpdesks and governments too. This caused huge disasters to the governments and people and institutions who are working towards eradication of Corona Virus attacks. (Osborne, 2020)

It was also seen that hackers, attackers preying on the anxiety prevalent in the users due to the corona virus outbreak, in order to maximize the impact of their attacks. (Palmer, 2020)

Cloudflare provides DDoS protection and mitigation solutions to individuals users and large organizations as well with the ability to request support even if you are not a customer but when you are under attack, for immediate intervention and support by their team.

Also, it is worth noting, that in mission critical systems such as the healthcare networks, where monitoring and transmission of data should be in real time for critically ill patients, interruption of this through DDoS attacks is critical and heavily disastrous as few seconds delay could result in a loss of lives, which cannot be afforded.

Ransomware Attack
Ransomware attacks dates back to twenty-six years from today, but due to technology advancement this attack is also evolved to a greater extent while there is huge possibility of more vicious type of attacks innovated in the future of this type, as this has become a common form of attack.

Ransomware attack is divided into two types, namely Crypto type and Locker type. This attack encrypts the files of the victim's host machine with a cryptographic key which makes the files in the host machine unreadable and requires decryption before use. The decryption will only be possible with the decryption key which is held by the hacker who will demand a ransom to be paid in order to provide the key which finally leads to decryption and usability of the locked files. The details of payment of ransom is provided in a text file or by a dialog box displayed in the victim's computer screen. Ransomware is most commonly received by opening and downloading attachments of emails received from unknown sources. (Imaji, 2019)(Loman, 2019)

It is however not guaranteed that regardless of the payment of ransom, the hacker may or may not provide with the key. Even the key is provided it may not be possible to unlock all the files most commonly due to decryptor software issues.

Ransomware attack seen a huge rise during COVID-19, especially targeting the healthcare sector. This caused huge impact and losses to the health sector, while the hackers assumed the healthcare organizations cannot afford to lose access to their data so the hackers believed they would pay the ransom, though this was factually and practically correct, led to huge ransom payment collections from hospitals, motivating the cyber criminals. The Corona Virus pandemic was another outbreak which was considered by the hackers to be successful in collecting ransoms by initiation Ransomware attacks. (INTERPOL, n.d.)

The trend of Ransomware attacks targeting healthcare providers started few years ago with WannaCry attack which targeted healthcare networks by locking access to data of the healthcare network resulted in huge losses. (Ernst and Young, 2015)

Hollywood Presbyterian Hospital in California was attacked by ransomware attacked, which delayed patient care; finally, the hospital resorted to pay the hackers $17,000 to restore data. (Center for Internet Security, n.d.)

Quarter 4 of 2019, which is the very recent report, suggests ransomware losses rose to 350% which is a significant increase. (Davis, 2020)

Malicious Domain

Domain name is an identity of a website which is available to the public view. This is also considered as the source or first step of online presence, while domain name resolves through the Public DNS server, and each domain will be pointed to a Public IP address which is the actual address of the content.

Domain registries who register domains are currently on a spree to block domain name registrations which are understood to be misleading the public (Scroxton, 2020), or suspected to be used for cyber-criminal activities such as but not limited to phishing, probably by manual detection or artificial intelligence tools.

The malicious domain registrations are a form of cyber threat (INTERPOL, n.d.) which seen a rise in registrations as huge as 1,700 which were suspected and blocked within the UK (1,700 number by only considering suspicions on .uk TLD) (Scroxton, 2020) and around 86,600 new suspicious domains registered shows the new reports by registries (Greig, 2020)shows the significance of this issue because there are 1,511 Top Level Domains (TLD) around the world (Wikipedia, n.d.), so the number is vast when considering the entire Internet network.

The hacker who registers these domains will then use many forms of cyber attacking strategies; most commonly phishing attacks were done using malicious domains. The domains look like providing genuine information while the study in “Introduction” shows the Internet user’s interest have seen a rise in the Coronavirus topic, justifies the Internet user ending up believing such domain names. These could phish the user to enter details such as name and address, or offer free trial of corona virus information by entering the credit card details (even free trial, the card details get into wrong hands, that is hacked). This was the common form of attack found during this pandemic and was highly financially beneficial for the hacker as well which is the underlying motivation behind this.

Malware

Malware is a form of virus which attacks the computer system by penetrating into the system and performing unpleasant, un required activities using the computing resources of the victim’s system.

Wide spread communications globally are taken advantage by the criminals of the cyber world to mask their activities. (INTERPOL, n.d.) This includes hacking or DDoS-ing an entire computer network, which requires huge resources, so by using computing resources present in victim’s computers. Using all the hacked computers and directing them to damage a network is possible because of huge resources available from hacked computers. Finally, this is a masking process; still the user is vulnerable and also could be confronted by the authorities for making cyber-attacks, which they are actually not aware of.

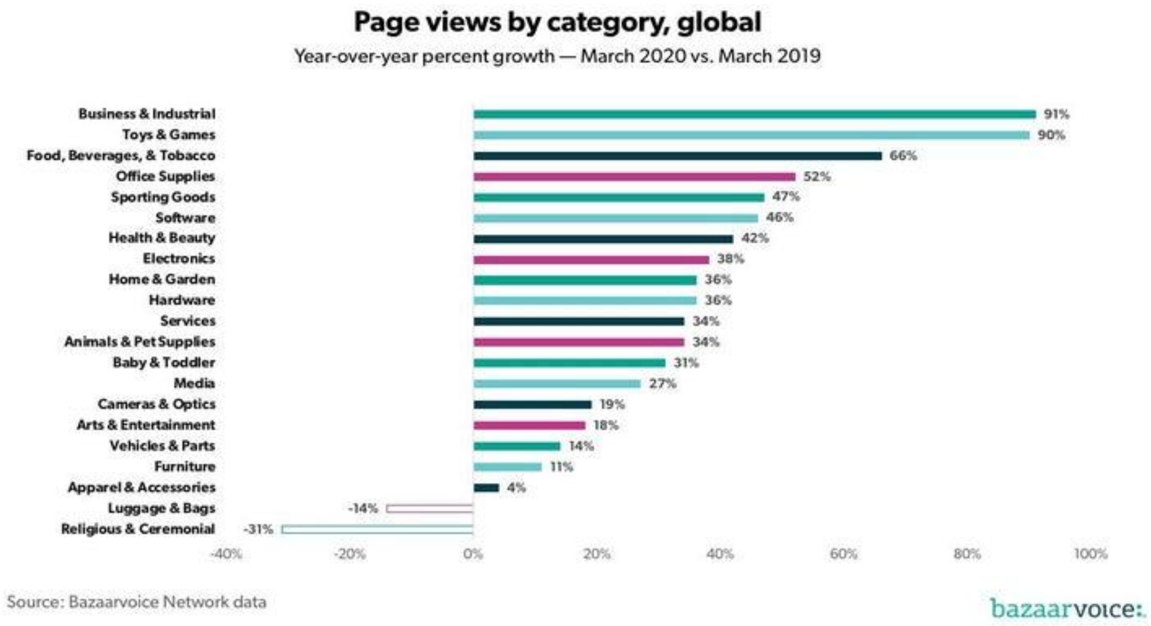
It was also seen corona virus maps and websites were embedded with viruses such as Trojan, spyware, malware etc. (INTERPOL, n.d.) This shows the significance of cyber threats during this corona virus pandemic.

Challenges faced by Organizations

Financial Implications – Increased cyber security prevention and appraisal spending was detected by organizations. It was revealed 70% of the organizations have increased their cyber security spending in a fear due to post COVID – 19 situations. (SECURITY Magazine, 2020)

Pre-COVID VS Post-COVID factors

During Pre COVID-19 pandemic, the usage of online meetings (video conferencing) were extremely limited and used only by IT, highly sophisticated companies which employed remote employees while rarely or occasionally used by others. The usage of social media, Skype and other video call services mostly for personal and official purposes were present. Online banking and online shopping were already in use, with some countries started adapting to them during COVID-19 due to inaccessibility of getting items/groceries.



Source: Bazaarvoice Network data

(Wold, 2020)

It is seen that business and industrial had seen 91% growth and toys and games saw 90% growth. Toys and games were seen rise because children were forced to stay home due to COVID-19. While Food, Beverages sew a rise of 66%. This is a enormous growth in just a year. This data compares year on year growth of last year March 2019, and this year March 2020 when the world was affected by COVID-19 pandemic.

Post COVID shows ramped up usage of streaming, internet telephony and teleconferencing services while usage of e-Commerce websites to purchase essential, day to day items were changed. (WTO, 2020)

This ultimately changed the consumer behaviour from visiting shops for day to day needs, to moving to ecommerce for their needs.

Vulnerability factors from Post COVID-19 Technologies

Video conferencing – Zoom, MS Team, Google Meet
Use of teleconference apps for team meetings and teacher-student conference for educational purposes.

New educational technologies – eLearning, LMS
Teaching transformed from traditional classroom-based learning into internet-based learning where Moodle as LMS and BigBlueButton as Video conference solution and other modes used as a common practice now.

3. Conclusion

This report also extensively discussed and explained of the types of cyber-attacks prevalent in the latest context and also discussed about threats which were seen long ago which had huge developments and expected to be seen in more vicious forms of such attacks in the years to come.

Factors such as financial implications, prevalence of increased cyber risks and analysis of corona virus related search results were also presented in this report.

In conclusion it is therefore understood that during the COVID-19 pandemic significant increase in cyber-attacks were monitored. The main target and reason of the hackers using this opportunity is to maximize the impact by attacking during such tough times.

It is also noted that increased online usage, which was actually made mandatory due to lockdown also have caused increased cyber security risks among the users. It is also seen that hackers and cyber criminals used this new change as an avenue in order to exploit and take advantage by victimizing and attacking the users, who are sometimes relatively new (who started using online services after lockdown) who are more vulnerable to such attacks.

4. Recommendation

It is utmost important, where the employers and teachers who require online teleconferencing services and new technological usage, should have been provided with a comprehensive booklet/e-Document which educates and prepares them with precautionary measures before start using of new advanced technologies.

Proper antivirus and secure protocols should be set in place in the organization, host and user PC's while necessary resources such as antivirus licenses are provided to them as needed.

Selection and usage of online service apps such as teleconference application (Zoom, MS Team) should be evaluated by an IT team/Cyber security Consultant for security leaks, risks and loopholes present in such application be thoroughly studied before start using it by the organization and users.

References

[1] Irish Examiner. (2005, 01 07). *Tsunami survivor tells of rape ordeal*. Retrieved 06 07, 2020, from Irish Examiner: https://www.irishexaminer.com/breakingnews/world/tsunami-survivor-tells-of-rape-ordeal-183623.html

[2] Alam, M. F. (2012). *DDOS ATTACKS: PREPARATION-DETECTION-MITIGATION.* Singapore: APRICOT.

[3] ALJAZEERA. (2019, 10 21). *Ransomware cripples US emergency services, local governments*. Retrieved from ALJAZEERA: https://www.aljazeera.com/economy/2019/10/21/ransomware-cripples-us-emergency-services-local-governments/

[4] BBC. (2005, 01 04). *Criminals target tsunami victims*. Retrieved 06 07, 2020, from BBC News: http://news.bbc.co.uk/2/hi/asia-pacific/4145591.stm

[5] Center for Internet Security. (n.d.). *Ransomware: In the Healthcare Sector*. Retrieved 06 07, 2020, from Center for Internet Security: https://www.cisecurity.org/blog/ransomware-in-the-healthcare-sector/

[6] CityPopulation.de. (2021, 02 25). *VAVUNIYA*. Retrieved from CityPopulation.de: http://citypopulation.de/en/srilanka/prov/admin/northern/43__vavuniya/

[7] Collier, K. (2020, 09 30). *Cleveland-area hospital goes offline after apparent cyberattack*. Retrieved from NBC News: https://www.nbcnews.com/tech/security/cleveland-area-hospital-goes-offline-after-apparent-cyberattack-n1241408

[8] Davis, J. (2020, 03 09). *Ransomware Attacks on Healthcare Providers Rose 350% in Q4 2019*. Retrieved 06 07, 2020, from HEALTH IT SECURITY: https://healthitsecurity.com/news/ransomware-attacks-on-healthcare-providers-rose-350-in-q4-2019#:~:text=In%20fact%2C%20Emsisoft%20research%20shows,last%20year%2C%20reaching%20crisis%20levels.&text=But%20health%20services%20and%20medical,successfully%20se

[9] DEKRA. (n.d.). *Are you dealing with a higher volume of cyber-attacks due to Covid-19?* Retrieved 06 07, 2020, from DEKRA: https://www.dekra.com/en/cyber-attacks-due-to-covid-19/

[10] Ernst and Young. (2015). *“WannaCry” ransomware attack*. Birmingham: Ernst and Young.

[11] Greig, J. (2020, 05 04). *More than 86,600 new domains related to the pandemic are considered "risky" or "malicious," according to a new report.* Retrieved 06 08, 2020, from TechRepublic: https://www.techrepublic.com/article/nearly-2000-malicious-covid-19-themed-domains-created-every-day/

[12] Grobler, M. &. (2011). Towards a Cyber security aware rural community.

[13] Imaji, A. O. (2019, 03 05). Ransomware Attacks: Critical Analysis, Threats, and Prevention methods. Hays, Kansas, Fort Hays State University.

[14] INTERPOL. (n.d.). *COVID-19 cyberthreats*. Retrieved 06 07, 2020, from INTERPOL: https://www.interpol.int/en/Crimes/Cybercrime/COVID-19-cyberthreats

[15] Janos Szurdi, Z. C. (2020, 04 22). *Increase in User Interest of Coronavirus-related Topics*. Retrieved 06 08, 2020, from paloalto Networks: https://unit42.paloaltonetworks.com/how-cybercriminals-prey-on-the-covid-19-pandemic/

[16] Kritzinger, P. E. (2020). *CYBER SECURITY AWARENESS AND EDUCATION RESEARCH.* Gauteng: University of South Africa.

[17] L. Bošnjak, J. S. (2018). Brute-force and dictionary attack on hashed real-world passwords. *International Convention on Information and Communication Technology, Electronics and Microelectronics* (pp. 1161-1166). MIPRO.

[18] Loman, M. (2019). *How Ransomware Attacks.* Burlington: SophosLabs.

[19] Moti Zwillinga, G. K. (2020). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. *JOURNAL OF COMPUTER INFORMATION SYSTEMS*, 1-15.

[20] Mudassar Raza, M. I. (2012). A Survey of Password Attacks and Comparative Analysis on Methods for Secure Authentication. *World Applied Sciences Journal* , 439-444.

[21] Myers, N. (2020). Cyber Security: Cyber Crime, Attacks and Terrorism. *ODU UN Day 2020 Issue*, 1-13.

[22] NEWMAN, L. H. (2018, 12 03). *How Creative DDOS Attacks Still Slip Past Defenses*. Retrieved 06 07, 2020, from WIRED: https://www.wired.com/story/creative-ddos-attacks-still-slip-past-defenses/

[23] O'BRIEN, L. (2019, 12 20). *Cybersecurity for Rural Communities is Often Neglected*. Retrieved from ARC Advisory Group: https://www.arcweb.com/blog/cybersecurity-rural-communities-often-neglected

[24] Osborne, C. (2020, 05 12). *DDoS surge driven by attacks on education, government, and coronavirus information sites*. Retrieved 06 07, 2020, from The Daily Swig: https://portswigger.net/daily-swig/ddos-surge-driven-by-attacks-on-education-government-and-coronavirus-information-sites

[25] page, E. T. (2019, 04 18). *The first DDoS attack was 20 years ago. This is what we’ve learned since.* Retrieved 06 07, 2020, from MIT Technology Review: https://www.technologyreview.com/2019/04/18/103186/the-first-ddos-attack-was-20-years-ago-this-is-what-weve-learned-since/

[26] Palmer, D. (2020, 04 03). *Ransomware and DDoS attacks: Cybercrooks are stepping up their activities in the midst of coronavirus*. Retrieved 06 07, 2020, from ZDNet: https://www.zdnet.com/article/ransomware-and-ddos-attacks-cybercrooks-are-stepping-up-their-activities-in-the-midst-of-coronavirus/

[27] RHIhub. (2020, 11 09). *Health Information Technology in Rural Healthcare*. Retrieved from RHIhub: https://www.ruralhealthinfo.org/topics/health-information-technology

[28] Robert B Mellor with Gary Coulton, e. (2009). *Entrepreneurship for Everyone: A Student Textbook.* London: SAGE.

[29] Ruwan Nagahawatta, e. (2020). A Study of Cybersecurity Awareness in Sri Lanka. *Australian Cyber Warfare* (pp. 46-58). Melbourne: Deakin University.

[30] Scroxton, A. (2020, 04 17). *Coronavirus: How Nominet fights back against malicious domains*. Retrieved 06 08, 2020, from Computer Weekly: https://www.computerweekly.com/news/252481777/Coronavirus-How-Nominet-fights-back-against-malicious-domains

[31] SECURITY Magazine. (2020, 05 21). *70% of Organizations to Increase Cybersecurity Spending Following COVID-19 Pandemic*. Retrieved 06 08, 2020, from SECURITY Magazine: https://www.securitymagazine.com/articles/92437-of-organizations-to-increase-cybersecurity-spending-following-covid-19-pandemic

[32] The Sydney Morning Herald. (2005, 01 05). *Criminals, opportunists take advantage of tsunami tragedy*. Retrieved 06 07, 2020, from The Sydney Morning Herald: https://www.smh.com.au/world/asia/criminals-opportunists-take-advantage-of-tsunami-tragedy-20050105-gdkfj5.html

[33] Thomas W.Edgar, D. O. (2017). Chapter 3 - Starting Your Research. In D. O. Thomas W.Edgar, *Research Methods for Cyber Security* (pp. 63-92). Burlington: Syngress.

[34] WHO. (2020, 04 23). *WHO reports fivefold increase in cyber attacks, urges vigilance*. Retrieved 06 07, 2020, from World Health Organization: https://www.who.int/news-room/detail/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance

[35] Wikipedia. (n.d.). *List of Internet top-level domains*. Retrieved 06 08, 2020, from Wikipedia: https://en.wikipedia.org/wiki/List_of_Internet_top-level_domains#:~:text=As%20of%20June%202020%2C%20their,not%20represented%20in%20ICANN's%20listing.

[36] Wivoda, J. (2016). *Cybersecurity Threats in Rural America : How to Protect Your Critical Access Hospitals.*

[37] Wold, S. (2020, 05 07). *How Covid-19 has changed shopper behaviour*. Retrieved 06 30, 2020, from MarketingWeek: https://www.marketingweek.com/how-covid-19-has-changed-shopper-behaviour/

[38] WTO. (2020). *E-COMMERCE, TRADE AND THE COVID-19 PANDEMIC.* Geneva: World Trade Organization.