Cybercrimes in E-commerce

Sujoy Kapoor

Abstract— The massive increase in the uptake of online transactions on the e-commerce platform has led to a new generation of associated security threats. The heightened use and implementation of technology in key markets all over the globe such as business and trading has not only expanded the horizons of commercial transactions but has also given rise to cyber terrorism. Numerous methods of cyber crime have been seen by the people of this world. There are now crimes like phishing scams, online harassment, invasion of people's privacy, etc. All such crimes lead us to one question. How can we prevent cyber crimes? How can we as responsible and informed individuals, citizens, and communities devise simple ways which can aid e-commerce companies to fight off this malice? The most fundamental reason behind the writing of this research paper is to discuss ways that may prove beneficial to prevent cyber crimes that online retail companies face in the e-commerce industry. I will be using both primary and secondary resources to enhance the quality of this research paper. I will be referring to journals and essays published by various reputed institutes so that the readers of this research paper can have a complete and concrete understanding of the subject at hand and can also have fruitful experience while reading the paper. Apart from published literature, I will also be studying the information provided on official government websites and the Police Cyber Crime Units' websites and will be inculcating it into my research paper as well.

Index Terms— attacks, cybercrimes, DDOS attack, e-commerce, encryption, HTTPS, malware, methods of preventing cyber attacks, POS attack, Perimeter Defenses

1 INTRODUCTION

In this day and age, various ventures and companies are employing the web to establish an online platform where people from all over the world can see and buy their products. This type of commerce is known as e-commerce or electronic commerce. Such online transactions require the transfer of information across the net. This involves the storage of a large amount of information in web services. Such information is frequently at risk of being obtained by unauthorized professionals such as hackers and unauthorized cyber experts. Millions of rupees and personal data are lost every year from the internet. Cyber-crimes are the obstacles in the path of success of e-commerce and online business. Cybercrime has become a quickly developing underground business worked by clever criminals, who purchase and sell highly classified financial data from a huge number of web clients in an online bootleg market. Such cyber experts are extremely adept at hacking into a large number of PCs consistently; the felony is conceivably a billion-dollar business. More often, cyber attacks come from malicious software being entered into our computer systems. This malware then takes complete control over our system and enables the criminals to get access to any information on our computer system. The whole process happens without the knowledge of the owner or user. To prevent such online frauds, there is a need of strong e-security policies which will make it extremely difficult for such cyber criminals to do their dirty job. Of course, plain human prudence is also essential, however policies, backed by the Law can prove more beneficial in the long run. However, in recent years, the efficiency of the Law has been questioned seriously because many of the tools that cyber criminals use are legal like various technologies or softwares. Electronic commerce and the internet may have become the part and parcel of almost half of the world population today but its perils are also present around us in disguise. [4], *[12], [13]*

- *Sujoy Kapoor is a grade XI student, currently pursuing the Indian Certificate of Secondary Education at The Doon School, Dehradun, 248001. E-mail: sujoykapoor657@gmail.com*

2 E-COMMERCE

As explained before, e-commerce, also known as electronic or internet commerce, refers to the buying and selling of various goods and services using the internet, and the transferring of private data and money to carry out transactions. Any sort of transaction facilitated through the internet essentially comes under the umbrella term of e-commerce.

2.1 History of E-commerce

The history of e-commerce can be traced back to the 1960s when Electronic Data Interchange (EDI) started getting implementing by businesses to share work related files or documents with other such companies and ventures. In 1979, an interesting development happened. The American National Standards Institute created the Accredited Standard Committee X12 (ASC X12) as a globally accepted standard for companies to share files and documents with each other through online networks. Gradually over a decade or two, the number of businesses sharing electronic files started increasing. Then, the rise of eBay and Amazon restructured the whole industry in 1990s. *[4]*

2.2 Applications of E-commerce

A range of applications are used to conduct the whole process of e-commerce like online catalogs and shopping carts, EDI, File Transfer Protocol, e-mail as well as web services. Business to business activities such as using e-mail for unwanted ads , more usually known as spam are included in these web applications to run e-commerce. These days, more and more companies, in order to attract a larger consumer base, are using various strategies such as digital coupons, targeted investments and social media marketing. First, Inter-organisational applications include supplier management, inventory man-

agement, distribution management and channel management. Second, Intra-organisational applications include workgroup management, collaborative publishing and sales force productivity. And third, customer to business applications include social portals as well as transactional portals. *[4]*

3 CYBER ATTACKS IN E-COMMERCE

There are a number of cyber attacks that retail and e-commerce companies face on a regular basis. Threats such as web application attacks, insider threats, POS attacks and others against a company's database are common problems for many online retail companies. It is also the responsibility of retail companies to reduce the number of people who have access to the system and database. Such access should only be allowed, given the employees job and should be monitored on a regular basis.

3.1 Types of Cyber Attacks

- **POS Cyber Attacks**

A very common type of attack on a company's customers' information is a POS or 'point of sale' attack wherein a customer's sensitive information such as their PINs or card numbers is stored. Cyber criminals often use malware to get access to this highly private financial information. They can get people's credit card information and PINs for any type of card used on a machine that has been infected with their malware. To understand this better, let us take an example and try to create a model where such classified information is lost.

Scenario: There is an online retail company which sells a range of food products. Cyber criminals have managed to install some sort of malware into the point of sale systems of the company. Point of sale systems may include portable devices and other emerging forms of online payments used to execute the transaction. The malware used by the criminals has also infected many other POS machines of the company, through which it can get the credit or debit card information of millions of customers. Furthermore, such private data is then sold for illegitimate purposes.

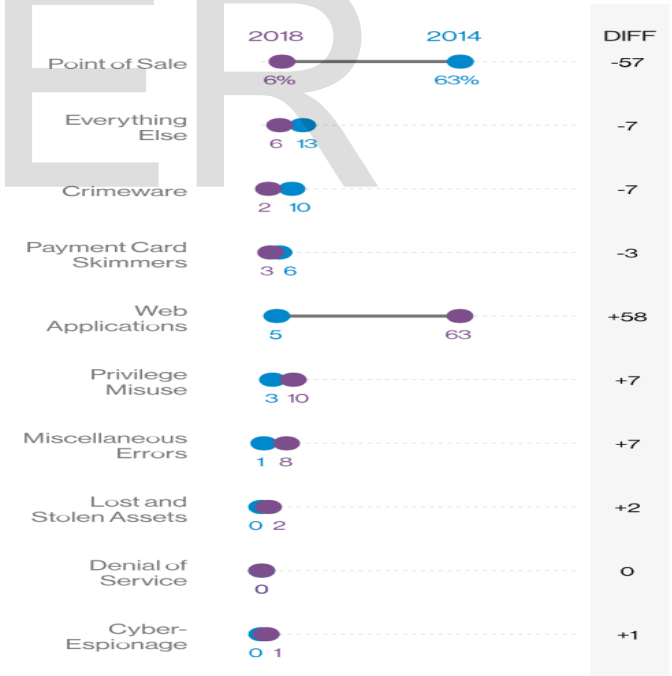
Methods Used: The malware which was used was most probably purchased on a bootleg market. It was then released into the company's retail environment from where it gradually spread onto POS platforms and got access to customer's data.

Financial Impacts: The company's brand name is damaged and there is also a drastic fall in sales. There were many financial implications like a deep cut in the market share of the company. It also had to compensate million of customers monetarily and offer free credit monitoring. [2], [3], [8]

- **Web Application Attacks**

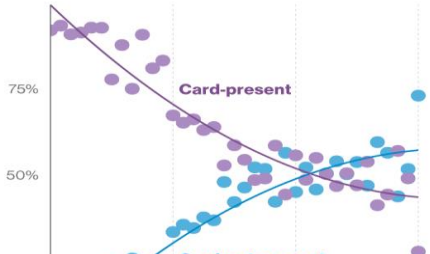
Another way of getting access to people's financial information is through attacking web applications of company's databases. A web application attack is when an attacker is able to find loopholes and vulnerabilities in the whole system and thereafter gains direct access to to personal data and financial details. Criminals will try to penetrate into a company's online payment application and then put a secret code which will record all information that the customer enters. Malware can also be inserted using a method called a tool called the SQL injection . This can allow them to do the following: Fake their identity, tamper with databases, gain complete access to all data, take control of computers and networks and end malicious emails on the company's behalf.

Verizon Wireless is a telecommunications company which provides services to approximately 154 million people. According to its 2019 Data Breach Investigation Report (DBIR), attacks against web applications have started to increase, leaving point of sale attacks in the second place. As the figure on the left shows, the difference between POS attacks from 2014 and 2018 is -57% . On the other hand, the difference between attacks on web applications from 2014 to 2018 is +58%. This distinctly shows that attacking web applications now appeals



more to cyber criminals. *[1], [3]*

The National Cyber Forensics and Training Alliance (NCFTA) has concluded that web application attacks have increased not only the number of card present fraud but card not present fraud as well. *[1], [3]*



- **Insider Threats**

People working for an organisation are its most valuable resource. However they may pose potential threats to the company as well. Insider threats essentially refer to threat from various employees or people who work in the company and have access to the company's crucial data. Companies often have several points of vulnerabilities and considering the high movement of employees within different departments of the company, insider threats may prove to be extremely dangerous. Retail giants like Amazon, eBay etc. have a huge number of people working in close quarters to some of the company's classified information. Adding all the other third parties and workers employed on a seasonal basis, it is not possible to keep a close eye on each and every one of them while they manage key business aspects. If we think about it, carrying out such an insider attack is no rocket science. For example, an employee might use a pen drive or any sort of data storage tool to duplicate or copy information of customers or the companies business strategies like pricing or marketing. Then the employee will simply walk out the door with all the data hidden in garments.
There are many definitions for Asset Loss but the most appropriate in context to the current online retail setting is : Asset Loss is when a company's classified or sensitive information, intellectual property, proprietary information or any other material is disclosed, leaked or compromised and causes damage to the company's reputation, sales, customer confidence, public interest and productivity.

Examples of insider threats that lead to asset loss:

- Corruption: Indulging in activities inconsistent with one's duty or other's rights in order to gain an advantage.
- Espionage: The practice of spying by any means to get access to secret information.
- Embezzlement: Misappropriation or theft of assets belonging to one's employer.
- Sabotage: Deliberate act of destruction or disruption of work processes or materials.
- Disclosure of Personally identifiable Information: Making employee or customer information public resulting in the misuse of assets.
- Stealing Intellectual Property: Robbing people or companies of their ideas and creative expressions and inventions. [4], [6]

- **Distributive Denial of Service (DDOS) Attacks**

A DDOS attack simply involves thousands of requests from undetectable IP addresses filling up a company's websites's servers. DDOS attacks can be potentially very harmful for companies as they not only do their harm but make way for other type of attacks to be executed too such as a malware installation. Such an attack is generally a result of several compromised systems flooding the targeted system with excess traffic.

On Black Friday, 23rd of November 2018, there was an exponential increase in the number of DDOS attacks on e-commerce companies. DDOS protection provider, Link11, observed a surge in this type of cyber attacks between Black Friday and Cyber Monday, the 26th of November 2018. In fact, on Cyber Monday, the frequency of attacks increased by 109% compared to the average number of attacks in November. These DDOS attacks were of up to 100 Gpbs and also represented a 40% compared to the previous quarter. Looking at the devastating financial implications of this attacks, it can be concluded that a company can possibly lose thousands and millions of dollars. The most harmful aspect will however be that the company will lose its customer base and customers will no more trust the company and will lose confidence. This will in turn lead to a sharp cut in sales. [6] ,[7]

- **Bad Bots**

Internet bots are basically automated programs which have a particular task on the web and they perform it. There are good bots which usually help search engines etc. However with good bots come bad bots as well. Bad bots specialise in imitating human like work processes across web applications and cause severe harm to a business. It has been roughly estimated that bad bots constituted one-fifth of all e-commerce traffic that took place in 2018. There are various ways through which bad bots can negatively affect an e-commerce company.

- Account Acquisition: A major industry that has developed in the dark web is the buying and selling of people's login details and credentials. Once any cyber criminal gets access to these credentials, an army of bots can be developed to figure out usernames and their passwords of people on different retail sites. Once successful, several orders of various products can be made, and details can be stolen and harm can reach to both customers and the company.
- Credit Card Fraud: It is also possible to programme bots in such a way that they test card verification value and credit card numbers of stolen credit cards repeatedly until they

manage to get into people's accounts. Again, once hackers get hold of this information and get into the accounts of people, they can simply place various orders and purchase products under the name of someone else.

- Price Scraping: It has become quite a frequent phenomenon that companies in competition to each other end bots to examine the business strategies, pricing strategies, marketing styles as well as stock value. This will benefit companies to establish their business strategies in a way that they outrank the others and gain the highest market share by eliminating competition. [6], [8]

- **Phishing and Spear Phishing**

Phishing is the fraudulent attack or social engineering attack often used to obtain user data like passwords and usernames as well as credit card and debit card details. It happens when a criminal, disguised as a trusted entity like an official of a retail company sends out malicious emails to customers who fall into their trap and open the unsafe malware links that are often attached in the email or text message. Estimated by the Anti-Phishing Working Group (APWG), the number of phishing attacks reported rose by 186% from 2013 to 2015. Spam filters can also catch such emails, however they are not able to do so in the face of spear phishing.

Spear phishing is a different, yet more hazardous variant of phishing that targets specific people with emails that appear as if they are from friends or close colleagues. Criminals indulging in spear phishing have to rely on impersonation. The potential business impacts of phishing and spear phishing are very serious. They include:

- Breach of customer data
- Outright theft
- Loss of potential revenue
- Damage to e-commerce brand name
- Compensating customers who have been affected
- Paying fines if bound by Payment Card Industry policies [6], [8], [9]

4 METHODS OF PREVENTING CYBER ATTACKS AGAINST E-COMMERCE

There are a few questions that a retail company should think about before creating a security network.

- How to store sensitive information?
- What general mistakes to avoid?
- Which methods and measures can be adopted in times of crisis? [4]

- **Choice of Hosting Provider**

A hosting provider is an internet hosting service that allows organisations and companies to serve content on the net. It runs the internet servers for whichever company and offers various levels of services such as web hosting. For retail companies, it is extremely essential to choose a hosting provider who provides most of the following services:

- Swift service
- Immediate disaster recovery
- AES Encryption (Advanced Encryption Standard)
- 24/7 technical help
- Network monitoring
- Scheduled backup program

Besides offering all these services, a hosting provider should always keep a companies website running without any technical breakdowns. Companies should keep one thing in kind that they should opt for reliability and quality over cost-affordability. [4]

- **HTTPS Encryption**

In its 2014 I/O conference, Google said that they would introduce the HTTPS encryption system as a major ranking system or search engines. This encryption system did not only give a boost to companies' websites but also made customers trust encrypted sites more. Adding an EV SSL (Extended Validation Secure Sockets layer) certificate works by putting a green HTTPS prefix to the URL of the site and a symbol of a green padlock on the address bar. The basic advantage of doing all this is to encrypt the transmission of data and information from the web server to the browser. It has also been concluded that sites with HTTPS encryption experience higher conversions than those which lack HTTPS encryption.
The following are the benefits of using an SSL certificate:

- SSL protects data. The primary role of an SSL certificate is to encrypt all the information in order to safeguard communication between the client and the server. SSL encryption basically makes a website unsurpassable and makes it very difficult for hackers to hack in.

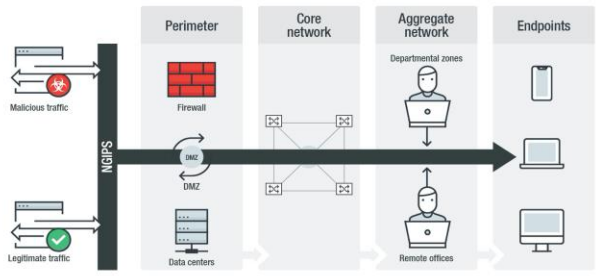
- Better search engine ranking. In 2014, changed were made to its algorithm by Google so that websites having HTTPS encryption could have an upper hand. Several studies have been conducted by SEO (Search Engine Optimisation) experts. The one conducted by the founder of backlinko.com, Brian Dean, distinctly demonstrates a strong, positive correlation of HTTPS encrypted sites against higher search engine rankings.

- SSL affirms identity. In order to install an SSL certificate, a website needs to go through a process of validation which is conducted by Certificate Authority (CA). The CA verifies a website depending upon the type of certificate. Then trust indicators vouch for the website's integrity, attracting customers. Such HTTPS encryption makes sure that no third party entity forms a fake website that pretends to be someone else's.

- SSL improves customer trust. Besides providing services of authentication and encryption, SSL certificates prove beneficial when it comes to the point of view of customers. They tend to trust encrypted websites more as they know their data will be secure. [4]

- **Compliance with PCI**

PCI, also known as Payment Card Industry makes is mandatory for websites that involve financial transactions to undergo an



How the next-generation intrusion prevention system protects networks

annual risk or vulnerability assessment. PCI compliance contains various levels, depending upon the number of financial transactions that are conducted in one year through a particular website. A PCI compliance assessment involves a website to undergo an annual risk assessment and a self-assessment questionnaire if the number of transactions in one year is 20,000 or less. The whole motive behind doing a PCI assessment is to protect and secure online transactions that happen in credit card companies.
The following are some of the benefits of being a PCI compliant:

- Boosts confidence of customers in one's websites.
- Manages risk around identity theft
- Helps to stay competitive in the market
- Avoids fines imposed by banks
- Protects customer information
- Reduces impacts of negative cash flow [4]

- **Strengthening Perimeter Defenses**

A very common method which hackers use to get into website servers or is by exploiting weak links or those which might be broken. There are several vulnerabilities in a company's website and hackers attempt to find them and then get through them. Some ways through which this can be prevented is using fire walls and VPNs. Securing one's website is very similar to securing one's home. People put barbed wire around the walls of their homes to prevent people with wrong intents to come in. The same applies to e-commerce websites. Firewalls can be added to allow only authorised people to enter.
One really beneficial method would be to develop the aNext Generation Firewall (NGFW). *Gartner* is a leading research and advisory company which provides business insights, advice and essential tools to companies which they need to build themselves up and protect themselves from harm. Gartner defines NGFW as a "*deep-packet inspection firewall that moves beyond port/protocol inspection and blocking to add application-level inspection, intrusion prevention, and bringing intelligence from outside the firewall.*" NGFWs are very similar to traditional firewalls. They have all the functions which a traditional firewall has like they use both dynamic and static packet filtering as well as support from VPN in order to make sure that the internet, firewall and network are all connected and secured. However the main difference is that they are able to filter packets based on applications. They are able to distinguish between a safe application and unwanted ones by using a signature based IPS (Intrusion Prevention System). [11]

- **Awareness and Employee Training**

First of all, the company should closely monitor those employees who work in close quarters with sensitive information. Access to classified information should only be given to trusted professionals and important passwords should be changed from time to time. Other than that, proper awareness about cyber hygiene and safety should be spread to the employees. The less the number of people knowing important and confidential credentials, the better. There should be a strict no-share policy within companies which may prevent employees from sharing each other's passwords or more im-

portantly the passwords of the company's accounts etc. Moreover, unauthorised USB devices, pen drives and others such as hard drives should not be allowed in the premises of the company's office. Usually, unauthorised pen drives have several different viruses in them which may enter the companies system if the pen drive is attached to any device. The accounts of those employees who leave the company, get retired or get fired should be deactivated to prevent any external leakage of information. [4], [12], [13]

5. CONCLUSION

There is a positive correlation between the increase in online business as well as the number of cyber crimes that happen as a result. Cyber crime has been growing its long tentacles across the globe and has affected both e-commerce and the lives of millions of people. Although not everyone in the world who is connected to the internet is a victim of cyber crime but almost everyone is at risk. According to the Gelmato Breach Index, more than 14 billion data records have been stolen from e-commerce companies since 2013. It has also been estimated that online businesses who lose less than 1% of their customers actually face an average loss of $2.8 million in real money. To get a clear picture of the magnitude at which cyber crimes happen in the e-commerce industry, we must know that 95% of breached records in 2016 were from three industries: Government, Retail and Technology. A Clark School study at the University of Maryland quantified the rate of hacker attacks. They estimated that in every 39 seconds on average, there is a hacking attack. All these numbers only tell us that committing cyber crimes these days is no mammoth task and preventing cyber crimes is just as colossal. Each and every person connected to the net is vulnerable in some way or the other. More specifically when we talk about e-commerce, we see an ocean of ways through which cyber criminals can commit crimes. Therefore, it is essential to devise ways, technical as well as non-technical in nature, to solve this problem. The cyber security problem will never be solved once and for all, however it is out duty to fight it with rigour and determination. [13], [14]

ACKNOWLEDGEMENT

I sincerely express my gratitude to Mr. Rakshit Tandon (Mentor/Coordinator/Advisor- Gurugram Police Cyber Security Summer Internship 2020, Director/Co Founder- Hackershala/CodesNag, Cyber Security Consultant- Internet and Mobile Association of India (IAMAI), for his extremely valuable knowledge and support.

REFERENCES

[1] Retail Data Breaches." Verizon Enterprise, Verizon, enterprise.verizon.com/resources/reports/dbir/2019/retail/.

[2]Retail - Cyber Executive Briefing: Deloitte: Analysis." Deloitte Bosnia and Herzegovina, 25 June 2014, www2.deloitte.com/ba/en/pages/risk/articles/retail.html.

[3] Cyber Threats For Retail & E-Commerce Companies - F-Secure Blog." F, 27 Feb. 2020, blog.f-secure.com/cyber-threats-for-retail-ecommerce/.

[4] Sireesha, C., Sowjanya, V., & .Venkataramana, K., Dr. (2017, May). Cyber security in E-commerce [Scholarly project]. In International Journal of Scientific and Engineering Research. Retrieved from ijser.org

[5] Munjal, Sourabh, and Anooja A. "(PDF) Cyber Crimes Threat for the E-Commerce." ResearchGate, Unknown, 1 Jan. 2016, www.researchgate.net/publication/306401151_Cyber_Crimes_Threat_for_the_E-Commerce.

[6] Dutta, Pallavi. "Top 5 Cyber Threats to E-Commerce Security." Kratikal Blog, 30 June 2020, www.kratikal.com/blog/top-5-cyber-threats-to-e-commerce-security/.

[7] Ashford, Warwick. "E-Commerce Sites Warned of Heightened DDoS Threat." ComputerWeekly.com, ComputerWeekly.com, 30 Nov. 2018, www.computerweekly.com/news/252453494/E-commerce-sites-warned-of-heightened-DDoS-threat.

[8]TeskaLabs. "TeskaLabs Blog · 5 Cyber Threats ECommerce Websites Should Watch Out For." TeskaLabs Blog, teskalabs.com/blog/ecommerce-website-cyber-threats.

[9]"E-Commerce Security Issues: Phishing and Spear Phishing." Vade Secure, 20 Dec. 2018, www.vadesecure.com/en/ecommerce-security-issues/.

[10]*What Is a Next Generation Firewall? Learn about the Differences between NGFW and Traditional Firewalls." Digital Guardian, 24 Oct. 2019, digitalguardian.com/blog/what-next-generation-firewall-learn-about-differences-between-ngfw-and-traditional-firewalls.*

[11] *Guide to Network Threats: Strengthening Network Perimeter Defenses with Next-Generation Intrusion Prevention." Security News - Trend Micro USA, www.trendmicro.com/vinfo/us/security/news/security-technology/guide-to-network-threats-strengthening-network-perimeter-defenses-with-next-generation-intrusion-prevention.*

[12]*Security Best Practices." Cyber Swachhta Kendra: Security Best Practices, Government of India, www.cyberswachhtakendra.gov.in/security-best-practices.html.*

[13]*Security Tools." Cyber Swachhta Kendra: Security Tools, www.cyberswachhtakendra.gov.in/security-tools.html.*

[14] 2019 Cyber Security Statistics Trends & Data. (2020, July 10). Retrieved July 30, 2020, from https://purplesec.us/resources/cyber-security-statistics/