**Project 3 – Anime Con**

**I have always been interested in anime, and I always wanted to make a website about the different popular anime and Project 3 gave me the opportunity to do so. Since we had to use extras as well, I decided to make a website about selling different anime shows on DVD and using JavaScript to keep a sale deadline on 25th of December.**

**For the layout I tried to go for the simplistic vision of mine. One of the major things I liked about my website was the CSS transition of hovering that I used. I liked the fact that the description of the shows was shown once the user’s cursor was on the image of the show. Another thing which I very much liked about my website would be the desktop and mobile layout. I was happy with using grid which made the whole transition from desktop view to mobile view much easier and overall, in the three different views (Desktop, mobile, tablet) I really liked how it turned out to be. I also did like the CSS transition I used for the main anime synopsis, and I very much liked the fact that it showed another image as well when the first image grew.**

**Personally, I do agree that I could have done better if I had a little more time. One major thing I disliked was the size of the YouTube video. I know it was a small thing to change which I could have with a blink of an eye, but I didn’t, and the I couldn’t figure out the right text fonts for the website.**

**Overall, I was extremely happy with my overall performance in this Project. It took me a while to figure out the JavaScript code, but it was a success. I did pour all of my personal interest in this website, so I was extremely happy.**

**References**

* <https://myanimelist.net/>
* <https://www.reddit.com/r/anime/>
* Google Pictures for the posters of different anime.

Sahil Dayal

Introduction to Cybersecurity

Extra-Credit Assignment

**Question 1**

Spam, phishing, and malware information are caught through various sources, including the Symantec Probe Network, a framework of more than 5 million imitation records, Symantec.cloud, and various other Symantec security innovations. Skeptic, the Symantec.cloud restrictive heuristic innovation, can distinguish new and refined designated dangers before they arrive at clients' organizations. Over 8 billion email messages are handled every month, and more than 2 billion web requests are separated every day across server farms. Symantec moreover accumulates phishing data through a broad anti-fraud community of enterprises, security merchants, and more than 60 million customers. Symantec Endpoint Protection's center assurance against known and obscure dangers utilizes a layered way for defense. The extensive methodology secures the organization before, during, and after an attack. Symantec Endpoint Protection decreases your threat of exposure by giving tools to build your security advantage before any assault.

**Question 2**

1. A software update supply chain attack is embedding a section of corrupt software into a generally authentic programming bundle at its specific dissemination area; which could happen throughout creation at the product merchant, at a third-party stockpiling site, or via rerouting.
2. Software update supply chain attacks can be alluring to attackers due to several reasons.

* They permit them to invade very much secured associations by taking advantage of a generally trusted channel.
* The number of infections can become rapidly because of programmed updates.
* They can also permit isolated targets, like those in current conditions, to be focused on.
* The attack can make it harder for casualties to sort out how the attackers got onto their frameworks as trusted processes are abused.

1. There are several ways in which Trojans can be pushed onto a victim’s machine

* A victim is targeted by phishing or various kinds of social engineering, when they open a contaminated email message, or taps on a link to a malignant website.
* A victim views an infected site and come across a drive-by download appealing to being valuable encoding or is provoked to download a plugin to play a film or sound transfer.
* A victim visits an safe website corrupted with noxious code for example, malvertising or cross-site presetting.

1. The possible ways to defend against software update supply chain attacks involve:

* Keeping an exceptionally protected form and update framework by quickly applying security patches for OS and programs, executing required integrity controls to guarantee just trusted software runs, and requiring multifaceted validation for administrators.
* Construct secure programming updaters as a feature of the product improvement lifecycle by requiring SSL for update channels and carry out declaration pinning, signing everything, including configuration documents, scripts, XML records, and packages and checking for digital signatures, and not letting the product updater acknowledge conventional info and commands.
* Foster an occurrence reaction process for inventory network assaults through uncovering inventory network occurrences and advising clients with precise and convenient data.

**Question 3**

1. Living-off-the-land: It is an approach used by attackers, where they utilize trusted off-shelf and preinstalled system tools to direct their assaults. A significant number of these tools are pervasive and used by framework administrators for real work, making it harder for defenders to hinder admittance to this software and permit the attackers to hide in plain view. Living off the land assaults allude to an attacker utilizing what is accessible in the climate rather than bringing along an entire pack of custom programming and malware. The advantage for the assailant is that their exercises are more averse to hail antivirus applications since they are utilizing confided in programming.
2. Pass-the-hash: The assault is a procedure by which an attacker catches a secret key hash instead of the secret key characters and afterward basically passes it through for validation and possibly lateral admittance to other organized frameworks. Criminal programmers utilize pass the hash to extricate extra data and certifications after previously gaining access to a gadget. By laterally gaining access among gadgets and records, criminals could pass the hash to acquire the proper permits to ultimately raise the area advantages they have and gain contact to more compelling frameworks, like a manager account on the domain regulator. A large portion of the development executed during a pass the hash assault utilizes remote programming software, for example, malware.
3. Grayware: It is a kind of adware that has the sole reason for making publicizing cash off your information, and on certain occasions, criminal uses for your data. Grayware is ordinarily downloaded alongside an app you may have deliberately downloaded, and you simply didn't realize that it would likewise be tracking your information. Malware, obviously, is portrayed by its malevolent purpose. Contingent upon the sort of malware, a contamination might have devastating impacts that limits admittance to a portion of your records as a whole. Grayware, however, is a less-unsettling sort of digital danger that does not have pernicious goal. All things considered, it basically causes performance issues while conceivably making the ways for other security hazards.
4. Coin miner: It is a file that is utilized to mine cryptographic forms of money. Digital criminals began attempting to bring in cash this way because there was an enormous ascent in the worth of cryptographic cash arrangements, making this sort of digital crime very profitable. The malware accomplishes steadiness by adding one of the opensource excavators on startup without the casualty's agreement. Most refined coin excavators use clock settings or cap the CPU use to stay covert.
5. Lateral movement: Refers to the procedures that a cybercriminal utilizes to move further into an organization looking for delicate information and other high-esteem resources in the wake of acquiring initial access. After infiltrating the network, the criminal keeps progressing access by going through the compromised environment and getting increased privileges using various tools.
6. Cryptojacking: Refers to a sort of cybercrime that includes the unapproved utilization of individuals' gadgets like Personal Computers, cell phones, tablets, and servers by cyber attackers to dig for digital money. In the same way as other types of cybercrime, the rationale is a benefit; however, it is intended to remain hidden from the victim in question in contrast to different dangers. Criminal programmers have a way of getting a victim’s Personal Computer to mine digital money subtly. They stunt victims into piling crypto mining program on their Personal Computers. The trick is done via phishing-like tactics where victims get an authentic like emails that encourages them to click on a link. The link runs a program that installs the crypto mining script on the personal computer’s system. The program then, runs behind the scenes as the victim operates the computer.

**Question 4**

1. Formjacking is the utilization of malicious JavaScript code to take Visa subtleties and other data from payment structures on the checkout site pages of Web based business locales.
2. 1. Drop of cryptocurrency value in 2018

The value of stolen credit card details was more assured than the value of cryptocurrency

1. $2.2 million in one month, $26.4 million in one year
2. Magecart focused on outsider services to get its code onto designated sites. In the prominent break of Ticketmaster, for instance, Magecart compromised an outsider chatbot, which stacked noxious code into the web programs of guests to Ticketmaster's site, with the point of gathering clients' installment information. It works the same way as though you were to have your telephone tapped by the police; however, it is centered on site structures. In a form jacking situation, a customer might come to your site determined to join your bulletin, be that as it may, after composing in their email to your bulletin administration, it additionally gets shipped off to the criminal. Form jacking is so powerful because its whole aim is to remain stowed away. You may never become mindful that you have been a casualty of it.

**Question 5**

* Torrentlocker- Trojan
* Emotet- worm
* Necurs- botnet
* Petya- ransomware
* Dridex- botnet
* Monero- Trojan
* Phonywall- disk wiper
* Mirai- worm

**Question 6**

1. False. During 2018, the highlight ransomware circulation technique was email crusades. Ventures tend to be more impacted by email-based assaults since email remains the essential specialized instrument for associations.
2. False, most of the cryptojacking movement kept on starting from program-based coin miners. Program-based coin mining happens inside an internet browser and is executed utilizing prearranging dialects. On the off chance that a website page contains a coin mining script, the site page criminals will use guests' processing power to dig for digital currency however long the website page is open.
3. True, switches and associated cameras were the most tainted gadgets in 2018. Switches were the most designated gadgets given their openness from the web. They're too appealing as they provide a successful bouncing-off point for criminals.
4. True, Supply chain attacks, which exploit outsider administrations and programming to think twice about definite objectives, take many structures, counting seizing programming refreshes and infusing malignant code into actual programming. Designers kept on being taken advantage of as a cause of production network assaults, either through aggressors taking certifications for adaptation control instruments or by aggressors compromising outsider libraries that are incorporated into more significant programming projects.
5. True, in 2018, S3 containers arose as an Achilles heel for associations, with more than 70 million records taken or spilled because of poor configuration. The occurrence closely followed a spate of ransomware assaults against open information bases, for example, MongoDB in 2017, which saw aggressors wipe their substance and look for installment to reestablish them.
6. False, a more tricky danger to the cloud arose in 2018 with disclosing a few weaknesses in equipment chips. Emergency and Specter exploit weaknesses in an interaction known as speculative execution. Effective abuse gives admittance to memory areas that are regularly forbidden.
7. True, there was a reduction in ransomware movement during 2018, with the available number of ransomware infections on endpoints dropping by almost 20 percent.