Dr. Lunsford

ICTN 4040

Drive-By Download Attacks

Coley J. Stevens

East Carolina University

Abstract

Over the past few years, we seen the rise of drive-by downloads. Drive-by download attacks are malicious automated programs, that are employed on systems without the user's permission or knowledge. Today, this method is one of the most common ways malware is spread. In this report we will learn about how drive-by downloads operate and the different methods used to implement drive-by downloads. Readers will also get to see how detrimental these attacks can be with some real-life examples. To end the report, we will look into a few ways to prevent drive-by downloads from doing serious damage and to better prepare readers to not fall victim to the process of the attacks.

What Are Drive-by-Downloads Attacks?

Drive-by-Downloads are automated applications (malware) that push out and execute malicious code on a system (Narvaez, 2010). They can affect applications (webpages), operating system and web browsers. In most cases, the malicious code is embedded into websites using and exploit kit. The exploit kit begins by scanning a system for openings. The openings, also known as vulnerabilities, allow the codes into the system, which then can lead to a complete takeover of the system. There are multiple ways these openings can be created. They can appear due to outdated applications, browser plugins and many more problematic situations. The code that can be executed can consist of many vicious elements such as JavaScript code to cross-site scripting attacks (XXS attacks).

How can the attacks occur?

The common drive-by download attack involves attackers taking control of authorized websites to gain access to sensitive information. In this case, end users are not aware of any criminal activity. The compromised webpages look normal most of the time. It is at this time when the attacks happen silently. Other forms of drive-by-download attacks include phishing schemes and social media attacks (Drive, 2019).

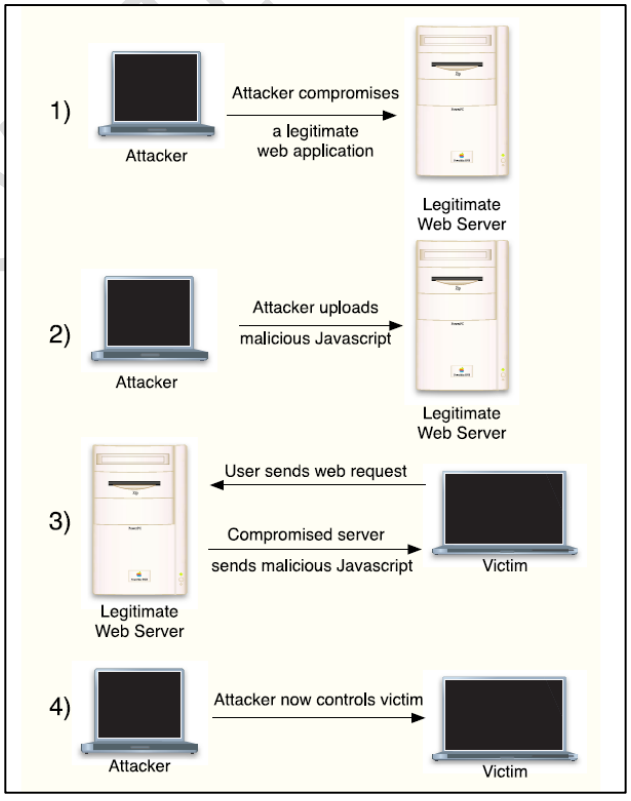

Figure 1: shows the attacker compromising the web application, uploading the malicious code and taking control of the victim

Other ways drive-by downloads can occur is through emails and pop-up ads. With E-mails, attackers' generally send emails to the victim who then opens the toxic link and is redirected to the malicious content. As mentioned before, that is the only step needed to initiate the attack. Pop-up advertisements work the exact same ways. It is important to always be familiar with what you are clicking on while browsing the internet. Clicking on unfamiliar content can lead to various malware infecting your system. The malware executed can range from adware, spyware and multiple viruses including worms and trojans. Another situation that drive-by downloads can lead to is Fraudulent applications. The most common effect of these attacks is spyware. The main type of spyware implemented by attackers is keyloggers. This type of spyware allows for the infected users keystrokes to be monitored, which allows attackers access to things such as passwords, private messages and browsed webpages (Yoder, 2019).

Recent Examples of Drive-by Downloads Attacks

It is important to know that these attacks can happen to anyone from novice users to large corporations. In these next few examples, we will see how the attacks have affected a few. One recent example includes the Issaquah attack that took place in Issaquah, Washington in 2017. In this attack, the drive-by download attacked the IT infrastructure of the entire city. The attack was aimed towards the city's backup system (which was not kept up to date). The form of the attack was a crypto locker ransomware attack. The attack also disguised itself as a pdf document, which an employee on the infrastructure team opened to check on possible grant information for the team. Once opened, the ransomware spread to other documents across the backup system. After discovering the attack, the IT infrastructure teams decided to begin with the restoration process. Altogether, the restoration process took four days to fully complete. This was due to the size of the documents on the drives. Another factor in the long restoration process was the age of the

backup system. After this experience, the city of Issaquah, Washington upgraded their backup system (Kumar, 2017).

Another real-life example of a drive-by download attack is the Mac Flashback outbreak. This attack utilized a created toolkit that when implemented, allowed a backdoor that infected WordPress-based blogs. Not only were these blogs infected, but those trying to reach the infected blog sites were being sent to a malicious webpage that lead to a flashback trojan be downloaded. The flashback trojan disguised itself as a part of Apple's software. Once the trojan was installed, it continued to install more and more malware, rendering the system useless. This drive-by download attack was contained by security officials in April 2012, but not before it affected over 600,000 Mac systems (Drive-By Downloads, 2014).

Mitigation and Defense

There are many ways that users can defend against drive-by download attacks. Stopping these attacks is a general process that mainly involves users keeping their systems and end devices up to date. The biggest security threat when dealing with drive-by download attacks is openings or vulnerabilities within a system. One way to stop the attacks is to keep operating systems updated. As operating systems continue growing and evolving, it is important to know that they are being created and updated to defend against these many forms of malware. Another way to keep a system updated, is to regularly remove old browser plug-ins along with any unnecessary software. Just like operating systems, unused plug-ins and unnecessary software can leave open potential points of entries for attackers (Egele, 2009).

A second way to defend against drive-by downloads is to have an antivirus software on the system. It would also be beneficial to have an antispyware program employed as well since

spyware plays a key role in this type attack. It is important to know that having these programs employed will not completely mitigate drive-by download attacks, but it does defend against known and updated security threats which is a great start to the process.

The third way to defend the attacks with a drive-by download attack (dedicated) mitigation tool. There are multiple dedicated tools out there. One of the most used tools is BLADE (Block All Drive-by download Exploits). When executed, BLADE searches for malicious code when trying to access webpages (Figure 2). Once the string of code is found, an alarm is triggered in BLADE, which leads to the stoppage of that request to the webpage (Lu, 2010).

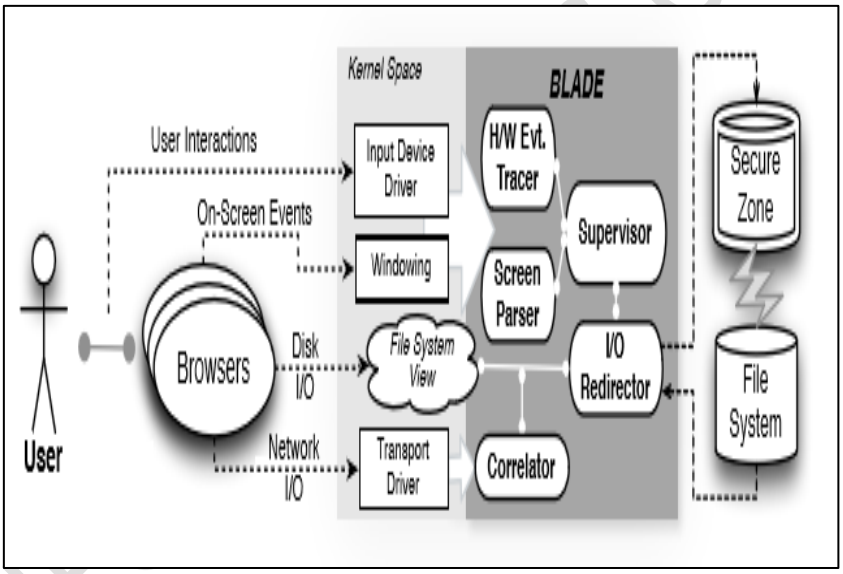

Figure 2: Overview of the BLADE system

Conclusion

Throughout the paper, we were able to learn about what drive-by downloads are and the many ways they can occur. We are also able to see that drive-by downloads can lead to serious damages with the real-life examples provided. To conclude the report, readers can see that these problems can be prevented by implementing a few common methods and continually learning and gaining information about the attacks.

Works Cited

Davis, G., Sarang, R., & Birdsong, T. (2017, September 15). What is a "Drive-By" Download? Retrieved April 3, 2019, from https://securingtomorrow.mcafee.com/consumer/family-safety/drive-by-download/

Drive-by Download (n.d.). In rsa.com. Retrieved March 25, 2019.

Drive-By Downloads: How They Attack and How to Defend Yourself. (2014, March 06). Retrieved April 13, 2019, from https://www.tomsguide.com/us/driveby-download,news-18329.html

Drive-By Downloads and How to Prevent Them. (2017, October 13). Retrieved April 2, 2019, from https://www.lastline.com/blog/drive-by-download/

*Egele, M., Kirda, E., & Kruegel, C. (2009). Mitigating Drive-By Download Attacks: Challenges and Open Problems. INetSec 2009 – Open Research Problems in Network Security IFIP Advances in Information and Communication Technology, 52-62. doi:10.1007/978-3-642-05437-2_5

Kumar, M. (2017, October 16). How A Drive-by Download Attack Locked Down Entire City for 4 Days. Retrieved April 4, 2019, from https://thehackernews.com/2017/10/drive-by-download-ransomware.html

*Lu, L., Yegneswaran, V., Porras, P., & Lee, W. (2010). Blade. Proceedings of the 17th ACM Conference on Computer and Communications Security - CCS 10. doi:10.1145/1866307.1866356

*Narvaez, J., Endicott-Popovsky, B., Seifert, C., Aval, C., & Frincke, D. A. (2010). Drive-by-downloads. Paper presented at the 1-10. doi:10.1109/HICSS.2010.160

Yoder, S. (2019, January 10). Different Types of Spyware. Retrieved April 3, 2019, from https://itstillworks.com/different-types-spyware-6457947.html