Assignment 1

a**) Formjacking**

A formjacking attack is a attack for a cybercriminal to intercept your banking information direct from an e-commerce site.

According to the Symantec Internet Security Threat Report 2019, formjackers compromised 4,818 unique websites every month in 2018. Over the course of the year, Symantec blocked over 3.7 million form jacking attempts. Furthermore, over 1 million of those form jacking attempts came during the final two months of 2018 ramping up towards the November Black Friday weekend, and onward throughout the December Christmas shopping period.

Form jacking involves inserting malicious code into the website of an e-commerce provider. The malicious code steals payment information such as card details, names, and other personal information commonly used while shopping online. The stolen data is sent to a server for reuse or sale, the victim unaware that their payment information is compromised. All in all, it seems basic. It is far from it. One hacker used 22 lines of code to modify scripts running on the British Airways site. The attacker stole 380,000 credit card details, netting over £13 million in the process. Most of the time, the stolen credentials are sold online. There are numerous international and Russian-language carding forums with long listings of stolen credit card and other banking information. They're not the illicit, seedy type of site you might imagine. Some of the most popular carding sites present themselves as a professional outfit—perfect English, perfect grammar, customer services; everything you expect from a legitimate e-commerce site.

Given the extent of the form jacking problem on the Internet, it is perhaps only natural to ask: What can be done to prevent similar types of attacks in the future and to avoid becoming a victim of form jacking? According to Chris Olson, CEO of The Media Trust, there are really only two options available to e-commerce site operators to block threat actors. The first is to check that all web apps or additional code for a website has been developed with adequate attention to both security and privacy. This might include testing any new software updates in small test environments. The second option is to use automated website vulnerability services (or white hat hacker teams) to continually scan a website for potential weaknesses.

b) Cryptojacking

Cryptojacking is the unauthorized use of someone else's computer to mine cryptocurrency. Hackers do this by either getting the victim to click on a malicious link in an email that loads cryptomining code on the computer, or by infecting a website or online ad with JavaScript code that auto-executes once loaded in the victim's browser.

Hackers have two primary ways to get a victim's computer to secretly mine cryptocurrencies. One is to trick victims into loading cryptomining code onto their computers. This is done through phishing-like tactics: Victims receive a legitimate-looking email that encourages them to click on a link. The link runs code that places the cryptomining script on the computer. The script then runs in the background as the victim works.

The other method is to inject a script on a website or an ad that is delivered to multiple websites. Once victims visit the website or the infected ad pops up in their browsers, the script automatically executes. No code is stored on the victims' computers. Whichever method is used, the code runs complex mathematical problems on the victims' computers and sends the results to a server that the hacker controls. Hackers often will use both methods to maximize their return. "Attacks use old malware tricks to deliver more reliable and persistent software (to the victims' computers) as a fall back," says Vaystikh. For example, of 100 devices mining cryptocurrencies for a hacker, 10 percent might be generating income from code on the victims' machines, while 90 percent do so through their web browsers.

Unlike most other types of malware, cryptojacking scripts do no damage to computers or victims' data. They do steal CPU processing resources. For individual users, slower computer performance might be just an annoyance. Organization with many cryptojacked systems can incur real costs in terms of help desk and IT time spent tracking down performance issues and replacing components or systems in the hope of solving the problem.

As with any other malware infection, there are some signs we may be able to notice on own. Symptoms of cryptojacking high processor usage on your device, sluggish or unusually slow response times, overheating of your device. We can use high security softwares to block cryptographing. In addition to using security software and educating ourselves on cryptojacking, we can also install ad-blocking or anti-cryptomining extensions on web browsers for an extra layer of protection. As always, be sure to remain wary of phishing emails, unknown attachments, and dubious links.

c) Ransomware

Ransomware is a subset of malware in which the data on a victim's computer is locked, typically by encryption, and payment is demanded before the ransomed data is decrypted and access is returned to the victim. The motive for ransomware attacks is nearly always monetary, and unlike other types of attacks, the victim is usually notified that an exploit has occurred and is given instructions for how to recover from the attack. Payment is often demanded in a virtual currency, such as Bitcoin, so that the cybercriminal's identity is not known. Ransomware malware can be spread through malicious email attachments, infected software apps, infected external storage devices and compromised websites. Attacks have also used remote desktop protocol and other approaches that do not rely on any form of user interaction.

There are some types of rand Ransomware can come in many shapes and sizes. Some variants may be more harmful than others, but they all have one thing in common: a ransom. The five types of ransomware are:

- **Crypto malware:** This is a well-known form of ransomware and can cause a great deal of damage. One of the most familiar examples is the 2017 WannaCry ransomware attack, which targeted thousands of computers around the world and spread itself within corporate networks globally.
- **Lockers:** This kind of ransomware is known for infecting your operating system to completely lock you out of your computer, making it impossible to access any of your files or applications.
- **Scareware:** This is fake software that acts like an antivirus or a cleaning tool. Scareware often claims to have found issues on your computer, demanding money to resolve the issue. Some types

of scareware lock your computer, while others flood your screen with annoying alerts and pop-up messages.

- **Doxware**: Commonly referred to as leakware, doxware threatens to publish your stolen information online if you don’t pay the ransom. As more people store sensitive files and personal photos on their computers, it’s understandable that many individuals panic and pay the ransom when their files have been hijacked.
- **RaaS**: Otherwise known as “Ransomware as a Service,” RaaS is a type of malware hosted anonymously by a hacker. These criminals handle everything from distributing the ransomware and collecting payments to managing decryptors — software that restores data access — in exchange for their cut of the ransom.

To protect against ransomware attacks and other types of cyberextortion, experts urge users to back up computing devices regularly and update software, including antivirus software, regularly. End users should beware of clicking on links in emails from strangers or opening email attachments. Victims should do all they can to avoid paying ransoms.

While ransomware attacks may be nearly impossible to stop, there are important data protection measures individuals and organizations can take to ensure that damage is minimal and recovery is as quick as possible. Strategies include compartmentalizing authentication systems and domains, keeping up-to-date storage snapshots outside the primary storage pool and enforcing hard limits on who can access data and when access is permitted.

d) Living off the Land, and Supply Chain attacks

In the cyber security world, living off the land attacks describe those attacks that make use of tools already installed on targeted computers or attacks that run simple scripts and shellcode directly in memory. Attackers use these tactics because they hide in plain sight and create fewer new files (or no new files) on the hard disk. There is less chance of being detected by traditional security tools and, ultimately, less risk of an attack being blocked. Living off the land, non-malware, fileless, and memory-based attacks all describe the same tactic: *using existing software, allowed applications, and authorized protocols to carry out malicious activities.* Tools employed in living off the land attacks include operating system features, legitimate tools, and cloud services.

Supply chain attacks are an emerging kind of threat that target software developers and suppliers. The goal is to access source codes, build processes, or update mechanisms by infecting legitimate apps to distribute malware.

Attackers hunt for unsecure network protocols, unprotected server infrastructures, and unsafe coding practices. They break in, change source codes, and hide malware in build and update processes.Because software is built and released by trusted vendors, these apps and updates are signed and certified. In software supply chain attacks, vendors are likely unaware that their apps or updates are infected with malicious code when they’re released to the public. The malicious code then runs with the same trust and permissions as the app.

The number of potential victims is significant, given the popularity of some apps. A case occurred where a free file compression app was poisoned and deployed to customers in a country where it was the top utility app.

With the frequency and malignancy of living-off-the-land attacks likely to increase, We will need to add specific countermeasures to your defensive arsenal. We can do following things,

- Create a white list: Build a list of the tools that are approved for use, then remove all other tools. Anything used that is not on the white list is suspicious.
- Check log files: Suspicious thing we can check with log files.
- Limit PowerShell: PowerShell enables administrators to set limits in a number of ways.The the administrators can limit name spaces, the commands that PowerShell can execute, the time that users are on their machines, and the amount of downloading that is done. These limits can prevent hackers from doing their thing.
- Be alert: Fresh attacks are constantly being developed, mutating and emerging in new and dangerous ways. Attackers are seeking to split their activity into multiple processes, each of which might look innocent in itself. One tool might collect IP addresses of your users, then another tool will write to a file, while still another tool uses the addresses for attacks.
- Use deception tokens: Deploy small tokens, such as files or dummy user accounts. When users try to find passwords or access files, they will stumble upon your tokens, alerting you.

e) The rise of Targeted Attacks

A targeted attack refers to a type of threat in which threat actors actively pursue and compromise a target entity’s infrastructure while maintaining anonymity. These attackers have a certain level of expertise and have sufficient resources to conduct their schemes over a long-term period. They can adapt, adjust, or improve their attacks to counter their victim’s defenses.

Targeted attacks often employ similar methods found in traditional online threats such as malicious emails, compromised or malicious sites, exploits, and malware. Targeted attacks differ from traditional online threats in many ways. They are typically conducted as campaigns. APTs are often conducted in campaigns a series of failed and successful attempts over time to get deeper and deeper into a target’s network and are thus not isolated incidents.They usually target specific industries such as businesses, government agencies, or political groups. Attackers often have long-term goals in mind, with motives that include, but are not limited to, political gain, monetary profit, or business data theft.

This form of attack is where an individual or organisation is singled out, usually via email. Now most of us receive lots of spam emails and we simply delete them. But what if you get an email that purports to be from your bank/credit card company and to prove it they put the last 4 digits of your credit card number and your date of birth? This looks much more credible and we are more likely to click on any links in the email. Such a link may contain malware. This in turn would also be finely tuned to the target’s operating system and applications that run on it. They could get information of this kind by trawling social networks for titbits of information and/or even calling staff at the organisation. By creating a specific piece of malware just to target one organisation, it stays under the radar of security companies and law enforcement agencies.Attackers often customize, modify and improve their methods depending on the nature of their target sector and to circumvent any security measures implemented.

The US Senate and the International Monetary Fund (IMF) are just the latest in a growing line of high profile companies that have been subjected to a targeted cyberattack. Sony made unwelcome headline news when it had to shut down its PlayStation network after hackers were able to steal customer information, including addresses, dates of birth, etc. In that case over 70 million people's details were exposed. Other examples include Citibank, where personal information was stolen also; and Google, who disclosed that some Gmail accounts had been compromised.

f) Security Challenges of Cloud

Cloud security is a set of control-based technologies & policies adapted to stick to regulatory compliances, rules & protect data application and cloud technology infrastructure. Because of cloud's nature of sharing resources, cloud security gives particular concern to identity management, privacy & access control. So the data in the cloud should have to be stored in an encrypted form. With the increase in the number of organizations using cloud technology for a data operation, proper security and other potentially vulnerable areas became a priority for organizations contracting with cloud providers. Cloud computing security processes the security control in cloud & provides customer data security, privacy & compliance with necessary regulations. There are a lot of security challenges of cloud.

Data Protection

Implementing a cloud computing strategy means placing critical data in the hands of a third party, so ensuring the data remains secure both at rest (data residing on storage media) as well as when in transit is of paramount importance. Data needs to be encrypted at all times, with clearly defined roles when it comes to who will be managing the encryption keys. In most cases, the only way to truly ensure confidentiality of encrypted data that resides on a cloud provider's storage servers is for the client to own and manage the data encryption keys.

User Authentication

Data resting in the cloud needs to be accessible only by those authorized to do so, making it critical to both restrict and monitor who will be accessing the company's data through the cloud. In order to ensure the integrity of user authentication, companies need to be able to view data access logs and audit trails to verify that only authorized users are accessing the data. These access logs and audit trails additionally need to be secured and maintained for as long as the company needs or legal purposes require. As with all cloud computing security challenges, it's the responsibility of the customer to ensure that the cloud provider has taken all necessary security measures to protect the customer's data and the access to that data.

Insecure access points

One of the great benefits of the cloud is it can be accessed from anywhere and from any device. But, what if the interfaces and APIs users interact with aren't secure? Hackers can find these types of vulnerabilities and exploit them.

A behavioral web application firewall examines HTTP requests to a website to ensure it is legitimate traffic. This always-on device helps protect web applications from security breaches.

DDoS attacks

As more and more businesses and operations move to the cloud, cloud providers are becoming a bigger target for malicious attacks. Distributed denial of service (DDoS) attacks are more common than ever before. A DDoS attack is designed to overwhelm website servers so it can no longer respond to legitimate user requests. If a DDoS attack is successful, it renders a website useless for hours, or even days. This can result in a loss of revenue, customer trust and brand authority.

g) IoT Attacks

An object, in the Internet of Things, can be any natural or man-made object that can be assigned an IP address and provided with the ability to transfer data over a network. A recent study from Hewlett Packard concluded that 70 percent of IoT devices contain serious vulnerabilities.

Hackers and government agencies can use vulnerabilities in IoT devices to gain access to a network to monitor users and potentially gain access to any other connected devices for any number of purposes. According to many security experts, our dependence on Internet-connected technology is outpacing our ability to secure it.

The Internet of Things (IoT) continues to grow as a prime target for cybercriminals to exploit, according to a new threat report from security firm Symantec. The number of IoT attacks increased from about 6,000 in 2016 to 50,000 in 2017—a 600% rise in just one year, the report found.The majority of IoT attacks in 2017 21% originated from China, the report found, followed by the US (11%), Brazil (7%), and Russia (6%). More than half of the attempted attacks against IoT devices targeted the Telnet service, the report found.

Botnet is a very common cyber attack in the IoT. A botnet is a network of systems combined together with the purpose of remotely taking control and distributing malware. Controlled by botnet operators via Command-and-Control-Servers (C&C Server), they are used by criminals on a grand scale for many things: stealing private information, exploiting online-banking data, DDos-attacks or for spam and phishing emails. With the rise of the IoT, many objects and devices are in danger of, or are already being part of, so called thingbots a botnet that incorporates independent connected objects.

Botnets as well as thingbots consist of many different devices, all connected to each other – from computers, laptops, smartphones and tablets to now also those “smart” devices. These things have two main characteristics in common: they are internet enabled and they are able to transfer data automatically via a network. Anti-spam technology can spot pretty reliably if one machine sends thousands of similar emails, but it’s a lot harder to spot if those emails are being sent from various devices that are part of a botnet. They all have one goal: sending thousands of email requests to a target in hopes that the platform crashes while struggling to cope with the enormous amount of requests.

h) Election Interference 2018

With Election Day 2018 behind that, many are breathing a sigh of relief. Those following closely the prospect of widespread election interference are indicating that, despite fears of everything from the changing of votes to the spread of disinformation, the 2018 midterms saw relatively little by way of such interference, or at least less than occurred in 2016. It’s true that there have been no credible reports of actual vote changing of the type that could call into question the Election Day results, and that’s reassuring. But, all told, it’s unfortunately misguided to suggest that this campaign season and ultimately this election were free from election interference. That’s for at least three reasons.

First, consider the changes in Russian tactics for reaching American audiences. Social media platforms like Facebook and Twitter have stepped up their efforts to address election interference and in so doing disrupted, at least to some extent, Moscow's attempts to repeat its 2016 tactics like the building of false personas with large followings. But make no mistake: the Kremlin has adapted. With a broader array of sources for disinformation—from newly created websites to greater numbers of social media accounts, each with smaller followings—overall Russia appears to have engaged in more disruptions to democratic dialogue in 2018 than in 2016, not fewer.

Second, consider the maturation in Russia's approach compared to what it did in 2016. Coverage of 2018 election interference has tended to focus on whether particular candidates were favored by online influence operations, whether particular votes were changed, or whether disinformation about whether, when, and how to vote on Election Day was circulating. But, even if there was less of that than some expected, the democratic dialogue leading up to Election Day 2018 was still unquestionably infected by Russian influence.

Third, consider Russia's domestic counterparts in the dark arts of disinformation. America's experience in 2016 trained us to focus on foreign election interference, in particular. But it's not only foreigners who can spread disinformation online in a deliberate effort to distort our democracy. Americans, too, can mislead and distort their fellow citizens and they are increasingly doing so, taking a page from hostile foreign actors. In so doing, they're pitting Americans against each other on cooked-up issues like the so-called migrant caravan and the purported influence of billionaire George Soros, as powerfully documented this week in the Washington Post.