Mayur Suresh

CSC 301

10 - -21

Article Review #3

Article Review of “New Attack Tricks Software”

Out of all the available article for this section this caught my eye because of the title “New Attack Software”. The topic of security and the different types of way a system/software can be compromised has always fascinated me.

The Article starts of by explaining what a basic antivirus software is, its basic job is to scan incoming code and spot unique code signatures which are akin to which are found in malicious viruses. Then it blocks the access to the code. But just like how technology and software are improving so are hackers and their code. This is much easier with websites where its main purpose is user input so it is much easier for it be compromised. ‘

The article goes on and introduces dynamic code obfuscation (DCO) which is a new way to use browser vulnerabilities by hiding in JavaScript. Detecting DCO is more difficult than the alternative because it uses polymorphism, and would need “thousand signatures for thousands different executables.” JavaScript plays a key factor in DCO due to this use in web sites and the easy access to its JavaScript code in “View Access” making it easier to add DCOs.

The article then goes onto to talk about how victims are formed. Hackers use spam or phishing through e-mails with links to virus infested sites. URLs are often disguised as trustworthy or popular sites to let the users drop their guard or lure them. The article goes into another trick hackers use classes iFrame which will embed HTML documents inside one another which can only be viewed with the source code.

The article now draws into the details of what a DCO attack is. DCO can combine many things and disguise itself like a Trojan horse or other types of malwares. DCO take advantage of obfuscation by taking many forms like random letters, numbers, symbols etc.

The article goes onto talk about how this was developed further. Unlike a normal polymorphic virus which make an alternative code, DCOs change the code itself. DCO works very well against antivirus due to this. Then the article talks about how we are not just standing around and waiting for this to take place and place some contingencies. Like the research done by Symantec in vivo block where it identifies the browser holes before vendors releasing a patch.

Next the article talks about DCO’s behavior. As stated DCO is very hard to be detected by antiviruses, so in order to detect malicious files there are behavioral techniques to check its actions. So what this means is that in order to even start removing DCOs you need to first locate it and then work on removing them.

Next the article talks about other approaches. Like with a web application that performs a static analysis of the DCO code and find patterns behind the obfuscation files. It goes to on to talk about how the previously failed pattern finder with antivirus can be used with the subroutine that can return the original DCO file.

As the article concludes there is a warning that DCO attacks will only increase and gives examples of real-life situations where this has already become a problem which need to in depth approach in solving them.