DOI: https://doi.org/10.33197/justinfo.vol1.iss2.2023.1245 ISSN: 3031-3449

Strategies for Enhancing Information System and Internet Security Towards Adware Threats

[1]Shelvia Nur Widiastuti, [2]Anisa Indriani, [3]Ucu Nugraha

[1]Sistem Informasi, Fakultas Teknik, Universitas Widyatama, Kota Cimahi, Indonesia, shelvia.nur@widyatama.ac.id
[2]Sistem Informasi, Fakultas Teknik, Universitas Widyatama, Kab. Bandung Barat, Indonesia, anisa.indriani@widyatama.ac.id
[3]Sistem Informasi, Fakultas Teknik, Universitas Widyatama, Kab. Bandung Barat, Indonesia, ucu.nugraha@widyatama.ac.id

ABSTRACT

Adware has emerged as a significant concern in today's information systems and internet security landscape. This malicious software type illicitly injects unwanted advertisements into user devices, disrupting user experience and posing threats to privacy and data security. Effective strategies are essential to mitigate adware threats and enhance information systems and internet security.This article explores several strategies to combat adware threats. Firstly, adopting a preventive approach is crucial. Utilizing reliable and regularly updated security software, alongside frequent updates of operating systems and applications, can effectively prevent adware infections. Secondly, avoiding clicking on suspicious links and pop-ups can minimize the risk of adware infiltration. Thirdly, regular clearing of cookies and caches aids in purging adware from user devices. Lastly, employing ad blockers serves as an additional measure to thwart adware presence on user devices. By implementing these strategies, organizations, and individuals can significantly reduce their vulnerability to adware attacks, thereby safeguarding both user experience and data integrity in the evolving landscape of information technology and internet usage.

Keywords: Adware Threats, Information System, Internet Security.

Corresponding Author:

Ucu Nugraha
Sistem Informasi, Fakultas Teknik, Universitas Widyatama
Bandung, Indonesia
ucu.nugraha@widyatama.ac.id

INTRODUCTION

In the current digital era, information systems and the internet have become important elements in everyday life, becoming the basis for obtaining information, communicating, and carrying out online transactions. However, behind the convenience and benefits of this technology, some threats need to be taken seriously. One threat that is increasingly worrying is adware. Adware is a type of software that is often embedded in applications or programs downloaded by users. Its primary purpose is to deliver advertising to users, either in the form of pop-ups, banners, or redirects to websites containing advertising.

Although sometimes considered a minor annoyance, adware can cause a variety of serious problems that can threaten users and their businesses. Adware affects the user's experience in using information systems and the internet. Irrelevant and intrusive ads often appear suddenly, disrupting navigation and reducing user concentration. Additionally, adware can also reduce system performance by consuming valuable resources such as disk space and internet speed.

More worryingly, adware can also threaten users' privacy by tracking their activities, such as search history and browsing habits, to target ads more precisely. This not only raises privacy concerns but also compromises the security of user data as adware can open the door to additional malware infections. Some types of adware can even function as a backdoor for malware that can damage the system, steal personal information, or even take control of the user's device.

With the increasing complexity and sophistication of adware threats, it is critical to develop effective strategies to combat adware and improve the overall security of information systems and the internet. This strategy should include adware prevention, detection, and response measures, as well as stronger privacy protection and data security.

LITERATURE REVIEW

Advertising, according to Jaiz (2014), is a form of communication that aims to convey information about products through the media to reach an audience of some or all of the population[1]. According to Fatihudin and Firmansyah (2019), advertising is a communication tool that can reach a wider audience, can build a long-term image, and increase sales quickly. Advertisements can be delivered repeatedly and have the potential to create a dramatic effect[1]–[4].

A computer virus is a program written or specifically designed to annoy computer users[5]. Viruses spread by replicating themselves without the user's knowledge, often exploiting vulnerabilities in computer network systems and personal computers[6]. The main goal of viruses is to damage computer systems and access personal information, causing harm in the form of data loss and operating system infections[7].

A website, according to Djamen (2018), is a collection of web pages that are connected and can be accessed via the internet, presenting various information such as text, images, video, and audio[8]. Websites can be used for various purposes such as business, education, and entertainment. Sebok, Vermat, and team (2018) define a website as a collection of connected pages that store documents and images on a web server, while a web app is an application that is accessed via a browser and displays user data from the server[9].

Malware, according to Zalavadiya & Priyanka (2017), is malicious software designed to damage a computer system or steal information without the owner's knowledge. Malware includes viruses, worms, Trojans, keyloggers, spyware, and ransomware, which aim to infect and damage computer systems or other devices[10].

Adware, according to Rizaldi (2022), is software that displays advertisements to users without permission. The goal is to generate revenue from unwanted advertising. Adware can appear in various forms such as pop-ups, banners, or redirects to certain websites[11].

Information systems, according to O'Brien (2011), are a structured combination of people, hardware, software, and databases that collect, change, and disseminate information within an organization. Information systems are vulnerable to adware threats which can disrupt data processing and distribution, as well as threaten information security[12].

The Internet, according to Sibero (2011), is a global network that connects various computers with the TCP/IP protocol. The internet provides wide access for adware to spread and infect connected devices. Internet users need to be wary of adware because it can disrupt the user experience, steal personal data, or redirect to malicious websites[13].

METHODOLOGY

This research uses descriptive research methods that aim to observe and understand the phenomenon of adware threats, including their characteristics, sources, distribution methods, and steps to overcome them in the future. The descriptive method was chosen to provide an accurate and in-depth picture of the phenomenon under study so that it can provide the insight needed to overcome the problem.

Data collection techniques used include observation and documentation studies. Observations are made by paying attention to user behavior towards adware, responses to advertisements or messages that appear, as well as application and internet usage patterns that show signs of adware. Meanwhile, documentation studies are carried out by collecting and analyzing various documents and related information, such as security reports, scientific articles, online sources, and application usage guidelines. An in-depth analysis of these documents provides relevant information about the characteristics of adware, its types and ways of spreading, as well as recommended steps to address the threat.

The combination of observational techniques and documentation studies allows researchers to obtain objective, comprehensive, and diverse data about adware threats. Direct observation provides insight into user interactions with adware, while documentation studies provide in-depth perspectives from a variety of trusted sources. By using this approach, it is hoped that this research can provide a deeper understanding of the adware threat and effective strategies for dealing with it.

RESULTS AND DISCUSSION

Adware is an abbreviation for "advertising-supported software", referring to a type of malicious software designed to automatically and relentlessly display advertisements to users. Adware can disrupt the user experience in several ways including:

1) Intrusive Ads. Adware often displays excessively intrusive ads such as pop-ups, pop-unders, banners, or text links that appear on web pages. This interferes with browsing activities and prevents access to the content you want to access.
2) Slows Down Performance. Adware running in the background can consume system resources such as CPU, memory, and bandwidth. As a result, the device can become slow and less responsive, disrupting the user experience and hindering the performance of other tasks.
3) Setting Changes and Forced Redirects. Some adware can change browser settings and redirect users to unwanted or malicious web pages. This includes changing the homepage or default search engine, as well as causing unexpected redirects when clicking on links or opening advertising pages automatically.
4) Privacy Violation. Some adware can track users' browsing activities and collect personal information without permission. This data may be used for unsolicited marketing purposes, such as targeting advertising or selling personal information to third parties.
5) Interruptions during Program Installation. Adware associated with the installation of other programs often makes the installation process complicated and confusing. Users should pay close attention and uninstall hidden adware components, wasting time and disrupting user experience.

By understanding these methods, users can be more aware of adware and take protective steps such as using the latest security software, updating the system regularly, and considering the source and type of applications installed to reduce the risk of being infected with adware.

The cause of the emergence of adware related to cellphone user behavior can be caused by several main factors, including:

1) Downloading and Installing Unofficial Applications. Downloading and installing applications from untrusted or unofficial sources, such as third-party websites or unverified forums, increases the risk of adware entering the device. Illegal or unofficial applications are often modified to include adware as an additional component.
2) Not Going Through Official App Stores. Installing apps from untrusted sources or ignoring official app stores like Google Play Store for Android or Apple App Store for iOS increases the risk of adware. Official app stores usually have better security mechanisms to detect and prevent malicious apps or adware from entering their platforms.
3) Carelessly Clicking on Ads. Clicking on ads from untrusted or unknown websites can open the door to adware. These ads often offer attractive deals or redirect users to suspicious websites. Users who accidentally click on such ads may download adware onto their devices.
4) Not Reading App Permissions Carefully. When installing apps from official app stores, it is important to carefully read the permissions requested by the app. Some applications may request

permissions that are not relevant to their function and can be exploited to insert adware into the device.

By understanding these factors, users can reduce the risk of exposure to adware by choosing applications from trusted sources, paying attention to the ads they click on, and always reading application permissions carefully before installing them. These precautions can help keep your device safe from potential adware threats.

Adware can be divided into two main types based on the infected device, namely computer adware and smartphone adware:

1) Computer Adware

Computer adware generally enters devices through the installation of freeware, shareware software, or extensions downloaded from untrusted sources. Users are often unaware that adware is installed along with the desired software. Frequent sources of computer adware include websites that provide illegal applications or unverified download links. Once infected, computer adware displays unwanted advertisements to users in the form of pop-ups, pop-unders, banners, or sponsored links on visited web pages. The main goal of computer adware is to generate income for its creators through pay-per-click (PPC) schemes, where they are paid every time a user clicks on the displayed advertisement.

2) Smartphone Adware

Adware can also infect smartphone devices if users click on links or advertisements from untrusted sources. Just like computer adware, smartphone adware can be installed unknowingly when downloading applications or visiting untrusted websites. Once infected, smartphone adware can cause decreased device performance, higher battery power consumption, or the appearance of annoying pop-up ads. Adware can also force users to download additional applications without their permission, causing confusion and frustration.

Adware can also be classified according to the level of dangerousness:

1) Legitimate Adware. This is a safe type of adware and does not contain malware. Users usually provide permission or consent before adware collects their data. Legitimate adware aims to generate revenue through displayed advertisements and generally does not cause significant harm to users.
2) Potentially Unwanted Applications (PUAs). PUAs are potentially dangerous adware. They can be installed automatically on users' devices without consent. PUAs can be divided into several categories:
   a) Illegal Malicious Adware PUA. Contains viruses, spyware, or other malware that can cause cyber crimes such as theft of personal data.
   b) Legal Abusive Adware PUA. Although it does not contain malware, it generates spam through ads that annoy users.
   c) Legal Deceptive Adware PUA. Confuses users when trying to remove adware applications already installed on their devices.

It is important for users to always be aware of the source of applications and the links they access, and to install only from official application stores to minimize the risk of exposure to adware.

Adware is a serious threat that can cause various negative impacts on users and their devices. Below are further details regarding the types of adware threats based on the level of damage they can cause:

1) Intrusive Ads. Adware displays intrusive banners or pop-up ads on web pages visited by users. These ads are often unrelated to the original content of the web page and can deceive users by offering fake updates or other software.
2) Link Alteration. Adware can change text on web pages into irrelevant links or redirect users to undesirable sites.
3) Personal Data Theft. Some adware can track users' online behavior and collect their data without permission. This data is used to create more targeted advertising or even sold to third parties.

4) Modify Browser Settings. Adware can modify internet browser settings without user consent. This could include opening a new tab, changing the home page, or redirecting to a malicious website.
5) Resource Usage. Adware can affect device performance by wasting battery power or resulting in a slow internet connection due to excessive use of network resources.
6) Infection with Malware. On a more serious level, adware can act as a gateway to infect a device with more dangerous malware such as spyware, Trojans, botnets, and so on. This could result in significant data loss, system damage, or unauthorized access to the device.

To protect themselves from adware threats, users can take several preventive steps such as:

1) Downloading from Trusted Sources. Always download apps only from official app stores like Google Play Store or Apple App Store.
2) Avoid Clicking on Untrusted Links. Do not click on links or advertisements from unknown or untrusted sources.
3) Pay Attention to App Permissions. When installing an app, pay attention to the permissions it asks for. Avoid apps that ask for irrelevant or too many permissions.
4) Updates and Security. Ensure devices and software are always updated with the latest versions to address known security vulnerabilities.

By understanding the types of adware threats and the impact they can have, users can be more alert and take the necessary steps to protect their privacy and security online.

To resolve Adware issues, the following steps can be taken to remove adware from the device and restore security and normal performance. Adware, in addition to generating unwanted advertisements, can also slow down device performance, disrupt the browsing experience, and even threaten the security of user data. Additionally, adware can install applications without user permission, display intrusive advertising pop-ups, and redirect users to unwanted websites. Preventive steps that can be taken include:

1) Avoid clicking on suspicious ad pop-ups. Ad pop-ups, especially those related to gambling, pornography, or unrealistic offers, are often targeted by adware to infect users' devices.
2) Stay away from illegal downloads. Downloading files or apps from untrusted sources or through illegal channels can trigger adware infections. It is recommended to use official app stores such as Play Store or App Store to download apps safely.
3) Remove suspicious software. If you find suspicious or unwanted applications or software on your device, immediately delete or uninstall them to prevent the spread of unwanted adware.
4) Install antivirus software. Installing a trusted antivirus can help protect your device from adware and other types of malware. Make sure to keep your antivirus updated and enable the adware detection feature.
5) Use an anti-malware plugin. For website owners, installing an anti-malware plugin can help protect a site from undetected adware attacks, as well as ensure additional protection through regular scanning.
6) Visit sites with SSL. When browsing the web, be sure to visit sites that use SSL (Secure Sockets Layer) to ensure the security and encryption of data sent between the user's device and the website. Sites with SSL are marked with a padlock symbol next to their URL.

By implementing these preventive measures, users can reduce the risk of being infected with adware and maintain the security and performance of their devices. It is also recommended to always be careful when browsing the internet, download applications from trusted sources, and update software regularly to minimize the risk of adware and other digital threats.

CONCLUSION

The research results show that adware is a serious threat to computer users because of its annoying characteristics such as the appearance of unwanted advertisements, browser redirects, and collection of personal data without user permission. Adware is spread through downloading applications from untrusted sources, clicking suspicious links, and combining with other software. To protect yourself from adware, it is recommended to use security software that can detect and remove adware, avoid downloads from untrusted sources, keep your operating system and software up to date, and be careful about clicking on suspicious links or advertisements. More education about adware is important to help users recognize and deal with this threat effectively, thereby keeping their devices safe.

REFERENCES

[1] M. Jaiz, *Dasar-dasar Periklanan*, I., vol. 1, no. 1. Yogyakarta: Graha Ilmu, 2014. [Online]. Available: https://grahailmu.co.id

[2] D. Fatihudin and M. A. Firmansyah, *Pemasaran Jasa (Strategi, Mengukur Kepuasan dan Loyalitas Pelanggan*, I. Sleman: Deepublish, 2019. [Online]. Available: https://penerbitbukudeepublish.com

[3] F. Zakariansyah, "PENGARUH IKLAN, DISKON, DAN KUALITAS PELAYANAN DRIVER TERHADAP KEPUASAN PELANGGAN GOFOOD (Studi Kasus Pada Wilayah Jakarta Timur)," Sekolah Tinggi Ilmu Ekonomi Indonesia, 2021. [Online]. Available: http://repository.stei.ac.id/6067/

[4] H. R. Hasnin, D. Megawati, D. Maulani, and D. Riany, "The Influence of Advertising and Discounts on Gofood Applications on Consumer Purchases in Bogor City," *Manag. J. Ilmu Manaj.*, vol. 6, no. 1, pp. 41–49, 2023, [Online]. Available: http://ejournal2.uika-bogor.ac.id/index.php/Manager/about

[5] M. A. Ritonga, H. Wintolo, and D. Nugraheny, "LAYANAN SCAN VIRUS MENGGUNAKAN KONSEP PEMROSESAN PARALEL," 2018. [Online]. Available: http://link.springer.com/10.1007/978-3-319-59379-1%0Ahttp://dx.doi.org/10.1016/B978-0-12-420070-8.00002-7%0Ahttp://dx.doi.org/10.1016/j.ab.2015.03.024%0Ahttps://doi.org/10.1080/07352689.2018.1441103%0Ahttp://www.chile.bmw-motorrad.cl/sync/showroom/lam/es/

[6] T. Urban, D. Tatang, T. Holz, and N. Pohlmann, "Towards Understanding Privacy Implications of Adware and Potentially Unwanted Programs BT - Computer Security," J. Lopez, J. Zhou, and M. Soriano, Eds., Cham: Springer International Publishing, 2018, pp. 449–469.

[7] Badan Siber dan Sandi Negara, "Lanskap Keamanan Siber Indonesia," Jakarta, 2023. [Online]. Available: https://www.bssn.go.id/

[8] A. C. Djamen, "Infrastruktur Jaringan Komputer Studi Kasus : Fakultas Teknik Universitas Negeri Manado," *Eng. Educ. J.*, vol. 7, no. 2, pp. 25–32, 2019.

[9] S. Nurhasanah and M. Rusdan, "Development of Front End on Tour and Travel Applications Using Python and Django Framework in PT. Industri Telekomunikasi Indonesia," *J. Informatics Commun. Technol.*, vol. 2, no. 1, pp. 31–38, 2020, doi: 10.52661/j_ict.v2i1.42.

[10] S. Situmorang, H. Lubis, and J. Manullang, "Analysis Of Malware Methods Using Dynamic Analysis In Detecting Malware," *J. Mantik*, vol. 6, no. 2, pp. 2639–2644, 2022.

[11] A. F. Sidiq, A. Yudhana, and R. Umar, "Virus Detection In Windows 10 Using Nist Method And Smadav Application 13.4," *J. Mantik*, vol. 4, no. 1, pp. 50–55, 2020, [Online]. Available: https://iocscience.org/ejournal/index.php/mantik/index

[12] J. A. O'brien and G. M. Marakas, *Management information systems*, vol. 6. McGraw-Hill Irwin New York, NY, USA:, 2006.

[13] A. F. K. Sibero, *Kitab Suci Web Programming*, vol. 75. 2011.