IT Security | Supply Chain | OT Security | Insider Threat | Physical Security | Interoperable Communications

CAPACITY ENHANCEMENT GUIDE

Securing Web Browsers and Defending Against Malvertising for Non-Federal Organizations

DEFEND TODAY,
SECURE TOMORROW

OVERVIEW

Organizations across the nation have expanded telework options to keep staff safe during the COVID-19 pandemic; however, this shift has increased opportunities for adversaries to gain unauthorized access to teleworkers' system endpoints—this includes their web browsing capabilities. One method of attack is malvertising, which can enter networks through unsecure or outdated web browsers. The following information can help business and government leaders employ appropriate IT security protections to reduce risk of malvertising and potential business impacts.

AT-A-GLANCE RECOMMENDATIONS

- Standardize and Secure Web Browsers
- Deploy Ad Blocking Software
- Implement Internet Browser Isolation
- Apply Protective DNS Technologies

WHAT IS MALVERTISING?

Malvertising uses malicious or hijacked website advertisements to spread malware, as well as insert malicious ads into legitimate ad networks to deliver harmful payloads that can interact directly with users or run hidden script. Unlike more familiar adware attacks, malvertising allows threat actors to embed malware in passive advertisements. In other words, malvertising can compromise a network even if you do not click on an ad.

HOW DOES MALVERTISING GET INTO YOUR NETWORK?

The primary way people interact with the internet is through web browsers. Like a broken front door to your network, poorly maintained browsers (*especially those that do not promptly install security updates*) can invite adversaries to exploit this opening.

Common vulnerabilities include:

- Browsers with unsecure configurations,
- Outdated browsers,
- Exposure to malicious websites and applications, and
- Poorly trained or unaware users with unsecure browsing habits.

HOW BAD IS IT?

Malvertising is a significant vector for exploiting networks. It bypasses built-in browser settings designed to protect against pop-ups and website redirects. These malicious ads can then generate a forced redirect or deliver a payload so adversaries can carry out their nefarious goals.

Adversaries can even create carefully tailored ads as part of a targeted campaign against a specific victim.

HOW TO PREVENT MALVERTISING

With some precautions, it is possible to reduce the threat of malvertising. Malvertising and poor web browser security go hand in hand, so organizations should focus on securing user endpoints capable of web browsing. Potential solutions range from the fairly simple and inexpensive to the complex that require more initial investment but may offer potential long-term cost savings. The Cybersecurity and Infrastructure Security Agency (CISA) recommends the following four approaches to prevent malvertising.

STANDARDIZE AND SECURE WEB BROWSERS

In general, the easiest and most cost-effective step is to limit browser types, versions, and configurations used and enforce standardized browser settings across your network. The more web browsers, browser versions, and configurations your organization allows, the more complex it will be to implement web browser security controls. Instead, limit your workforce's options to just the browsers, versions, and settings that your organization permits/approves, so you are working with a consistent and manageable network portfolio.

Benefits of Secure Web Browsers

- Reduces the organization's attack surface
- Increases efficiency when it comes to monitoring, as well as managing and updating patches
- Potentially improves response efforts to newly disclosed vulnerabilities by simplifying the number of types and configurations in use

DEPLOY AD BLOCKING SOFTWARE

Ad blocking software is usually more complex and expensive to implement than browser standardization. However, it could still be a good option to consider.

Benefits of Using Ad Blocking Software

- Reduces risk of malicious advertisements or redirects to malicious or phishing sites
- Enhances client-side performance and faster page loading
- Reduces risk of data collection by third parties

How Does Ad Blocking Work?

Ad blocking software prevents different types of ads from displaying or removes them altogether, reducing the risk of receiving malicious advertisements or being redirected to malicious websites. A common ad blocking technique uses web browser extensions that allow organizations to customize and control how online advertisements appear. CISA encourages organizations to evaluate solutions that would allow the ability to block a malicious advertisement.

However, browser extensions present their own potential security concerns. Ad blocking browser extensions operate with high levels of privilege and have access to all data traffic between the user workstation and the network. Because of this, such browser extensions can collect data or perform other malicious actions. Some browser extensions are known to accept payment from advertisers to ensure that paid for ads are allowlisted from blocking.

How to Select Ad Blocking Software

Selecting an appropriate ad blocking software solution requires diligence. Organizations should apply standard software decision criteria—such as commercial vs. open-source, product standards (in this case, what entity maintains and updates the allowlist of acceptable sites or the blocklist of unacceptable sites), and whether the product operates at the lowest level of privilege necessary for the task.

IMPLEMENT INTERNET BROWSING ISOLATION

Browser isolation implementation is a strategic architectural decision embraced by major corporations. The breadth of implementation options and functionality makes the design, implementation, and maintenance of internet browser isolation more complex than the other recommendations in this guidance. Also, it potentially carries the greatest initial cost of the four recommendations. However, over its life cycle, browser isolation may yield cost savings, based on reduced costs for maintaining ad blocking software, lower incident response and recovery costs, and bandwidth efficiencies. In most cases, this option should be considered as part of a broader architectural change or network refresh. As with deploying ad blocking software, it requires an outlay of resources beyond staff cycles.

How Does Browser Isolation Work?

Internet browser isolation creates a logical barrier between the web browser and the rest of the system. This barrier operates under the premise that all web traffic is untrustworthy and potentially harmful. The traditional method is local browser isolation, usually done by using a sandbox or virtual machine on the user's local computer. It isolates the user's browser data away from the operating system to a temporary environment.

Remote browser isolation takes this a step further and transfers web data processing off the local system (end-user workstation) to a secure, virtualized environment or isolated cloud-based platform with sandbox-like containers.

Data transfer from the web occurs in the container or virtualized environment; malicious code is removed, and the cleaned transmission is then forwarded to the user. Isolation is highly customizable and can be used in combination with web content filtering, data loss prevention solutions, secure email/web gateways, and other security approaches. Finally, isolation is available from third-party service providers or as a software-as-a-service offering.

Benefits of Internet Browser Isolation

- Eliminates the need for website allowlisting and blocklisting and for web browser security user training
- Gives administrators the flexibility to set scalable policies ranging from isolating a portion of traffic to isolating every download, attachment, and link
- When coupled with a file-transfer solution to permit webmail and webpage document downloads (i.e., a "save as" to local storage), diminishes significant attack avenues by substantially reducing risks from malicious file content
- Potentially reduces network maintenance costs by reducing internet bandwidth requirements

APPLY DOMAIN NAME SYSTEM PROTECTION TECHNOLOGIES

Operated defensively, protective Domain Name System (DNS) technologies are an additional layer of security to enhance resilience of online systems and to help guard organizations and their users from attacks. Protective DNS is an evolving technology that seeks to neutralize domain names used in ransomware, phishing, botnets, and malware campaigns. Using government and commercial threat intelligence feeds, protective DNS can block access to malicious internet infrastructure. According to studies, more than 91 percent of malware uses DNS for cyberattacks, and one out of every three cyber incidents could be prevented with protective DNS services. Organizations should consider applying this technology.

Benefits of Using Domain Name System Protection Technologies

- Adds layer of security to enhance resilience
- Neutralizes domain names used in ransomware, phishing, botnets campaigns
- Prevents 1 of 3 cyber incidents, according to studies

MORE INFORMATION AND ASSISTANCE

The executives and IT professionals in every organization should assess their networks, consider various attack vectors, and apply these or other mitigation strategies based on their unique environment.

Many of CISA's recommendations are based on guidance issued by the National Institute of Standards and Technology (NIST). NIST can be a valuable resource for more in-depth guidance and checklists. In addition, CISA has experts who can help assess an organization's risk and offer technical assistance with cybersecurity issues.

For more information or to seek additional help from CISA, contact us at Central@cisa.dhs.gov.