MALVERTISING: THE USE OF MALICIOUS ADVERTISING TO SPREAD MALWARE, AND ITS NEGATIVE EFFECTS ON THE WORLD ECONOMY

Radoslav BALTEZAREVIĆ
Senior Research Fellow, Institute of International Politics and Economics, Belgrade, Republic of Serbia
ORCID ID: https://orcid.org/0000-0001-7162-3510

Ivana BALTEZAREVIĆ
Associate Professor, Megatrend University, Faculty of Law, Belgrade, Republic of Serbia
ORCID ID: https://orcid.org/0000-0003-4605-1420

ABSTRACT

Cyberattacks like ransomware, spyware, and viruses are referred to as malware, or malicious software. Malvertising is the term for the malicious advertising that cybercriminals employ to trick victims into installing malware or steal data from their devices. While the attack might take many different forms, online advertising is always used to attract in the victim. For companies of all sizes, malware poses a serious risk. They have a significant impact both directly and indirectly. These include of financial loss, data loss, sensitive information theft, and disruption of operations. Cyberattacks also have an impact on the company's reputation and the trust that both clients and staff have in it. Malware can result in additional expenses that are directly related to a malware attack, as well as decreased user productivity, lost income from a system that is malfunctioning or performing poorly. Malvertising is thought to cause a loss of more than a billion dollars a year worldwide, and analysts believe the problem is growing and continues to negatively impact the global economy. To stop these cybercriminal acts, it appears that much more work must be done. For the time being, businesses and regular Internet users must take all available preventative measures to lessen the threat posed by malware. These precautions include installing Ad Blockers, Click-to-Play Plugins, updating software on a regular basis, configuring web browsers, and installing software updates. However, the most important advice is to not blindly trust Internet advertisements and to continually check devices.

Keywords: Malvertising, Cyberattacks, Malware, Global Economy.

INTRODUCTION

With the rise of malicious scams, which may seriously harm users' finances and emotional well-being, the Internet has evolved into a place where people can find more than just amusement and conversation (Baltezarević, 2023). The world's third-largest economy by GDP is represented by the $9.5 trillion global cybercrime economy (Bloomberg, 2024). Because of the structure of the Internet advertising ecosystem and the constantly shifting group

[1] The paper presents findings of a study developed as a part of the research project “Serbia and challenges in international relations in 2024”, financed by the Ministry of Science, Technological Development and Innovation of the Republic of Serbia, and conducted by Institute of International Politics and Economics, Belgrade during year 2024.

of businesses involved in online advertising, malicious actors now have a chance to pose as advertisers (Zarras et al., 2014).

Malvertising is the practise of disseminating malware via online advertisements. It entails inserting malware-filled or harmful adverts onto trustworthy, reputable websites (Grandoni, 2015). Malvertising can be found on any advertisement on any website, including the ones you frequent on a daily basis. Malvertising usually involves installing a small piece of malware that gives criminal command and control (C&C) servers access to your computer. After determining the location and software installed on your machine, the server selects the most effective malware to distribute to you (Malwarebytes, N/A). It has two negative effects that impact both consumers and brands. When users see deceptive ads, they may experience a number of problems, such as data breaches, system compromise, identity theft, and financial loss. On the other side, in terms of monetary losses and harm to their reputation, brands suffer the most from malvertising. Brands run the danger of damaging their reputation and losing the confidence of their clientele when their advertisements inadvertently act as distribution channels for malware. Consumers frequently accuse the brand of not taking adequate security precautions and actioning against these threats. Furthermore, it can be expensive to mitigate the effects of a malvertising incident, including legal bills, public relations campaigns, and user compensation (Smartprotection, 2024).

In its latest report on ad safety, Google claims to have blocked 1.4 billion of these ads that were designed to evade the company's ad review procedures. Google deleted 5.2 billion unwanted advertising in total, which is 1.8 billion more than in 2021. The volume of other prohibited ad types that violate the company's standards is significantly lower, as our figure demonstrates (Zandt, 2023). More than 438 thousand mobile malware installation packages were found in the third quarter of 2023 compared to the second quarter, a 19% increase (Petrosyan, 2024). These practices grow to be a major issue for regular people, small- and large-business systems, and the states themselves. Although this is a topic of much international discussion, it appears that cybercriminals are constantly coming up with inventive ways to get around security measures and continue their illegal activity (Baltezarevic & Baltezarevic, 2021).

LITERATURE REVIEW

Combining the terms "malware" and "advertising" yields the phrase malvertising. Malvertising is the practice of installing undesirable or downright dangerous software via the use of online exchanges, media networks, and other user-supplied content publishing services that are widely used in the arena of social networking (Salusky, 2007). Malvertising is the practise of an attacker, sometimes known as a "malvertiser," posing as an advertiser and displaying adverts with the intention of compromising the security of the devices on which they are displayed (for example, by convincing the user to install malware) (Jyotiyana & Maheshwari, 2016).

Malvertising attacks can be divided into two categories. In the first kind, the attacker inserts code into the advertisement to search for places where the user's device is vulnerable to infection. A proactive response from the user is not necessary to counter this attack. Malvertisers employ an enticing ad campaign to lure users to their website, which is controlled by them. This is known as the second kind of attack. The technique being imitated here is actually the same as that of phishing assaults (Hong, 2012). The technique known as "drive-by-downloads" is the riskiest form of the malware. Drive-by downloads carry the danger that

a user could infect their computer just by going to the website, even if they don't engage with any malicious content directly. In this instance, the malicious exploit looks for browser vulnerabilities and comes from the ad network server. Attackers most frequently target computers with out-of-date Java and Flash plugins (Zarras et al., 2014).

Malvertising attacs include: a) Angler Take Advantage of Kit. This drive-by download was one instance of a malvertising assault. Visitors were automatically forwarded to a malicious website, where an exploit kit was able to take advantage of flaws in widely used web extensions. b) Using a succession of dynamic URLs, the RoughTed malvertising campaign managed to evade ad-blockers and numerous anti-virus programs. c) The harmful advertisements seen in mobile apps are the focus of the KS Clean malvertising effort. After the virus was downloaded, it would warn the user to a security issue and encourage them to update the program through an in-app message. On the other hand, if the user accepted the update, it really finished the installation process and gave hackers access to their mobile device's administrative settings (Lenaerts-Bergmans, 2022). Malware attacks have the ability to penetrate systems deeply, break weak passwords, propagate throughout networks, and interfere with an organization's or firm's regular business operations. Other malware can cause a computer to slow down, lock up crucial data, bombard it with advertisements, or reroute users to dangerous websites (Regan & Belcic, 2024).

Exploit kits, a type of malware made to scan the system and find vulnerabilities or weaknesses within it, can also be used in malvertising attacks. The virus that is distributed through malvertising campaigns functions just like any other malware after it is installed. It has the ability to corrupt files, reroute internet traffic, track user behaviour, steal confidential information, and create backdoor entry points for the system. Data that has been erased, blocked, altered, leaked, or copied by malware may potentially be sold back to the user for ransom or on the dark web (Lenaerts-Bergmans, 2022). The rise in mistrust of trade in the digital sphere is a result of several real-world examples attesting to the actions of cybercriminals and the severe repercussions these activities have on governments, businesses, and individuals. Naturally, this kind of customer view harms the reputation of businesses that prioritize conducting business virtually, which has an immediate impact on earnings and, consequently, the ability of these businesses to remain in the marketplace (Baltezarević & Baltezarević, 2021).

A series of disclosures that may culminate in "one of the largest data breaches ever" have been triggered by a hack of the cloud storage business Snowflake. The hack exposed an unknown amount of client databases, which resulted in additional breaches at several other businesses, such as Santander and Ticketmaster. According to Snowflake, hackers used credentials obtained by malware to target customers who depended on single-factor authentication. Instead of enforcing MFA, the corporation lets customers take care of their own security. "Snowflake is a cloud product, and anyone can sign up for an account at any time," the company said in its initial statement. A threat actor might be able to access the account if they get their hands on the customer's credentials (Farrelly, 2024). Malvertising, as opposed to direct attacks, can jeopardize a user device's security without any direct intervention. Because of this, it is a difficult menace to totally eradicate. However, there are a number of measures to reduce the danger that may be done with prudence and the correct tools, like: a) Regular Software Updates; b) Ad Blockers; c) Anti-Malware Tools; d) Click-to-Play Plugins; e) Be Skeptical of Ads; f) Web Browser Configuration; and g) Regular Device Monitoring (Shelwell, 2024).

A disagreement between publishers and the creators of ad-blocking software has revolved around ad blockers. Some publishers, like wired.com and forbes.com, prohibit users using ad blockers from accessing their material (Schneier, 2016). Malvertising and genuine advertisements are blocked by ad blockers, which do not distinguish between the two. The advertisement is banned if the web page contains the expression of the code pattern. This has a double-edged effect. Adblockers remove most malware, but they also block genuine ad material that appears on websites, thanks to an updated database and active community. Because ad blockers reduce publishers' revenue, some have taken to refusing to display their material (or demanding a fee) if they identify that a user has an ad blocker installed on their browser (Dwyer & Kanguri, 2017).

Malvertising cost the internet advertising industry an estimated $1.13 billion in 2017, and it was predicted to increase at a rate of 20–30% per year (GeoEdge Add Integrity, 2017). An estimated $1 billion in income was lost in 2020 as a result of malvertising, according to experts (Grigoruk, 2021). Of all ad impressions worldwide, 17% were fake in the second quarter of 2022 (Statista Research Department, 2023). The percentage of worldwide malware infections that happened through email rose from 33 to 88 percent between 2018 and 2023. The cybersecurity market's worldwide indicator, "Estimated Cost of Cybercrime," was predicted to rise steadily between 2024 and 2029, totalling 6.4 trillion US dollars (+69.41 percent). The indicator is predicted to reach 15.63 trillion US dollars, a new top in 2029, following the eleventh year of increases. Notably, during the previous years, the cybersecurity market's "Estimated Cost of Cybercrime" indicator has been steadily rising (Petrosyan, 2024a). To put the magnitude of the problem into perspective, the Malwarebytes Threat Intelligence team identified over 800 malvertising efforts in the first half of 2023 alone, while also acknowledging that the actual number of attacks that went unnoticed by researchers was probably significantly higher (Balaban, 2024).

Ransomware is the “go-to method of attack” for cybercriminals. It is a type of malware that infects computers (and mobile devices) and restricts access to files, frequently threatening irreversible data destruction unless a ransom is paid. Ransomware has reached pandemic proportions worldwide (Morgan & Calif, 2020). Ransomware actors stepped up their operations in 2023, focusing on prominent organizations and vital infrastructure, such as government offices, hospitals, and schools. Large-scale supply chain assaults using ransomware were launched, taking advantage of the popular file transfer program MOVEit, affecting organizations like British Airways and the BBC. Ransomware groups have now collected over $1 billion in bitcoin payments from victims through extortion, an extraordinary milestone that was made possible by these and previous operations (Chainalysis Team, 2024).

CONCLUSION

When consumers visit fraudulent websites or click on an online advertisement, scammers can infect their computers with malware through a practice known as malvertising, also called malicious advertising. The difficulty in identifying malvertising is one of its main drawbacks. It's getting harder for the typical user to distinguish between legitimate and malicious ad snippets since scammers and malware operators are getting better at imitating well-known businesses. Attacks using malware have a detrimental effect on companies by harming their brand and reputation. A forced redirect or click ruins a customer's experience on a publisher's website, increases their vulnerability to malware, and damages the visitor's

impression of the publisher. It also deters them from visiting that site again. Malvertising poses a risk to users' security when they click on a malicious ad. Malicious advertisement may contain code that, when clicked, can infect a user's computer with malicious software. In addition, harmful advertisements have the ability to confuse and mislead visitors into exposing private information by rerouting them to websites that closely resemble trustworthy ones.

Not simply for specific businesses and internet users, malvertising is having a growing detrimental effect on the global economy, and it can cause $1 billion in income loss annually Cybercriminals are becoming increasingly crafty and inventive in their aims as these quickly emerging phenomena continues. Malvertising cases are now reported each year at a rate of roughly one thousand, and a significant portion of these cases are probably still unreported and unnoticed. Users are advised to be wary of internet advertisements and to frequently check their devices, even with the abundance of software programs that are available to protect against this issue. Even while there are commendable efforts to stifle cyberattack activity, it seems that the academic community and professionals in this sector do not take the issue of cyberattack defence seriously enough (Baltezarević et al., 2023). The benefits that technology may provide to people and businesses will make it a major force in the coming generation (Safieddine & Baltezarević, 2016). However, that justification makes it imperative to allocate all available resources toward effectively combating cybercrime, including malvertising, and safeguarding the online safety of future users.

REFERENCES

Balaban, D. (2024). Malvertising Is a Cybercrime Heavyweight, Not an Underdog. Retrieved from: https://www.secureworld.io/industry-news/malvertising-cybercrime-heavyweight (Accessed: 10.08.2024.)

Baltezarevic, R. & Baltezarevic, I. (2021). The Dangers and Threats that Digital Users Face in Cyberspace. *IPSI Transactions on Internet Research*, Vol. 17, No. 1, January 2021, pp. 46-52.

Baltezarević, I. & Baltezarević, R. (2021). Sajber bezbednost: izgradnja digitalnog poverenja, *Megatrend Revija*, Vol. 18 (4). pp. 269-280. DOI: 10.5937/MegRev2104269B

Baltezarević, R. (2023). Deceptive advertising in the online environment. 3rd International Black Sea Modern Scientific Research Congress, March 23-24, 2023, Proceedings: IKSAD – Congress book, (Ed. Prof. Dr. Mariam Jikia), Samsun, Turkiye, IKSAD Publications – 2023, p.p. 360 – 369. ISBN - 978-625-367-026-9

Baltezarević, V., Baltezarević, R. & Baltezarević, I. (2023). Sajber uznemiravanje dece sa posebnim osvrtom na digitalne igre, *Temida,* Volume 26, Issue 2, Pages: 261-284. https://doi.org/10.2298/TEM2302261B

Bloomberg (2024). The World's Third-Largest Economy Has Bad Intentions — and It's Only Getting Bigger. Retreived from: https://sponsored.bloomberg.com/quicksight/check-point/the-worlds-third-largest-economy-has-bad-intentions-and-its-only-getting-bigger (Accessed: 12/08/2024.)

Chainalysis Team (2024). Ransomware Payments Exceed $1 Billion in 2023, Hitting Record High After 2022 Decline. Retrieved from: https://www.chainalysis.com/blog/ransomware-2024/ (Accesed: 11/08/2024.).

Dwyer, C. & Kanguri, A.A. (2017). Malvertising-A Rising Threat To The Online Ecosystem. Journal of Information Systems Applied Research (JISAR). 10. 29.

Farrelly, J. (2024). High-Profile Company Data Breaches. Retrieved from: https://www.electric.ai/blog/recent-big-company-data-breaches (Accessed: 10/08/2024.)

GeoEdge Add Integrity (2017). The Battle Against Auto-Redirects: Saving Publishers and Advertisers $1.13 Annually. Retrieved from: https://site.geoedge.com/downloads/documents/Auto_Redirects.pdf (Accesed: 12/08/2024.).

Grandoni, D. (2015). Hackers Exploit 'Flash' Vulnerability in Yahoo Ads. Retrieved from: https://archive.nytimes.com/bits.blogs.nytimes.com/2015/08/03/hackers-exploit-flash-vulnerability-in-yahoo-ads/ (Accessed: 12/08/2024.)

Grigoruk, T. (2021). As publishers recognize the true cost of malvertising, recent cases highlight the damage. Retrieved from: https://digiday.com/sponsored/as-publishers-recognize-the-true-cost-of-malvertising-recent-cases-highlight-the-damage/ (Accesed: 12/08/2024.).

Hong, J. (2012). The State of Phishing Attacks. Commun. ACM, 55, 74–81.

Jyotiyana, P. & Maheshwari, S. (2016). A Literature Survey on Malware and Online Advertisement Hidden Hazards. In Intelligent Systems Technologies and Applications 2016; Corchado Rodriguez, J.M., Mitra, S., Thampi, S.M., El-Alfy, E.S., Eds.; Springer International Publishing: Cham, Switzerland, pp. 449–460.

Lenaerts-Bergmans, B. (2022). What is Malvertising? Retrieved from: https://www.crowdstrike.com/cybersecurity-101/malware/malvertising/ (Accessed: 10/08/2024.)

Malwarebytes (N/A). Malvertising. Retrieved from: https://www.malwarebytes.com/malvertising?srsltid=AfmBOooWWSqbiXPFg9GiQrFkhXvXfwnkoT-xUORVGebPK5utI2TJxkwg (Accessed: 10/08/2024.)

Morgan, S. & Calif, S. (2020). Cybercrime To Cost The World $10.5 Trillion Annually By 2025. Retrieved from: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/ (Accesed: 11/08/2024.).

Petrosyan, A. (2024). Volume of detected mobile malware packages as of Q3 2023. Retrieved from: https://www.statista.com/statistics/653680/volume-of-detected-mobile-malware-packages/ (Accessed: 10/08/2024.)

Petrosyan, A. (2024a). Annual cost of cybercrime worldwide 2018-2029. Retrieved from: https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide (Accesed: 12/08/2024.).

Regan, J. & Belcic, I. (2024). What Is Malware? The Ultimate Guide to Malicious Software. Retrieved from: https://www.avg.com/en/signal/what-is-malware (Accessed: 10/08/2024.)

Safieddine, F. & Baltezarević, R. (2016). Advances in technologies evolving new dimensions in e-society. In: The Internet as a Tool of Modern Business and Communication Saarbrücken, Germany: Lap Lambert Academic Publishing, pp. 43-75. ISBN 978-3-330-01350-6.

Salusky, W. (2007). Malvertising. Retrieved from: https://isc.sans.edu/diary/Malvertising/3727/ (Accessed: 13/08/2024.)

Schneier, B. (2016). The Ads Versus Ad Blockers Arms Race. Retrieved from: https://www.schneier.com/blog/archives/2016/02/the_ads_vs_ad_b.html (Accessed: 12/08/2024.)

Shelwell, G. (2024). What Is Malvertising? Retrieved from: https://caniphish.com/what-is-malvertising#WhatIs (Accessed: 11/08/2024.)

Smartprotection (2024). What is Malvertising and its consequences? What is Malvertising and its consequences? Retrieved from: https://www.smartprotection.com/articles/what-is-malvertising-and-its-consequences (Accessed: 12/08/2024.)

Statista Research Department (2023). Advertising fraud rate worldwide from 4th quarter 2021 to 2nd quarter 2022. Retrieved from: https://www.statista.com/statistics/1332538/ad-fraud-rate-worldwide/ (Accesed: 11/08/2024.).

Zandt, F. (2023). Deceptive Ads & Malware Make Up Bulk of Blocked Google Ads. Retrieved from: https://www.statista.com/chart/29626/ads-blocked-removed-by-google-by-enforced-policy/ (Accessed: 10/08/2024.)

Zarras, A., Kapravelos, A., Stringhini, G., Holz, T., Kruegel, C., & Vigna, G. (2014). The Dark Alleys of Madison Avenue: Understanding Malicious Advertisements. Paper presented at the Proceedings of the 2014 Conference on Internet Measurement Conference, Vancouver, BC, Canada.