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

# CAPACITY ENHANCEMENT GUIDE

## Securing Web Browsers and Defending Against Malvertising for Federal Agencies

DEFEND TODAY, SECURE TOMORROW

## AT-A-GLANCE RECOMMENDATIONS

- ✓ Standardize and Secure Web Browsers
- ✓ Deploy Advertisement Blocking Software
- ✓ Isolate Web Browsers from Operating Systems
- ✓ Implement Protective Domain Name System Technologies

## OVERVIEW

Web browsers are the primary mechanism for user interaction with the internet. As such, their security is a constant concern due to the ease of exploitation and the ability of adversaries to interact directly with users. Common vulnerabilities associated with browsers include unsecure configurations, exposure to malicious websites and applications, and unsecure browsing habits due to poorly trained or unaware users.

## WHAT IS MALVERTISING

Malvertising is the use of malicious or hijacked website advertisements to spread malware and is a significant vector for exploitation. It bypasses built-in browser protections against pop-ups and forced redirects and inserts malicious ads into legitimate ad networks. These ads spawn a forced redirect or load a payload for malicious purposes. Adversaries can use carefully crafted and tailored malicious ads as part of a targeted campaign against a specific victim, not just as broad-spectrum attacks.

## AUDIENCE AND SCOPE

- ➢ This guidance advises **federal agencies** on the threat posed by malicious advertisements (malvertising) and recommends actions to protect web browsers from malicious advertising.
- ➢ This guide provides information to inform federal agencies' executive leadership about this threat and also provides sufficient detail to support a technical discussion with implementation teams.
- ➢ For federal agencies, network-based technologies and controls are addressed, in part, by services provided by CISA—such as EINSTEIN 3 Accelerated (E3A)—and are services provided outside of the concise scope of this guidance. CISA encourages organizations to also manage access to advertisements through their own network-based technologies, such as web proxies, centralized Domain Name System sink-holing, web filtering, and firewalls.
- ➢ Capacity Enhancement Guides support CISA's role as the Nation's cybersecurity risk advisor by sharing high priority recommendations, best practices, and operational insights in response to systemic threats, vulnerabilities, and risks.

## HOW TO DEFEND AGAINST MALVERTISING

For federal agencies, defending against these attacks is complicated by variations in control selection, implementation, and standardization across the Federal Government and the different sectors of critical infrastructure; these complications result in inconsistent mitigation. Failure to implement effective browser security inhibits mitigation of web browser risks—including malvertising—and increases the possibility that federal networks will suffer data breaches, mission degradation, increased response costs, and loss of public trust.

With many agencies greatly expanding telework options, agencies should increase attention on securing federal endpoints, including associated web browsing capabilities.

## RECOMMENDED ACTIONS

The Cybersecurity and Infrastructure Security Agency (CISA) recommends the following actions to protect web browsers from malicious advertising.

### Standardize and Secure Web Browsers

Simplify your web browser infrastructure via standardization. This is often the easiest, quickest, and most cost-effective approach.

Permitting the use of multiple web browsers, browser versions, and browser configurations results in several disadvantages for agencies. These include a larger attack surface, increased complexity in implementing web browser security controls, and a compromised ability to maintain situational awareness within the agency. Implementing managed approvals for browser version and configuration options can reduce the risks associated with deprecated technologies and establish strict exception policies with enhanced compensating controls for legacy applications that need to run outdated or difficult-to-secure code. Additional guidance can be found in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-28 v2, *Guidelines on the use of Active Content and Mobile Code*.[1] The National Security Agency (NSA) has also produced an open-source tool—deployable on agency networks—to block outdated browser versions.[2]

**Standardizing and securing web browsers according to leading practices provides the following benefits:**

- Reduces agency attack surface by specifically addressing multiple web browser and plug-in vulnerabilities—many current browser exploits can be addressed with the execution of applicable browser checklists
- Enables increased agency efficiency in monitoring and update and patch management, and may improve response efforts to newly disclosed vulnerabilities by simplifying the number of types and configurations in use
- Streamlines and facilitates software configuration management and patch management processes

CISA recommends securing web browsers according to the configuration guidance defined in NIST SP 800-70 r4, *National Checklist Program for IT Products – Guidelines for Checklist Users and Developers*[3] and managing configurations on an ongoing basis as technology changes and checklists are updated. CISA recommends implementing a comprehensive and efficient patching program. NIST's SP 800-40 r3, *Guide to Enterprise Patch Management Technologies*, can assist in developing and refining approaches to patching.[4]

### Deploy Advertising Blocking Software

An additional measure is to implement advertisement blocking. In most cases, this solution is generally more complex and expensive to implement than browser standardization.

Ad-blocking software prevents advertisements from displaying or removes different types of ads (e.g., pop-ups, banner ads) when a user visits a website or uses an application. This software reduces a user's risk in receiving malicious ads or being redirected to malicious websites. One common ad-blocking technique is the use of web browser extensions that enable a user or agency to customize and control the appearance of online ads. CISA encourages agencies to evaluate solutions that would enable malicious ad blocking.

**The benefits of using advertising blocking software include the following:**

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

[1] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-28ver2.pdf
[2] https://github.com/nsacyber/Blocking-Outdated-Web-Technologies
[3] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-70r4.pdf
[4] See also: NIST SP 800-40 r3, Guide to Enterprise Patch Management Technologies, July 2013
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r3.pdf

Note: ad-blocking browser extensions operate with high levels of privilege and have access to all data traffic between the client and the network, allowing them to collect data or perform other potentially malicious actions. Additionally, some browser extensions are known to accept payment from advertisers to ensure their ads are allowlisted from blocking.[5]

## Consider Isolating Web Browsers from Operating Systems

Embraced by the Department of Defense and major corporations, browser isolation is a strategic architectural decision. The breadth of options and functionality makes the design, implementation, and maintenance of web browser isolation more complex than the other recommended actions in this guidance. Also, it potentially carries the greatest initial cost of the three recommendations. However, over its lifecycle, browser isolation may have a lower cost, 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.

Web browser isolation creates a logical barrier—between the browser and the operating system—that operates under the premise that all web traffic is untrusted. Separating the browser from the operating system decreases the impact of exploits by limiting malicious code to a temporary environment. Remote browser isolation takes this a step further and transfers the processing of web data off the local system 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—if present—is removed, and the cleaned transmission is forwarded to the user. Isolation is highly customizable and can be combined with web content filtering, data loss prevention solutions, secure email/web gateways, and other security approaches. Browser isolation is available from third-party service providers or as a software-as-a-service offering.

**Internet browser isolation provides the following benefits:**

- Isolates potential malicious code and content within the “protected” cloud platform, separating the threat from direct connections to the host operating system, eliminating ransomware attacks, and allowing users to click on any website
- Reduces the need for website allowlisting and blocklisting and for web browser security user training
- Gives administrators the flexibility to set tunable policies ranging from isolating a portion of traffic to isolating every download, attachment, and link
- Diminishes significant attack avenues by substantially reducing file risk content when coupled with a file-transfer solution to permit webmail and webpage document downloads (i.e., a “save as” to local storage)
- Provides a rich source of insider threat intelligence within the virtual browser logs because it allows users to visit high-risk websites
- Neutralizes existing malware in the network by disrupting the link to the command and control site
- Does not increase the browser’s memory usage, slow processing, or adversely impact the user’s web browsing experience—unlike the site isolation capability currently offered by most web browsers

## Consider Implementing Protective Domain Name System Technologies

Agencies should consider deploying protective Domain Name System (DNS) technologies (also known as DNS firewall) to block malicious content associated with malvertising. Studies suggest that more than 91 percent of cyberattacks use DNS and that protective DNS services could mitigate one out of every three incidents from occurring. Protective DNS technologies diminish attack vectors by preventing redirects to and DNS resolution of known malvertising domains, preventing user interface with domains identified as malicious.

[5] See also: Senator Ron Wyden’s letter concerning these practices https://www.wyden.senate.gov/imo/media/doc/011420 Wyden Ad Blocking Letter to FTC.pdf