CO325:Assignment 1
E/15/211

(01) **Internet Security**

Introduction

Internet security is a branch of computer security specifically related to not only Internet, often involving browser security and the World Wide Web, but also network security as it applies to other applications or operating systems as a whole.Generally, Internet security encompasses browser security, the security of data entered through a Web form, and overall authentication and protection of data sent via Internet Protocol. Its objective is to establish rules and measures to use against attacks over the Internet. The Internet represents an insecure channel for exchanging information, which leads to a high risk of intrusionor fraud, such as phishing, online viruses, trojans, worms and more. Many methods are used to protect the transfer of data, including encryption and from-the-ground-up engineering. The current focus is on prevention as much as on real time protection against well known and new threats.

Objectives

Objectives of Internet security is to establish rules and measures to use against attacks over theInternet. The Internet represents an insecure channel for exchanging information, which leads to a high risk of intrusion or fraud, such as phishing, online viruses, trojans, worms and more.

Discussion

Internet security threats

Internet security threats impact the network, data security and other internet connected systems. Cyber criminals have evolved several techniques to threat privacy and integrity of bank accounts, businesses, and organizations.

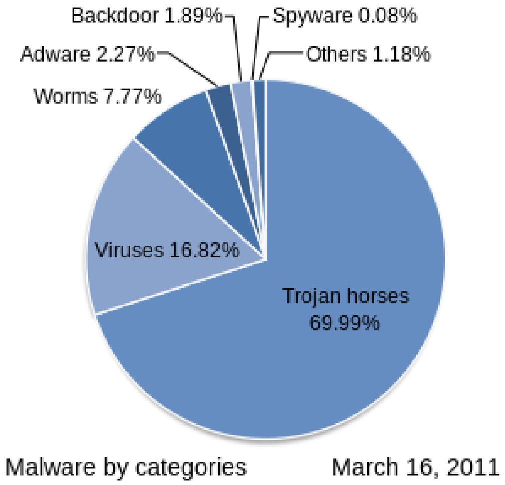
Malicious software

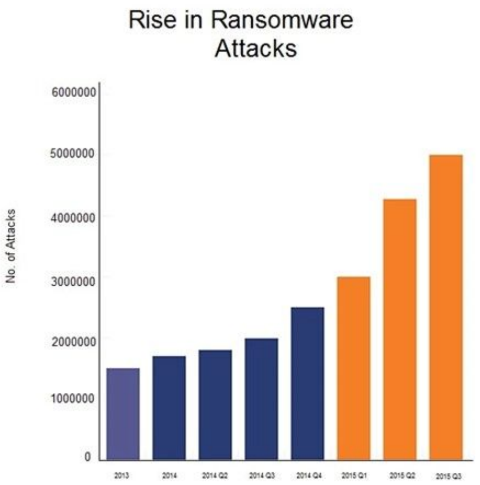
Malicious software (Malware) refers to any malicious program that causes harm to a computer system or network. Malicious Software attacks a computer or network in the form of viruses, worms, trojans, spyware, adware or rootkits.It is a program designed to gain access to computer systems, normally for the benefit of some third party, without the user’s permission. Malware includes computer viruses, worms, Trojan horses, ransomware, spyware and other malicious programs.

Types of Malware:

- **Viruses** –
  A Virus is a malicious executable code attached to another executable file. The virus spreads when an infected file is passed from system to system. Viruses can be harmless or they can modify or delete data. Opening a file can trigger a virus. Once a program virus is active, it will infect other programs on the computer.

- **Computer Worms** –
  Worms replicate themselves on the system, attaching themselves to different files and looking for pathways between computers, such as computer network that shares common file storage areas. Worms usually slow down networks. A virus needs a host program to run but worms can run by themselves. After a worm affects a host, it is able to spread very quickly over the network.





- **Spyware** –

  refers to programs that surreptitiously monitor activity on a computer system and report that information to others without the user's consent.

- **Trojan horse** –

  A Trojan horse is malware that carries out malicious operations under the appearance of a desired operation such as playing an online game. A Trojan horse varies from a virus because the Trojan binds itself to non-executable files, such as image files, audio files.

- **Ransomware** –

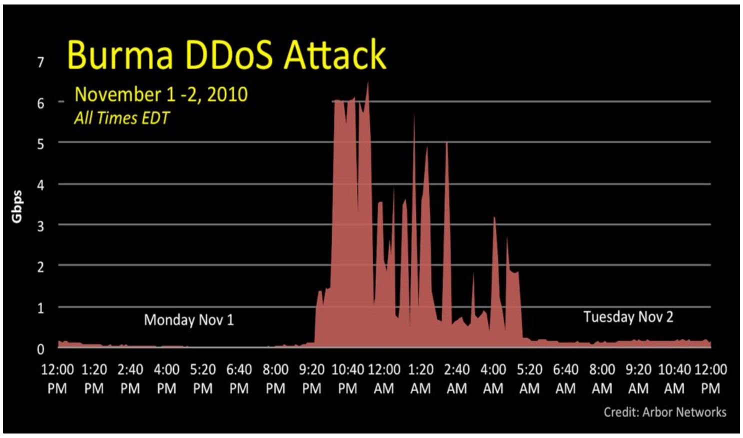
  Ransomware grasps a computer system or the data it contains until the victim makes a payment. Ransomware encrypts data in the computer with a key which is unknown to the user. The user has to pay a ransom (price) to the criminals to retrieve data. Once the amount is paid the victim can resume using his/her system.

- **Rootkits** –

  A rootkit modifies the OS to make a backdoor. Attackers then use the backdoor to access the computer distantly. Most rootkits take advantage of software vulnerabilities to modify system files.

- **Keyloggers** –

  Keylogger records everything the user types on his/her computer system to obtain passwords and other sensitive information and send them to the source of the keylogging program.



Denial-of-service attacks

A denial-of-service attack (DoS attack) is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. These are the attacks where the attackers (hackers) attempt to prevent legitimate users from accessing the service. In a DoS attack, the attacker usually sends excessive messages asking the network or server to authenticate requests that have invalid return addresses.

Phishing

Phishing is a method of trying to gather personal information using deceptive e-mails and websites.It is a cyber attack that uses disguised email as a weapon. The attacker uses phishing emails to distribute malicious links or attachments that can perform a variety of functions, including the extraction of login credentials or account information from victims.Victims are directed to fake web pages, which are dressed to look legitimate, via spoof emails, instant messenger/social media or other avenues.

Often tactics such as email spoofing are used to make emails appear to be from legitimate senders, or long complex subdomains hide the real website host.

Remedies for Internet Security

1.Computer access control

Network layer security-

Network layer security controls have been used frequently for securing communications, particularly over shared networks such as the Internet because they can provide protection for many applications at once without modifying them.TCP/IP protocols may be secured with cryptographic methods and security protocols.These protocols include Secure Sockets Layer (SSL), succeeded by Transport Layer Security (TLS) for web traffic, Pretty Good Privacy (PGP) for email, and IPsec for the network layer security.

Internet Protocol Security (IPsec)-

IPsec is designed to protect TCP/IP communication in a secure manner. It provides security and authentication at the IP layer by transforming data using encryption. The two protocols Authentication Header (AH) and ESP provide data integrity, data origin authentication, and anti-replay service.The set of security services provided at the IP layer includes access control, data origin integrity, protection against replays, and confidentiality. The IPsec security architecture is consist of security protocols for AH and ESP, security association for policy management and traffic processing, manual and automatic key management for the Internet key exchange (IKE) and algorithms for authentication and encryption

2.Authentication. Multi-factor authentication

A method of computer access control in which a user is granted access only after successfully presenting several separate pieces of evidence to an authentication mechanism.It has at least two of the following categories: knowledge, possession,and inherence . Internet resources, such as websites and email, may be secured using multi-factor authentication.

3.Authorization

Authorization is a security mechanism used to determine user/client privileges or access levels related to system resources, including computer programs, files, services, data and application features. Authorization is normally preceded by authentication for user identity verification.

4.Data-centric security

Data-centric security is an approach to security that emphasizes the security of the data itself rather than the security of networks, servers, or applications.Data-centric security also allows organizations to overcome the disconnect between IT security technology and the objectives of business strategy by relating security services directly to the data they implicitly protect; a relationship that is often obscured by the presentation of security as an end in itself.

5.Encryption

Network encryption is the process of encrypting or encoding data and messages transmitted or communicated over a computer network.In cryptography, encryption is the process of encoding a message or information in such a way that only authorized parties can access it and those who are not authorized cannot. Encryption does not itself prevent interference, but denies the intelligible content to a would-be interceptor. In an encryption scheme, the intended information or message, referred to as plaintext, is encrypted using an encryption algorithm a cipher generating ciphertext that can be read only if decrypted.

6.Firewall

A computer firewall controls access between networks. It generally consists of gateways and filters which vary from one firewall to another. Firewalls also screen network traffic and are able to block traffic that is dangerous. Firewalls act as the intermediate server between SMTP and Hypertext Transfer Protocol (HTTP) connections.Firewalls can help secure a network from both internal and external dangers.A firewall performs two major roles: Provides defense against external threats by refusing unauthorized connections to the router from potential attackers such as hackers. It also protects the network infrastructure from within. For that there are several types of firewalls for specific purposes. They are Packet filter firewall, stateful firewall, application-level firewall

Internet security products

- **Antivirus**

Antivirus software is a class of program designed to prevent, detect and remove malware infections on individual computing devices, networks and IT systems. Antivirus software, originally designed to detect and remove viruses from computers, can also protect against a wide variety

- **Password managers**

A password manager is a software application that is used to store and manage the passwordsthat a user has for various online accounts and security features. Password managers store the passwords in an encrypted format and provide secure access to all the password information with the help of a master password.

- **Security suites**

A collection of software utilities that protect a user's computer from viruses and other malware. Managed by a single control panel interface that displays all the functions, antivirus and firewall are typically the primary elements.

Conclusion

Internet security relies on specific resources and standards for protecting data that gets sent through the Internet. This includes various kinds of encryption such as Pretty Good Privacy (PGP). Other aspects of a secure Web setup includes firewalls, which block unwanted traffic, and anti-malware, anti-spyware and anti-virus programs that work from specific networks or devices to monitor Internet traffic for dangerous attachments.Internet security is generally becoming a top priority for both businesses and governments. Good Internet security protects financial details and much more of what is handled by a business or agency’s servers and network hardware. Insufficient Internet security can threaten to collapse an e-commerce business or any other operation where data gets routed over the Web.

References

(1)https://theconversation.com/us/topics/internet-security-9416

(2)https://www.comodo.com/home/internet-security/free-internet-security.php

(3)https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-executive-summary-en.pdf

(4)https://www.csoonline.com/article/2117843/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html

(5)https://enterprise.comodo.com/blog/what-is-malicious-software/

(02) The vicissitude of CyberCrime Threat Landscape: The past, present and the future

Cybercrime is any criminal activity that involves a computer, networked device or a network. While most cybercrimes are carried out in order to generate profit for the cyber criminals, some cyber crimes are carried out against computers or devices directly to damage or disable them, while others use computers or networks to spread malware, illegal information, images or other materials. Some cyber crimes do both, such as target computers to infect them with viruses, which are then spread to other machines and, sometimes, entire networks.Issues surrounding these types of crimes have become high-profile, particularly those surrounding hacking, copyright infringement, unwarranted mass-surveillance, sextortion, child pornography, and child grooming.A primary impact from cybercrime is financial, and cybercrime can include many different types of profit-driven criminal activity, including ransomware attacks, email and internet fraud and identity fraud, as well as attempts to steal financial account, credit card or other payment card information. Cybercriminals may target private personal information, as well as corporate data for theft and resale.

Cybercrime can begin wherever there is digital data, opportunity, and motive. Cybercriminals include everyone from the lone user engaged in cyberbullying to state-sponsored actors, like China's intelligence services. Cyber crimes generally do not occur in a vacuum; they are, in many ways, distributed in nature. That is, cyber criminals typically rely on other actors to complete the crime, whether it's the creator of malware using the dark web to sell code, the distributor of illegal pharmaceuticals using cryptocurrencybrokers to hold virtual money in escrow, or state threat actors relying on technology subcontractors to steal intellectual property.

Cybercriminals use a number of attack vectors to carry out their cyberattacks and are constantly seeking new methods and techniques for achieving their goals, while avoiding detection and arrest.Adversaries are taking malware to unprecedented levels of sophistication and impact. The growing number and variety of malware types and families perpetuate chaos in the attack landscape by undermining defenders' efforts to gain and hold ground on threats. **Distributed DoS attacks (DDoS) ,Infecting systems and networks with malware, Phishing, Credentials attacks** are common types of attacks cybercriminals have been known to use.

One of the most important developments in the attack landscape in 2017 was the evolution of ransomware. The advent of network-based ransomware worms eliminates the need for the human element in launching ransomware campaigns. And for some adversaries, the prize isn't ransom, but the destruction of systems and data. Ransomware attacks have been committed against a vast variety of organisations every year by financially motivated attackers for more than a decade. The ransomware attacker gains ownership of files and/or various devices and blocks the real owner from accessing them. To return the ownership the attacker demands a ransom in cryptocurrency . Ransomware attacks are nowadays evolving from stand-alone to cyber-adversary campaigns. This morphing is mostly due to the level of sophistication of attackers, often elevated by leaked or stolen classified tools developed by government agencies. The victims of these attacks not only suffer certain financial losses, but they also lose their credibility. Even though the ransomware landscape is changing, many sectors still suffer from these attacks.

For example, over than 85% of the malware targeting medical devices in 2018 was ransomware . Additionally, 973 out of a total of 30.362 security breach incidents (3,2%) in all sectors was due to ransomware. This keeps ransomware as a threat that cannot be ignored.And Ransomed medical devices becomes an ongoing threat now. As predicted in the past, this year more than 85% of all the malware that affected healthcare organizations was ransomware. Unfortunately, the healthcare sector provides an easy target to attackers due to the usual lack of integration between IT policies and the core hospital operations. By considering reports ransomware hit 15% of businesses in the top 10 industry sectors: education, IT/telecom, entertainment, financial services, construction, government, manufacturing, transport, healthcare and retail. In early 2018, a trend towards cryptojacking rather than ransomware attacks has been observed. In cryptojacking, the intruders invade a computer in a way similar to ransomware, but instead of demanding a ransom, they install malicious software to start cryptocurrency mining without the computer owner's noticing.

Distributed DoS attacks (DDoS) are often used to shut down systems and networks. This type of attack uses a network's own communications protocol against it by overwhelming its ability to respond to connection requests. DoS attacks are sometimes carried out simply for malicious reasons or as part of a cyber extortion scheme, but they may also be used to distract the victim organization from some other attack or exploit carried out at the same time.

It is the largest reflection-amplification attacks, still on the rise.As example, GitHub became a victim of a 1.35Tbps (126.9 million pps) amplified DDoS attack. The attack was originating from different autonomous systems misusing memcached services (UDP port 11211). Five days after that incident, on 5th of March 2018 Arbor networks announced214 a 1.7Tbps attack targeting a US service provider facilitating the same memcached technique. Interesting enough since the first incident on GitHub the number of vulnerable memcached servers was cited publicly as 17000 and only 500 were remained vulnerable by June 2018.

When observing DDoS attacks since past, Memcached (reflected) amplification attacks,Multi target DDoS, Cache Busting DDoS,Persistent DDoS Attacks, Encrypted Attacks are the most common DDoS attacks. Memcached (reflected) amplification attacks. A legitimate service which is developed for handling a distributed memory caching system (using UDP) can be easily exploited to reflect the traffic to target with an amplification factor of 50.000 times of the original request. In multi target DDoS. When the attackers are not seeing the desired impact on their target they tend to extend their impact to the wider network range to have a more distributed impact.This methodology was observed by facilitating multiple DDoS vectors (i.e. SYN floods, amplification and application layer) targeting the entire /24 subnet. In Cache Busting DDoS attack the malicious actor aims to bypass the application's caching capability by sending random (or not recognizable) GET requests to flood the application server with requests to handle. In Encrypted Attacks, the rise of using encrypted services and traffic (SSL) on the web has attracted different levels of DDoS attacks. This includes attacks on the application level (flood attacks, bruteforce etc.), network level and the protocol level (i.e. SSL renegotiation or downgrade) making it harder for defenders and toolsets to recognise malicious traffic from legitimate

According to Netscout , the maximum number of DDoS attacks observed during the first half of 2018 increased (174%) compared to the same time period in 2017234 . The frequency though decreased by 13%. Most of the attacks were focused on hit-run tactics and specifically during peak times to strike their targets with UDP, TCP (SYN) and ICMP floods being the top 3 vectors. The duration of these malicious attempts were mostly recorded as lasting less than 90 minutes and the longest to more than 6 days.   We can say that the overall trend of denial of service attacks in 2018 is INCREASING.

Infecting systems and networks with malware is used to damage the system or harm users by, for example, damaging the system, software or data stored on the system. Ransomware attacks are similar, but the malware acts by encrypting or shutting down victim systems until a ransom is paid. Notable observations include the shift from ransomware to cryptojacking, the blurred lines between cyber criminals and cyber espionage actors, the high effectiveness of fileless attack techniques, the decline of exploit kits resulting in increased difficulty of delivering malware as well as the growing mobile threat landscape.Fileless attack techniques are the new norm. Fileless malware techniques operate without placing malicious executables on the file system . Fileless attacks are divided into 4 major techniques malicious documents (e.g. Microsoft Office with malicious macros, PDF files containing malicious JavaScript and abuse of DDE) malicious scripts (e.g. PowerShell, VBScript, batch files and JavaScript) living-off-the-land techniques (e.g. WMI, LOLBins and LOLScripts) malicious code in memory (e.g. PowerSploit93, Doppelgänging). The mobile malware threats increase year-overyear and the continued use of older operating systems amplifies the problem. Major mobile threats include credential theft, mobile remote access trojans and SIM card abuse/hijacking (followed by adware and cryptomining , especially for Android devices).

Phishing campaigns are used to infiltrate corporate networks by sending fraudulent email to users in an organization, enticing them to download attachments or click on links that then spread viruses or malware to their systems and through their systems to their company's networks. Phishing is the preferred way of compromising organisations and it has been reported that 75% of EU's Member States disclosed cases of phishing . Phishing is so heavily leveraged that over 90% of malware infections and 72% of data breaches in organisations originate from phishing attacks.

In past Phishing attacks became more targeted. It is reported that while the traditional spam-related phishing still exists, the number of targeted phishing attacks continue to grow.The volumes of hacked and leaked personal data give the opportunity for phishers to conduct convincing and targeted phishing campaigns(eg:-targeted sextortion scams).When considering the distribution of this cyber-attack, attackers, shift from consumer to enterprise targets . While phishers mostly targeted consumers during the previous years, an evolution has been observed that malicious actors are focusing on enterprise targets. This trend also aligned with the fact that, email services (e.g. Microsoft) and online services (e.g. DocuSign and Dropbox) were the top phishing target (26%) for first time above financial institutions (21%).Then, steady growth in mobile phishing attacks.Phishing attacks on mobile devices have grown by an average of 85% year-over-year since 2011. Mobile devices give opportunities for cyber criminals to utilize more attack vectors instead of email phishing. . It has been observed that phishing via SMS, mobile messaging (WhatsApp, Facebook Messenger, etc.) and social media apps (e.g. Instagram) has grown significantly. More specifically, phishing of social media users has tripled during 2017 with phishers exploiting the inherent trust relationship between users and the social media platforms .

After that there is a rapid increase in phishing sites using HTTPS.It has been reported that one third of phishing web sites have been served via HTTPS during 2017 compared to 5% during 2016 . Business Email Compromise (BEC)C is a type of phishing attack (also known as whaling) targeting C-level executives and employees in finance or human resources aiming to steal money from their organisations. From October 2013 to May 2018, ca. 78.000 BEC attacks have been reported worldwide responsible for US $12,5 billion of reported losses. The majority of BEC attacks have targeted the real estate sector. During 2017, phishers used 28% more malicious attachments compared to malicious URLs within phishing emails. The most common malicious file types in phishing emails were Microsoft Office documents, archive files, JavaScript files, Visual Basic Scripts and PDFdocuments. The most common vulnerability exploited in phishing campaigns was CVE-2017-0199 , targeting Microsoft Office OLE features.Dropbox account phishing , Generic email credential phishing ,Google Drive phishing,Netflix phishing, Paypal phishing ,Microsoft Excel Online phishing,LinkedIn account phishing are some example phishing attack methods in today.We can say that the overall trend of phishing attacks in 2018 is INCREASING.

Credentials attacks, where the cybercriminal aims to steal or guess user IDs and passwords for the victim's systems or personal accounts, can be carried out through the use of brute force attacks by installing key sniffer software or by exploiting vulnerabilities in software or hardware that can expose the victim's credentials.

Cybercriminals may also attempt to hijack a website to change or delete content or to access or modify databases without authorization. For example, an attacker may use an SQL injection exploit to insert malicious code into a website, which can then be used to exploit vulnerabilities in the website's database, enabling a hacker to access and tamper with records or gain unauthorized access to data, such as customer passwords, credit card numbers, personally identifiable information (PII), trade secrets, intellectual property and other sensitive information. Cybercriminals often carry out their activities using malware and other types of software, but social engineering is often an important component for executing most types of cybercrime. Phishing email is an important component to many types of cybercrime, but especially so for targeted attacks, like business email compromise (BEC), in which the attacker attempts to impersonate, via email, a business owner in order to convince employees to pay out bogus invoices.

Social engineering still a critical launchpad for email attacks.Phishing and spear phishing are well-worn tactics for stealing users' credentials and other sensitive information, and that's because they are very effective. In fact, phishing and spear phishing emails were at the root of some of the biggest, headline-grabbing breaches in recent years. Two examples from 2017 include a widespread attack that targeted Gmail users and a hack of Irish energy systems.To gauge how prevalent phishing URLs and domains are on today's Internet, Cisco threat researchers examined data from sources that investigate potentially "phishy" emails submitted by users through community-based, anti-phishing threat intelligence.

Threat Landscape (ETL) provides an overview of threats, together with current and emerging trends. It is based on publicly available data and provides an independent view on observed threats, threat agents and threat trends.The ENISA (European Union Agency For Network and Information Security) Threat Landscape consists of a report summarizing cyber threats that have been accessed by collecting publicly available information. This report appears on a yearly basis. Moreover, every year thematic threat landscapes are developed.

We know that attackers are evolving and adapting their techniques at a faster pace than defenders. They are also weaponizing and field testing their exploits, evasion strategies, and skills so they can launch attacks of increasing magnitude. John Bruce says **"With cyber attacks becoming smarter and more relentless, business needs a three-part cyber-security defence: prevent, detect and respond"** From worms and viruses to data breaches, cyber attacks have evolved rapidly in the past 25 years – becoming increasingly sophisticated and tenacious. It's been a tremendous challenge for the cyber-security professionals, technology vendors, law enforcement – to keep up.

In the modern threat landscape, adversaries are adept at evading detection. They have more effective tools, like encryption, and more advanced and clever tactics, such as the abuse of legitimate Internet services, to conceal their activity and undermine traditional security technologies. And they are constantly evolving their tactics to keep their malware fresh and effective. Even threats known to the security community can take a long time to identify.

(03)

(a)Formjacking

What is formjacking?

Formjacking is a relatively new form of digital information theft caused by hacker attacks on commercial websites involved in banking, e-commerce and other activities that collect customers' personal information.It is a term that is used to describe the use of malicious JavaScript code to steal credit card details and other information from payment forms on the checkout web pages of e-commerce sites. Because of formjacking there is a major increase in attacks on online retailers.

As an example we can take that the symantec has blocked almost a quater of a million instances of attempted formjacking. Symantec has seen a major uptick in formjacking attacks recently, with publicly reported attacks on the websites of companies including Ticketmaster, British Airways, Feedify, and Newegg by a group called Magecart being the most notable examples.

How does formjacking work?

When a customer of an e-commerce site clicks “submit” or its equivalent after entering their details into a website’s payment form, malicious JavaScript code that has been injected there by the cyber criminals collects all entered information, such as payment card details and the user’s name and address. This information is then sent to the attacker’s servers. Attackers can then use this information to perform payment card fraud or sell these details to other criminals on the dark web.

By looking about the publicly reported attacks, Magecart(a group who used this attacks) is targeting large e-commerce businesses like Ticketmaster and British Airways which is the attack group behind the recent formjacking attacks.The group injects web-based card skimmers onto websites to steal payment card data and other sensitive information from online payment forms.This shows that it is using formjacking and supply chain compromise to steal payment card data.

How to protect from formjacking?

Victims may not realize they are victims of formjacking, because in generally their websites continue to operate as normal, and attackers like Magecart are sophisticated and stealthy and take steps to avoid detection.Protection is devided into two categories network-based protection and file-based protection.

Website owners should also be aware of the dangers of software supply chain attacks, as these have been used as the infection vector in some of these formjacking attacks. There are some steps that website owners can take:

- Test new updates, even seemingly legitimate ones, in small test environments or sandboxes first, to detect any suspicious behavior.
- Behavior monitoring of all activity on a system can also help identify any unwanted patterns and allow you to block a suspicious application before any damage can be done.

Producers of software packages should ensure that they are able to detect unwanted changes in the software update process and on their website.And aslo website owners can use content security policies with Subresource Integrity tags (SRI) to lock down any integrated third-party script.

(b)Cryptojacking

What is Cryptojacking?

Cryptojacking (malicious cryptomining) is defined as the secret use of your computing device to mine cryptocurrency.**It** used to be confined to the victim unknowingly installing a program that secretly mines cryptocurrency.

Cryptojacking attack is an emerging form of malware that hides on your device and steals its computing resources in order to mine for valuable online currencies like Bitcoin. It's a burgeoning menace that can take over web browsers, as well as compromise all kinds of devices, from desktops and laptops, to smart phones and even network servers.In-browser cryptojacking doesn't need a program to be installed and t is caused to happen in-browser cryptojacking. This theft of your computing resources slows down other processes, increases your electricity bills, and shortens the life of your device. Depending on how subtle the attack is, you may notice certain red flags. If your PC or Mac slows down or uses its cooling fan more than normal, you may have reason to suspect cryptojacking.

How does cryptojacking work?

Cryptojackers have more than one way to enslave your computer. One method works like classic malware. You click on a malicious link in an email and it loads cryptomining code directly onto your computer. Once your computer is infected, the cryptojacker starts working around the clock to mine cryptocurrency while staying hidden in the background. Because it resides on your PC, it's local—a persistent threat that has infected the computer itself.

An alternative cryptojacking approach is sometimes called drive-by cryptomining. Similar to malicious advertising exploits, the scheme involves embedding a piece of JavaScript code into a Web page. After that, it performs cryptocurrency mining on user machines that visit the page. And also drive-by cryptomining can even infect the Android mobile device.

How user can protect from cryptojacking?

Whether you've been cryptojacked locally on your system, or through the browser, it can be difficult to manually detect the intrusion after the fact. Likewise, finding the origin of the high CPU usage can be difficult as the processes might be hiding themselves. As a result of the cryptojacking, when your computer is running at maximum capacity, it will run ultra slow, and therefore be harder to troubleshoot. Therefore with all other malware precautions, it's much better to install security before the computer become a victim.One obvious option is to block JavaScript in the browser that you use to surf the web. It interrupts the drive-by cryptojacking.Whether attackers try to use malware, a browser-based drive-by download, or a Trojan, you're protected against cryptojacking.

(c)Ransomware

What is Ransomware?

Ransomware is a type of malicious software, or malware, designed to deny access to a computer system or data until a ransom is paid. It typically spreads through malicious email attachments or by unknowingly visiting an infected software apps ,external storage devices and websites.**It** can be devastating to an individual or an organization.There are three main types of ransomware that attacker is used. **Scareware**, **Screen lockers and Encrypting ransomware are those.**

How can ransomware happen?

It is like a virus.There are several different ways that ransomware can infect to the computer. One of the most common method is **malicious spam**, or malspam, which is unsolicited email that is used to deliver malware. The email might include booby-trapped attachments, such as PDFs or Word documents. It might also contain links to malicious websites.Malspam uses social engineering in order to trick people into opening attachments or clicking on links by appearing as legitimate.Cybercriminals also use social engineering in other types of ransomware attacks,like posing as the FBI in order to scare users into paying them a sum of money to unlock their files.

Another method is **Malvertising.**(Malicious advertising) It uses the online advertising to distribute malware with little to no user interaction required. While browsing the web users can be directed to criminal servers without ever clicking on an advertisement.

How to protect from ransomware?

According to security experts the best way to protect from ransomware is to prevent it from happening in the first place.To protect against ransomware attacks users can 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.

If the user is already a victim of ransomware,

User can check and see if there is a decryptor. In some rare cases user may be able to decrypt their data without paying, but ransomware threats evolve constantly with the aim of making it harder and harder to decrypt their files.User can avoiding from paying the ransom.(Don’t pay the ransom) Cybercriminals don’t have scruples and there’s no guarantee you’ll get your files back. Moreover, by paying the ransom you’re showing cybercriminals that ransomware attacks work.

How can user prevent from becoming a victim of mobile ransomware?

Mobile ransomware is malware that holds a victim’s data hostage, afflicting mobile devices ,commonly smartphones.Mobile device users should also have their data backed up in a different location in the case their device is inflicted.Following are some methods to avoid becoming a victim of mobile ransomware,

- Do not download apps using third-party app stores
- Keep mobile devices and mobile apps up to date
- Do not click on links that appear in spam emails or in text messages from unknown sources.

(d)Living off the Land, and Supply Chain attacks

Supply chain and so-called living off the land attacks (scorning custom malware in favor of publicly available hacking tools and software already installed on targeted computers) spiked nearly 80 percent last year. Living off the Land techniques allow attackers to “maintain a low profile and hide their activity in a mass of legitimate processes,” Symantec said. Living off the Land is increased again in popularity. It is Simple, but effective Consider malicious PowerShell scripts, which increased 1,000 percent last year, by Symantec’s measure: The security specialist blocks 115,000 of them each month but said that’s less than one percent of overall PowerShell usage.

Living off attacks

"Living off the land" (LotL) style of attacks has made the malicious use of PowerShell a "staple" for cybercrimes, showcased by a 1,000% uptick of blocked malicious PowerShell scripts on the endpoint in 2018, according to **Symantec's Internet Security Threat Report**.Living off the land tactics are increasingly being adopted by cyber criminals and are used in almost every targeted attack. Attackers use these tactics because they hide in plain sight and create fewer new files (or no new files) on the hard disk. There are four main categories in Living off the land.They are,

(1)Dual-use tools, such as PsExec, which are used by the attacker
(2)Memory only threats, such as the Code Red worm
(3)Fileless persistence, such as VBS in the registry
(4)Non-PE file attacks, such as Office documents with macros or scripts

In considering Battling Living Off the Land Attacks,for users, thwarting living off the land attacks means following standard guidance like delete any suspicious-looking emails, especially if they contain links or attachments. Attachments advising you to enable macros should be avoided unless you are absolutely sure the email is from a trusted source.

Supply chain attacks

Supply chain attacks, where attackers can compromise a company through its use of third-party services, increased nearly 80% in 2018. Attackers exploit developers by hacking third-party libraries "that are integrated into larger software projects," according to Symantec. It occurs when someone infiltrates your system through an outside partner or provider with access to your systems and data.

How to prevent from supply chain attacks?

Defining your company's security requirements and having a cyber-risk management program to evaluate third-party services can reduce the risk of attacks on supply chain software.Increasingly, hackers are using more sophisticated methods to attack companies' supply chain management software, ultimately disrupting operations and wreaking havoc on their networks.

Although there are steps organizations can take to minimize the damage caused by supply chain attacks, as well as to shore up defenses after attacks, the smartest option is to prevent these breaches from ever happening.

(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.Targeted Attacks remain undetected for as long as possible, move lateral to many systems. The number of attack groups using malware such as spear-phishing, custom designed to destroy and disrupt business operations can be considered as targeted attacks.

The number of targeted attacks has dramatically increased. Unlike largely indiscriminate attacks that focus on stealing credit card and banking information associated with cybercrime, targeted attacks noticeably differ and are better characterized as cyber espionage. Highly targeted attacks are computer intrusions threat actors' stage in order to aggressively pursue and compromise specific targets, often leveraging social engineering, in order to maintain persistent presence within the victim's network so they can move laterally and extract sensitive information.In a typical targeted attack, a target receives a contextually relevant e-mail that encourages a potential victim to click a link or open a file. The links and files the attackers send contain malicious code that exploits vulnerabilities in popular software.

Targeted attacks have been extremely successful, making the scope of the problem truly global. These have been affecting governments, militaries, defense industries, high-technology companies, intergovernmental organizations, non-governmental organizations (NGOs), media organizations, academic institutions, and activists worldwide.

Targeted attacks are not isolated smash-and-grab incidents. They are part of consistent campaigns that aim to establish persistent, covert presence in a target's network so that information can be extracted as needed. Targeted attacks may not be easy to understand but careful monitoring allows researchers to leverage the mistakes attackers make to get a glimpse inside their operations. Moreover, we can track cyber-espionage campaigns over time using a combination of technical and contextual indicators.

Targeted attacks that exploit vulnerabilities in popular software in order to compromise specific target sets are becoming increasingly commonplace. These attacks are not automated and indiscriminate nor are they conducted by opportunistic amateurs. These computer intrusions are staged by threat actors that aggressively pursue and compromise specific targets. Such attacks are typically part of broader campaigns, a series of failed and successful compromises, by specific threat actors and not isolated attacks. Since such attacks focus on the acquisition of sensitive data, strategies that focus on protecting the data itself, wherever it resides, are extremely important components of defense. By effectively using threat intelligence derived from external and internal sources combined with context-aware data protection and security tools that empower and inform human analysts, organizations are better positioned to detect and mitigate targeted attacks.

(f) Security Challenges of Cloud

What is cloud security?

It 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.So the aim of the cloud security & its researchers to help enterprise information technology and decision makers to analyze the security implications of cloud computing in their business. When a customer moves toward cloud computing, they have a clear understanding of potential security & risk associated with cloud computing.

Cloud security is a debated topic, with some claiming that the cloud is not secure. Some companies are concerned with the fact that if their data is stored on someone else’s servers (cloud provider), and that data is accessible from anywhere, how can they be sure that their data is safe from unwanted use by cyber criminals.Most of these concerns are unwarranted. Huge amount of businesses saw an improvement in security after switching to the cloud. The key to this amped-up security is the encryption of data being transmitted over networks and stored in databases.By using encryption, information is less accessible by hackers or anyone not authorized to view your data. As an added security measure, with most cloud
- based services, different security settings can be set based on the user. Cloud security is often as good as or better than other traditional systems, in part because service providers are able to devote resources to solving security issues that many customers cannot afford to tackle or which they lack the technical skills to address.

Cloud security faces some challenges and threats that need to be addressed to make sure that all data is safely stored.They are,

- **Data breaches**-It is a primary objective of a targeted attack or simply the result of human error, application vulnerabilities, or poor security practices.It involves any kind of information that was not intended for public release, including personal health /financial/personal information, trade secrets, and intellectual property.

- **Access Management** - Due to cloud enables access to company’s data from anywhere, companies need to make sure that not everyone has access to that data.

- **Data Encryption** - Data needs to be encrypted at all times, with clearly defined roles when it comes to who will be managing the encryption keys.

- **Denial of service(DoS/DDoS attacks)** - Distributed DoS and also DDoS attacks has as its aiml to stop the functioning of the targeted site so that no one can access it. The services of the targeted host connected to the internet are then stopped temporarily, or even indefinitely.

- **Advanced persistent threats(APTs)** - APTs are parasitical form of cyber attack that infiltrates systems to establish a foothold in the IT infrastructure of target companies, from which they steal data.It often adapting to the security measures intended to defend against them.

(g)IoT Attacks

What is IoT attacks?

The **IoT attack** surface is the sum total of all potential security vulnerabilities in IoT devices and associated software and infrastructure in a given network, be it local or the entire Internet.If anyone have IoT devices in their home, the truly frightening thing is that their devices might have already been attacked and compromised. And they might not even know. Because most IoT devices have built-in vulnerabilities , and there are lots of them connected to the Internet.

How IoT attacks happen?

IoT delivers substantial benefits to end users. However, it also brings unprecedented security challenges. A part of the central security issue is that connected devices share implicit trust. This shared trust between connected devices means that the devices automatically transmit their data to each other immediately upon recognition without first running any malware detection tests. The worst-case scenarios of these IoT security-dangers result in physical harm or even the loss of life.Once the attacker has exploited an attack vector, they identify and attack your IoT devices using a number of known vulnerabilities. Weak passwords ,lack of encryption & device exploits are most common attack vectors.

Weak passwords - It creates mainly three problems:

1. After the device is set up, the vast majority of users then go about their merry way and leave the device’s login credentials unchanged from the default
2. Often the same userid/password is the same for all the same devices (and printed in the user manual, or on the side of the packaging), allowing attackers to simply add the default userid/password to a list of known exploits for that particular device.
3. Manufacturers use easy userid/password combinations (for example, admin/admin, user/user, and so forth), or make up new, equally simple ones, which then quickly join the ranks of known vectors.

Lack of encryption - Because security is unfortunately often an afterthought in the IoT device development lifecycle, security features like encryption are often overlooked or not even considered. The industry is requesting embedded cryptography, such as cryptographic co-processors that can handle encryption and authentication in IoT devices.

How to prevent from IoT attacks?

Following are some tips to protect devices from IoT attacks.

Always change default passwords-When you provision a new device, always change the default password. Go into the management interface and change the password. From that the device doesn’t get turned into a bot, but malware writers love optimists.
Remove devices with telnet backdoors - A device with an open telnet backdoor should be removed from the network.There are IoT device scanners like this one from BullGuard, which scan an IoT search engine called Shodan to reveal if your devices are vulnerable based on the IP address of the computer where you originate the scan.

(h)Election Interference 2018

With all eyes on the 2018 US Midterms,, no major disruptions landed. But social media continued as a hyperactive battlefield. Malicious domains mimicking legitimate political websites were discovered and shut down, while Russia-linked accounts used third parties to purchase social media ads for them. Social media companies took a more active role in combatting election interference. Facebook set up a war room to tackle election interference; Twitter removed over 10,000 bots posting messages encouraging people not to vote.

So wrote a Russian national allegedly working for a Russian influence operation on social media on Feb. 16, 2018—the day that Special Counsel Robert Mueller handed down a indictment of figures connected to the Internet Research Agency (IRA). The IRA indictment alleged that Russian nationals used troll farms to illegally influence American electoral politics by radicalizing all sides of the American landscape. It now turns out, at least if you believe the Justice Department, that the person wrote this was actually part of the same project. Indeed, suggesting that the IRA defendants get sent to Guantanamo is now alleged by the Justice Department to be part of the very same influence operation as the IRA troll farms themselves. This is according to a Sept. 28 criminal complaint unsealed by the Justice Department on Friday, Oct. 19, against yet another member of the supposed conspiracy: one Elena Alekseevna Khusyaynova, who is alleged to have been the chief accountant in the Russian operation to influence the 2016 presidential election and the 2018 midterm elections upcoming in the next three weeks.

The complaint was released publicly mere hours after the Office of the Director of National Intelligence (ODNI) issued a statement along with the FBI, the Justice Department, and the Department of Homeland Security on "Combating Foreign Influence in U.S. Elections," warning—among other things—of "ongoing campaigns" to "influence vote perceptions and decision making in the 2018 and 2020 U.S. elections." It is not explicit that the actions were coordinated—but it doesn't seem like a coincidence either.The complaint is a rich document and is worth examining in depth—and it raises questions the document itself does not answer. As a preliminary matter, the mechanics of the case are curious.