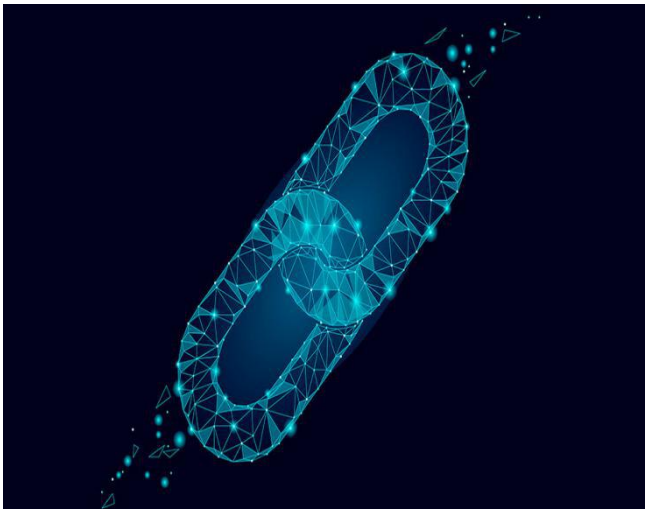
Supply Chain threats



Course : Cyber Security
Yuan Wang
A00258427

Abstract

Supply chains are critical for the operation of almost all daily activity from food delivery to manufacturing. This report will give an overview of supply-chain technology and describe the main threat types including recent examples.

Introduction

Our world is becoming more and more digital, and all kinds of threats are becoming more and more complex. Threats can be remotely detected and attacked us remotely under the cover of the Internet. Modern supply chains are a complex and fragile network through which goods and services flow. It is no exaggeration to say that the supply chain is the lifeblood of the modern economy and the basis of our daily lives. It ensures that we have food, energy supplies, products that can be consumed, as well as our healthcare and banking businesses. Alternative physical attacks like theft and piracy occur, which might be either an internal or external operation.

Supply chain security plays an important role in our lives and there are many key messages about individuals. The importance of the supply chain is no exaggeration. For companies, if the products range from 0 to 1, they depend on research and development. From 1 to N, they rely on the supply chain to guaranteeing. For individuals, as a consumer, the products and services you receive depend on the supply chain. In the current digital world trend, with the development of the Internet of Things (IoT), the development of supply chain to digital, automation and integration is an unchangeable trend. For example, cloud computing, robotics, and artificial intelligence are improving productivity. Improve customer service applications. In fact, in recent years, the logistics and transportation industry has been developing drones and storage robots. But as the pace of enterprise digital transformation is getting faster and faster, from the old supply chain to the modern supply chain, a very serious problem becomes more and more prominent: there are loopholes in the supply chain system that can be exploited by hackers and various organizations. It is easy to be attacked, posing a huge threat to the privacy information of the enterprise itself and individuals. The physical threat we can assume is the more obvious and glaring ones that can happen at numerous stages in the supply chain – for example, hoodlums or terrorists vandalizing an oil pipeline for an oil producing industry. According to Limor Weinstein, terrorism in the supply chain has been much more terrible in recent years with over 3.1% of attacks on supply chain faced every week all around the world [1].

Besides the perpetual physical threats, there has also been an increase in the threats supply chains encounter in relation to Information Security. This has been because

technology has grown to the level that well organized and planned supply chains rely more on software and hardware performing in unison, collecting and sharing important information on consignments, records and also the state of machineries used in the manufacture of parts. This recent reliance on the internet and technology has given rise to new areas for ill-minded individuals who want to damage supply chains to gather private information or cash. A typical example of this situation is an attack that was made on Maersk, a Danish company, in 2017 where the repercussions of this attack were instantaneous and catastrophic, taking down the global network of a company in charge of up to one-fifth of the worlds shipping volume [2]. This attack was termed NotPetya and is quite famous till date.

Supply chain in software

As the digitization process accelerates, the concept of the software supply chain also emerges. The traditional supply chain concept refers to the contact or business contact of the related party before the goods arrive at the consumer. The final product - the final sales network - provides products to consumers in an overall supply chain structure. For the software supply chain, the traditional supply chain concept still applies, that is, the software supply chain is a pipeline composed of software source code, source code compilation, software distribution, software download, and software update. The software supply chain can be divided into three stages. The first stage is development, corresponding source code writing and source code compilation, involving software and hardware development environment, development tools, third-party libraries, software development, and the second is the delivery part, corresponding to software download, Users get the software products they need, online downloads, software installation CDs and other storage media, resource sharing and other ways. The third is to use the corresponding software update, which is the entire life cycle of the user software product, including software upgrades, maintenance and other processes.

SUPPLY CHAIN IN THE CLOUD

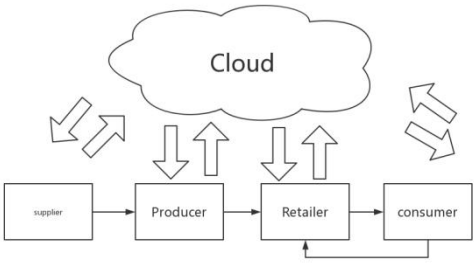


Figure 1. data flow in the supply chain in cloud computing

Cloud computing is having a significant impact on supply chains in this new technological era, enterprises are studying the most advanced practices to optimize the cost and operational efficiency of their supply chains. As a meaningful technology, cloud computing[3] can facilitate this optimization by Infrastructure,

platforms and software solutions for the entire supply chain network through The Internet. Using cloud-based services in supply chain management can bring financial and operational benefits, and all supply chain partners should consider potential risks and constraints. In this paradigm, resources Likes, storage, and applications are utilized are utilities, attainable through private or public networks. According to the content shown in Figure 1, all end objects interact with the cloud's existing data. It's now more of an anomaly rather than the norm, companies Not using cloud-based supply chain management software.
A typical example of a supply chain management enterprise is Rangespan, whose total IT architecture is rooted to AWS (Amazon Web Services). Rangespan utilises Amazon Relational database Service (RDS) to save client and inventory records and Elastic Block Store (EBS) volumes [4].

The impact of attacks on the supply chain is also diverse. For traditional supply chains, after the attack, R&D and manufacturing companies may face the theft of intellectual property rights, which may also lead to the company losing its competitive advantage and serious financial crisis. For the medium transportation industry, its untrustworthy upstream manufacturing industry is an unprecedented crisis of confidence for downstream consumers. If it is international trade, such as weapons, it will not only have a general impact, but it may also lead to national security risks and even exacerbate tensions. For software provisioning and supply chains that use cloud technology, there may be software tampering, bundled viruses, and even stealing users' personal information, data theft and the possibility of generating a large amount of spam data, which may even cause the entire system to crash. Whether it is for our traditional supply chain or the new era supply chain, the threat it poses cannot be ignored. Ultimately, rights and interests are hurt, not only companies, but also people at every stage of the supply chain.

COMMON CONCERNS IN SUPPLY CHAIN SECURITY

The threat to the supply chain is much more serious than we think. For traditional supply chains, we not only need to face the risks that the entity may encounter in this allocation (such as the risks that the transportation vehicle may encounter, the risks that the warehouse may encounter, or the risks that occur during transportation), as well as the traditional Supply chain related risks that arise in the digitalization process of the supply chain.

1. Inventory Thievery:Inventory theft is often not taken seriously in many supply chain security threats, but it is the most common threat. There are two types of these thefts. The first is the end of the supply chain. That is to say, the first step of delivering goods to consumers, that is, in-store display, displaying goods in display cases, customers choose to purchase is the most important step of the real economy,

consumers can watch and even touch goods at close distance, and In this process, as long as the goods are not purchased by the customers in the showcase, they can be considered as "in the warehouse" state, and this stage is also the most vulnerable to theft. And the hope of recovering stolen items in this way is also very embarrassing. The second type is primarily performed by employees in the distribution center. The number of goods passing through these centers makes it difficult to accurately monitor all items, and theft is more complicated, involving internal staff working with external complicity. An example is the driver mobile product and reselling it to private customers.

2. Smuggling: Smuggling is a problem in the supply chain that is valued by all countries in the world, and sneaking both legal and illegal products showcase a threatening danger to the security of supply chains. Fake products can be snuck in through the international flow of consignments that are used to move authorized goods. Another disadvantage this is that smuggling actually consumes the available spaces in containers meant for goods to match the high customer demands, thereby impacting supply chains.

3. Piracy: Piracy has been one of the biggest supply chain threats in history. The consequence of piracy is that the manufacturer's intellectual property is stolen, and pirated products have problems with quality assurance and follow-up service providers. They don't have as strict technical requirements as the real thing. The raw materials used to produce the product often have various problems to save costs. Damage is not only the reputation of the manufacturer but also the consumer who buys pirated products. In West Africa alone, the cost of piracy exceeded $793.7 million in 2016, and the company hired more labor to protect high-sea cargo [5]. This involves not only the supply chain but also the lives of workers working along these dangerous routes. Another danger of piracy is that it will limit the overall development of the economy. Since the sales price of pirated products is often lower than that of genuine products, more consumers who lack relevant legal knowledge will often choose cheap pirated products, and the result is to reduce the production of genuine manufacturers. The market share of genuine manufacturers will gradually shrink, and the overall shipments of products will be reduced, thus threatening the source of the entire supply chain. The irrational benefits of piracy intuitively reflect the economic losses of real manufacturers and the entire supply chain.

4. Tampering of Devices: Intentional sabotage of devices is another major threat in the security of supply chains. This particular threat has daring consequences for the electronics supply chains, with a report in 2013 mentioning the great complexity in determining electronic chip tinkering. These kinds of meddling could damage or weaken vital defense information or distort machines that make use of these chips.

5. Threat during transportation : After the manufacturer produces the goods, the goods cannot be delivered directly to the user and often need to be transported by various means of transport. There are also threats in this area, no matter how complex the machine is, there is no guarantee of error, let alone the means of transport that people drive, and some unpredictable accidents that often occur

during transportation. Unpredictable accidents are often an invisible threat to the supply chain. However, the consequences of a transport accident are usually the first two types. After the accident, the transported goods are affected by physical factors, burned or destroyed, and cannot maintain the original value, thus affecting the manufacturer. Second, the losses caused by the robbery of goods after the accident cannot be ignored. Recently, a Panamanian cargo ship near the Netherlands recently shipped the cargo. Due to the bad weather, more than 270 containers fell into the sea and were washed onto the Dutch coast. The goods in these discarded containers were robbed by the surrounding people and caused significant losses. [6]

COMMON CONCERNS IN SOFTWARE ,CLOUD ,AND CYBER SECURITY SUPPLY CHAIN

CLOUD SUPPLY CHAIN SECURITY

Cloud Access Mismanagement: The migration of management software and storage to the cloud demands an upgrade with heavy consideration of security to protect cloud application and data. Ignorance of this is what leads to major IT dangers, like giving users over-privileges or exposing storage repositories [7].

SOFTWARE SUPPLY CHAIN SECURITY

For the software supply chain, the main threat comes from the three stages of software development, software delivery, and software maintenance. If the attacker attacks each stage of the above, it may affect the final software product and the entire usage scenario security. The security risks associated with the supply chain, such as the development tools, the development of hardware and software environments, the channels of reaching users, and the process of using software and hardware products, are not lower than the security risks caused by security vulnerabilities of software applications and corresponding operating systems.

1. Development stage:

Software development involves software and hardware development environment deployment, development tools, software development testing, etc., all stages may be maliciously attacked, and in the attack software development environment, there are development machines infected with Trojans, development tools embedded malicious code third-party libraries Contaminated and other methods of attack. Specific software development is a complex process, not only source code, but also complex phases such as requirements analysis, algorithms, outsourcing development, etc., all of which can be attacked with serious consequences.

1.Development tools are contaminated:The most influential attack on development tools is XcodeGhost (Xcode unofficial version of malicious code pollution incident). In 1894, Ken Thompson proposed the attack concept for development tools, called the Ken Thompson. Hack (KTH).[8] The most influential XcodeGhost is one of them.

Xcode is Apple's integrated development tool (IDE), which runs on the operating system Mac OS X and is the most popular tool for developing OS X and iOS

applications. In the September 2015 XGhost incident, the attacker injected the virus Xcode Ghost into unofficial Xcode, tampering with Xcode, adding malicious modules, and enabling a large number of unsuspecting developers to build development environments using contaminated versions. The main way to communicate is Xcode, which can be downloaded via an unofficial link. Applications compiled with the contaminated Xcode version will secretly write to the malicious module, mainly including transferring user information to the domain name registered with the attacker, connecting to the phishing website in the form of a pop-up window, and even remotely controlling the user's computer. The number of corresponding APPs affected by this incident in China reached 692, including many apps that people use every day, such as WeChat (an app similar to what's up), Weibo (an app similar to Facebook).[9]

2.Source code is contaminated:Source code pollution is a very difficult thing to discover compared to other threats in the development phase. If the software product embeds malicious code at the source code level, the malicious code will have the same legal code as the vendor. It is legally recognized, so it is easier to avoid detection of security software products, and it will lurk in the user's computer for a long time and cannot be detected.

The Xshell backdoor event that took place in August 2017 is a case of this type of attack. Xshell is a secure terminal emulation software developed by NetSarang. The software released on July 18, 2017, was found to have the malicious backdoor code. The malicious backdoor code exists in the nssock2.dll module with a legal signature. Kaspersky, the world-famous anti-virus software manufacturer, released relevant event descriptions and technical analysis afterward, clarifying the malicious code embedding based on the source code level. According to the results of the code analysis, the attacker is likely to inject the back door in the source code by invading the relevant developer's computer, and many anti-virus software did not detect the virus according to its whitelist mechanism, which eventually led to the back door event. The impact of this incident is that the information that caused the user to log in remotely is leaked from the background to the attacker.[10]

3.Manufacturer reserved back door:This problem is mainly caused by the inattention of the manufacturer. In the development process, in order to facilitate the debugging and testing of the program, some backdoors are usually reserved. However, when the software is officially launched, these backdoors, which are used for testing and debugging, are forgotten to be deleted or hidden. The consequence is that the attacker can use these backdoors to steal user information.

More famous for this aspect is the prism program. The Prism Program (PRISM) is a top-secret electronic monitoring program implemented by the National Security Agency (NSA) since 2007. The official name of the program is “US-984XN”. NSA directly enters the central server of the US Internet company to mine data and collect intelligence. Nine international network giants including Microsoft, Yahoo, Google, and Apple are all involved.[11]The other thing is the mobiSage ad library backdoor code event that happened in 2015.[12] Through the control of the server, these ad libraries can record and screen, upload GPS information, add and delete

app data, read and write app keychains, send data to the server, use URL schemes to open other apps or web pages, install enterprise applications, etc. Features.

2. Delivery stage:

After the software is developed, it will belong to the interactive stage until it reaches the user's hands. It can be transmitted by means of CD, USB and other hardware media. It can also be downloaded from the Internet through network download and resource sharing.

1. Bundle download： When talking about bundled downloads, I have to mention the blackware supply chain. The software supply chain mainly includes third-party download sites that are not officially authorized. Users who download software from these download sites often do not have proper software protection and are more likely to embed malicious code or even bundle malware. In addition, in the regular download sites and the application market, because of the lack of strict oversight, there have been incidents of maliciously implanting code by attackers, such as WireX Android Botnet polluting Google Play app market events.[13]In this incident, a botnet called WireX BotNet infects Android devices and launches large-scale DDoS attacks by masquerading as a normal Android application.

2. Download hijack:Download hijacking, that is, attacks that users may be exposed to during downloading software from various network channels, such as being bundled with malware, tampering, hijacking downloaded domain names, and so on. The typical one is domain name hijacking. The attacker hijacks the domain name of the download site so that the user accesses the download site specified by the attacker to download the malware, but the user does not know until the malicious software is downloaded to the computer, causing the computer to be infected by the virus.

3.Update maintenance stage:

After the software product successfully arrives at the consumer or is downloaded to the computer, its use, upgrade, and maintenance are at this stage. In this phase, in addition to the threat posed by the security flaws of the software itself, the use environment is also vulnerable to threats. For example, in use, the core key of the software product is leaked.

Upgrade hijacking:In the entire life cycle of the software, it is necessary to perform multiple updates and maintenance to ensure its own use value. Common functions include function update and upgrade, repair software product BUG, and so on. The attacker can aim at this stage, for example, by hijacking the software update channel, redirecting the address pointed to by the download link to hijack the software upgrade process and then implanting malicious code. One of the famous cases is the NotPetya event mentioned earlier.

The virus threat is to extort the users by encrypting the user's computer. The overall impact in Europe is very wide, and even the government, banks, power systems, communication systems, etc. are affected to varying degrees. According to

Microsoft's survey and published reports, Petya ransomware attacks were spread by hacked software updater.[14]

SUPPLY CHAIN CYBER SECURITY THREATS

When speaking about cyber security, the general consensus is the thought of firewalls, WAF (Web Application Firewall), DLP, IDS/IPS, SIEM, etc., [15] to protect networks, data, and applications.In fact, the entire supply chain is analyzed as a whole (from the source software supply chain to the logistics supply chain that uses the software later). How about a situation whereby solutions that have been deployed have existing bugs? Cyber Security in supply chain is a breakdown of security in supply chains with a focus on the management and control of security requirements for IT systems, networks, and software, which are enhanced by threats like cyber terrorism, data pilfering, malware and APT (Advanced Persistent Threat). Some notable examples of cyber security threats in Supply chain are:

-Delivered hardware with pre-installed malware like the case of Superfish in Lenovo industries.

-Malware installed into the hardware or software. An example is Dragonfly.

-Weaknesses in networks and software applications exposed by malicious attackers.

The security of one organization within a supply chain is only as strong as the weakest unit of the supply chain. A driven attacker will take advantage of this by pinpointing out the weakest link in the cyber security within the supply chain and making use of these existing weaknesses to gain entry into other units of the supply chain. An example of this is the vulnerability attack in Lenovo notebooks, dubbed “Superfish-Visual Discovery”and another attack known as MITM (Man-In-The-Middle) was recently uncovered. The result of this was that all security controls already installed in the notebooks could not catch the malware because it was already installed in the software components by default.

OTHER RECENT EXAMPLES OF CYBER SECURITY OUTBREAKS IN SUPPLY CHAINS

1. The above-mentioned example, Superfish, in Lenovo notebooks can be explained here in detail. Neither the end users nor the antivirus software pre-installed on the computer detected it to be malicious because it was already installed by default during manufacture, and as a result considered to be a trusted software. Superfish installs a self-assigned root HTTPS certificate that intercepts encrypted traffic for visits by users on websites. Anytime a user accesses an HTTPS website, the certificate is signed and managed by Superfish, fallaciously depicting itself as the legal website certificate. Also, the private encryption key that comes with the signed Superfish TLS certificate is the same for all Lenovo machines. Attackers may eventually make use of this key to certify fake HTTPS websites that disguise as Bank of Ireland on the

internet. In such scenarios, computers with Superfish root certificates will fail to identify these sites as fakes.

2. A cyber infiltration group, Dragonfly, attacked a pharmaceutical sector by infecting software with trojans. This allowed the Dragonfly group to replace authentic files in the software with malicious files. When downloaded from the supplier ' s website, this malicious software provided remote access functionalities that could gain total control over systems where the software was installed or eventually even made the systems behave like bots.

3. The Shylock banking trojans is another classic example of cyber-attack in supply chain. Attackers here use website builders to undermine authentic websites, rerouting requests to another malicious domain. As soon as the requests arrive, the malware is downloaded into the system and attacks MITB (Man-In-The-Browser) occurs. This attack is so serious that it evades exposure and guards itself from analysis, thus attackers focus on the builders of websites used by numerous companies resulting in a larger scope of infections.

Conclusion

Supply chain security is an enduring problem that needs to be considered and solved in the security field. Through previous case demonstrations and analysis, it is not difficult to see that the security of the supply chain is now under great pressure, facing the present. A wide variety of threats. For the traditional supply chain, not only need to do a good job of cargo safety inspection, improve the safety awareness of its employees, but also need to develop a detailed emergency plan, do the first time to reduce the loss received, for the software supply For the chain and network supply chain, for software practitioners, the first thing is to do software security protection design. For enterprise users, it is also necessary to use more software security specifications. For individual users, it is necessary to standardize yourself, download software from trusted sources or sites, and not spread pirated or downloaded software from third-party sites. The attack on the supply chain will never be reduced. What we can do is to consider prevention from all aspects. With the advancement of technology and the emergence of new technologies, the supply chain involves broad interests, so its security The challenges will be greater and greater. How to improve the attack defense measures is a consideration in the future supply chain security field.

References:

[1] L. Wainstein, "7 SUPPLY CHAIN SECURITY CONCERNS TO ADDRESS IN 2019," The Network Effect, 10

December 2018. [Online]. Available: https://supplychainbeyond.com/7-supply-chain-security-concerns-to-address-in-2019/. [Accessed 7 April 2019].

[2] A. GREENBERG and M. Mike, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," Wired, 22 August 2018. [Online]. Available: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/. [Accessed 6 April 2019].

[3] Supply & Demand Chain Executive. (2019). Cloud Computing Is Transforming Supply Chain Management. [online] vailable at:https://www.sdcexec.com/sourcing-procurement/article/12125647/cloud-computing-is-transforming-supply-chain-management [Accessed 12 Apr. 2019].

[4] G. Kovacs, "All About AWS EBS (Plus Five AWS EBS Functions You Aren't Using)," NetApp, 9 August 2018. [Online]. Available: https://cloud.netapp.com/blog/ebs-volumes-5-lesser-known-functions. [Accessed 6 April 2019].

[5] A. Allen, "Piracy on the rise and costing billions," Smart by Gep, 26 June 2017. [Online]. Available: https://www.cips.org/en-GB/supply-management/news/2017/june/piracy-on-the-rise-and-costing-billions/. [Accessed 7 April 2019].

[6] https://www.dw.com/en/cargo-ship-loses-270-containers-near-german-island-in-north-sea/a-46937361

[7] D. Stephens, "PERMISSIBILITY IN A PLATFORM FOR NMMES-TR AND THE DEPARTMENT OF DEFENSE," The Network Effect, 19 September 2017. [Online]. Available: https://supplychainbeyond.com/permissibility-platform-department-defense-nmmes-tr/. [Accessed 7 April 2019].

[8] threat?, I., Borgwardt, M., Pflughoeft, B. and snail, M. (2019). Is Ken Thompson's compiler hack still a threat?. [online] Software Engineering Stack Exchange. Available at: https://softwareengineering.stackexchange.com/questions/184874/is-ken-thompsons-compiler-hack-still-a-threat/184880 [Accessed 7 Apr. 2019].

[9] Antiy.com. (2019). XcodeAnalysis and review of unofficial versions of malicious code pollution incidents (XcodeGhost). [online] Available at: https://www.antiy.com/response/xcodeghost.html [Accessed 7 Apr. 2019].

[10] Securelist.com. (2019). ShadowPad in corporate networks. [online] Available at: https://securelist.com/shadowpad-in-corporate-networks/81432/ [Accessed 7 Apr. 2019].

[11] En.wikipedia.org. (2019). PRISM (surveillance program). [online] Available at: https://en.wikipedia.org/wiki/PRISM_(surveillance_program) [Accessed 7 Apr. 2019].

[12] Platform, H., Forensics, N., Security, E., Security, E., Demand, E., Defense, M., Portfolio, T., Services, F., Systems, I., Response, I., Retainer, I., Assessment, C., Assessments, R., Testing, P., Assessment, S., Assessment, R., Assessment, A., Exercise, T., Healthcheck, I., Training, E., Range, T., Development, C., Resellers, F., Partners, T., Partners, C., MSSPs, G., Enablement, P., Portal, P., Center, P., Locator, P., FireEye, P., Partner, B., Accreditations, P., Support, C., Portal, C., Programs, S., Products, S., Notices, S., Portal, D., Exploits, R., Reports, A., Reports, T., Industry, T., Groups, A., Security?, W., Vision, T., Email, N., Blogs, R., Downloads, F., Market, F., Training, E., FireEye?, W., Honors, A., Directors, B., Relations, I., Success, C., Stories, C., Opportunities, J., Relations, U., Releases, P., FireEye, C., Blogs,

F., Research, T. and Apps, i. (2019). iBackDoor: High-Risk Code Hits iOS Apps « iBackDoor: High-Risk Code Hits iOS Apps. [online] FireEye. Available at: https://www.fireeye.com/blog/threat-research/2015/11/ibackdoor_high-risk.html [Accessed 7 Apr. 2019].

[13] Supply & Demand Chain Executive. (2019). Cloud Computing Is Transforming Supply Chain Management. [online] Available at: https://www.sdcexec.com/sourcing-procurement/article/12125647/cloud-computing-is-transforming-supply-chain-management [Accessed 7 Apr. 2019].

[14] Tung, L. (2019). Microsoft: Petya ransomware attacks were spread by hacked software updater | ZDNet. [online] ZDNet. Available at: https://www.zdnet.com/article/microsoft-petya-ransomware-attacks-were-spread-by-hacked-software-updater/ [Accessed 7 Apr. 2019].

[15] "Cyber Security Risk in Supply Chain Management: Part 1," InfoSec, [Online]. Available: https://resources.infosecinstitute.com/cyber-security-in-supply-chain-management-part-1/#gref. [Accessed 7 April 2019].