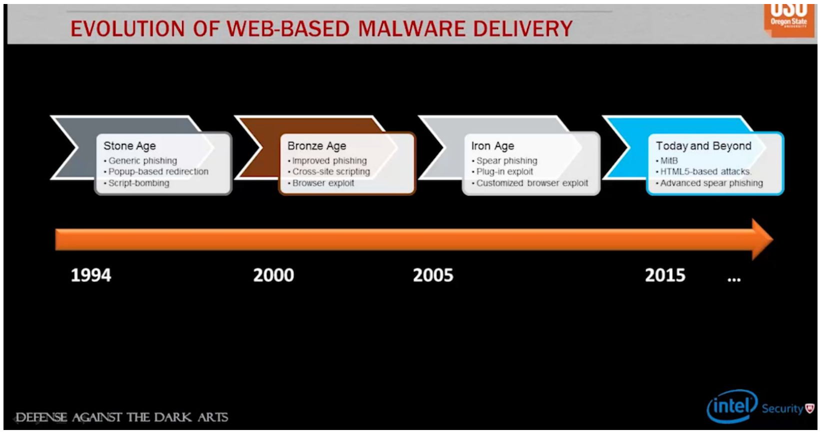
Nicolas Barraclough
11/15/2020
CS373 - Defense Against the Dark Arts

Week 7 Write-Up

This week, we learned about web security. We had a bit of a review of security threats and how malware is delivered. This is a game of cat and mouse for security professionals and attackers because as technology and practices evolve, so does malware and exploit techniques. The best security practices for the present may not (probably will not) be sufficient in the near future.



EVOLUTION OF WEB-BASED MALWARE DELIVERY

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

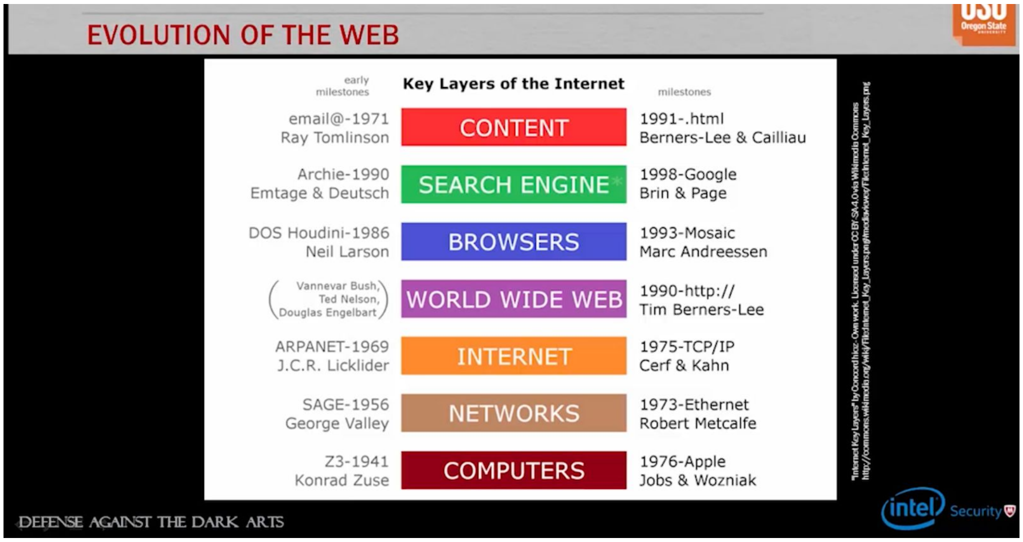
Today and Beyond
- MitB
- HTML5-based attacks
- Advanced spear phishing

One attack that I did not know prior to this week was Man-in-the-Browser or Boy-in-the-Browser. I’ll admit, sometimes I don’t close my browser and I had no idea that that action could be exploited. In my research about the attack, it is usually an attempt to steal financial information from when a user visits a banking website. Thankfully, I don’t do my banking on my laptop, so my leaving my browser open most likely had no real negative impact.

Another key for this week was user-level attacks. I’ve always heard that people are the weakest link for security and people are often the most effective form of vulnerability to be exploited. Social engineering is a popular form of hacking and arguably poses the maximum harm to a system. I’ve always been fascinated with the idea of social engineering and the ability for some people to carefully extract information that they otherwise would have no other means of obtaining.

Social engineering is not the only way that people can be exploited. If a person makes a mistake (as most successful phishing attacks occur because the person didn’t know they were accessing something malicious) by opening an attachment or link, that action could bypass any security that was put in place by security professionals. I’ve had phishing emails sent to my place of work by penetration testers and a coworker of mine clicked on a suspicious link. Luckily, the email was not sent by anyone malicious and our network was not immediately compromised.

I’ve heard of URL obfuscation, but I’ve never actually seen this form of attack in the real world. This is a scary subject to me because malicious black-hats are getting more and more sophisticated with their techniques. Nowadays, a website can look 99% real on the surface, but a false URL or a false-positively signed page can be the minor detail that can give a malicious site away. Knowing where and how to look for these details takes knowledge of said attacks, which most people lack.



EVOLUTION OF THE WEB

early milestones	Key Layers of the Internet	milestones
email@-1971 Ray Tomlinson	CONTENT	1991-.html Berners-Lee & Cailliau
Archie-1990 Emtage & Deutsch	SEARCH ENGINE	1998-Google Brin & Page
DOS Houdini-1986 Neil Larson	BROWSERS	1993-Mosaic Marc Andreessen
(Vannevar Bush, Ted Nelson, Douglas Engelbart)	WORLD WIDE WEB	1990-http:// Tim Berners-Lee
ARPANET-1969 J.C.R. Licklider	INTERNET	1975-TCP/IP Cerf & Kahn
SAGE-1956 George Valley	NETWORKS	1973-Ethernet Robert Metcalfe
Z3-1941 Konrad Zuse	COMPUTERS	1976-Apple Jobs & Wozniak

"Internet Key Layers" by Concord hioz - Own work. Licensed under CC BY-SA 4.0 via Wikimedia Commons
http://commons.wikimedia.org/wiki/File:Internet_Key_Layers.png#mediaviewer/File:Internet_Key_Layers.png

DEFENSE AGAINST THE DARK ARTS

Tools for this week:

- **archive.org** will show how a site has changed over time.
- **Site Dossier** can give general site info like IP, DNS servers, and inbound links.
- **Burp Suite** intercepts traffic from a remote website and can modify it
- **WebScarab** is similar to Burp Suite.
- OWASP’s **WebGoat** is a tool used for practicing penetration techniques.
- **Virus Total** (which we learned about in the earlier weeks) is an online web scanning tool that can compare to a list of recent malware. It provides classification so that the user can see the family of malware that the subject is most related to.