HC3: Analyst Note

September 25, 2024 TLP:CLEAR Report: 202409251500

Malvertising and Healthcare

Executive Summary

Malvertising is a cyberattack method where legitimate advertising networks are infiltrated with malicious advertisements. The term malvertising is a combination of “malicious” and “advertising,” which refers to the use of online advertising to spread malware. It exploits the infrastructure of digital advertising to deliver malicious content to users, often without their knowledge or interaction. These ads can appear on reputable websites and are designed to automatically infect devices with malware upon viewing or interacting with the ad. This form of attack leverages the trust users have in well-known websites, and ultimately exploits the complexity of the online advertising ecosystem. This report provides an in-depth look at malvertising, its methods and impacts, and mitigation strategies to prevent its risks. To prevent serious damage to the Healthcare and Public Health (HPH) sector, HC3 encourages organizations to review the following report to increase awareness of these types of attacks and to employ available mitigations.

Report

The healthcare sector commonly makes use of digital technologies that can make it more susceptible to malvertising attacks. In today’s digital era, with a large amount of ads being created and used online through digital ad exchanges, it can be challenging for users to detect the malicious programs that are disguised to look like legitimate ads. Malvertising can appear on any site where advertising is used. Additionally, since not every user will click on online ads, it can make it even more challenging for defenders to decipher between which one is malicious or safe. Malvertising can be used to deliver multiple types of malicious programs that can pose a serious risk to the HPH sector:

- **Ransomware:** Encrypts the user’s files and demands a ransom for their release.
- **Spyware:** Gathers sensitive information from the user’s device without their knowledge.
- **Adware:** Displays unwanted advertisements and may track user behavior.
- **Trojans:** Disguised as legitimate software, Trojans provide unauthorized access to the user’s device.
- **Cryptojacking:** Uses the victim's device resources to mine cryptocurrency without their consent.

Types of Malvertising Attacks

When a user visits a website that displays ads from the compromised network, the malicious ad is shown alongside legitimate content. From this point, the malvertising attack can happen in multiple different ways depending on how advanced the attacker’s code is:

1. **Drive-by Downloads**: Involves malicious code that automatically downloads and installs malware on a user’s device without any user interaction required.
2. **Click-based Exploit:** Many forms of malvertisment require a user to click on an advertisment that redirects the user to a malicious website, where further exploitation can occur.
3. **Click Fraud**: With this attack, malware is designed to generate fraudulent clicks on ads to generate revenue for the attacker.
4. **Phishing Ads**: These ads direct users to phishing sites designed to steal sensitive information, such as login credentials.

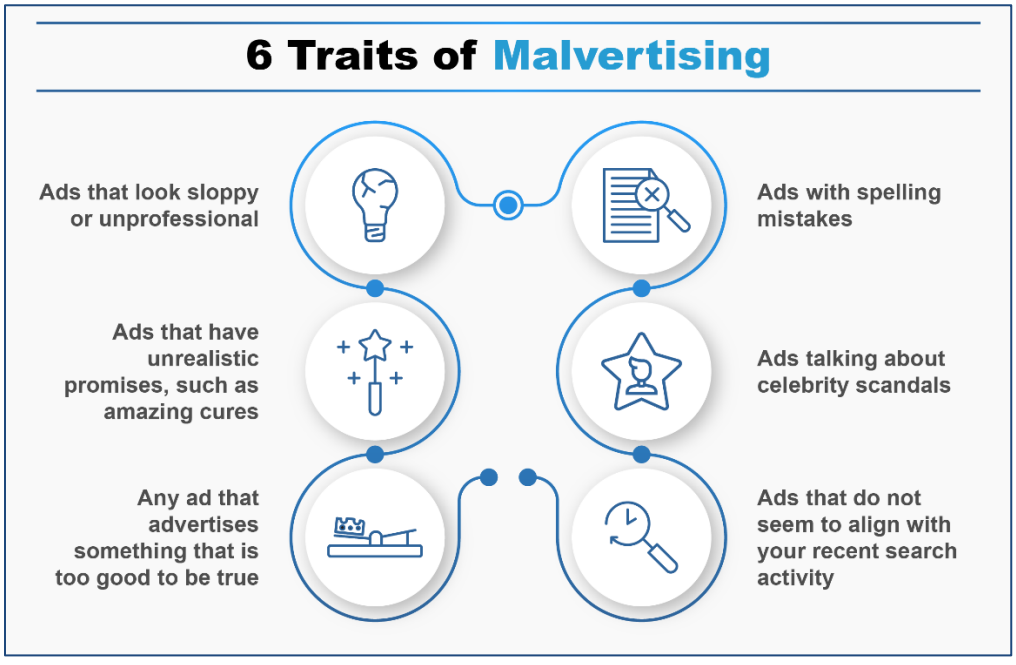
Search Engine Optimization (SEO) Poisoning

SEO poisoning, another variation of malvertising, is a malicious tactic used by cybercriminals to manipulate search engine results that can lead users to harmful websites. There are several different ways SEO poisoning works and can impact the HPH sector:

1. **Manipulating SEO Techniques**: Attackers use SEO techniques to boost the ranking of their malicious websites on search engines. This often involves the use of popular keywords and phrases, creating backlinks, and optimizing website content to appear legitimate and relevant.
2. **Infecting Legitimate Sites**: Sometimes, attackers may compromise legitimate websites, injecting malicious code or links that redirect users to harmful sites. This can increase the chances of their malicious sites appearing in search results.
3. **Creating Fake Content**: Cybercriminals create fake but convincing content that appears relevant to popular search queries. This content is often designed to lure users into clicking on links that lead to malware, phishing sites, or other harmful destinations.
4. **Exploiting Trending Topics**: Attackers often exploit trending topics, news events, or popular searches to increase the likelihood of their malicious sites being clicked. By capitalizing on what users are currently interested in, they can drive more traffic to their harmful websites.
5. **Phishing and Malware Distribution**: Once users click on the manipulated search results, they may be directed to websites that steal personal information (phishing) or automatically download malware onto their devices.

Prevention and Mitigations

1. **Ad Network Security**: Ad networks should implement strict security measures, including the use of firewalls, intrusion detection systems, and secure web gateways that can help identify and block malicious traffic associated with malvertising.
2. **User Awareness**: Educating users about the risks of clicking on unknown ads and the importance of keeping software up to date can reduce the risk of malvertising.
3. **Network Segmentation**: By segmenting networks, healthcare organizations can limit the spread of malware to other critical systems and help isolate data from the attack.
4. **Browser Security**: Users should use browsers with strong security features and keep them updated.
5. **Incident Response Planning**: Having an incident response plan in place ensures that organizations can quickly and effectively respond to malvertising incidents.



HC3: Analyst Note
September 25, 2024 TLP:CLEAR Report: 202409251500

Impact to the Health Sector
Malvertising poses a serious risk the HPH sector since healthcare organizations rely on and use digital systems for their daily operations. Medical professionals, administrative staff, and even patients can potentially interact with these malicious ads through avenues like medical portals or health information websites. If compromised, the malware has the potential or spread throughout the entire network.

1. **Data Breaches**: Malvertising can facilitate data breaches, exposing sensitive patient, personal, or corporate information.
2. **Operational Disruption**: Malvertising can disrupt business operations by causing system failures, data loss, and downtime. Recovery from such disruptions can be time-consuming and impede patient care.
3. **Financial Loss:** Malvertising can lead to significant financial losses for individuals and businesses. Ransomware demands, fraudulent transactions, and the cost of recovery operations can all contribute to these potential losses.
4. **Deployment of Other Malware:** Interaction with these malicious forms of advertisement can also operate as a payload delivery method for other attacks, such as ransomware, which frequently targets the HPH sector.

Helpful Resources
The following links contain a list of beneficial resources to help enhance organizational understanding of what malvertising is and how to protect yourself from being a victim from one of these attacks:

- https://www.cisa.gov/sites/default/files/publications/Capacity_Enhancement_Guide-Securing_Web_Browsers_and_Defending_Against_Malvertising_for_Federal_Agencies.pdf
- https://www.justice.gov/criminal/file/1404806/dl?inline
- https://attack.mitre.org/techniques/T1583/008/
- https://www.cisecurity.org/insights/blog/malvertising
- https://www.crowdstrike.com/cybersecurity-101/malware/malvertising/
- https://www.mcafee.com/learn/what-is-malvertising-and-how-do-you-avoid-it/
- https://www.zscaler.com/blogs/security-research/malvertising-campaign-targeting-it-teams-madmxshell
- https://www.gdatasoftware.com/blog/2023/10/37814-meta-hijacked-malicious-ads
- https://www.imperva.com/learn/application-security/malvertising/
- https://caniphish.com/what-is-malvertising#prevention
- https://www.trendmicro.com/en_us/research/23/f/malvertising-used-as-entry-vector-for-blackcat-actors-also-lever.html
- https://www.threatdown.com/blog/a-peek-inside-a-malvertising-campaign/
- https://www.rapid7.com/blog/post/2024/05/13/ongoing-malvertising-campaign-leads-to-ransomware/

Conclusion
Malvertising represents a significant threat to the healthcare sector, through leveraging the widespread reach of online advertising to distribute malware to unsuspecting users. The risks associated with malvertising can be substantial, including financial losses, data breaches, operational disruptions, and even leading to attacks like ransomware deployment. By understanding the mechanisms of malvertising

and implementing comprehensive security measures, organizations can better protect themselves against this threat.

References

Bergmans-Lenaerts, Bart. What is Malvertising?. CrowdStrike. October 17, 2022. https://www.crowdstrike.com/cybersecurity-101/malware/malvertising/

Iao, Kapua. SEO Poisoning and the healthcare industry. PauBox. December 01, 2023. https://www.paubox.com/blog/seo-poisoning-and-the-healthcare-industry

Malvertising. Imperva. https://www.imperva.com/learn/application-security/malvertising/#:~:text=Malvertising%20is%20a%20malicious%20attack,leading%20them%20to%20unsafe%20destinations.

What Is Malvertising?. Fortinet. https://www.fortinet.com/resources/cyberglossary/malvertising

Malvertising: The Dark Side of Online Advertising. StoneFly. https://stonefly.com/blog/malvertising-the-dark-side-of-online-advertising/

Sheldon, Robert. SEO poisoning (search engine). TechTarget. https://www.techtarget.com/whatis/definition/search-poisoning

Malvertising. MalwareBytes. https://www.malwarebytes.com/malvertising

What is Malvertising?. Zennarmor. https://www.zenarmor.com/docs/network-security-tutorials/what-is-malvertising

Contact Information

If you have any additional questions, we encourage you to contact us at HC3@hhs.gov.

We want to know how satisfied you are with the resources HC3 provides. Your answers will be anonymous, and we will use the responses to improve all future updates, features, and distributions. Share Your Feedback