EURASIAN EXPERIMENT JOURNAL OF SCIENTIFIC AND APPLIED RESEARCH
(EEJSAR) ISSN: 2992-4146
©EEJSAR Publications Volume 6 Issue 1 2024

Advancements in Computer Virus Protection: From Origins to Future Trends

Echegu Darlington Arinze, and Chukwuemeka Odi Agwu

School of Mathematics and Computing, Kampala International University, Uganda
Email: darlington.echegu@kiu.ac.ug nzeechegu@gmail.com
ORCID: 0009-0002-6644-1709

ABSTRACT

With the increasing dependency on computers in today's world, it becomes imperative to differentiate between the two. This review examines the Advancements in Computer Virus Protection: From Origins to Future Trends. Computer viruses are software programs that self-replicate and spread from one computer to another with disruptive and damaging intentions, such as stealing, altering, or deleting data. There are several types of computer viruses; these include file infectors, boot sector viruses, macro viruses, polymorphic viruses, metamorphic viruses, resident viruses, non-resident viruses, and the earliest known computer viruses date back to the 1970s, when a programmer named Fred Cohen created the Creeper virus on ARPANET. Elk Cloner, which infected an Apple II operating through floppy discs in the 1980s, stands as the first identifiable example of a computer virus. Viruses started targeting both email and the web in 2000, leading to the creation of new, more advanced antivirus solutions. Some of the malware that emerged and gained popularity in the 2010s included financially motivated malware like ransomware, as well as new-generation viruses like "Stuxnet" that posed a threat to industrial control systems. The effects of computer viruses pose a huge threat to individuals and organisations, particularly in terms of data and privacy losses, financial losses, and reduced system performance. We utilized relevant published data (2004–2014) from diverse, reliable databases. Finding suggests prevention measures are also important, including the use of antivirus software, keeping one's computer software up-to-date, and safe browsing practices. It is, therefore, important to be on the lookout for other viruses and take measures to protect computers from viruses as much as possible.

Keywords: advancements, computer virus protection, origins, antivirus, future trends

INTRODUCTION

A computer virus is a software programme that may slow down systems, delete files, or reproduce itself on other machines. Among the numerous categories of computer viruses are infectors, boot sector viruses, macro viruses, polymorphic viruses, metamorphic viruses, resident viruses, non-resident viruses, and multipartite viruses [1]. Computer viruses first appeared as an experimental self-replicating virus on ARPANET in the 1970s, known as the "Creeper" application. 'Elk Cloner', the first computer virus, proliferated over floppy discs and infected several Apple II systems in the 1980s. The introduction of the World Wide Web and personal computers in the 1990s sparked the development of ever more sophisticated viruses, including those with stealthy shapes and macro commands. Greater-complexity viruses with macro commands and covert forms first appeared in the 1990s. In 2000, the spread of viruses via the internet and e-mail increased their sophistication. When ransomware and other financially driven malware first appeared in the 2010s and beyond, along with sophisticated viruses like "uxnet" that targeted structural control systems, cyberwarfare reached a new high [2]. Computer viruses can impact individuals and businesses in various ways. Data loss, privacy leakage, financial losses, system degradation, and tarnished images are among the risks that individuals and businesses may encounter. This can result in disruption of business operations, financial losses, and even reputational damage. Direct costs include repair, recovery, and sometimes ransom, whereas indirect costs include productivity and revenue loss. Direct costs encompass repair, recovery, and occasionally ransom, while indirect costs encompass loss of productivity and revenue.

Understanding these aspects of computer viruses is crucial. This is because virus-induced breaches can result in fines and legal action if they do not comply with data protection regulations. Virus-induced breaches can lead to fines and legal action due to non-compliance with data protection regulations.

Prevention Strategies

Antivirus software plays a significant role in preventing malware and in diagnosing and eradicating viruses to minimise their impact. minimise their impact [3] They include real-time protection, prevention, performance enhancement, and safeguarding of data. Some of the most widely used antivirus software are Norton Antivirus, McAfee Total Protection, Bitdefender Antivirus Plus, Kaspersky Total Security, Avast Free Antivirus, and When choosing an antivirus, consider factors such as protection level, available features, performance, interface, price, reliability, and compatibility. Regular software updates address security issues, introduce new features, rectify defects, conform to new standards, and guarantee compatibility with new software and hardware [4]. Automatic updates are less tedious and more timely than manual updates, allowing users to preview and schedule updates at their convenience. However, there may be drawbacks, such as the need to restart the system at an inconvenient time. Safe browsing habits include avoiding untrustworthy websites, paying attention to URLs, only clicking links from unknown sources, using security warnings, identifying phishing scams, looking for signs of danger, and confirming before taking any action. The tools used include secure browsers such as Google Chrome, Mozilla Firefox, or Microsoft Edge, as well as plugins such as ad blockers, anti-phishing tools, and privacy extensions. It's crucial to regularly update your software to take advantage of the latest the technologies include plugins like ad blockers, anti-phishing tools, or privacy extensions, in addition to securely enabled browsers like Google Chrome, Mozilla Firefox, or Microsoft Edge. One critical step is to make sure you are running the most recent version of a program, as they often include the latest security fixes. For example, among other security services, Norton Antivirus offers active virus security, a firewall, and identity protection. Antivirus, anti-phishing, and a password manager that allows secure saving on a range of devices are some of the features of McAfee Total Security. Regarding capabilities, McAfee Total Protection provides anti-phishing, antivirus, and a password manager that allows safe storage of several devices. One of its main features, antivirals, provides a comprehensive and sophisticated defense against viruses and other dangers. With added features including kid-friendly Internet, safe money, and Kaspersky Secure Connection (VPN), Kaspersky Total Security is a security package that protects the computer against viruses and other dangers. To sum up, antivirus software plays two critical roles: eradicating viruses and protecting vital data [5]. The greatest features of antivirus software may protect and render your machine unattackable. You will protect your PC and stay away from practically every possible risk. curity improvements. For instance, Norton Antivirus includes firewalls, identity theft protection, and real-time virus scanning. Antivirus, anti-phishing, and a password manager with encrypted storage across several devices are among the features of McAfee Total Protection. Among the features of McAfee Total Protection are an antivirus, anti-phishing, and password manager that allows encrypted storage across several devices. One of its key features is thorough and efficient virus and other threat defense. Kaspersky Total Security offers secure money, kid-friendly Internet, and Kaspersky Secure Connection VPN, in addition to strong protection against viruses and other dangers. All things considered, antivirus software is essential to fighting viruses and protecting private information. The top antivirus software can help you avoid all types of dangers and ensure the safety of your computer. The best antivirus software allows you to shield your machine from many dangers.

Detection and removal techniques

It's a complex process that is a crucial step in ensuring that the system does not contain any malware. There are three types of scans: fast, customisable, and flexible. Full scans dissect all the files, directories, and programmes of the complete system, including exterior moves, and search the entire system for any malware. Quick scans target specific areas of the computer, such as various system folders, running processes, and other areas where malware is likely to lurk [6]. Custom scans are designed to target certain perpetrators or meet specific requirements, such as choosing which files, folders, or drives to scan. Make sure your computer has a robust antivirus programme installed, or install one if it doesn't, and update it to the most recent version to identify new viruses. Select a type of scan, choose a method for detecting viruses, execute the scan, review the results, take the necessary actions, and repeat the scan if required. The manual process of virus removal encompasses the following general steps: A virus may cause a slow response, a tendency to freeze or crash, changes in behaviour, a high level of network activity, deleted files, unknown files, or disabled security components [7]. These measures include disconnecting the infected computer from the Internet and booting it in Safe Mode. Open the task manager, identify any malicious processes, proceed to terminate them, identify the virus files, and delete them. Clean the virus from the registry. After that, he should shut down the system normally and run a virus scan to make sure they have removed every virus. Before installing any software or making changes to the system, you can use the provided System Restore

Points for backup and recovery. To launch system, restore, go to Control Panel > System and Security > System > System Protection > System Restore. Select a restore point that was set before the computer got infected, use it, restart, and then perform a scan. The processes to reinstall operating systems include copying and saving vital data, preparing installation media, installing the operating system, restoring the data, updating, and securing the new OS. Fortunately, by applying these measures, your system can never lack protection against malware and other related threats.

System and network security

Firewalls are important tools for eliminating threats that may originate from the outside world [8]. You can install these firewalls on a specific computer to control network traffic using security parameters. Despite its versatility, portability, and ease of modification, it consumes significant system resources and necessitates separate installation and updates [9]. A hardware firewall is a physical appliance that sits between the network and the internet and delivers full protection to all devices. They offer high versatility but can be costly and time-consuming to establish, as well as often requiring constant monitoring and modification [10]. To effectively implement firewalls, follow these steps: Develop a security policy; upgrade both firmware and software; employ strict passwords; log and monitor frequently; block ports that are not necessary; and enable IPS (Intrusion Prevention System). To secure the networks, you should use good encryption, change the default settings, turn off WPS, and hide the SSID, as well as use guest mode. VPNs use a less secure network to establish an encrypted connection, thus offering privacy, security, and access to intranets and geographically restricted content [11]. Look for a service with robust encryption, a no-logging policy, and other features such as a kill switch, DNS leak protection, and compatibility with multiple devices. Malware detection is one of IDS's core functions because it constantly analyses traffic and system activity for possible intrusion. There are two types of IDS: We programmed the signature-based IDS to monitor network traffic and system activities using a database of threat signatures [12]. The anomaly-based IDS, on the other hand, sets a baseline of normalcy and then finds any changes from it. Applications of these methods can complement one another and strengthen an organisation's protection against viruses and other cyber threats.

Safe computing practices

It is important for people and businesses to protect themselves against cyber threats through email security. Do not open emails from unknown people; always look at the sender's address; be on the lookout for signs of phishing schemes; and always contact the sender. Avoid opening emails with links or attachments, and use email filtering tools like spam filters, phishing filters, custom filters, and email authentication protocols [13]. This requires regular updates to safeguard against new threats. Downloading software from official websites reduces the risk of malware infection, ensures legal usage, and opens the door to support options. Updates need to be frequent to fix security flaws and bring more improvements. Downloaded files' checksums provide cryptographic assurances that the software remains unaltered and originates from the correct source [14]. To verify signatures, you must open the file's properties by right-clicking them and then looking at the Digital Signatures tab. Search for reliable certificates and notifications about the invalid signature. No one should use pirated software for business or personal reasons, as it undermines integrity. Piracy can result in legal repercussions, ethical ramifications, and business effects. To prevent exposure to computer viruses or other security threats, adhere to the following safe computing practices: Therefore, by adhering to the listed practices, individuals and institutions can reduce the likelihood of contracting computer viruses and other security threats.

Backup and data recovery

Data backup is crucial for safeguarding against various risks, such as breaches, maintaining operational continuity, adhering to legal mandates, and ensuring peace of mind. The means of data backup available are cloud backup, USB backup, network-attached storage (NAS), and hybrid backups. Cloud storage makes it possible to get accessibility, automation, scalability, and security, while, on the other hand, external drives provide aspects such as physical control, cost, speed, and offline accessibility [15]. NAS devices provide local network backup, data mirroring, and remote access support. Hybrid solutions incorporate cloud and external drive backup solutions in addition to local data storage. Disaster recovery planning, for its part, consists of risk analysis, identification of critical data, backup strategy and procedure, recovery process, communication plan, resources, documentation, testing, and improvement, among others. Exercises apply the plan in realistic conditions; reviews occur because of new changes in the IT environment, changes in business processes, and threats. Backup verification checks whether backups are reliable, accessible, and viable, while training employees on a disaster recovery plan familiarises them with the activities they are required to undertake in the event of an information loss [16]. To modify the plan, continuous improvement uses the results of tests and reviews.

Individuals and organisations can greatly manage the probabilities of data loss and achieve rapid recovery in the event of a disaster by setting reasonable backup routines and creating an elaborate disaster recovery plan.

User education and awareness

Cybersecurity training for employees can be important as it protects organisations from cyber threats, reduces human vulnerability, ensures every organisation is compliant with laws, and is significant for organisational culture [17]. Organisations can develop appropriate training models by defining specific risks and training requirements, incorporating engaging and interesting elements into the training material, considering various training options based on employees' job descriptions, regularly updating the programmes, incorporating quizzes, and making resources easily accessible to employees. Awareness campaigns should adhere to several key principles, including timely information dissemination to combat emerging threats, the provision of real-life examples, the use of multiple channels, the invitation of experts, and the use of graphics to enhance presentations. Users' best practices include insisting on using weak passwords, raising awareness about phishing, guiding users on how to protect their personal and work devices, imparting knowledge on data handling, implementing sound measures for reporting security breaches, and rewarding employees who embrace these practices, among others. To recap, cybersecurity training for employees plays a significant role in being able to identify threats, reduce the risks associated with human mistakes, adhere to the law, and promote a culture that supports security. The ideal training programme should prioritise risk-appropriate training, engage the trainee, incorporate role play, implement regular updates, and dispose of tools appropriately [18]. We can implement these practices to guarantee the effective protection of organisational information and assets.

Advanced protection methods

Security systems use behavioural analysis as a technique to detect unknown threats. It is a process of observing how software functions and how users interact with it, then analysing that information to look for signs of irregularities. This approach enables security systems to identify threats that may not be identifiable with traditional methods that employ signature-based detection technologies. Behavioural analysis commonly uses machine learning and artificial intelligence to assess large amounts of data and identify signs of malicious behavior [19]. EDR, UEBA, and NTA are some of the tools and technologies used in analysing behavioural patterns. Cybersecurity uses sandboxing as a security approach to run potentially dangerous or malicious files and applications in a safe, monitored virtual environment. It is an effective method to run a piece of code that can potentially harm the system and study its activity in the process. Sandboxing excels at detecting novel threats and unreported malware types. Endpoint Protection Platforms (EPP) are security products that aim at defending endpoint devices against multiple threats. These are programmes that combine a variety of security features into a single solution that provides real-time threat protection. EPP solutions typically include management consoles where administrators can set security policies, oversee endpoints, and investigate security breaches all at once. EPP solutions offer features such as malware protection, endpoint firewall features, DLP, and EDR features. These tools help the organisation identify threats when they are in their early stages and prevent them from escalating.

Future trends in virus protection

We're effectively combining AI and machine learning to prevent and eradicate malware [19]. AI and ML algorithms can learn from data, identify signs of destructive behaviour, and take response measures on their own. They are also highly proficient in behavioural analysis, which provides security solutions with the ability to detect previously unseen types of malware as well as new and emerging threats like zero-day threats. Other threat response actions might include the use of self-learning AI to automatically quarantine infected files, block known malicious network traffic, or isolate compromised end points ahead of human intervention. Over time, the ML algorithms enhance their abilities to detect and manage cybersecurity threats by learning from new threat patterns. Future advancements in AI and ML could concentrate on explainable AI models, adversarial ML techniques, and threat intelligence. Cybersecurity experts view blockchain as having an array of applications, including a decentralised ledger, identity management, secure data transfer, and cryptographic solutions [20]. Blockchain-based platforms can facilitate the process by which security researchers, organisations, and individuals can submit threat data to the global threat database, thereby improving threat detection and prevention. This entails demonstrating how existing algorithms such as the RSA and ECC are vulnerable to quantum attacks, as well as how quantum computing can break them. Quantum computing is progressively developing, and it will render legacy encryption mechanisms increasingly vulnerable, making it necessary to come up with quantum-safe cryptography techniques. Quantum cryptography introduces new cryptosystems based on quantum mechanics principles, such as quantum key distribution (QKD), which ensures secure communication without interception or spying [21]. We can define post-quantum cryptography as cryptographic methods that withstand attacks

executed on quantum computers. Experts are constantly working on the creation and further standardisation of post-quantum cryptographic protocols for further use, key among them being lattice-based cryptography, hash-based cryptography, and code-based cryptography. To move from traditional cryptographic algorithms to post-quantum cryptographic algorithms, organisations need to come up with risk management plans. They must also consider the potential impact of quantum computing on the existing cryptographic framework, explore technologies suitable for post-quantum cryptography, and strategize a gradual transition to guarantee security and compatibility [22].

Case Studies and Real-World Examples

The WannaCry ransomware outbreak in 2017 and the Stuxnet Worm in 2010 were significant cyber attacks that highlighted the importance of timely software patching and vulnerability management [23]. These attacks highlighted the need for proactive patch management, network segmentation, and robust backup and recovery strategies. To mitigate the impact of malware outbreaks, organisations should adopt a layered approach to cybersecurity, including network segmentation, intrusion detection systems, endpoint protection solutions, and user education programs. Regular data backups and disaster recovery plans are also crucial. Successful organisations that successfully mitigated a virus attack include Maersk, which successfully recovered and resumed operations after falling victim to the NotPetya ransomware attack, and Sony Pictures Entertainment, which successfully recovered and rebuilt its infrastructure after a devastating cyber attack attributed to North Korean hackers. Successful defences include incident response planning, threat intelligence sharing, and endpoint detection and response (EDR) solutions. These tools help organisations respond effectively to cyber attacks, stay informed about emerging threats, and monitor and analyse endpoint activities for signs of malicious behavior [24].

CONCLUSION

The topic of virus protection comprises the following subtopics: Virus science pertains to the study of virions, or modified or altered virus particles. I am looking for an explanation for the term computer virus. Of what types of viruses? The origin of computer viruses: What impact does a virus attack have on an individual or an organization? Precautions include using an antivirus, regularly updating system software, and avoiding security risks such as uninterested browsing. Detection and eradication techniques include using an antivirus, manually removing the virus, restoring the system, and recovering, among other measures. The book also illustrates safe computing practices, backup and data recovery, user education and awareness, potential future protection methods, and case studies. It is crucial to choose an all-encompassing virus protection solution, as virus and malware threats persist in today's world. The threat no longer remains in check through conventional antivirus programs and methods, which means there is a need to come up with a new proactive method for protection, identification, and handling at both macro and micro levels. This includes employing antivirus, firewalls, IDS, and programmes that can educate end-users regarding the threats posed by viruses and malicious software. The current cybersecurity measures include defence-in-depth, employing up-to-date patches and updates, practicing safe computing, keeping copies of important data in secure media, security training and awareness, and monitoring and early response systems. By considering these recommendations and implementing a more comprehensive virus protection strategy, organisations and individuals will become more resilient to threats in a world increasingly connected to computer systems.

REFERENCES

1. Sulianta, F.: Comparison of The Computer Viruses from Time to Time. 2022 (2022). https://doi.org/10.37178/ca-c.23.1.139
2. Seumo Ntsiepdjap, B.: Dynamic Risk Assessment for Critical Infrastructures Under Attack. International Journal of Advanced Research. 10, 868–908 (2022). https://doi.org/10.21474/IJAR01/15433
3. Basil, N.N., Ambe, S., Ekhator, C., Fonkem, E.: Health Records Database and Inherent Security Concerns: A Review of the Literature. Cureus. 14, e30168. https://doi.org/10.7759/cureus.30168
4. Mugarza, I., Flores, J.L., Montero, J.: Security Issues and Software Updates Management in the Industrial Internet of Things (IIoT) Era. Sensors. 20, (2020). https://doi.org/10.3390/s20247160
5. Borky, J.M., Bradley, T.H.: Protecting Information with Cybersecurity. Effective Model-Based Systems Engineering. 345–404 (2018). https://doi.org/10.1007/978-3-319-95669-5_10
6. Alanazi, M., Mahmood, A., Chowdhury, M.J.M.: SCADA vulnerabilities and attacks: A review of the state-of-the-art and open issues. Computers & Security. 125, 103028 (2023). https://doi.org/10.1016/j.cose.2022.103028
7. Jaiswal, M.: Computer Viruses: Principles of Exertion, Occurrence and Awareness. SSRN Electronic Journal. 5, 648–651 (2017). https://doi.org/10.1729/Journal.23273

8. Wang, P.: Research on firewall technology and its application in computer network security strategy. Frontiers in Computing and Intelligent Systems. 2, 42–46 (2022). https://doi.org/10.54097/fcis.v2i2.3931
9. Javaid, M., Haleem, A., Singh, R.P., Rab, S., Suman, R., Khan, I.H.: Evolutionary trends in progressive cloud computing based healthcare: Ideas, enablers, and barriers. International Journal of Cognitive Computing in Engineering. 3, 124–135 (2022). https://doi.org/10.1016/j.ijcce.2022.06.001
10. Allioui, H., Mourdi, Y.: Exploring the Full Potentials of IoT for Better Financial Growth and Stability: A Comprehensive Survey. Sensors (Basel). 23, 8015 (2023). https://doi.org/10.3390/s23198015
11. Jyothi, K., Reddy, B.I.: CSEIT1835225 | Study on Virtual Private Network (VPN), VPN's Protocols and Security. (2023)
12. Yousef, M., Abdelmajeed, N.: Dynamically Detecting Security Threats and Updating a Signature-Based Intrusion Detection System's Database. Procedia Computer Science. 159, 1507–1516 (2019). https://doi.org/10.1016/j.procs.2019.09.321
13. Dada, E.G., Bassi, J.S., Chiroma, H., Abdulhamid, S.M., Adetunmbi, A.O., Ajibuwa, O.E.: Machine learning for email spam filtering: review, approaches and open research problems. Heliyon. 5, e01802 (2019). https://doi.org/10.1016/j.heliyon.2019.e01802
14. Cherubini, M., Meylan, A., Chapuis, B., Humbert, M., Bilogrevic, I., Huguenin, K.: Towards Usable Checksums: Automating the Integrity Verification of Web Downloads for the Masses. (2018)
15. Tahir, A., Chen, F., Khan, H.U., Ming, Z., Ahmad, A., Nazir, S., Shafiq, M.: A Systematic Review on Cloud Storage Mechanisms Concerning e-Healthcare Systems. Sensors (Basel). 20, 5392 (2020). https://doi.org/10.3390/s20185392
16. Olaoye, G., Luz, A.: Data backup and disaster recovery in the cloud. (2024)
17. Olabode, O.: The Relevance of Cybersecurity Awareness Training For Employees In Small and Medium Enterprises (SMEs). (2023)
18. Gutterman, A.: Training and Development. (2023)
19. Galli, A., La Gatta, V., Moscato, V., Postiglione, M., Sperlì, G.: Explainability in AI-based behavioral malware detection systems. Computers & Security. 141, 103842 (2024). https://doi.org/10.1016/j.cose.2024.103842
20. Dong, S., Abbas, K., Li, M., Kamruzzaman, J.: Blockchain technology and application: an overview. PeerJ Computer Science. 9, e1705 (2023). https://doi.org/10.7717/peerj-cs.1705
21. Abhang, R., Anugu, N., Bale, S., Beeram, G., Bhattu, Z.S.R., Mahmoud, M.: Employing Quantum Mechanics for Quantum Cryptography. (2023)
22. Sood, N.: Cryptography in Post Quantum Computing Era. (2024)
23. Benmalek, M.: Ransomware on cyber-physical systems: Taxonomies, case studies, security gaps, and open challenges. Internet of Things and Cyber-Physical Systems. 4, (2024). https://doi.org/10.1016/j.iotcps.2023.12.001
24. Kaur, R., Gabrijelčič, D., Klobučar, T.: Artificial intelligence for cybersecurity: Literature review and future research directions. Information Fusion. 97, 101804 (2023). https://doi.org/10.1016/j.inffus.2023.101804

CITE AS: Echegu Darlington Arinze, and Chukwuemeka Odi Agwu. (2024). Advancements in Computer Virus Protection: From Origins to Future Trends. EURASIAN EXPERIMENT JOURNAL OF SCIENTIFIC AND APPLIED RESEARCH, 6(1):11-16