Jason Chow
W202, Summer 2022, Section 2
Homework # 8

Problem # 1: Web Security

1) Compromise of underlying system:

The 2017 ‘WannaCry’ attack is an example of malware that completely compromises Windows operating systems. The WannaCry malware propagated to target machines through a vulnerable SMB port exposed to the internet. Once installed, the malware would encrypt the core operating system, thus completely paralyzing the computer from its owner. To restore the computer, the malware displayed a method for payment (in the form of bitcoin) in exchange for a private key to decrypt their computer. If payment was not made, the operating system / computer was compromised and completely unusable to the owner.

2) Gateway to enabling attacks on client:

The 2019 ‘BlueKeep’ vulnerability is an example of a gateway that enables attacks on client. The vulnerability originated in Microsoft’s Remote Desktop Services (RDS), where it was discovered that an attacker could trigger a use-after-free weakness, spray shell-code into heap-memory, then force the RDS service to execute the shell-code on a victim’s computer (client). When the shell-code was executed, the victim’s RDS client provided a gateway that enabled attackers to remotely access the victim’s computer, with ‘System’ level privileges on the client. This allowed the attacker to harvest information on the client (i.e., sensitive files), install malicious software (i.e., crypto-mining software, ransomware, etc.) or completely destroy the operating system (i.e., delete system files). The vulnerability was patched by a March 2019 patch from Microsoft across the affected operating systems.

3) Disclosure of sensitive or private information:

In 2018, Marriott disclosed a massive data breach of its guest reservation system. Records included guest names, contact information, credit card numbers, passport ID, travel history and more for over ~500 million guests. While the publicly available details are limited, the high-level analysis shows a combination of factors leading to the 2018 compromise (and Marriott’s 7 other breaches, including the recent June 2022 breach). Those factors included a poor security culture, difficulty securing the reservation system, a lack of due diligence during Marriott’s acquisition of Starwood (original owner of guest reservation system, prior to its migration to Marriott’s guest reservation system), and a massive series of layoffs in the IT organization in order to reduce operational costs. It was believed a phishing campaign ultimately gave attackers a privileged credentials of an IT Administrator, which was later used by attackers to access the Starwood/Marriott network and guest reservation system.

4) Impersonation (of servers, or vice versa):

In 2017, Equifax setup https://www.equifaxsecurity2017.com in order to support victims of the earlier data breach. There were two massive issues with the new website: (1) Equifax was re-directing victims to a completely different site that did not look like the root Equifax website, thus enabling attackers to create their own look alike websites and (2), the website used a shared SSL certificate from vendor Cloudfare, thus creating a man-in-the-middle vulnerability if the private SSL key was ever exposed. Unfortunately, attackers seized the opportunity, and were able to re-direct victims to look alike website, such as https://securityequifax2017.com, which was created by a security professional to highlight the vulnerabilities above. The separate website Equifax setup to handle their data breach ultimately lead to other look alike websites (servers) that impersonated Equifax, and was able to further harvest sensitive information from victims.

5) Defacement:

In 2015, the Ashley Madison website was defaced by attackers, whom threatened to publicly release the names of all customers if the company did shut down immediately. Ashley Madison was a consumer-based website that enabled anonymous extramarital affairs with subscriptions a subscription fee. The company also charged customers an additional fee to delete customer records (a profit of ~$1.7 million per year) which the attackers were able to prove was not true. It was believed hackers breached Ashley Madison servers through a phishing campaign, and was able to harvest ~60 gigabytes worth of sensitive user information before defacing the website with its demands. The defacement triggered widespread panic as both the Ashley Madison company and all of its users were informed of the attack, leading to exposure of public figures and suicides of others.

References

1. WannaCry Attack: https://en.wikipedia.org/wiki/WannaCry_ransomware_attack
2. BlueKeep: https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2019-0708
3. Marriott Breach: https://news.marriott.com/news/2018/11/30/marriott-announces-starwood-guest-reservation-database-security-incident
4. Equifax Breach: https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html
5. Ashley Madison Breach: https://www.ftc.gov/legal-library/browse/cases-proceedings/152-3284-ashley-madison

Note: I worked alone on this homework assignment.