Development of Cyber Threats In The Past 30 Years And What The Future Holds

Marcelo Fernandes
Wellington, New Zealand
Email: marceelofernandes@gmail.com

***Abstract*—This paper presents a summary of the development of cyber attacks and security counter-responses from the 1990s until the present date. A section is dedicated to the prediction of cyber risks for the next decade and what implications these risks might have in law, ethics, and across governments and organisations. This paper also provides examples on how cyber criminals might exploit technologies such as cloud computing, artificial intelligence, machine learning, and other techniques to their advantage. A conclusion is provided with recommendations for organisations and governments to manage and assess cyber-security risks in the future.**

March 8, 2021

I. 1990s

This discussion starts by looking at the 1990s - the decade where the internet started to scale globally. In the beginning of this decade computer engineers had been aware of cyber threats and the first companies creating antivirus scanners had already been operating for a few years [1]. Due to both the way computers were used and the small number of networks, the dissemination of threats was many times slower than what we have today. Antivirus programs were mainly focused on scanning computer folders and finding files that matched against a database of known viruses. This approach was an early implementation of signature-based intrusion detection, and though it was able to identify some existing viruses, the protection was nonexistent for any virus not pre-recorded in the database [2]. Antivirus programs were usually installed via physical media, and updates with protection against new viruses took several months to be produced.

In response to a rise of antivirus programs, malwares started to implement novel techniques. A popular hacker from the early 1990s named "Dark Avenger" was a prolific writer of polymorphic code, a technique used for mutating a virus' binary code and therefore avoiding identification by antivirus programs [3,4]. The mid 90s also encountered the first wild macro-virus "Concept", discovered in 1995 [5]. This category of virus is not based on a program of its own, but runs through macro functionalities delivered by other programs such as Microsoft Word, PowerPoint and Excel. This new way of creating malware made possible the rapid dissemination of viruses through email attachments, networks, and media sharing in general. Later in 1999, the macro-virus Melissa caused around $80 million worth of damage [6].

As cyber threats became more overwhelming, the antivirus industry started to damage itself at the end of the decade. McAfee Associates Inc. accused the competitor Dr. Solomon's Group of forging an antivirus that performed well on tests but was ineffective in real life scenarios. Dr. Solomon's group replied that McAfee's criticism came from the fact that they couldn't keep up with the ever rising number of viruses [7]. McAfee also sued Symantec Corp. alleging defamation [8].

II. 2000s

The following decade was marked by the institutionalisation of cyber attacks. Governments started to invest money to build malwares capable of disrupting political enemies and cyber-crime organisations emerged as a way for groups of individuals to rationally plan and execute unlawful endeavours [9,10]. In the 2000s, attackers had an increasingly large volume of computers and softwares to exploit. Additionally, more information was stored in computer databases than ever before and therefore cyber criminals' profits grew exponentially. One cyber-crime organisation that made a large profit was "ShadowCrew". This organisation was responsible for stealing money from more than 130 million bank accounts through credit card fraud, phishing, malwares, and other hacking techniques [11].

The 2000s also saw the increase in antivirus usage due to the creation of multiple open-source antivirus repositories, making such programs more accessible to the wider computer user-base [12,13]. Although the number of antivirus users were rising, one obstacle was the slow performance of antivirus programs and the impact that they had on user experience, as many users could not use their computer properly when an antivirus scan was running in the background. The creation of cloud-based antivirus software was an innovation directed to resolve this problem [14,15]. As many users were already connected to the internet, they could scan their files online to check against the presence of malware instead of installing an application that would greatly affect computer processing resources.

III. 2010s - Present

The variety of devices connected to the internet and the increase in digitalisation of many aspects of human life brought a new level of possibilities for hackers, and bigger challenges for antivirus software companies. Cybersecurity shifted from a single user protection approach to a bottom-up business protection approach, where one's computer is no longer so significant, and the entirety of a business' data is the

most valuable resource any hacker can get their hands on. This shift marked the end of an era of signature-based antivirus methods. Companies offering cybersecurity had to innovate and provide new ways to deal with cyber attacks. These new approaches included using artificial intelligence, behavioral analysis and detection of malicious activity, web application firewalls, machine learning for pattern recognition, multi-factor authentication, forensics, and even providing teams of experts to analyse inhouse software and mitigate zero-day attacks [16-18].

The biggest breaches of this decade include:

- 2019 - DDoS attack on New Zealand's stock market [19].
- 2017 - Equifax data breach, exposing the personal data of 145.5 million users, including their credit card, addresses, and birth dates [20].
- 2017 - The WannaCry attack, infecting more than 230,000 computers in one day and demanding payment to unblock the machine. Many business, government agencies, universities, and hospitals were affected by the attack, which had an estimated cost of $4 billion [21, 22].
- 2012, 2013, and 2014 - Yahoo accounts breach, exposing more than 453,000 user accounts [23-25]

IV. Cyber security risks for the next decade and their legal, ethical and professional implications

Cyberattacks are dynamically exploiting new vulnerabilities as they appear. The theft of personal identity data and of credit cards is a critical and recurring problem, but our current digital life already has far more information that also needs to be secured. Humanity has taken the digitalisation of the real world far beyond what was dreamed of by the experts three decades ago. Our hospitals, medical devices, city infrastructure, homes, and even our bodies have been using network-connected devices that are susceptible to hacking. Further recent developments in cloud computing, artificial intelligence, and IoT have both contributed to the defense and the attack of digital assets [26,27], showing that while our technologies to solve complex problems evolve, these same technologies can be used by cyber criminals for malicious purposes.

Future malwares will have more sophistication, potential to scale, and will also be faster than ever before. These malwares will likely use technologies that are maturing nowadays to their advantage such as deep fakes, crypto currency mining software, self-driving cars, quantum computing, robotic process automation, edge computing, virtual and augmented reality, blockchains, and more.

Senior executives will become increasingly unaware of the extension of cyber risks faced by their organisations, as the necessary knowledge to manage and assess these risks becomes distributed among third-party digital service providers and the IT professionals working closely to the organisation tech stack. This change will promote the importance of cyber security engineers and a more serious take on existent cyber security standards such as ISO/IEC 27001. It is also possible that new standards will need to be created to target future issues directly.

Future cyber attacks will become harder to address as more companies become dependent on external digital services such as cloud providers, internet hosting for software version control, video conference software, and more. As soon as any of those providers becomes unavailable due to a cyber attack, all the companies relying on those will become partially or fully nonoperational. A single Amazon Web Service outage was enough to put a great number of websites offline in 2020 [28]. As businesses become more integrated with each other, it only takes one big service to fall and then the whole chain of businesses collapses.

Moreover, cyber attacks will become harder to identify. Malwares are getting more intelligent by the day, and real user behaviour imitation becomes easier to fabricate as machine learning technologies improve. Companies will soon be unable to separate real users from malicious bots.

Cloud platforms will scale up the volume and aggressiveness of attacks by providing cyber criminals with enough computing power to execute large attacks. Additionally, such platforms already provide many automation tools [29] that can be used by cyber criminals to make their activities easier to orchestrate. Having this power along with the ability to mimic user behaviour will allow cybercriminals to make organisations clueless when trying to distinguish between a legitimate load of users or a single cyber attack with many bots. Apply this to a credit card company attack scenario where money is being exchanged and legitimacy cannot be contested and you will have the recipe for an economic collapse.

Phishing will become more sophisticated with improvements to deep fake technology. Phone scams will become more frequent as the technology to mimic voices and accents becomes more accessible. This will also raise new legal and ethical issues as fake evidence can be generated to incriminate or absolve someone for a certain crime. From a broader perspective, deep fakes can be used to disseminate false messages on social media, potentially causing numerous political issues such as election manipulation, public opinion engineering, mass behaviour exploitation, and more.

V. Conclusions and Recommendations

The management and assessment of cybersecurity risks will continue to be paramount to organisations and governments for as long as we have active cyber criminals. History has already shown that cyber attacks can be extremely creative and whether they are going to happen is no longer a question, it is a matter of "when" and not "if".

The threats that society will face in the future are many, and organisations will have to respond by investing in initiatives that promote awareness of cyber security risks. Many companies that depend on digital services will need to either create specific cybersecurity roles or hire specialised providers to provide guidance. Governments must also make sufficient investments in cybersecurity resources and these same resources

should be used to facilitate updating old technology-related laws [30,31].

Digital systems need to account for human errors and minimise them as much as possible so that phishing and other kinds of scams can be reduced. On the other hand, the complexity of technology must also be reduced as a means to facilitate protection routines and to decrease the number of potential vulnerabilities.

REFERENCES

[1] Inventors and inventions. New York: Marshall Cavendish, 2008, p. 1033.

[2] C. Douligeris, Network security. 2007, p. 86.

[3] Anonymous "Bulgarian 'Dark Avenger' Part of East-Bloc Legacy: [All 05/19/92 Edition]," The Christian Science Monitor (Pre-1997 Fulltext), 1992. Available: https://search.proquest.com/newspapers/bulgarian-dark-avenger-part-east-bloc-legacy/docview/291199550/se-2?accountid=12838.

[4] S. Gibson, "At Last, How to Protect Yourself from Polymorphic Viruses," InfoWorld, vol. 14, (17), pp. 36, 1992. Available: https://search.proquest.com/trade-journals/at-last-how-protect-yourself-polymorphic-viruses/docview/194255106/se-2?accountid=12838.

[5] "Concept", Softpanorama.org, 1997. [Online]. Available: http://www.softpanorama.org/Malware/Malware_defense_history/Ch05-macro_viruses/Zoo/concept.shtml. [Accessed: 08-Mar-2021].

[6] "The Melissa Virus — Federal Bureau of Investigation", Federal Bureau of Investigation, 2019. [Online]. Available: https://www.fbi.gov/news/stories/melissa-virus-20th-anniversary-032519. [Accessed: 08-Mar-2021].

[7] A. NewsRoundup, "Dueling McAfee, Dr. SolomonUse Press Releases As Weapons", WSJ, 1997. [Online]. Available: https://www.wsj.com/articles/SB860517929897048500. [Accessed: 08-Mar-2021].

[8] "McAfee Suit Accuses Symantec of Defamation", Los Angeles Times, 1997. [Online]. Available: https://www.latimes.com/archives/la-xpm-1997-aug-23-fi-25051-story.html. [Accessed: 08-Mar-2021].

[9] N. Anderson, "Confirmed: US and Israel created Stuxnet, lost control of it", Ars Technica, 2012. [Online]. Available: https://arstechnica.com/tech-policy/2012/06/confirmed-us-israel-created-stuxnet-lost-control-of-it/?comments=1. [Accessed: 08-Mar-2021].

[10] "Military Computer Attack Confirmed (Published 2010)", Nytimes.com, 2010. [Online]. Available: https://www.nytimes.com/2010/08/26/technology/26cyber.html?_r=1&ref=technology. [Accessed: 08-Mar-2021].

[11] A. News, "Hacker Behind Massive Credit Data Theft Gets 20 Years", ABC News, 2010. [Online]. Available: https://abcnews.go.com/GMA/TheLaw/hacker-sentenced-largest-theft-credit-debit-card-numbers/story?id=10208613. [Accessed: 08-Mar-2021].

[12] "OpenAntiVirus Project", Web.archive.org, 2014. [Online]. Available: https://web.archive.org/web/20140703090640/http://www.openantivirus.org/. [Accessed: 08-Mar-2021].

[13] "ClamavNet". [Online]. Available: http://www.clamav.net/about. [Accessed: 08-Mar-2021].

[14] "CloudAV: N-Version Antivirus in the Network Cloud", Web.archive.org, 2014. [Online]. Available: https://web.archive.org/web/20140826115701/https://www.usenix.org/legacy/event/sec08/tech/full_papers/oberheide/oberheide_html/index.html. [Accessed: 08-Mar-2021].

[15] "Wayback Machine", Web.archive.org, 2008. [Online]. Available: https://web.archive.org/web/20160403020632/http://library.corporate-ir.net/library/10/104/104920/items/313409/MFEFQ308Oct30Final.pdf. [Accessed: 08-Mar-2021].

[16] T. Brewster, "Duelling Unicorns: CrowdStrike Vs. Cylance In Brutal Battle To Knock Hackers Out", Forbes, 2016. [Online]. Available: https://www.forbes.com/sites/thomasbrewster/2016/07/06/duelling-unicorns-crowdstrike-vs-cylance-in-brutal-battle-to-knock-hackers-out/?sh=41fd75303f75. [Accessed: 08-Mar-2021].

[17] "Homeland Security Today: Bromium Research Reveals Insecurity in Existing Endpoint Malware Protection Deployments", Web.archive.org, 2014. [Online]. Available: https://web.archive.org/web/20150924031641/http://www.hstoday.us/briefings/industry-news/single-article/bromium-research-reveals-insecurity-in-existing-endpoint-malware-protection-deployments/05ccfa234d62872b3d3a5422f2cbd4bd.html. [Accessed: 08-Mar-2021].

[18] E. Messmer, "Start-up offers up endpoint detection and response for behavior-based malware detection", Network World, 2014. [Online]. Available: https://web.archive.org/web/20150205023309/http://www.networkworld.com/article/2466793/security0/start-up-offers-up-endpoint-detection-and-response-for-behavior-based-malware-detection.html. [Accessed: 08-Mar-2021].

[19] "New Zealand Stock Exchange Shut Down By DDoS Attack", 2020. [Online]. Available: https://www.cpomagazine.com/cyber-security/new-zealand-stock-exchange-shut-down-by-ddos-cyber-attack/. [Accessed: 08-Mar-2021].

[20] "The Equifax Data Breach: What to Do", Consumer Information, 2017. [Online]. Available: https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do. [Accessed: 08-Mar-2021].

[21] "What is WannaCry?" 2020. [Online]. Available: https://www.avast.com/c-wannacry. [Accessed: 08-Mar-2021].

[22] ""WannaCry" ransomware attack losses could reach $4 billion", Cbsnews.com, 2017. [Online]. Available: https://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/. [Accessed: 08-Mar-2021].

[23] D. Goodin, "Hackers expose 453,000 credentials allegedly taken from Yahoo service (Updated)", Ars Technica, 2012. [Online]. Available: https://arstechnica.com/information-technology/2012/07/yahoo-service-hacked/. [Accessed: 08-Mar-2021].

[24] D. Goodin, "How Yahoo allowed hackers to hijack my neighbor's e-mail account (Updated)", Ars Technica, 2013. [Online]. Available: https://arstechnica.com/information-technology/2013/01/how-yahoo-allowed-hackers-to-hijack-my-neighbors-e-mail-account/. [Accessed: 08-Mar-2021].

[25] D. Goodin, "Mass hack attack on Yahoo Mail accounts prompts password reset", Ars Technica, 2014. [Online]. Available: https://arstechnica.com/information-technology/2014/01/mass-hack-attack-on-yahoo-mail-accounts-prompts-password-reset/. [Accessed: 08-Mar-2021].

[26] J. Damiani, "A Voice Deepfake Was Used To Scam A CEO Out Of $243,000", Forbes, 2019. [Online]. Available: https://www.forbes.com/sites/jessedamiani/2019/09/03/a-voice-deepfake-was-used-to-scam-a-ceo-out-of-243000/?sh=6859d9cf2241. [Accessed: 08-Mar-2021].

[27] A. Basit, M. Zafar, X. Liu, A. Javed, Z. Jalil and K. Kifayat, "A comprehensive survey of AI-enabled phishing attacks detection techniques", Telecommunication Systems, vol. 76, no. 1, pp. 139-154, 2020. Available: 10.1007/s11235-020-00733-2 [Accessed 8 March 2021].

[28] "Prolonged AWS outage takes down a big chunk of the internet", The Verge, 2020. [Online]. Available: https://www.theverge.com/2020/11/25/21719396/amazon-web-services-aws-outage-down-internet. [Accessed: 08-Mar-2021].

[29] "DevOps - Amazon Web Services (AWS)", Amazon Web Services, Inc.. [Online]. Available: https://aws.amazon.com/devops/. [Accessed: 08-Mar-2021].

[30] "Government can't keep up with technology's growth", Harvard Gazette, 2019. [Online]. Available: https://news.harvard.edu/gazette/story/2019/02/government-cant-keep-up-with-technologys-growth/. [Accessed: 08-Mar-2021].

[31] "Policymaking must catch up with technology - before it's too late", World Economic Forum, 2019. [Online]. Available: https://www.weforum.org/agenda/2019/11/we-must-bridge-the-gap-between-technology-and-policy-our-future-depends-on-it/. [Accessed: 08-Mar-2021].