NEW TRENDS IN CYBER-CRIME AND ITS IMPACT ON BUSINESS

Dr. Sandeep*

Assistant Professor in CSE, OM Sterling Global University, Hisar, Haryana, India

***Email ID**: ssg0177@gmail.com*

Accepted: 14.04.2023 **Published**: 27.04.2023

Keywords: Cybercrime, Digital DNA theft, Botnets, QR code, Ransomware.

Abstract

Cyber threats are evolving faster than ever and the cybercrime underground has become an organized cyber crime ecosystem. In 2021, ransomware activity increased significantly. The number of hacked companies found in our sources has almost doubled – from 1,460 to 2,860 victims. To effectively combat these threats, it is essential for cybersecurity professionals to stay abreast of the latest trends in cybercrime. New technology increases the reach and impact of cybercrime: malware and ransomware attacks (the latter threatening to release data or block it permanently if a ransom is not paid) increased by more than 350 percent and 430 percent respectively in 2020. Next-generation tools are antivirus bypassing, which is why living off the land (LOtL) attacks, where attackers use legitimate software and features to commit malicious actions, accounted for nearly two-thirds of all reported incidents in 2021. In this paper, we look at the trends shaping the future of cybercrime threat intelligence and how organizations can protect themselves. We'll also discuss how these trends are impacting the way businesses need to protect themselves from attacks.

Paper Identification

**Corresponding Author*

1.Introduction :-

Cybercrime' is an umbrella term used to refer to all crook activities which might be done over the internet. computer crime, also called computer crime, using a computer as a tool for other illegal purposes, such as committing fraud, trafficking in child pornography and intellectual property, identity theft, or invasion of privacy. Cybercrime, especially via the Internet, has grown in importance as the computer has become central to business, entertainment and government.

New technologies create new opportunities for crime, but few new types of crime. What distinguishes cybercrime from traditional crime? Obviously, one of the differences is the use of a digital computer, but technology alone is not enough to make the distinction that might exist between different areas of criminal activity. Criminals don't need a computer to commit fraud, traffic in child pornography and intellectual property, steal identities, or invade someone's privacy. All of these activities existed before the prefix "cyber" became ubiquitous. Cybercrime, especially involving the Internet, represents an extension of existing criminal behavior alongside some new illegal activities.

The size of the global cybersecurity market is expected to expand at a compound annual growth rate of 12 percent between 2022 and 2030 from $184.93 billion last year, according to US firm Grand View Research. Increasing number of cyber-attacks and rapid proliferation of online shopping platforms, increased adoption of cloud-based solutions, and rapid proliferation of smart machines and connected devices are some of the factors driving the growth of the market.

2. New trends in cybercrime

As the industry grows at a fruitful pace, *The National* looks at the top 10 cyber security threats and trends of the year ahead.

2.1.Digital DNA theft:-

In 2023, deep fakes will become so authentic that not only will we see our digital identities stolen, but digital versions of our DNA will be at risk, according to experts. Exposing our digital DNA on the internet will allow deep fakes to replicate and create digital humans. A deep fake is an impersonation of a person created using advanced technologies, including artificial intelligence and machine learning. It's only a matter of time before attackers create realistic digital avatars of anyone, and it will be incredibly difficult to tell the difference without sophisticated raw data analysis technology.

2.2.Cybercriminals are becoming more collaborative and specialized:-

Today, almost all cybercrime is committed by organized groups. The solo hacker is basically a thing of the past. Even script kiddies work in small groups. The largest and most sophisticated

attacks require the skills of tens or even hundreds of attackers. The most prolific cybercriminals are divided by expertise and collaborate with other hackers or criminal groups.

2.3. Botnets and automated malware deployment tools are becoming increasingly sophisticated:-

As the Internet of Things expands, so do the opportunities for attackers. More and more devices are connected to the Internet, providing new entry points for malicious actors. And as these devices become more sophisticated, so do the tools and techniques used by attackers. There has also been an increase in the use of encrypted communications by attackers. This makes it difficult for security teams to track and trace attackers. As encryption expands, it becomes increasingly difficult to defend against attacks that use it. These trends underscore the need for better threat intelligence across all domains, not just critical infrastructure providers. As attacks become more sophisticated, all businesses must ensure that their threat intelligence sources provide timely, accurate and relevant security data.

2.4Strategies to thwart supply chain threats:-

The range of threats related to supply chains has never been higher. Attackers now have more resources and tools at their disposal to disrupt supply chains, which are critical to maintaining an adequate supply of goods and services, especially during a pandemic such as Covid-19. Standard care and security assessments performed by chief security officers at third parties are no longer adequate given the escalating frequency and impact of supply chain attacks,

2.5Camera-based malware:-

The camera on mobile devices is a powerful tool for documenting memories and everyday life. These cameras have been enhanced with software algorithms that recognize artificial intelligence tools to enhance the quality of images and videos.

In 2023, we [expect] to see the first of many exploits that challenge smart cameras and the technology embedded in them to exploit vulnerabilities," said Brian Chappell, BeyondTrust's chief cybersecurity strategist for Europe, Middle East, Africa and Asia and the Pacific.

2.6 Cyber-attacks transferring between smart devices:- The smart home and Internet of Things (IoT) devices are increasingly targeted by cybercriminals as the most vulnerable entry points into any home or business security network. A typical cyberattack shifts from the hacker to the device, but 2023 may bring cyberattacks that jump to smart devices, including wearables, voice-activated assistants, smartphones and home temperature control devices, experts said.

2.7Collaboration between state-sponsored actors and cybercriminals is on the rise :- The increased collaboration between nation-state threat actors and cybercriminals is a dangerous trend with far-reaching consequences. On the one hand, nation states have access to an abundance of resources and talent that criminals can use to carry out sophisticated cyber attacks. On the other hand, cybercriminals are motivated by profit, not politics, and are therefore more likely to be willing to sell their skills to the highest bidder. The combination of these two factors makes it inevitable that we will see more and more cases of highly sophisticated cybercrime in the future. This is a trend that businesses need to be very alert to as it has the potential to bypass the security processes of organizations that are caught unawares.

2.8.QR code threat getting real:- A QR code is a machine-readable code used to store information for reading by a smart device. It is like a digital business card that usually contains various details such as phone number, email and home address.

2.9**Jump of ransomware:-**

Ransomware use has picked up pace and become more dangerous in 2022. It will continue to rise rapidly in the coming year and its variations will increase with the frequency of attacks. A recent report by security firm Cybereason found that 73 percent of organizations suffered at least one ransomware attack in 2022, compared to just 55 percent in 2021.

A Global Study on Ransomware Business Impact[2]

In response to these evolving threats, Cybereason has released the second annual *Ransomware: The True Cost to Business 2022* report, to assist organizations in defending against ransomware attacks.

Key Highlights:

- 73% of respondents said their organization had been the target of at least one ransomware attack over the past 24 months (an increase of 33% percent from the 2021 survey).

-Nearly half **(49%) paid to avoid any loss of revenue**, while **41% paid to expedite recovery**

- Of the 46% of organizations that reported losses from a ransomware attack, **67% said their combined losses reached between $1 million and $10 million (USD)**.

- Of the 28% of respondents who paid the ransom, **80% of them got hit with a second ransomware attack** and **68% percent got hit a second time within a month** and for a higher ransom.

2.10.Cyberattacks are on the rise and becoming more expensive:- According to some estimates, nearly two-thirds of companies say they have been the victim of a cyberattack in the past year. The economic impact of these attacks is significant, costing the global economy about $445 billion each year and only getting worse.

3. Types of cybercrimes that affect businesses :- Cybercrime against businesses can take many forms, including data breaches, ransomware attacks, malware infections, phishing scams, denial of service attacks, and identity theft. Data breaches involve the unauthorized release or access to secure information such as customer data or financial information. Ransomware attacks are when malicious software encrypts a company's data until a ransom is paid for the encryption key. Malware infections are when malicious code infiltrates a computer system and disrupts operations or collects sensitive data. Phishing scams utilize deceptive emails that appear to be from legitimate sources to gain access to usernames and passwords. Denial of service attacks floods a network with traffic in an attempt to shut down systems and prevent access. Identity theft involves stealing someone's personal information, such as Social Security numbers or credit card numbers in order to commit fraud.

4.Cybercrimes effects on businesses :- Cybercrime has become a disruptive and costly problem for businesses of all sizes. From data breaches to ransomware and phishing scams, cybercriminals have found many ways to exploit technological vulnerabilities to steal valuable business data or extort money. These attacks can not only cause financial losses, but can also lead to reputational damage, regulatory fines and long-term litigation costs. The best way for businesses to protect themselves from cybercrime is to proactively implement security measures such as firewalls and anti-virus software, regularly update their systems with the latest patches, use strong passwords, and train employees to spot potential threats.

4.1Financial losses:- Cyber security breaches can cause various financial losses to businesses. These include the costs of mitigating the breach, such as hiring experts to investigate and repair the damage, informing customers, and handling legal claims. A breach can also result in lost revenue from delayed or canceled projects and reputational damage if sensitive customer data is leaked. Companies can also face heavy fines from government regulators if they fail to meet minimum security requirements. In extreme cases, a cyber security breach can even cause businesses to shut down.

4.2Customer trust :- In the same vein, customers may no longer feel safe trusting a company with their sensitive information due to a security breach and may choose to take their business elsewhere. A company can also suffer from negative publicity that can damage its reputation and lead to a loss of customers and revenue. In addition, if customers file lawsuits against the company for failing to meet its security obligations, trust in the company could be further eroded.

4.3Reputational damage:- Reputational damage from cybersecurity breaches occurs when sensitive customer data is leaked or stolen. This can lead to a loss of trust in the company and negative publicity that could damage its brand and reputation. Companies may also face legal consequences if they fail to protect consumer data adequately. In some cases, customers may file lawsuits against the company for failing to meet their security obligations. Reputational damage from cybercrime can be difficult and expensive to repair, so businesses should take all possible precautions to protect themselves and their customers from cyber threats.

5. Cybersecurity cost to businesses :-

The cost of cyber security for businesses can vary widely depending on the size and complexity of the organization. Small businesses may be able to deploy basic security measures such as firewalls, anti-virus software, and strong passwords for a few hundred dollars a year. However, larger organizations with more complex networks may need to invest tens or even hundreds of thousands of dollars annually to adequately protect themselves from cybercrime threats. In addition to these costs, companies also face potential financial losses related to data breaches, ransomware attacks, malware infections, phishing scams, denial-of-service attacks, and identity theft.

6.How to protect your business from cybercrimes:- Here are some best practices to establish to help protect yourself and your business against a wide variety of cybercrimes today:

6.1Use reliable security solutions:- With the wide range of cybercrimes targeting your business, you'll need to take advantage of security software solutions to ensure comprehensive protection, including:

• A reliable antivirus/antimalware solution, ideally with AI-driven behavior detection technology.

• Bot detection and mitigation solution to monitor and protect your network from malicious bots in real time.

A real-time brand protection solution to detect trademark and copyright infringement and perform automatic takedown requests

6.2. Use strong and unique passwords:- Make sure your passwords are long (at least ten characters) and complex enough (use a combination of at least ten letters, numbers and symbols).

6.3.Keep everything updated:- Cybercriminals regularly try to exploit known vulnerabilities and bugs in your software or operating system to gain access to your system. Make it a habit to regularly update all software and operating systems, including and especially your Internet security solution (ie, antivirus.).

6. 4. Educate and train your employees:- Your company's security is only as strong as the least knowledgeable people on your team. Even if only one employee is compromised by a phishing scheme, it can be a gateway for cybercriminals to access your entire system.

7.What's next:- Cybercrime is no longer the exclusive concern of larger and more popular businesses, but smaller businesses and even individuals are also at risk. The cost of cybercrime could reach $10.5 trillion annually by 2025. This means that it is everyone's responsibility to protect themselves from cybercrime, otherwise the danger may increase. By following the practical tips we've shared above, you now have a solid foundation to protect yourself and your business from any cybercrime attempt**.**

Technology will deepen inequalities, while cyber security risks will remain a constant problem. The technology sector will be one of the main targets of stronger industrial policies and enhanced state intervention. Fueled by government aid and military spending as well as private investment, research and development of new technologies will continue apace over the next decade, bringing advances in artificial intelligence, quantum computing, and biotechnology, among other technologies. For countries that can afford it, these technologies will provide partial solutions to a range of emerging crises, from addressing new health threats and critical

healthcare capacity to expanding food security and climate mitigation. For those who cannot, inequality and divergence will grow. In all economies, these technologies also bring risks, from spreading disinformation and misinformation to uncontrollably rapid exodus of both blue-collar and white-collar workers. However, the rapid development and deployment of new technologies, which often come with limited protocols governing their use, presents its own set of risks. The ever-increasing intertwining of technology with the critical functioning of societies exposes the population to direct domestic threats, including those that seek to disrupt the functioning of society. Along with the rise of cybercrime, attempts to disrupt critical technology resources and services will become increasingly common, with attacks expected on agriculture and water, financial systems, public safety, transportation, energy, and domestic, space, and undersea communications infrastructure. Technological risks are not limited to rogue actors. Sophisticated analysis of larger data sets will enable the misuse of personal data through legitimate legal mechanisms, weakening individual digital sovereignty and the right to privacy, even in well-regulated democratic regimes.

Conclusion:-

The growth of potential sales in cyberspace is the reason for increasing attention to cyber crime. Consumers should seek more information regarding online shopping issues in the virtual world and the risks associated with expectations that are not in line with reality. Companies must increase the trust of customers by creating security systems in cyberspace. The security system is not only for companies, but also to protect consumer information

In this we have discussed an important problem that most countries in the world are facing today and in the coming years, which is cyber crime. In this context, we have described in detail the area of cybercrime and outlined the issue of cyber security. In fact, this barrier appears to be hard and almost insurmountable for most countries. Instead, researchers are implementing various measures to stop or reduce the side effects of cyber attacks. Our methodology comes to shed light on the use of standards and methods highly recognized in the security domain and select the best processes of these trademark frameworks and mostly adapt them to the entire cyber security process using multi-agent systems. The methodology we used is an implementation of our EAS-SGR framework combined with an action plan applied to cyber security. In addition, we paired it with team members responsible and mostly responsible for following the procedures and regulations set by governments through laws. The growth of potential sales in cyberspace is the reason for the increased attention to cybercrime. Consumers should seek more information about the challenges of online shopping in the virtual world and the risks associated with unrealistic

expectations. Companies must increase customer trust by creating security systems in cyberspace. The security system is not only for companies, but also for the protection of consumer information.

References

1.https://www.forbes.com/sites/forbestechcouncil/2022/12/19/5-trends-shaping-the-future-of-cybercrime-threat intelligence/?sh=4f42313f30a6

2.https://www.cybereason.com/ransomware-the-true-cost-to-business-2022

3.https://www.businesstoday.in/latest/economy/story/india-reports-118-jumps-in-cyber-crime-in-2020-ncrb-data-306890-2021-09-16

4.https://www.businesstoday.in/latest/economy/story/india-reports-118-jumps-in-cyber-crime-in-2020-ncrb-data-306890-2021-09-16

5.https://www.weforum.org/agenda/2023/01/global-rules-crack-down-cybercrime/

6.2013 NSA Competition for the Best Scientific Cybersecurity Paper, Official website, 2012.

7.London conference on cyberspace, Vice President Biden, "Vice President Biden delivers remarks in the London Conference for Cyberspace .WebSite for "Prizes for Cyber Security challenge", UK , 2013

8.Holm, H.,sommestad, t.;ekstedt, m.;Nordstrom, l. ; "Cysemol: a tool for cyber security analysis of enterprises"R. Inst. of Technology, Proc. Of the 22nd International Conference and Exibition on Electricity Distribution,2013,Stockholm

10. von Solms R, van Niekerk J, From information security to cyber security, Computers & Security (2013) in press,

11.Hajar Iguer, Hicham Medromi, and Adil Sayouti, "The Impact of the 4th Wave on the Governance of Information Systems: IT Risk Architecture- EAS –SGRBased on Multi-Agents Systems," International Journal of Computer Theory and Engineering vol. 6, no. 5, pp. 432-437, 2014.

12. Gustavo Alberto de Oliveira Alves, Luiz Fernando Rust da Costa Carmo and Ana Cristina Ribeiro Dutra deAlmeida "Enterprise Security Governance :A practical guide to implement and control Information Security Governance (ISG)" The First IEEE/IFIP International Workshop on Business-Driven IT Management, 2006. BDIM '06 pages 71 - 80.

13.Mark Brown, Director for Advisory Risk & Information Security at Ernst & Young,"Enterprise Security Architecture" , computer weelk

14. Grabner-Kraeuter, S. (2002). The role of consumers' trust in online-shopping. Journal of Business Ethics, 39(1-2), 43-50.

15. Fishman, R. M., Josephberg, K., Linn, J., Pollack, J., & Victoriano, J. (2002). Threat of international cyberterrorism on the rise. Intellectual Property & Technology Law Journal, 14(10), 23-23.

16. Koufaris, M. (2002). Applying the technology acceptance model and flow theory to online consumer behavior. Information systems research, 13(2), 205-223.

17. Isaac, R. G., Zerbe, W. J., & Pitt, D. C. (2001). Leadership and motivation: The effective application of expectancy theory. Journal of managerial issues, 212-226.

18. Smith, A. D. (2002). Loyalty and e-marketing issues: customer retention on the web. Quarterly Journal of Electronic Commerce, 3, 149-162.

19. Saban, K. A., McGivern, E., & Saykiewicz, J. N. (2002). A critical look at the impact of cybercrime on consumer Internet behavior. Journal of Marketing Theory and Practice, 10 (2), 29-37.

20. Miyazaki, A. D., & Fernandez, A. (2000). Internet privacy and security: An examination of online retailer disclosures. Journal of Public Policy & Marketing, 19(1), 54-61.

21.Smith, A. D., & Rupp, W. T. (2002). Issues in cybersecurity; understanding the potential risks associated with hackers/crackers. Information Management & Computer Security, 10(4), 178-183.

22. Berkowitz, B., & Hahn, R. W. (2003). Cybersecurity: Who's watching the store?. Issues in Science and Technology, 19(3), 55-62.

23. Smith, A. D., & Rupp, W. T. (2002). Application service providers (ASP): moving downstream to enhance competitive advantage. Information Management & Computer Security, 10(2), 64-72.

24. Movahedi-Lankarani, S. J. (2002). E-commerce: Resources for doing business on the Internet. Reference & User Services Quarterly, 41(4), 316.

25. Rossanty, Y. & Nasution, M.D.T.P. (2018). Information Search, And Intentions to Purchase: The Role of Country of Origin Image, Product Knowledge, and Product Involvement. Journal of Theoretical & Applied Information Technology, 96(10).

26.https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf