Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Mitigating Drive-by Downloads

JUNE 2020

Introduction

Adversaries are increasingly using drive-by download techniques to deliver malicious software that compromises computers. This document explains how drive-by downloads operate and how compromise from these techniques can be mitigated.

What happens in a drive-by download?

A drive-by download occurs when a user visits a legitimate but compromised website. When the user accesses the website, an adversary's malicious code exploits weaknesses or other security vulnerabilities in the user's web browser or web browser plug-ins allowing the download of malicious files to the user's computer. The downloaded files enable the adversary to have full access and control of the user's computer, either to steal valuable information or to launch denial-of-service attacks against other users on the internet.

Another form of a drive-by download is 'malvertisement', which is commonly Flash Player-based and takes advantage of unpatched software. Disguised as legitimate advertisers, an adversary implants their malicious software in an advertisement on a legitimate website. When a user views the advertisement, the malware infects their computer.

Most drive-by downloads require scripts to be loaded from third party websites. An adversary can inject inline frame codes into legitimate websites, which then load malicious software hosted on other websites operated by the adversary when a compromised website is visited.

Search Engine Optimisation (SEO) is another technique often used in conjunction with a drive-by download exploit. SEO increases a website's visibility in a search engine. Generally, the higher or more often a website appears in a search result, the more traffic the website is likely to receive from the search engine's users. An adversary can use SEO to promote their malicious websites in search engines to increase the chance of getting traffic to their website for the exploit to occur.

There are malware kits available which target specific web browsers or software flaws, including Adobe Reader, Microsoft Internet Explorer and web browser plug-ins. The server to which these kits are connected can use HTTP request headers from a web browser, to determine which specific exploits are most likely to work on a user's computer.

Mitigating drive-by downloads

To mitigate drive-by downloads, the following mitigation strategies should be implemented:

- Implement application control. In many successful cyber security incidents application control would have been the only mitigation strategy able to stop drive-by downloads from executing malicious software.

- Patch applications and operating system security vulnerabilities, especially Java and Flash. Old versions of applications are more vulnerable to drive-by downloads. Keep all applications up-to-date.
- Minimise the use of domain and administrator privileges. Limit the ability for users with domain or administrator privileges to have access to email and the internet by employing separate unprivileged workstations or accounts for these purposes.

Organisations should also consider implementing the following mitigation strategies:

- Implement robust web content filtering that inspects the content of all web traffic for potentially malicious downloads and blocks it. Preferably block ActiveX, Java, Flash, HTML inline frames and JavaScript, except from a list of approved websites.
- Implement a list of approved domains, including HTTPS domains, to only allow trusted domains to be accessed by users. This will not prevent drive-by downloads but it will prevent secondary malicious websites from loading.
- Install and maintain updated antivirus software capable of scanning internet traffic and detecting exploits.

Further information

The ***Australian Government Information Security Manual*** (ISM) assists in the protection of information that is processed, stored or communicated by organisations' systems. It can be found at https://www.cyber.gov.au/acsc/view-all-content/ism.

The ***Strategies to Mitigate Cyber Security Incidents*** complements the advice in the ISM. The complete list of strategies can be found at https://www.cyber.gov.au/acsc/view-all-content/publications/strategies-mitigate-cyber-security-incidents.

Contact details

If you have any questions regarding this guidance you can contact us via 1300 CYBER1 (1300 292 371) or https://www.cyber.gov.au/acsc/contact.