Drive-by-Download Attack: An Observation

By | Ahmad Azizan Bin Idris

Introduction

Attacking methods used by adversaries to get into a user's computer are increasingly sophisticated through their malicious code and complexities in attacking infrastructure settings. Malware spreading are no longer limited via e-mail spam and instant messaging clients but also through various techniques especially the use of web applications.

A clear approach to this situation is what we call the Drive-by-Download attack. Drive-by-Download attack allows the adversary to massively infect a user's computer by simply getting them to enter a particular malicious website. By using this technique, the adversary spreads the malware, usually an exploit kit, by taking advantage of vulnerabilities in those websites and the user's computer applications.

Usually, the attack process is conducted in an automated manner and pre-programmed to cater for the most common vulnerabilities to exploit from the user's computer applications. Such popular vulnerabilities targeting the user's web browser are applications such as a PDF reader or various documents' applications.

Attack Process

To obtain a better understanding of this method, the attack flow of a drive-by-download may be represented as in Figure 1:

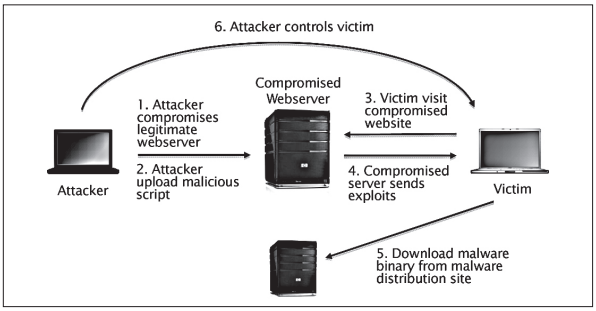

Figure 1 *Drive-by-download attack*

In the beginning of the process, the attacker inserts the malicious script inside the vulnerable website, usually an obfuscated malicious JavaScript code, and then the process continues as follows:

1. Attacker compromises the legitimate web server through a loophole in the web application's vulnerabilities or the system itself.
2. Once access is obtained, attacker uploads the malicious scripts and/or exploits and embeds it into the legitimate website.
3. The victim visits the website that was compromised by the attacker.
4. The website sends along the requested page containing the malicious scripts that the attacker injected. Malicious scripts/exploits received by the victim exploits the vulnerabilities of his computer's applications. Attempts of exploits proceed one after another with different vulnerabilities, until the exploitation is successful. (e.g: check vulnerabilities in MS IE, Adobe Reader, etc).
5. If the exploitation succeeds, the exploited payloads are usually invoked to download a malware executable file from a malware distribution site and install it in the user's computer unnoticed.
6. Through malware installed inside a victim's computer, an attacker can control the system and carry out malicious activities inside the computer (e.g: keylogging, collect victim's personal information, send spam, etc).

This is how the Drive-by-Download starts in general where the malware executables are downloaded and automatically installed and executed inside a victim's computer. Thus, infection of the malware is indeed effectively carried out through vulnerabilities in the user's system.

Software manufacturers might have already solved exploited vulnerabilities a long time ago. However, attacks are successful because the user did not patch the necessary applications. The only case in which the user will not be infected is one in which the system is fully patched and no application vulnerability can be exploited.

Malicious Script

The malicious script attacks involved in Drive-by-Download used to spread malware generally contains one or more associated exploit code to a URL which is, in short, checks for vulnerabilities on the victim's system and then exploits them.

This methodology is widely used in such attacks and involves the insertion of, for example, a HTML tag called iframe. The iframe tag allows for the opening of a second web document within the main browser window.

The technique to conceal the iframe from visualising the second page is by making it small. The iframe usually opens within a frame size of 0x0 pixels or 1x1 pixels, which will cause a user to be unaware of its existence within the page visited.

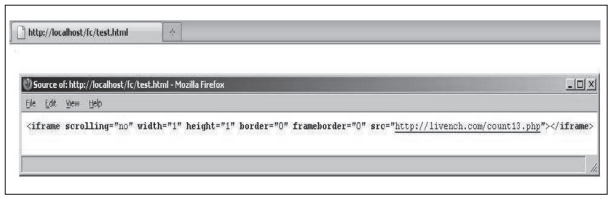

Figure 2 *Iframe tag inside HTML code*

Figure 2 illustrates how an iframe becomes one of the crucial components for a Drive-by-Download attack where a harmful one is embedded in the source code of a compromised website. The HTML iframe tag interpreted by the web browser is not visible to the user since the tag option is meant to prevent it from being detected from the main window view.

Inevitably, when the malicious website is visited, it directs the second malicious web page contained in the iframe tag which in the end invokes the download and executes a payload to get the malware executable.

Obfuscation Techniques in Malicious Script

Such method also comes with a version of obfuscated codes, and most adversaries prefer to use it. In order to extend the survival duration of malware spreading, the malicious code needs to be hidden by making it complicated to read and decode with static analysis. This makes the URL of malware distribution sites not visible, thus lengthening the time of its existence.

JavaScript is one of the most used codes inside malicious activities, and one of the most preferable to obfuscate. With its rich amount of functionalities, JavaScript codes as shown in Figure 3 can be obfuscated to certain extent in order to hinder others from getting the real or genuine JavaScript code. To name some of the popular functions that adversaries use, are eval and unescape, from CharCode, CharCodeAt, ParseInt etc.

Figure 3 *Obfuscation used in JavaScript code*

Obfuscation techniques are increasingly common to find. Even though the duration in performing static analysis can take some time with obfuscated codes, but it's worth the effort in order to analyse the behaviour and trend of new techniques applied by adversaries. Either way, performing dynamic analysis would also help in getting the work done.

Prevention and Best Practices

Prevention is better than cure; it is true, because the effort put into not getting infected with malware is less cumbersome than having to deal with it after being infected. It is a worthwhile initiative for a user to look at their computer security as a whole and carry out regular security practices to ensure optimum protection. This may, for example, involve:

- Having a robust anti-virus/full security solution installed on their computers.
- Making sure to update the operating system with the latest security patches.
- Keeping all applications running on the computer up-to-date and download updates on a regular basis as they are released to avoid vulnerabilities.
- Making it a habit to run regular full system scans to check for problems and remove them.
- Avoid clicking on links from websites of unknown origins or are embedded in the body of emails, especially in spam e-mails.
- Checking the redirection of links. By hovering on top of the links, you can see where the links will redirect from the status bar.
- Installing security plug-ins provided by the web browser, such as automatic blockage of JavaScript execution or force download activities.
- For web administrators, take note on upgrading all web applications and monitoring them to locate any type of scripts that may have been inserted by third parties.

Conclusion

By having a multi-layer security solution, much of the work and effort towards preventing such attacks can be saved for something useful rather than being a victim of a cybercrime and having to deal with the losses and pain resulting from it. This includes having antivirus for the system, security add-ons for the web browser, like NoScript and Adware pop-ups prevention, regular updates of patches, fixes, and upgrades for the Operating System and applications.

The most important thing in prevention is to inculcate security awareness in the hearts and minds of the users. By doing this, much of the attacking incidents can be eliminated. The Internet is a big world with everything being just a click away, whether it is good or bad. By making wise considerations on the choices on the Internet will help you remain safe while surfing. Without being aware of the possible dangers that might occur, having a very strong and secure system will be useless as the most important component of the system, humans, can be exploited easily. ■

References

1. *http://www.spywarewarrior.com/uiuc/dbd-anatomy.htm*
2. *http://www.securelist.com/en/analysis/204792056/Drive_by_D ownloads_The_Web_Under_Siege*
3. *http://www.iseclab.org/papers/driveby.pdf*
4. *http://community.ca.com/blogs/securityadvisor/archive/2010/03/12/command-and-conquer-with-backdoor-wisp.aspx*