Republic of the Philippines
NATIONAL POLICE COMMISSION
PHILIPPINE NATIONAL POLICE
ANTI-CYBERCRIME GROUP
Camp BGen Rafael T Crame, Quezon City

ACG-CYBER SECURITY BULLETIN NR 169

ACG-CSB 072219169

Reference Number ACG-CSB 072219169

What is Drive-By Download Attack?

The following information was obtained from different cyber security sources for notification to all parties concerned pursuant to the mandate of the Philippine National Police Anti-Cybercrime Group (PNP ACG) and classified as “Restricted” pursuant to the PNP Regulation 200-012 on Document Security and Impact Rating as high based on PNP Information Communication Technology (ICT) Security Manual s.2010-01 p. 22 and p.129.

SUMMARY

A drive-by download refers to the unintentional download of malicious code onto a computer or mobile device that exposes users to different types of threats. Cybercriminals make use of drive-by downloads to steal and collect personal information, inject banking Trojans, or introduce exploit kits or other malware to endpoints, among many others.

What sets this type of attack apart from others is that users need not click on anything to initiate the download. Simply accessing or browsing a website can activate the download.

The malicious code is designed to download malicious files onto the victim’s PC without the user being aware that anything untoward has happened. A drive-by download abuses insecure, vulnerable, or outdated apps, browsers, or even operating systems.

Drive-by-download malware often uses small pieces of code designed to slip past simple defenses and go largely unnoticed. The code doesn't need to be highly complex because it mainly has one job which is to contact another computer to introduce the rest of the code it needs to access a mobile device or computer.

Drive-by downloads is a common technique used by attackers to silently install malware on a victim’s computer. Once a target website has been weaponized with some form of exploit typically browser or plugin exploits, hidden iframes, and JavaScript, among other techniques, the attacker may lure or wait for their target to browse to the web page. The compromised page will typically look completely normal to the end user, while the exploit executes and installs malware on the victim’s computer silently in the background. Once the malware makes its way onto the target computer, the attacker can act on their objectives

Oftentimes the malicious code is distributed by compromised websites. Hackers make use of an exploit kit. These kits contain software designed to run on web servers and identify software vulnerabilities on machines and web browsers to determine which systems are ripe for the plucking. The software may seem innocuous, but it is contained on sites corrupted by malware. In fact, one of the greatest dangers is the ease of attracting visitors to sites that seems innocent.

The growing complexity of internet browsers also contributes to the increase in drive-by download attacks. As the number of plug-ins, add-ons and browser versions proliferate, there are more weaknesses for cybercriminals to exploit.

In lieu, every individual must be cautious in visiting web pages with malicious code on it. This would disallow the attacker to compromise through system infection. It is best to install security software with warning signals for the detection of malicious software.

RECOMMENDATION

The public are advised to follow these tips in order to understand the risks and prevent being victimized by Drive-by download attack, to wit:

- Update your software quickly and constantly;
- Remove unnecessary software and plug-ins;
- Stop using a privileged account for day-to-day work;
- Use a reliable antivirus with a built-in URL checker;
- Disable Java and JavaScript; and
- Install an ad blocker.

For additional information, please refer to the following websites:

- https://www.kaspersky.com/resource-center/definitions/drive-by-download
- https://www.lastline.com/blog/drive-by-download/
- https://heimdalsecurity.com/blog/how-drive-by-download-attacks-work/
- https://www.thesecuritybuddy.com/malware-prevention/what-is-drive-by-download-and-how-to-prevent-it/

POINT OF CONTACT

Please contact PMAJ ANGELICA STARLIGHT L. RIVERA, Asst. Chief, ARMD thru e-mail address acg@pnp.gov.ph or contact us on telephone number (632) 7230401 local 3562 for any inquiries related to this CYBER SECURITY BULLETIN.