

Minnie Zhu  
APCSP  
Mr. Ta  
19 03, 2019

The name of the attack is drive-by attack. It is a malware delivery technique that usually appears when people click on insecure web sites and plant a malicious script into HTTP or PHP code on one of the pages, which would install malware directly to the website visitor. It is different than other cyber attack as drive-by attack would automatically download the malware without click something on the website. When people enter the website, their serve would be invaded when there is no antivirus application. People can detect it by examining contents of HTML pages to identify malicious websites, and using characteristics of web servers to determine whether the page contains malicious content or not. It does not target a certain company or individual. In the early days, a cyber drive - by attack wasn't much of a threat, mainly to gain free Wi - Fi access. Hackers would drive through a city's streets, locate a Wi - Fi signal, and if the signal were unsafe, they would hack into Internet siphoning. Cyber criminals are now using the same practice, but more sophisticatedly. They often target routers that are badly secured and find out the router manufacturer first. Once that information has been obtained, they will then tap and listen to the traffic and find ways to compromise the password, which will eventually give them access to a computer or phone. The next stage of an attack with all systems weakened. According to the article, there is no solutions but there are ways to prevent it. It has been implented in some legitimate websites that appeal people to click into the websites. However, when they click the link to the website, the malware would be automatiacally download. It would exploiting API calls for various plugins and also involves writing shellcode

to memory. Then exploiting vulnerabilities in the web browser or plugin to divert the control flow of the program to the shell code. Virtually, It is applicable to defend yourself from drive-by attack. People can install antivirus software on all your devices and remember to update your software when there is a new one released.