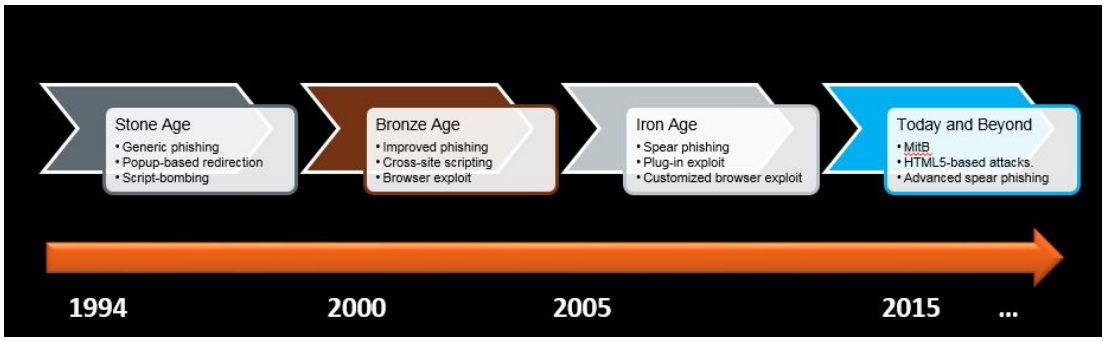
CS 373 Summer 2019

Week 7 Write Up

Kirsten Wollam

Web Security

In one way or another 95% of all malware is delivered through the internet. The technology moves extremely fast, and the malware has evolved over time as well. The internet is made up of many layers that can be attacked. Content, Search Engines, Browsers, The World Wide Web, Networks, and the computers connected to them all offer unique attack vectors. HTTP and HTML play a large role, and these days JavaScrit plays a role across the layers as well.



Web Security Slide 11

As with all malware, The user is the weak point when it comes to malware. There are many ways to take advantage of the user to work evil deeds over the web. These often involve some extent of social engineering, getting the user to do something willingly that they normally would not. Sometimes these are based on exploiting the fact that people are lazy and impatient, but the can also be cleverly disguised.

Phishing is a technique that is used across many mediums, but in Web security it usually involved creating a fake user interface that looks as close to the actual as possible. The url is usually made to look close enough to valid that it does not immediately raise suspicion. Most people have heard oh these sorts of attacks being used to gather banking and financial information but they are now being more widely used across all sorts sites especially social media.

Web Security Slide 19

Another tactic is Search Engine Poisoning, or SEO poisoning. All search engines base their results on algorithms. Malicious actors have found ways to work those algorithms to put their results at the top of the list. They trick you into clicking on the result that seems interesting and good and then take you to a malicious site or a site with links to malicious content. Google is fairly good at sifting these out, but other search engines are not as good. In most cases these sites are short lived, and often target specific events or pop culture happenings.

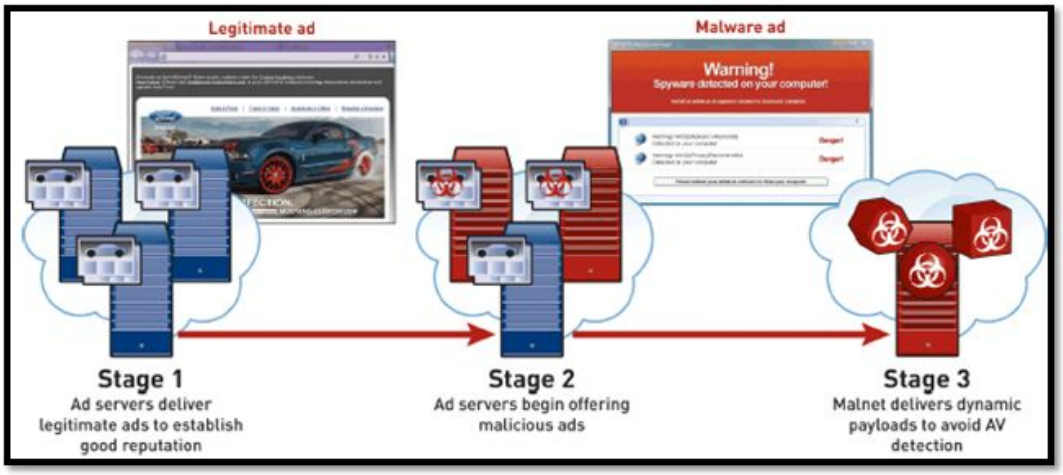
Fake updates and fake antivirus are also common on the internet. User gets a pop up stating that they need to update their software or that a virus or malware has been detected and believing this, install the malware themselves. They will often pay for the malware removal, but in reality there is nothing on the system and nothing is actually removed. In other cases clicking actually the pop up is what installs malware. These threats can look very convincing.

Web Security Slide 21

What you see on the internet is not always what you get. URL obfuscation can be as simple as a ‘rn’ instead of an m in a url. These days browsers are smart enough to protect users from attacks using odd combinations of unusual characters, but even with just the latin alphabet there are lots of possibilities.

Social media is also an easy gateway to deliver malware. It makes the delivery of malicious links extremely easy. Impersonating other people instills trust in targets, as does the perceived security of a large commonly used platform.

The main business of the internet these days seems to be advertising. Because it is such a big business and so common on sites attackers have found ways to use it to infiltrate users. They start with innocuous ads that make it past content filters. Then, once they are trusted, make a switch to deliver the malicious ads. This is a good way to get malicious content to folks as the ads often can show up on very high profile sites.



Web Security slide 24

Unfortunately there are not very many fool proof ways to prevent the user from harming themselves. Site certifications, reputation systems, safe url shorteners, and client/gateway antivirus can make a dent. At the end of the day though user education is the best way to prevent infection. This is a long road, but newer generations are getting smarter about attacks.

Browsers are also a point of potential injection. Browsers are easy to attack as they execute all sorts of content. Once a payload is downloaded or executed by the browser it can deliver any type of malware to the system.

One common browser based attack is the Man in the Middle attack. This attack involves intercepting and changing or redirecting network traffic in real time. This requires the attacker to use some method to set up the interception, like DNS poisoning or hacking the wifi. Once they have that they can easily deliver malicious content or read secure information from the traffic.

Another new evolution is the Man in the Browser attack. One major problem with malware is that it has to survive on the users system. Man in the browser gets around this by never installing anything on the system. Instead it relies on the fact that people keep their systems running and browsers open. It can implant in the browser and have constant access. This is dangerous, and hard to identify and combat once installed.

Another very common technique is SQL injection. This is very powerful because most websites are database driven and use get/post submissions to accept user input. If security is not tight it can be easy to manipulate via injecting code that will work to satisfy the conditions of the SQL statements. MySQL is easier to hack than some others because it will concat strings and integers together. People can also use error messages to gather information to help with hacking. Sometimes very specific, but can seem benign like the language of the error pointing to a particular language or OS the system is using. All of that information can be used to craft more sophisticated attacks.

web malware toolbox

With as dangerous as the internet is there are many tools that have been developed to help identify malicious sites or content.

alexa - This is a log of how prevalent a domain is. Extremely prevalent sites over a long time periods are likely safe. Malicious sites often show large spikes of traffic, but for a very short period of time before they die.

archive.org - can be used to go back and see malicious sites that have been reverted to clean or died

ipvoid - Checks across a large set of blacklists and provides other useful information on IPs. IPs are hard to come by so they can include clues. Sites with only 1 IP, no mail server, consumer IP can be indicators of suspicious sites.

check short URL - This service is to verify the actual url of a shortened url to ensure that it is what it claims to be.

In addition to simply gathering information, there are significant research tools that can be used to deeper dive.

phantomjs - automated tool to render and try to find malware on sites

JSunpack - can unpack the scripts to inspect them for malware

burp suite - can be a proxy, can follow links and map them (spidering), and log resource requests

webScarab - intercept and modify requests, similar to burp suite

URL classification plays a major role in anti malware efforts as it is used to create blacklists and algorithms to determine where threats might be.

Manual - actual inspection of a URL by a person. This is a very low volume technique but good for very important decisions and serious zero day attacks. It is important to record everything because you may only get 1 shot before the malware identifies a researcher.

Static - automated methods that scan and look for known malicious content. They do not execute any of the content. This method can scan very fast and get through high volume quickly which is necessary with the quantity of threats that come through each day.

low- interaction - automated tool that will execute content and note features. This will catch many remaining malicious sites but takes more time that static analysis.

high interaction - using sandboxes or virtual environments that will render and execute content with a real browser so it looks real. This has very low throughput, but can be a good way to get additional information on a threat and what it is doing.

graph-based tools - these are a recent development that allows known information to be extended to better understand the lay of the land. Once threats are identified, a map of how they are connected to other sites can be crafted through the use of large data sets. This information can paint a picture of what other sites may also be malicious.