1.Prepare a Case Study on the shortage of cybersecurity professionals in India, its impact on organizations, and the measures needed to address this challenge(Discuss the specific implications for the indian Context.

A big fight is underway for cybersecurity professionals, with a nearly 30% demand-supply gap for cybersecurity jobs.

There are between 20,000 and 25,000 unfilled positions in cyber security profiles in India currently, and this number is expected to expand as telcos push 5G roll out, and companies continue their digital transformation journeys, staffing experts said.

Telcos will also have to fight not only technology companies, but also enterprises for cybersecurity professionals going forward, they added.

"(Between) 70-75% of tech companies in India, including IT companies, are looking to hire more cyber security professionals as their existing teams are understaffed or do not have adequate skills to handle the evolving dynamics of internet privacy," said Sanjay Shetty, director, professional search & selection, and strategic accounts at Randstad India.

Staffing experts add that apart from tech firms, even enterprises are investing in building a cybersecurity workforce as they adopt di ..

The demand for cybersecurity professionals has far exceeded supply, causing many businesses to struggle to recruit qualified personnel. Cyber Security skill sets that are in high demand include data privacy, cloud security, AI security, and network security. Soft skills such as problem-solving, communication, teamwork, and collaboration were also most sought after. The top job roles include IT auditor, Information Security analyst, Network/IT Security Engineer/Specialist, Security Testing/Penetration Tester, and Computer Forensics analyst, according to an analysis conducted by TeamLease Digital.

Sunil Chemmankotil, Chief Executive Officer, TeamLease Digital, said, as India Inc. embraced digital infrastructures, the heightened vulnerability to cyber threats necessitates proactive measures. The prevalence of malware attacks, social engineering tactics, and other sophisticated cyber threats require a comprehensive approach to safeguarding our digital frontiers, he added.

For instance, enterprises in the country have experienced over 2000 attacks every week in Q1 2023, marking an 18% increase compared to the previous year. The healthcare industry was a prime target, with 7.7% of attacks directed towards it, found TeamLease Digital.

“By staying vigilant and resilient against emerging challenges such as AI-based attacks, IoT vulnerabilities, and metaverse cyber threats, we can fortify our digital landscape and pave the way for a secure and prosperous digital transformation,’‘ he added.

2. Analyze a significant cyber attack(s) that has affected an Indian organization or institution. Evaluate the specific challenges faced, the response to the incident, and the lessons learned.

Today's cybercriminals are not part-time amateurs or script kiddies but rather state-sponsored adversaries and professional criminals looking to steal information and make large amounts of money. Disruption and vandalism are still prevalent, and espionage has replaced hacktivism as the second main driving force behind cyberattacks -- after financial profit. With these different motives and the increasing sophistication of attackers, many security teams are struggling to keep their IT systems secure.

A variety of cyberattacks are launched against organizations every day. According to threat intelligence provider Check Point Research, there was a weekly average of 1,158 attacks per organization worldwide in 2023. Consulting services and software provider IT Governance reported that a total of 8.2 billion records were breached in publicly disclosed attacks during the year as a whole.

Research and publishing firm Cybersecurity Ventures has predicted that the global cost of cybercrime would hit $8 trillion in 2023 and increase to $9.5 trillion in 2024. The average cost of a data breach at 553 organizations worldwide in the 12 months ending in March 2023 was a record high of $4.45 million, according to a report that IBM publishes annually. The costs of cyberattacks are both tangible and intangible, including not only direct loss of assets, revenue and productivity, but also reputational damage that can lead to loss of customer trust and the confidence of business partners.

Cybercrime is built around the efficient exploitation of vulnerabilities, and security teams are always at a disadvantage because they must defend all possible entry points, while an attacker only needs to find and exploit one weakness or vulnerability. This asymmetry highly favors attackers. The result is that even large enterprises struggle to prevent cybercriminals from monetizing access to their networks, which typically must maintain open

access and connectivity while security professionals try to protect enterprise resources.

Not only large organizations are at risk of cyberattacks, though. Cybercriminals use any internet-connected device as a weapon, a target or both, and SMBs tend to deploy less sophisticated cybersecurity measures, opening them up to potential security incidents, too.

Security managers and their teams also need to be prepared for all the different attacks they might face. To help with that, here are 16 of the most damaging types of cyberattacks and how they work.

1. Malware attack

Malware, short for *malicious software*, is an umbrella term used to refer to a hostile or intrusive program or file that's designed to exploit devices at the expense of the user and to the benefit of the attacker. There are various forms of malware that all use evasion and obfuscation techniques designed to not only fool users, but also elude security controls so they can install themselves on a system or device surreptitiously without permission.

Currently, the most feared form is ransomware, a program that attackers use to encrypt a victim's files and then demand a ransom payment in order to receive the decryption key. Because of ransomware's prominence, it's covered in more detail below in its own section. The following are some other common types of malware:

- **Rootkit.** Unlike other malware, a rootkit is a collection of software tools used to open a backdoor on a victim's device. That enables the attacker to install additional malware, such as ransomware and keyloggers, or to gain remote access to and control of other devices on the network. To avoid detection, rootkits often disable security software. Once the rootkit has control over a device, it can be used to send spam email, join a botnet or collect sensitive data and send it back to the attacker.

- **Trojan.** A Trojan horse is a program downloaded and installed on a computer that appears harmless but is, in fact, malicious. Typically, this malware is hidden in an innocent-looking email attachment or free download. When a user clicks on the attachment or downloads the program, the malware is transferred to their computing device. Once inside, the malicious code executes whatever task the attacker designed it to perform. Often, this is to launch an immediate attack, but it can also create a backdoor for the hacker to use in future attacks.
- **Spyware.** Once installed, spyware monitors the victim's internet activity, tracks login credentials and spies on sensitive information -- all without the user's consent or knowledge. For example, cybercriminals use spyware to obtain credit card and bank account numbers and to get passwords. Government agencies in many countries also use spyware -- most prominently, a program named Pegasus -- to spy on activists, politicians, diplomats, bloggers, research laboratories and allies.

Security teams need to be prepared for all of these cyberattacks.

2. Ransomware attack

Ransomware is usually installed when a user visits a malicious website or opens a doctored email attachment. Traditionally, it exploits vulnerabilities on an infected device to encrypt important files, such as Word documents, Excel spreadsheets, PDFs, databases and system files, making them unusable. The attacker then demands a ransom in exchange for the decryption key needed to restore the locked files. The attack might target a mission-critical server or try to install the ransomware on other devices connected to the network before activating the encryption process so they're all hit simultaneously.

To increase the pressure on victims, attackers also often threaten to sell or leak data exfiltrated during an attack if the ransom isn't paid. In fact, in a shift in ransomware tactics, some attackers are now relying solely on data theft and potential public disclosures to extort payments without even bothering to encrypt the data. That change might have contributed to record-breaking numbers of ransomware attacks reported in 2023 by cybersecurity vendors

and researchers. Check Point Research said 10% of organizations worldwide were targeted by attempted attacks.

Everyone is a possible ransomware target, from individuals and small businesses to large organizations and government agencies. The attacks can have a seriously damaging impact. In a well-known incident, the WannaCry ransomware attack in 2017 affected organizations in over 150 countries with the disruption to hospitals costing the U.K.'s National Health Service alone around $111 million. More recently, the U.K.'s Royal Mail fell victim to a ransomware attack in 2023 that encrypted crucial files, preventing international shipments for six weeks. Royal Mail refused to pay the initial ransom demand of $80 million or subsequent reduced amounts but said it spent almost $13 million on remediation work and security improvements. In addition, data stolen in the attack was posted online.

Also in 2023, a ransomware attack on MGM Resorts International cost the hotel and casino company an estimated $100 million, disrupted its operations and resulted in the theft of personal information on customers. Caesars Entertainment negotiated a ransom payment of $15 million after a similar attack in an effort to prevent stolen data from being published online, according to *The Wall Street Journal*. Ransomware is such a serious problem that the U.S. government in 2021 created a website called StopRansomware that provides resources to help organizations prevent attacks, as well as a checklist on how to respond to one.

3. Password attack

Despite their many known weaknesses, passwords are still the most common authentication method used for computer-based services, so obtaining a target's password is an easy way to bypass security controls and gain access to critical data and systems. Attackers use various methods to illicitly acquire passwords, including these:

- **Brute-force attack.** An attacker can try well-known passwords, such as password123, or ones based on information gathered from a target's

social media posts, like the name of a pet, to guess user login credentials through trial and error. In other cases, they deploy automated password cracking tools to try every possible combination of characters.

- **Dictionary attack.** Similar to a brute-force attack, a dictionary attack uses a preselected library of commonly used words and phrases, depending on the location or nationality of the victim.
- **Social engineering.** It's easy for an attacker to craft a personalized email or text message that looks genuine by collecting information about someone from their social media posts and other sources. As a form of social engineering, these messages can be used to obtain login credentials under false pretenses by manipulating or tricking the person into disclosing the information, particularly if they're sent from a fake account impersonating someone the victim knows.
- **Keylogging.** A keylogger is a software program that secretly monitors and logs every keystroke by users to capture passwords, PIN codes and other confidential information entered via the keyboard. This information is sent back to the attacker via the internet.
- **Password sniffing.** A password sniffer is a small program installed on a network that extracts usernames and passwords sent across the network in cleartext. While still used by attackers, it's no longer the threat it used to be because most network traffic is now encrypted.
- **Stealing or buying a password database.** Hackers can try to breach an organization's network defenses to steal its database of user credentials and then either use the data themselves or sell it to others.

In a 2023 survey by TechTarget's Enterprise Strategy Group research division, 45% of the 377 respondents said they knew user accounts or credentials had been compromised in their organization during the past 12 months, while 32% suspected they had been. Of all those respondents, 59% said such compromises led to successful cyberattacks. Also, Verizon's "2023 Data Breach Investigations Report" found that using stolen credentials was by far the top way in which attackers accessed systems in breached organizations with 49% of 4,291 documented breaches involving their use.

4. DDoS attack

A distributed denial-of-service (DDoS) attack involves the use of numerous compromised computer systems or mobile devices to target a server, website or other network resource. The goal is to slow it down or crash it completely by sending a flood of messages, connection requests or malformed packets, thereby denying service to legitimate users.

Almost 7.9 million DDoS attacks were launched in the first half of 2023, a 31% year-over-year increase, according to a report by performance management and security software vendor Netscout. Political or ideological motives are behind many of the attacks, but they're also used to seek ransom payments -- in some cases, attackers threaten an organization with a DDoS attack if it doesn't meet their ransom demand. Attackers are also harnessing the power of AI tools to improve attack techniques and direct their networks of slave machines to perform DDoS attacks accordingly. Worryingly, AI is now being used to enhance all forms of cyberattacks, although it has potential cybersecurity uses, too.

5. Phishing

In phishing, an attacker masquerades as a reputable organization or individual to trick an unsuspecting victim into handing over valuable information, such as passwords, credit card details and intellectual property. Based on social engineering techniques, phishing campaigns are easy to launch and surprisingly effective. Emails are most commonly used to distribute malicious links or attachments, but phishing attacks can also be conducted through text messages (SMS phishing, or smishing) and phone calls (voice phishing, or vishing).

Spear phishing targets specific people or companies, while whaling attacks are a type of spear phishing aimed at senior executives in an organization. A related attack is the business email compromise (BEC) in which an attacker poses as a top executive or other person of authority and asks employees to transfer money, buy gift cards or take other actions. The FBI's Internet Crime Complaint Center puts phishing and BEC attacks in

separate categories. In 2022, the last year for which data has been released, it received 21,832 complaints about BEC attacks with total losses of more than $2.7 billion and 300,497 phishing complaints that generated $52 million in losses.

6. SQL injection attack

Any website that is database-driven -- and that's the majority of websites -- is susceptible to SQL injection attacks. A SQL query is a request for some action to be performed on a database, and a well-constructed malicious request can create, modify or delete the data stored in the database. It can also read and extract data such as intellectual property, personal information of customers or employees, administrative credentials and private business details.

SQL injection continues to be a widely used attack vector. It was third on the 2023 Common Weakness Enumeration (CWE) Top 25 list of the most dangerous software weaknesses, which is maintained by The Mitre Corp. In 2023, according to the website CVEdetails.com, more than 2,100 SQL injection vulnerabilities were added to the CVE database, a separate catalog of common vulnerabilities and exposures that Mitre also manages. In a high-profile example of a SQL injection attack, attackers used one of those new vulnerabilities to gain access to Progress Software's MoveIt Transfer web application, leading to data breaches at thousands of organizations that use the file transfer software.

7. Cross-site scripting

This is another type of injection attack in which an attacker adds a malicious script to content on a legitimate website. Cross-site scripting (XSS) attacks occur when an untrusted source is able to inject code into a web application and the malicious code is then included in webpages that are dynamically generated and delivered to a victim's browser. This enables the attacker to execute scripts written in languages such as JavaScript, Java and HTML in the browsers of unsuspecting website users.

Attackers can use XSS to steal session cookies, which lets them pretend to be victimized users. But they can also distribute malware, deface websites, seek user credentials and take other damaging actions through XSS. In many cases, it's combined with social engineering techniques, such as phishing. A constant among common attack vectors, XSS ranked second on the CWE Top 25 list for 2023.

8. Man-in-the-middle attack

In a man-in-the-middle (MitM) attack, the attacker secretly intercepts messages between two parties -- for example, an end user and a web application. The legitimate parties believe they're communicating directly with each other, but in fact, the attacker has inserted themselves in the middle of the electronic conversation and taken control of it. The attacker can read, copy and change messages, including the data they contain, before forwarding them on to the unsuspecting recipient, all in real time.

A successful MitM attack enables attackers to capture or manipulate sensitive personal information, such as login credentials, transaction details, account records and credit card numbers. Such attacks often target the users of online banking applications and e-commerce sites, and many involve the use of phishing emails to lure users into installing malware that enables an attack.

9. URL interpretation/URL poisoning

It's easy for attackers to modify a URL in an effort to access information or resources. For example, if an attacker logs in to a user account they've created on a website and can view their account settings at https://www.awebsite.com/acount?user=2748, they can easily change the URL to, say, https://www.awebsite.com/acount?user=1733 to see if they can access the account settings of the corresponding user. If the site's web server doesn't check whether each user has the correct authorization to access the requested resource, particularly if it includes user-supplied input, the attacker likely will be able to view the account settings of every other user on the site.

A URL interpretation attack, also sometimes referred to as *URL poisoning*, is used to gather confidential information, such as usernames and database records, or to access admin pages that are used to manage a website. If an attacker does manage to access privileged resources by manipulating a URL, it's commonly due to an insecure direct object reference vulnerability in which the site doesn't properly apply access control checks to verify user identities.

10. DNS spoofing

The DNS enables users to access websites by mapping domain names and URLs to the IP addresses that computers use to locate sites. Hackers have long exploited the insecure nature of DNS to overwrite stored IP addresses on DNS servers and resolvers with fake entries so victims are directed to an attacker-controlled website instead of the legitimate one. These fake sites are designed to look exactly like the sites that users expected to visit. As a result, victims of a DNS spoofing attack aren't suspicious when asked to enter their account login credentials on what they think is a genuine site. That information enables the attackers to log in to user accounts on the sites being spoofed.

11. DNS tunneling

Because DNS is a trusted service, DNS messages typically travel through an organization's firewalls in both directions with little monitoring. However, this means an attacker can embed malicious data, such as command-and-control messages, in DNS queries and responses to bypass -- or tunnel around -- security controls. For example, the hacker group OilRig, which has suspected ties to Iran, is known to use DNS tunneling to maintain a connection between its command-and-control server and the systems it's attacking.

A DNS tunneling attack uses a tunneling malware program deployed on a web server with a registered domain name. Once the attacker has infected a computer behind an organization's firewall, malware installed there attempts to connect to the server with the tunneling program, which involves

a DNS request to locate it. This provides a connection for the attacker into a protected network.

There also are valid uses for DNS tunneling -- for example, antivirus software vendors send malware profile updates in the background via DNS tunneling. As a result, DNS traffic must be monitored to ensure that only trusted traffic is allowed to flow through a network.

12. Botnet attack

A botnet is a group of internet-connected computers and networking devices that are infected with malware and controlled remotely by cybercriminals. Vulnerable IoT devices are also being compromised by attackers to increase the size and power of botnets. They're often used to send email spam, engage in click fraud campaigns and generate malicious traffic for DDoS attacks.

When the Meris botnet was discovered in 2021, for example, security researchers at software vendor Cloudflare said attackers were using it to launch DDoS attacks against about 50 different websites daily. Meris is also responsible for some of the largest DDoS attacks on record thanks to its use of HTTP pipelining and its size, which was estimated at about 250,000 bots in 2021. The objective for creating a botnet is to infect as many devices as possible and then use the combined computing power and resources of those devices to automate and magnify malicious activities.

13. Watering hole attack

In what's known as a *drive-by attack*, an attacker uses a security vulnerability to add malicious code to a legitimate website so that, when users go to the site, the code automatically executes and infects their computer or mobile device. It's one form of a watering hole attack in which attackers identify and take advantage of insecure sites that are frequently visited by users they wish to target -- for example, employees or customers of a specific organization or even in an entire sector, such as finance, healthcare and the military.

Because it's hard for users to identify a website that has been compromised by a watering hole attack, it's a highly effective way to install malware on their devices. With the prospective victims trusting the site, an attacker might even hide the malware in a file that users intentionally download. The malware in watering hole attacks is often a remote access Trojan that gives the attacker remote control of infected systems.

14. Insider threat

Employees and contractors have legitimate access to an organization's systems, and some have an in-depth understanding of its cybersecurity defenses. This can be used maliciously to gain access to restricted resources, make damaging system configuration changes or install malware. Insiders can also inadvertently cause problems through negligence or a lack of awareness and training on cybersecurity policies and best practices.

It was once widely thought that insider threat incidents outnumbered attacks by outside sources, but that's no longer the case. Verizon's 2023 data breach report said external actors were responsible for more than 80% of the breaches that were investigated. However, insiders were involved in 19% of them -- nearly one in five. Some of the most prominent data breaches have been carried out by insiders with access to privileged accounts. For example, Edward Snowden, a National Security Agency contractor with administrative account access, was behind one of the largest leaks of classified information in U.S. history starting in 2013. In 2023, a member of the Massachusetts Air National Guard was arrested and charged with posting top-secret and highly classified military documents online.

15. Eavesdropping attack

Also known as *network* or *packet sniffing*, an eavesdropping attack takes advantage of poorly secured communications to capture traffic in real time as information is transmitted over a network by computers and other devices. Hardware, software or a combination of both can be used to passively monitor and log information and "eavesdrop" on unencrypted data from network packets. Network sniffing can be a legitimate activity done by

network administrators and IT security teams to resolve network issues or verify traffic. However, attackers can exploit similar measures to steal sensitive data or obtain information that enables them to penetrate further into a network.

To enable an eavesdropping attack, phishing emails can be used to install malware on a network-connected device, or hardware can be plugged into a system by a malicious insider. An attack doesn't require a constant connection to the compromised device -- the captured data can be retrieved later, either physically or by remote access. Due to the complexity of modern networks and the sheer number of devices connected to them, an eavesdropping attack can be difficult to detect, particularly because it has no noticeable impact on network transmissions.

16. Birthday attack

This is a type of cryptographic brute-force attack for obtaining digital signatures, passwords and encryption keys by targeting the hash values used to represent them. It's based on the "birthday paradox," which states that, in a random group of 23 people, the chance that two of them have the same birthday is more than 50%. Similar logic can be applied to hash values to enable birthday attacks.

A key property of a hash function is collision resistance, which makes it exceedingly difficult to generate the same hash value from two different inputs. However, if an attacker generates thousands of random inputs and calculates their hash values, the probability of matching stolen values to discover a user's login credentials increases, particularly if the hash function is weak or passwords are short. Such attacks can also be used to create fake messages or forge digital signatures. As a result, developers need to use strong cryptographic algorithms and techniques that are designed to be resistant to birthday attacks, such as message authentication codes and hash-based message authentication codes.

How to prevent common types of cyberattacks

The more devices that are connected to a network, the greater its value. For example, Metcalfe's law asserts that the value of a network is proportional to the square of its connected users. Especially in large networks, that makes it harder to increase the cost of an attack to the point where attackers give up. Security teams have to accept that their networks will be under constant attack. But, by understanding how different types of cyberattacks work, mitigation controls and strategies can be put in place to minimize the damage they do. Here are the main points to keep in mind:

- Attackers, of course, first need to gain a foothold in a network before they can achieve whatever objectives they have, so they need to find and exploit vulnerabilities or weaknesses in an organization's IT infrastructure. Being diligent about identifying and fixing those issues -- through an effective vulnerability management program, for example -- reduces the potential for attacks.
- Vulnerabilities aren't only technology-based. According to the 2023 Verizon data breach report, 74% of the examined breaches involved a human element, such as errors and falling prey to social engineering techniques. Errors can be either unintentional actions or lack of action, from downloading a malware-infected attachment to failing to use a strong password. This makes security awareness training a top priority in the fight against cyberattacks, and because attack techniques are constantly evolving, training must be constantly updated as well. Cyberattack simulations can assess the level of cyber awareness among employees and drive additional training when there are obvious shortcomings.
- While security-conscious users can reduce the success rate of cyberattacks, a defense-in-depth strategy is also essential. It should be tested regularly via vulnerability assessments and penetration tests to check for exploitable security vulnerabilities in OSes and applications.
- End-to-end encryption across a network stops many attacks from being able to successfully extract valuable data even if they manage to breach perimeter defenses or intercept network traffic.

- To deal with zero-day exploits, where cybercriminals discover and exploit a previously unknown vulnerability before a fix becomes available, enterprises need to consider adding content disarm and reconstruction technology to their threat prevention controls. Instead of trying to detect malware functionality that continually evolves, it assumes all content is malicious and uses a known-bad vs. known-good approach to remove file components that don't comply with the file type's specifications and format.
- Security teams also need to proactively monitor the entire IT environment for signs of suspicious or inappropriate activity to detect cyberattacks as early as possible. Network segmentation creates a more resilient network that is able to detect, isolate and disrupt an attack. And there should be a well-rehearsed incident response plan if an attack is detected.

Ultimately, if the connected world is going to survive the never-ending battle against cyberattacks, cybersecurity strategies and budgets need to build in the ability to adapt to changing threats and deploy new security controls when needed, while also now harnessing the power of AI to help security teams.

3. Investigate the top cybersecurity problems faced by universities and colleges, with a focus on the specific types of cyberattacks targeting higher education institutions.

Top 5 Cyber Security Challenges Facing Higher Education

The cost of cybercrime is predicted to cost the world $8 trillion / £6.4 trillion in 2023.

With Higher Education institutions falling under one of the most vulnerable categories for cybercriminal targets (with 6 in 10 reporting cyber attacks weekly), universities need to consider their security strategy more than ever to fend off these potential financial consequences.

Here's why we at Talion believe Higher Education are at higher risk and the unique challenges Higher Education face (in comparison to other industries) which makes it harder for them to fight cybercrime.

Challenge 1: Small Budgets

Since the pandemic, it's clear that higher institutions are focusing a lot more heavily on the digital estate than the physical, even with in-person classes returning. However, the budget hasn't necessarily aligned with this. The digital landscape is, in some ways, more expensive – especially in terms of securely protecting a huge, sensitive digital estate that holds valuable student and professor data.

This budget gap has caused numerous problems for institutions, meaning their business continuity now requires a security partner that really understands the sector and can leverage Threat Intelligence with financial effectiveness.

Challenge 2: Meeting Cyber Security Best Practices When Moving Across Institutions

Universities are surrounded by an open and collaborative environment, and this positively affects their cross-institutional work. However, from a cyber security standpoint, it leaves huge risk of data vulnerability. Cyber security best practices, whilst sensible and easy to follow at times, can be easily overlooked in importance. This slacking in compliance means that, as colleagues travel in and out of other institutions, there is no awareness of where their data is and who can access it. This "head in the sand" approach can prove difficult for CISOs to change.

Challenge 3: Protecting Highly Sensitive Data

Universities are known for storing vast amounts of Personal Identifiable Data (PID), especially as students move in and out of the system annually. From salaries and bank details, to addresses and pastoral care notes, there is endless data that's considered attractive to a cybercriminal. There is even commercially valuable intellectual property, such as the Oxford Astra Zeneca Vaccine, as universities drive research projects. As a result, Higher Education institutions remain high targets and must stay aware

of ever-changing trends in the cybersecurity landscape to make relevant amendments to their security posture.

Challenge 4: Employee Conformity

Although CISOs may try hard to put new security regulations and best practices in place, these aren't necessarily adopted by colleagues – or at least not with much willingness. Academics like their familiar systems and processes, even if they may be outdated, and this makes it particularly difficult for institutions to make changes widespread.

Challenge 5: Lack Of Communication Outside Of Higher Education

Although university CISOs are very willing to collaborate and share insight with colleagues at other universities, this can hinder them in the long run as they focus more on their peers than seeking external support. Whilst internal advice can be helpful, further knowledge and expertise can be gained by considering solutions such as Threat Intelligence, which draws upon in-depth research of cybercriminal tactics, techniques and procedures (TTPs) to produce actionable recommendations – ones which many universities are currently lacking.

As a CISO at a university, you may resonate with some or all of these challenges within your institution. Yes, these challenges are present, but that doesn't mean security improvements are unachievable; it's about working past these issues to show your colleagues the value in adopting best practices and safeguarding sensitive data.

4. Select and analyze three real-world malware attacks, covering different malware types such as viruses, worms, and ransomware. For each case, describe the attack vector, the target, the impact.

THE 12 MOST COMMON TYPES OF MALWARE

What are the Types of Malware?

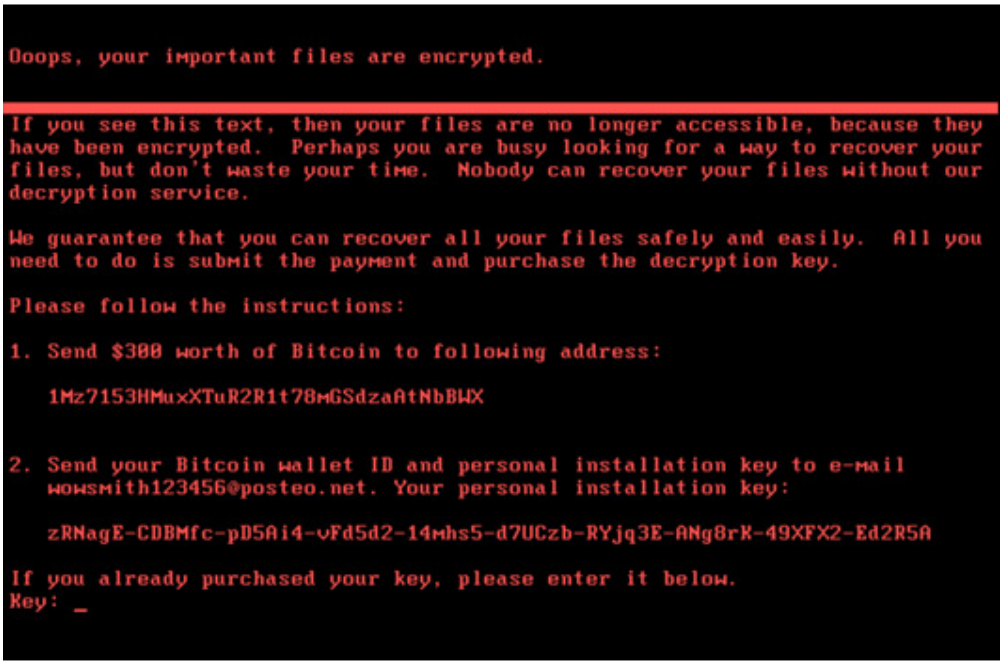
While there are many different variations of malware, you are most likely to encounter the following malware types:

Type	What It Does	Real-World Example
Ransomware	Disables victim's access to data until ransom is paid	RYUK
Fileless Malware	Makes changes to files that are native to the OS	Astaroth
Spyware	Collects user activity data without their knowledge	DarkHotel
Adware	Serves unwanted advertisements	Fireball
Trojans	Disguises itself as desirable code	Emotet
Worms	Spreads through a network by replicating itself	Stuxnet
Rootkits	Gives hackers remote control of a victim's device	Zacinlo
Keyloggers	Monitors users' keystrokes	Olympic Vision
Bots	Launches a broad flood of attacks	Echobot
Mobile Malware	Infects mobile devices	Triada
Wiper Malware	Erases user data beyond recoverability.	WhisperGate

Below, we describe how they work and provide real-world examples of each.

1. Ransomware

Ransomware is software that uses encryption to disable a target's access to its data until a ransom is paid. The victim organization is rendered partially or totally unable to operate until it pays, but there is no guarantee that payment will result in the necessary decryption key or that the decryption key provided will function properly.



Example of a ransom letter

Ransomware Example:

This year, the city of Baltimore was hit by a type of ransomware named RobbinHood, which halted all city activities, including tax collection, property transfers, and government email for weeks. This attack has cost the city more than $18 million so far, and costs continue to accrue. The same type of malware was used against the city of Atlanta in 2018, resulting in costs of $17 million.

2. Fileless Malware

Fileless malware doesn't install anything initially, instead, it makes changes to files that are native to the operating system, such as PowerShell or WMI. Because the operating system recognizes the edited files as legitimate, a fileless attack is not caught by antivirus software — and because these attacks are stealthy, they are up to ten times more successful than traditional malware attacks.

Fileless Malware Example:

Astaroth is a fileless malware campaign that spammed users with links to a .LNK shortcut file. When users downloaded the file, a WMIC tool was launched, along with a number of other legitimate Windows tools. These tools downloaded additional code that was executed only in memory, leaving no evidence that could be detected by vulnerability scanners. Then the attacker downloaded and ran a Trojan that stole credentials and uploaded them to a remote server.

3. Spyware

Spyware collects information about users' activities without their knowledge or consent. This can include passwords, pins, payment information and unstructured messages.

The use of spyware is not limited to the desktop browser: it can also operate in a critical app or on a mobile phone.

Even if the data stolen is not critical, the effects of spyware often ripple throughout the organization as performance is degraded and productivity eroded.

Spyware Example:

DarkHotel, which targeted business and government leaders using hotel WIFI, used several types of malware in order to gain access to the systems belonging to specific powerful people. Once that access was gained, the attackers installed keyloggers to capture their targets passwords and other sensitive information.

4. Adware

Adware tracks a user's surfing activity to determine which ads to serve them. Although adware is similar to spyware, it does not install any software on a user's computer, nor does it capture keystrokes.

The danger in adware is the erosion of a user's privacy — the data captured by adware is collated with data captured, overtly or covertly, about the user's activity elsewhere on the internet and used to create a profile of that person which includes who their friends are, what they've purchased, where they've traveled, and more. That information can be shared or sold to advertisers without the user's consent.

Adware Example:

Adware called Fireball infected 250 million computers and devices in 2017, hijacking browsers to change default search engines and track web activity. However, the malware had the potential to become more than a mere nuisance. Three-quarters of it was able to run code remotely and download malicious files.

EXPERT TIP

Download CrowdInspect: a free community tool for Microsoft Windows systems that is aimed to help alert you to the presence of potential malware are on your computer that may be communicating over the network.**Download CrowdInspect**

5. Trojan

A Trojan disguises itself as desirable code or software. Once downloaded by unsuspecting users, the Trojan can take control of victims' systems for malicious purposes. Trojans may hide in games, apps, or even software patches, or they may be embedded in attachments included in phishing emails.

Trojan Example:

Emotet is a sophisticated banking trojan that has been around since 2014. It is hard to fight Emotet because it evades signature-based detection, is persistent, and includes spreader modules that help it propagate. The trojan is so widespread that it is the subject of a US Department of Homeland Security alert, which notes that Emotet has cost state, local, tribal and territorial governments up to $1 million per incident to remediate.

LEARN MORE

TrickBot malware is a type of banking Trojan released in 2016 that has since evolved into a modular, multi-phase malware capable of a wide variety of illicit operations. Learn more about what makes TrickBot highly concerning here.**Read: What is TrickBot Malware**

6. Worms

Worms target vulnerabilities in operating systems to install themselves into networks. They may gain access in several ways: through backdoors built into software, through unintentional software vulnerabilities, or through flash drives. Once in place, worms can be used by malicious actors to launch DDoS attacks, steal sensitive data, or conduct ransomware attacks.

Worm Example:

Stuxnet was probably developed by the US and Israeli intelligence forces with the intent of setting back Iran's nuclear program. It was introduced into Iran's environment through a flash drive. Because the environment was air-gapped, its creators never thought Stuxnet would escape its target's network — but it did. Once in the wild, Stuxnet spread aggressively but did little damage, since its only function was to interfere with industrial controllers that managed the uranium enrichment process.

LEARN MORE

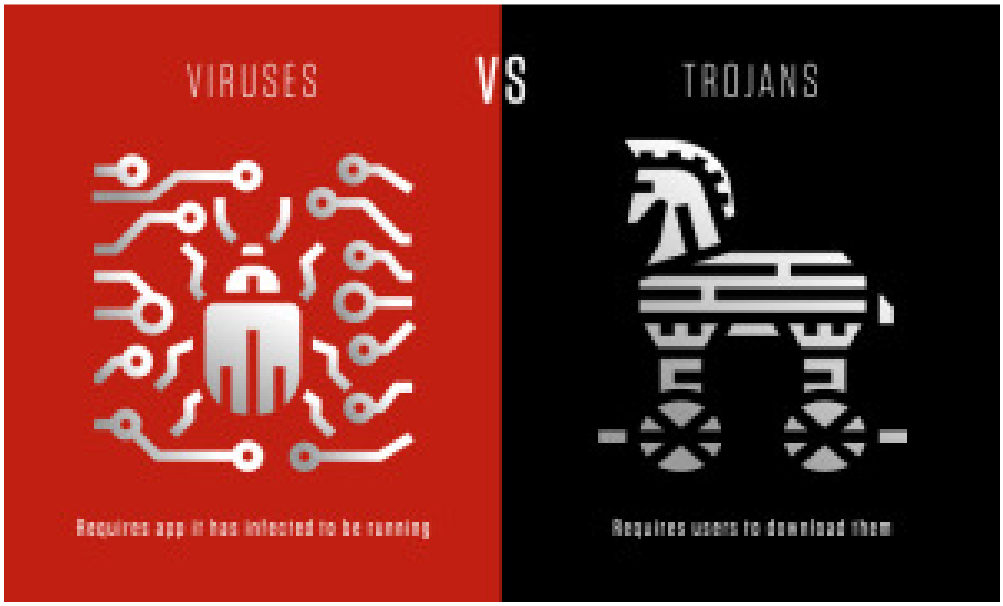
Want to stay up to date on recent adversary activities? Stop by the Research and Threat Intel Blog for the latest research, trends, and insights on emerging cyber threats.**Research and Threat Intel Blog**

7. Virus

A virus is a piece of code that inserts itself into an application and executes when the app is run. Once inside a network, a virus may be used to steal sensitive data, launch DDoS attacks or conduct ransomware attacks.

Viruses vs. Trojans

A virus cannot execute or reproduce unless the app it has infected is running. This dependence on a host application makes viruses different from trojans, which require users to download them, and worms, which do not use applications to execute. Many instances of malware fit into multiple categories: for instance, Stuxnet is a worm, a virus and a rootkit.



8. Rootkits

A rootkit is software that gives malicious actors remote control of a victim's computer with full administrative privileges. Rootkits can be injected into applications, kernels, hypervisors, or firmware. They spread through phishing, malicious attachments, malicious downloads, and compromised shared drives. Rootkits can also be used to conceal other malware, such as keyloggers.

Rootkit Example:

Zacinlo infects systems when users download a fake VPN app. Once installed, Zacinlo conducts a security sweep for competing malware and tries to remove it. Then it opens invisible browsers and interacts with content like a human would — by scrolling, highlighting and clicking. This activity is meant to fool behavioral analysis software. Zacinlo's payload occurs when the malware clicks on ads in the invisible browsers. This advertising click fraud provides malicious actors with a cut of the commission.

LEARN MORE

Learn more about bootkit, an infection that uses rootkit tools to attach malicious software into a computer system.**Learn More**

9. Keyloggers

A keylogger is a type of spyware that monitors user activity. Keyloggers have legitimate uses; businesses can use them to monitor employee activity and families may use them to keep track of children's online behaviors.

However, when installed for malicious purposes, keyloggers can be used to steal password data, banking information and other sensitive information. Keyloggers can be inserted into a system through phishing, social engineering or malicious downloads.

Keylogger Example:

A keylogger called Olympic Vision has been used to target US, Middle Eastern and Asian businessmen for business email compromise (BEC) attacks. Olympic Vision uses spear-phishing and social engineering techniques to infect its targets' systems in order to steal sensitive data and spy on business transactions. The keylogger is not sophisticated, but it's available on the black market for $25 so it's highly accessible to malicious actors.

10. Bots/Botnets

A bot is a software application that performs automated tasks on command. They're used for legitimate purposes, such as indexing search engines, but when used for malicious purposes, they take the form of self-propagating malware that can connect back to a central server.

Usually, bots are used in large numbers to create a botnet, which is a network of bots used to launch broad remotely-controlled floods of attacks, such as DDoS attacks. Botnets can become quite expansive. For example, the Mirai IoT botnet ranged from 800,000 to 2.5M computers.

Botnet Example:

Echobot is a variant of the well-known Mirai. Echobot attacks a wide range of IoT devices, exploiting over 50 different vulnerabilities, but it also includes exploits for Oracle WebLogic Server and VMWare's SD-Wan networking software. In addition, the malware looks for unpatched legacy systems. Echobot could be used by malicious actors to launch DDoS attacks, interrupt supply chains, steal sensitive supply chain information and conduct corporate sabotage.

11. Mobile Malware

Attacks targeting mobile devices have risen 50 percent since last year. Mobile malware threats are as various as those targeting desktops and include Trojans, ransomware, advertising click fraud and more. They are distributed through phishing and malicious downloads and are a particular problem for jailbroken phones, which tend to lack the default protections that were part of those devices' original operating systems.

12. Mobile Malware Example:

Triada is a rooting Trojan that was injected into the supply chain when millions of Android devices shipped with the malware pre-installed. Triada gains access to sensitive areas in the operating system and installs spam apps. The spam apps display ads, sometimes replacing legitimate ads. When a user clicks on one of the unauthorized ads, the revenue from that click goes to Triada's developers.

13. Wiper Malware

A wiper is a type of malware with a single purpose: to erase user data and ensure it can't be recovered. Wipers are used to take down computer networks in public or private companies across various sectors. Threat actors also use wipers to cover up traces left after an intrusion, weakening their victim's ability to respond.

14.Wiper Malware Example:

On Jan. 15, 2022, a set of malware dubbed *WhisperGate* was reported to have been deployed against Ukrainian targets. The incident is widely reported to contain three individual components deployed by the same adversary, including a malicious bootloader that corrupts detected local

disks, a Discord-based downloader and a file wiper. The activity occurred at approximately the same time multiple websites belonging to the Ukrainian government were defaced.

5.Provide the Comparative Analysis of DES,AES, RSA.

Encryption is a well-known technology for protecting sensitive data. Use of the combination of Public and Private Key encryption to hide the sensitive data of users, and cipher text retrieval.

.

a) Data Encryption Standard (DES)

DES (Data Encryption Standard) algorithm purpose is to provide a standard method for protecting sensitive commercial and unclassified data. In this same key used for encryption and decryption process.

DES algorithm consists of the following steps

i.Encryption

1. DES accepts an input of 64-bit long plaintext and 56-bitkey (8 bits of parity) and produce output of 64-bit block.
2. The plaintext block has to shift the bits around.
3. The 8 parity bits are removed from the key by subjecting the key to its Key Permutation.
4. The plaintext and key will have processed by following
i. The key is split into two 28 halves
ii. Each half of the key is shifted (rotated) by one or two bits, depending on the round.
iii.The halves are recombined and subject to a compression permutation to reduce the key from 56 bits to 48 bits. This compressed keys used to encrypt this round's plaintext block.
iv. The rotated key halves from step 2 are used in next round.
v. The data block is split into two 32-bit halves.
vi. One half is subject to an expansion permutation to increase its size to 48 bits.
vii. Output of step 6 is exclusive-OR'ed with the 48-itcompressed key from step 3.
viii. Output of step 7 is fed into an S-box, which substitutes key bits and reduces the 48-bit block back down to 32-bits.
ix. Output of step 8 is subject to a P-box to permute the bits.
x. The output from the P-box is exclusive-OR'ed with other half of the data block. k. The two data halves are swapped and become the next round's input.

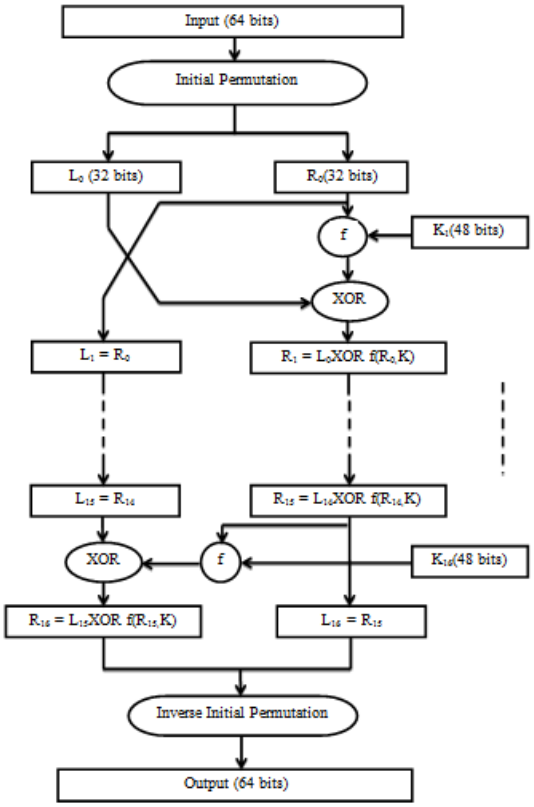


Figure 1 : Diagram of DES Algorithm

b) Advanced Encryption Standard (AES)

Advanced Encryption Standard (AES) algorithm not only for security but also for great speed. Bothhardware and software implementation are faster still.New encryption standard recommended by NIST to replace DES. Encrypts data blocks of 128 bits in 10, 12 and 14 round depending on key size as shown in Figure - 2. It can be implemented on various platforms specially in small devices. It is carefully tested for many securities applications.

i. Algorithm Steps : These steps used to encrypt 128-bit block

1. The set of round keys from the cipher key.
2. Initialize state array and add the initial round key to the starting state array.
3. Perform round = 1 to 9 : Execute Usual Round.
4. Execute Final Round.
5. Corresponding cipher text chunk output of Final Round Step

ii. Usual Round

Execute the following operations which are described above.

1. Sub Bytes
2. Shift Rows
3. Mix Columns
4. Add Round Key , using K(round)

iii. Final Round:

Execute the following operations which are described above.

1. Sub Bytes
2. Shift Rows
3. Add Round Key, using K(10)

iv. Encryption : Each round consists of the following four steps:

I Sub Bytes : The first transformation, Sub Bytes, is used at the encryption site. To substitute a byte,

we interpret the byte as two hexadecimal digits.

Ii Shift Rows : In the encryption, the transformation is called Shift Rows.

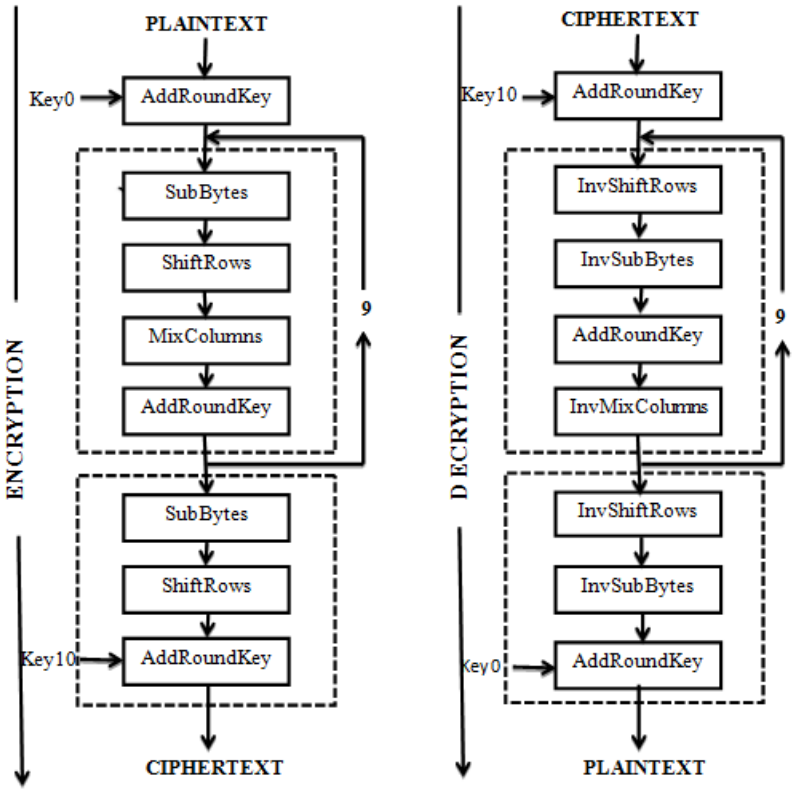


Figure 2 : AES Encryption and Decryption

C. Rivest-Shamir-Adleman (RSA)

RSA is widely used Public-Key algorithm. RSA firstly described in 1977. In our proposed work, we are using RSA algorithm to encrypt the data to provide security so that only the concerned user can access it.

RSA algorithm involves these steps:

1. Key Generation
2. Encryption
3. Decryption

In the table below a comparative study between AES, DES and RSA is presented in to eighteen factors, which are Key Size, Block Size, Ciphering & Deciphering key, Scalability, Algorithm, Encryption, Decryption, Power Consumption, Security, Deposit of keys, Inherent Vulnerabilities, Key used, Rounds, Stimulation Speed, Trojan Horse, Hardware & Software Implementation and Ciphering & Deciphering Algorithm.

Table 1: Comparison between AES, DES and RSA

Factors	AES	DES	RSA
Developed	2000	1977	1978
Key Size	128, 192, 256 bits	56 bits	>1024 bits
Block Size	128 bits	64 bits	Minimum 512 bits
Ciphering & deciphering key	Same	Same	Different
Scalability	Not Scalable	It is scalable algorithm due to varying the key size and Block size.	Not Scalable
Algorithm	Symmetric Algorithm	Symmetric Algorithm	Asymmetric Algorithm
Encryption	Faster	Moderate	Slower
Decryption	Faster	Moderate	Slower
Power Consumption	Low	Low	High
Security	Excellent Secured	Not Secure Enough	Least Secure
Deposit of keys	Needed	Needed	Needed
Inherent Vulnerabilities	Brute Forced Attack	Brute Forced, Linear and differential cryptanalysis attack	Brute Forced and Oracle attack
Key Used	Same key used for Encrypt and Decrypt	Same key used for Encrypt and Decrypt	Different key used for Encrypt and Decrypt
Rounds	10/12/14	16	1
Stimulation Speed	Faster	Faster	Faster
Trojan Horse	Not proved	No	No
Hardware & Software Implementation	Faster	Better in hardware than in software	Not Efficient
Ciphering & Deciphering Algorithm	Different	Different	Same