Tu Lam

CS 373 (Defense Against the Dark Arts)

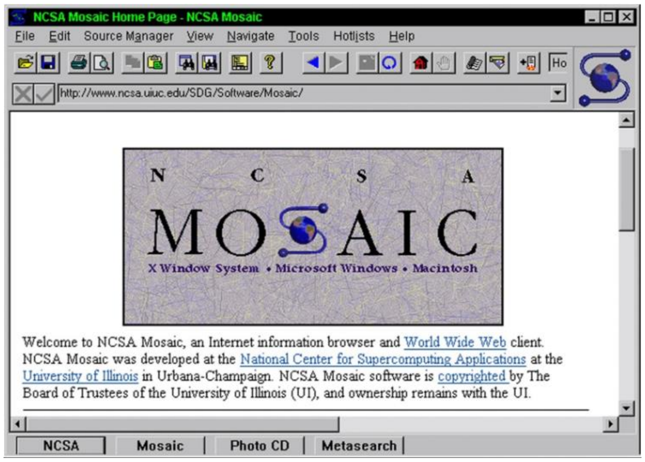
Dr. Bram Lewis

November 8th, 2021

Homework #7 Write-Up

Week #7 of the class have a special guest; their name was Cedric Cochin. They work for Intel as Intel Security at the McAfee Labs. Through this week lecture, we will be dealing with the ***web security*** basic on the topic of the ***web-centric attack vectors***. We will also dive into the topic of ***web research tools***, and the ***client-side threat defense***.

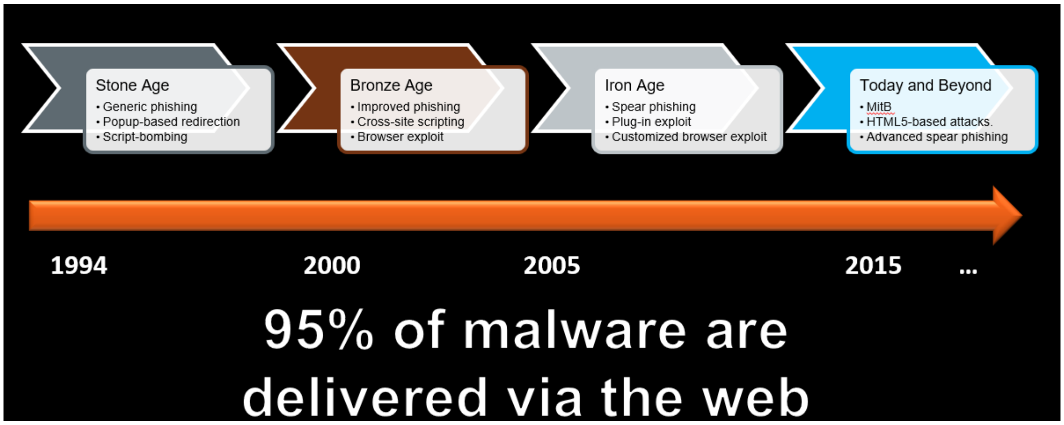
First, we dive into a reminder of the ***Oregon Computer Crime Law*** that Oregon have. This law breaks down into three main categories that section out mainly what is it computing criminal. The first one is around ***accessing network or computer purposely to do fraudulent***. Second is on the spectrum of ***purposely destroying, modify, or damaging software or data***. And lastly, just ***accessing something without anyone permission***. Both the first two clauses can cause somebody to be in a class C violation and they can end up spending five years in prison while the other clause only a year. Next, we move onto the web mechanism and how things are delivered. We learned that through the power of ***HTTP (Hypertext Transfer Protocol)***, that's how most of web data are transfer and do communication worldwide. Learning about the history of thing, the first world wide web was developed at the NCSA (National Center for Supercomputing Application) in University of Illinois called MOSAIC. Below will be a layout of how MOSAIC look like.


NCSA Mosaic Home Page - NCSA Mosaic
File
Edit
Source Manager
View
Navigate
Tools
Hotlists
Help
Ho
http://www.ncsa.uiuc.edu/SDG/Software/Mosaic/
N C S A
MOSAIC
X Window System • Microsoft Windows • Macintosh
NCSA
Mosaic
Photo CD
Metasearch

Welcome to NCSA Mosaic, an Internet information browser and World Wide Web client. NCSA Mosaic was developed at the National Center for Supercomputing Applications at the University of Illinois in Urbana-Champaign. NCSA Mosaic software is copyrighted by The Board of Trustees of the University of Illinois (UI), and ownership remains with the UI.

<u>Figure #1</u>: [**From Lecture**] *The layout of MOSAIC*

To the next topic, the evolution of web data has changed so much throughout the year as time goes on and more technology and web stuff becomes more prevalent. This would apply to the same thing as ***malware***. Most of the malware attack are ***95% attack base on the web*** and we have different categories of ages of how they are evolved. Below is an image showing their evolution through different ages.



Stone Age
- Generic phishing
- Popup-based redirection
- Script-bombing

Bronze Age
- Improved phishing
- Cross-site scripting
- Browser exploit

Iron Age
- Spear phishing
- Plug-in exploit
- Customized browser exploit

Today and Beyond
- MitB
- HTML5-based attacks.
- Advanced spear phishing

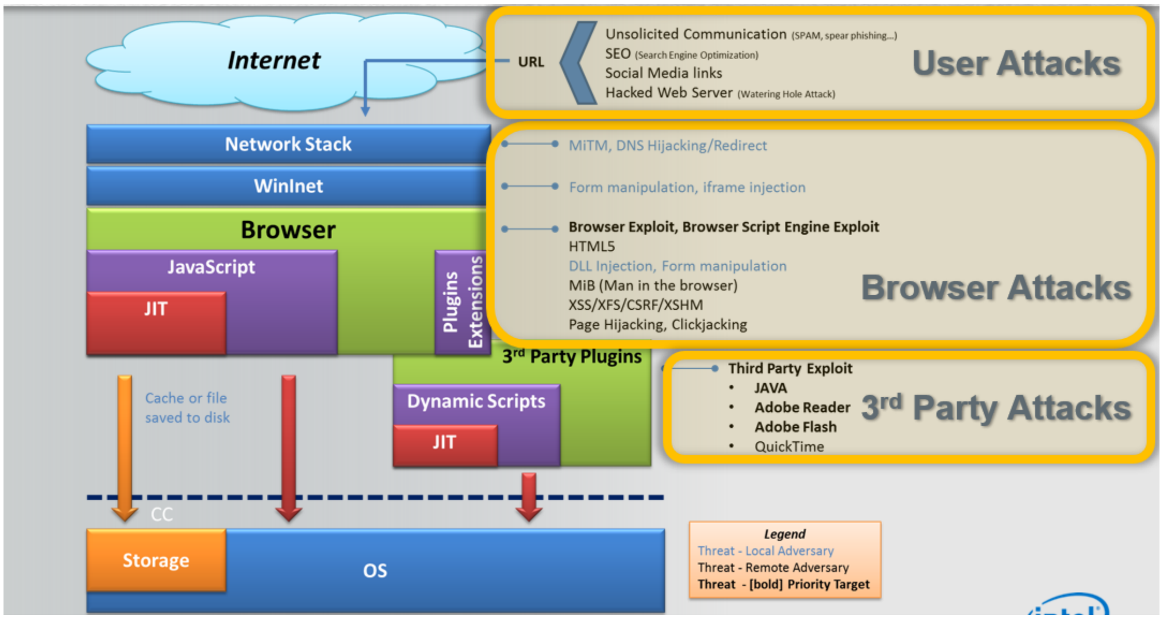
1994 2000 2005 2015 ...

95% of malware are delivered via the web

<u>*Figure #2*</u>: [**From Lecture**] *Displaying the evolution of Malware*

Tackling on the first topic of malware via web, we have ***user-level attack***. This deems as a really weak link to the user as the user can ***exploit their common trait*** such as lazy, impatient, clickaholic, or self-proclaimed omniscience. Through this, the malware can deploy the user with phishing, fake AV, forum link insert, malvertising, and more. Through ***phishing***, hacker can deploy fake URL that makes it look real to get user to enter in a portal site that is not secure. With ***fake AV***, they deploy innocent update through the OS interface, but make you pay or buy it to receive the update. And then there is ***malvertising***, where they use the deploy of popup message saying that your computer has been infected, but turn out it is not and you believe it is and called the number to get it fix. Turn out they are doing nothing to your computer and try to get money out of you. There are a few tools that we can use to prevent any of these user-level attack from happening.

Couple of tools that is recommended to us are URL/Domain Reputation Systems, Safe URL Shorteners, Content provider education, Client and Gateway AV/AM, and more. Now moving to the next topic of malware, we will take a dive in deeper from the outer surface into the middle surface of malware attack, that is the ***browser-level attack***. Below will show the layout of the browser attack and what kind of thing are found in that layer during the attack. As mention from the attack, these attacks derive from browser exploit via ***Chrome, Explorer, Script Engine***, and etc…

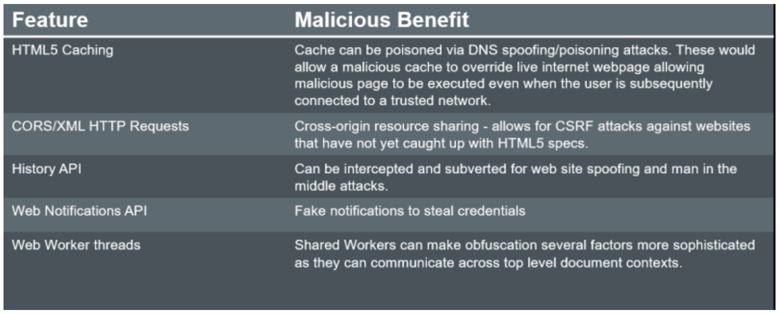


Internet
URL
Unsolicited Communication (SPAM, spear phishing…)
SEO (Search Engine Optimization)
Social Media links
Hacked Web Server (Watering Hole Attack)
User Attacks
Network Stack
WinInet
Browser
JavaScript
JIT
Plugins
Extensions
MiTM, DNS Hijacking/Redirect
Form manipulation, iframe injection
Browser Exploit, Browser Script Engine Exploit
HTML5
DLL Injection, Form manipulation
MiB (Man in the browser)
XSS/XFS/CSRF/XSHM
Page Hijacking, Clickjacking
Browser Attacks
3rd Party Plugins
Third Party Exploit
JAVA
Adobe Reader
Adobe Flash
QuickTime
3rd Party Attacks
Cache or file saved to disk
Dynamic Scripts
JIT
CC
Storage
OS
Legend
Threat - Local Adversary
Threat - Remote Adversary
Threat - [bold] Priority Target

Figure #3: [**From Lecture**] *Showing the browser-level attack*

The technology behind this exploit of browser is through the process of downloading the file off from the web and then they inject, renders, and executes maliciously crafted web content onto the browser. Then there are ***Man-in-the-middle-attack***, this attack is the hacker intercept the thing you requested through HTTP and modify it and attack it and resend it to you without notice. And there is more and more attack out there that the browser faces when it comes to the web security layout.

Then we have something called Cross-site Scripting (XSS), this is where we are injecting client-side script into other user's browsers by bypassing SOP. Through this method, we can run the executable directly and manipulate anything we want in the browsing. But with this, we have HTML security to help us protect this if it ever happens. ***HTML*** as involve so much now and below will be an image of ***HTML5*** and it benefit of using it.



Feature	Malicious Benefit
HTML5 Caching	Cache can be poisoned via DNS spoofing/poisoning attacks. These would allow a malicious cache to override live internet webpage allowing malicious page to be executed even when the user is subsequently connected to a trusted network.
CORS/XML HTTP Requests	Cross-origin resource sharing - allows for CSRF attacks against websites that have not yet caught up with HTML5 specs.
History API	Can be intercepted and subverted for web site spoofing and man in the middle attacks.
Web Notifications API	Fake notifications to steal credentials
Web Worker threads	Shared Workers can make obfuscation several factors more sophisticated as they can communicate across top level document contexts.

Figure #4: [**From Lecture**] *List of benefit from HTML5*

Lastly, moving onto tools that could help us out when it comes to ***web security***. Some of the tools that was recommended are ***IPVOID***, ***Archive.org***, ***Alexa, CheckShortURL***, and more. Through these tools, we can identify exploit and prevent any other attacks that could happen as hacker try to infiltrate into the web based through HTTP. But with a little practice using this tool, you can help identify and help other learn on how to prevent attack from happening in the future.

Throughout this week, we learn the backbone of the malware attack and how to identify these attack that are happening throughout the web. Web security is still evolving throughout the year and hacker are getting smarter bypassing the security system we setup. With this, it is smart to stay on current news and learn way to prevent yourself from being attack on the web.

References

1. Cochin, C. (2015, February). Web Security. Canvas. Retrieved November 8, 2021, from https://canvas.oregonstate.edu/courses/1877198/pages/module-7-learning-materials?module_item_id=21556819.