Jashore University of Science and Technology

Department of Computer Science and Engineering

Course Code: CSE-3201

Course Title: Computer Networks

An Assignment on
Computer Networks

Submitted to	Submitted by
Monishanker Halder Assistant Professor, Department of Computer Science and Engineering Jashore University of Science and Technology	**Md. Monirul Islam** Roll: 180126 3rd Year 2nd Semester Session: 2018-2019 Dept. of Computer Science and Engineering Jashore University of Science and Technology.

Submission Date: 25.10.2022

Diagnosis the problem of network topologies

Discussion on security issues in Computer network

- ✓ Network Security

Network security is a broad term that covers a multitude of technologies, devices and processes. In its simplest term, it is a set of rules and configurations designed to protect the integrity, confidentiality and accessibility of computer networks and data using both software and hardware technologies. Every organization, regardless of size, industry or infrastructure, requires a degree of network security solutions in place to protect it from the ever-growing landscape of cyber threats in the wild today.

Today's network architecture is complex and is faced with a threat environment that is always changing and attackers that are always trying to find and exploit vulnerabilities. These vulnerabilities can exist in a broad number of areas, including devices, data, applications, users and locations. For this reason, there are many network security management tools and applications in use today that address individual threats and exploits and also regulatory non-compliance. When just a few minutes of downtime can cause widespread disruption and massive damage to an organization's bottom line and reputation, it is essential that these protection measures are in place.

✓ Security issues

There are most 7 issues in computer security. Those are

- ✓ Internal security threats.
- ✓ Distributed Denial-of – Service (DDoS) attack.
- ✓ Rogue security software.
- ✓ Malware.
- ✓ Ransomware.
- ✓ Phishing attacks.
- ✓ Viruses.

✓ Internal security threats

Research conducted by the US Computer Emergency Response Team (Cert) estimates that almost 40 percent of IT security breaches are perpetrated by people inside the company.

Criminal attacks are particularly likely to happen from the inside: one recent study estimated that 90 percent of criminal computer crimes were committed by employees of the company attacked.

- **Malicious cyber-attacks:**

  Research conducted by Cert has found the most likely perpetrators of cyberattacks are system administrators or other IT staff with privileged system access.

  Technically proficient employees can use their system access to open back doors into computer systems, or leave programs on the network to steal information or wreak havoc. In 2006, IT programmer Roger Duronio was found guilty of planting a type of malware known as UNIX logic bombs in the network of investment bank UBS. The company claimed the resulting damage cost more than $3m (£1.5m).

  Prosecutors argued that Duronio had launched the attack when he received a bonus he felt was unreasonably low. He complained and eventually resigned from his job, but not without leaving behind a memorable parting gift.

  The best protection against this sort of attack is to monitor employees closely and be alert for disgruntled employees who might abuse their positions. In addition, experts advise immediately cancelling network access and passwords when employees leave the company, to avoid them using passwords to remotely access the network in future.

- **Social engineering**

  Perhaps one of the most common ways for attackers to gain access to a network is by exploiting the trusting nature of your employees. After all, why go to the trouble of creating a program to steal passwords from the network, if people will simply give out this information on the telephone?

"You can have the best technical systems in place, but they're not effective if people aren't educated about the risks," says Mike Maddison, head of security and privacy services at Deloitte UK. A recent survey conducted by Deloitte found three-quarters of companies have not trained staff in the risks of information leakage and social engineering.

"It's vital that people understand, for example, that they shouldn't provide their password over the telephone, or that they recognise a phishing email," says Toralv Dirro, a security strategist with McAfee. "These sorts of messages are becoming increasingly sophisticated, and we're now seeing very personalised, targeted phishing emails that may even refer to projects that people work on, or members of their team."

- **Downloading malicious internet contents**

Some reports suggest the average employee in a small business spends up to an hour a day surfing the web for personal use — perhaps looking at video or file-sharing websites, playing games or using social media websites such as Facebook.

It's not just time that this activity could cost you. Analyst reports show that the number of malware and virus threats is increasing by more than 50 percent each year, and many of these destructive payloads can be inadvertently introduced to the network by employees.

"It's very easy for a rootkit to be hidden in a game or a video clip, and a novice user may not notice anything out of the ordinary," warns Graham Titterington, a principal analyst with Ovum.

The best advice is to constantly update and patch your IT systems to ensure you are protected...

...against new threats as they emerge, advises Paul Vlissidis, a technical director with NCC Group. "Don't rely on monthly or quarterly security downloads," he says. "The time between vulnerabilities being discovered and then exploited is shrinking all the time, so it's important to update patches and antivirus software regularly, and ideally layer several antivirus products rather than using just one."

In addition, consider whether your antivirus software can filter, monitor and block video content: few products can do this today, but a video of someone falling over can provide a cover for downloading all sorts of content onto the network, says Bob Tarzey, a service director with analyst firm Quocirca.

- **Information leakage**

There are now a staggering number of ways that information can be taken from your computer networks and released outside the organisation. Whether it's an MP3 player, a CD-ROM, a digital camera or USB data stick, today's employees could easily take a significant chunk of your customer database out of the door in their back pocket.

"These types of devices are effectively very portable, very high-capacity hard drives," says Andy Kellett, a senior research analyst with Butler Group. "Someone can walk away with up to 60GB of data on a USB stick, so it's not a trivial matter."

Research conducted by Websense found that a quarter of UK workers who use PCs at work admit copying data onto mobile devices at least once a week. In addition, 40 percent say they use USB sticks to move data around, and a fifth have revealed their passwords to third parties.

Kellett advises companies to use software to specify policies on what devices can be connected to the corporate network, and what data can be downloaded. This should be enforced by the company — but workers should also be educated about why the policies are in place — or they will simply find a way to work around them. "It's not difficult to specify that the USB ports on desktop computers are disabled, or that CD-ROM drives are removed from computers where they aren't needed," Kellet says. "But you have to work with your employees to balance security and usability."

In addition, Kellett recommends considering whether to block access to web-based email and data-storage services, such as Gmail. "If someone can store confidential documents to an online storage site, that information is completely beyond your control," he says.

Finally, consider locking down networks to prevent wireless access using Bluetooth or Wi-Fi — except for authorised users with authorised devices. "Information loss over Bluetooth on an unsecured network is very difficult to detect indeed," says Kellett.

- **Illegal activities:**

  It's important to remember that, as an employer, you are responsible for pretty much anything your employees do using your computer network — unless you can show you have taken reasonable steps to prevent this. Famously, the US-based Citibank was sued for $2m (£1m) when employees downloaded pornography from the internet, and UK companies have dismissed workers for a range of misdeeds, from selling drugs using company email to distributing racially and sexually offensive material over corporate intranets.

  To protect yourself, expert advice a two-pronged approach. First, use monitoring software to check email and internet traffic for certain keywords or file types. You might also choose to block certain websites and applications completely.

  Second, devise an Acceptable Use Policy spelling out employees' responsibility for network security, ensure it's signed by everyone and that workers fully understand the risks and their responsibilities. According to software company Websense, one in five UK workers say they don't really understand their company's security policy.

- **Distributed Denial-of – Service (DDoS) attack**

  DDoS Attack means "Distributed Denial-of-Service (DDoS) Attack" and it is a cybercrime in which the attacker floods a server with internet traffic to prevent users from accessing connected online services and sites.

  Motivations for carrying out a DDoS vary widely, as do the types of individuals and organizations eager to perpetrate this form of cyberattack. Some attacks are carried out by disgruntled individuals and hacktivists wanting to take down a company's servers simply to make a statement, have fun by exploiting cyber weakness, or express disapproval.

Other distributed denial-of-service attacks are financially motivated, such as a competitor disrupting or shutting down another business's online operations to steal business away in the meantime. Others involve extortion, in which perpetrators attack a company and install hostageware or ransomware on their servers, then force them to pay a large financial sum for the damage to be reversed.

DDoS attacks are on the rise, and even some of the largest global companies are not immune to being "DDoS'ed". The largest attack in history occurred in February 2020 to none other than Amazon Web Services (AWS), overtaking an earlier attack on GitHub two years prior. DDoS ramifications include a drop in legitimate traffic, lost business, and reputation damage.

As the Internet of Things (IoT) continues to proliferate, as do the number of remote employees working from home, and so will the number of devices connected to a network. The security of each IoT device may not necessarily keep up, leaving the network to which it is connected vulnerable to attack. As such, the importance of DDoS protection and mitigation is crucial.

A DDoS attack aims to overwhelm the devices, services, and network of its intended target with fake internet traffic, rendering them inaccessible to or useless for legitimate users.

➢ Types of attack

Different attacks target different parts of a network, and they are classified according to the network connection layers they target. A connection on the internet is comprised of seven different “layers," as defined by the Open Systems Interconnection (OSI) model created by the International Organization for Standardization. The model allows different computer systems to be able to "talk" to each other.

Volume based or volumetric attacks

This type of attack aims to control all available bandwidth between the victim and the larger internet. Domain name system (DNS) amplification is an example of a volume-based attack. In this scenario, the attacker spoofs the target's address, then sends a DNS name lookup request to an open DNS server with the spoofed address.

When the DNS server sends the DNS record response, it is sent instead to the target, resulting in the target receiving an amplification of the attacker's initially small query.

Protocol attacks

Protocol attacks consume all available capacity of web servers or other resources, such as firewalls. They expose weaknesses in Layers 3 and 4 of the OSI protocol stack to render the target inaccessible.

A SYN flood is an example of a protocol attack, in which the attacker sends the target an overwhelming number of transmission control protocol (TCP) handshake requests with spoofed source Internet Protocol (IP) addresses. The targeted servers attempt to respond to each connection request, but the final handshake never occurs, overwhelming the target in the process.

Application layer attacks

These attacks also aim to exhaust or overwhelm the target's resources but are difficult to flag as malicious. Often referred to as a Layer 7 DDoS attack—referring to Layer 7 of the OSI model—an application-layer attack targets the layer where web pages are generated in response to Hypertext Transfer Protocol (HTTP) requests.

A server runs database queries to generate a web page. In this form of attack, the attacker forces the victim's server to handle more than it normally does. An HTTP flood is a type of application-layer attack and is similar to constantly refreshing a web browser on different computers all at once. In this manner, the excessive number of HTTP requests overwhelms the server, resulting in a DDoS.

➢ Prevention of DDoS attack

Even if you know what is a DDoS attack, It is extremely difficult to avoid attacks because detection is a challenge. This is because the symptoms of the attack may not very much from typical service issues, such as slow-loading web pages, and the level of sophistication and complexity of DDoS techniques continues to grow.

Further, many companies welcome a spike in internet traffic, especially if the company recently launched new products or services or announced market-moving news. As such, prevention is not always possible, so it is best for an organization to plan a response for when these attacks occur.

✓ Rogue security software

Rogue security software has more than doubled in the last decade. These malicious apps are designed to mimic antivirus programs but are actually a sinister malware scam. Once downloaded, they cause endless frustration and even trick users into making-payments.

As cybercriminals innovate, it's hard to tell legitimate anti-malware from money-grabbing scams. Learning the difference is crucial to avoid becoming the next victim of rogue security software.

➢ Features

Countless rogue antivirus programs exist, but most include similar features. Certain elements mimic other malware types, such as scareware and rootkits, which indicates that the software isn't legitimate.

Defining characteristics of rogue security software include:

Mimics Anti-malware

Most anti-malware performs scans, alerts you of threats, and allows you to resolve these issues. Rogue anti-malware mimics this except, instead of addressing the problem, it demands a payment.

Constant Alerts

Rogue security software encourages the user to act by flooding their desktop with endless messages about supposed threats. In reality, the only malware you have is the app itself.

Requires Extra Payments

Once the software has overwhelmed you with reports of infections, it prompts you to take action. However, instead of instantly deleting the files, it asks for a payment. Handing over the money might stop the alerts temporarily, but the cycle will just start again until another payment is required.

Modifies Actual Security Software

Like most rootkit infections, rogue security software can modify your antivirus. Cybercriminals don’t want you to know that their program is a fraud, so they put a chokehold on other apps that might alert you.

Freezes Entire Computer

This software may freeze your computer. Either it will create so many pop-ups that the system is overwhelmed, or crash your desktop entirely until a payment is made.

Rogue security software can take a while before users realize they’re victims. Knowing how to distinguish rogue programs from the real thing is essential to staying safe.

➢ Avoid downloading these software

Rogue antivirus software can be downloaded actively or passively, so it requires more vigilance than other malware. Develop these habits to avoid it.

Always read antivirus reviews carefully. Look at the negative responses first, as some companies hire people to write positive reviews. If there are any reports that the download is malware, look elsewhere.

- Use well-known security brands with years of industry experience. Internationally trusted companies, such as Norton and McAfee, won’t offer rogue software.
- Hackers are known to copy branding from reliable sources, so never download from unofficial vendors. Always visit the official site of a brand when buying or installing their products.
- Smart clicking should already be an everyday security practice, but it’s even more critical for security software. Standard rules apply; don’t open email

attachments from unknown senders, click on ads or pop-ups, or use shortened URLs.

- Regularly updating your software will reduce the chances of hackers installing the app via a security hole. These vulnerabilities are identified by software companies and patched when they provide updates.
- Most rogue apps use urgency to prompt users into clicking. They might claim you have a severe infection, say you've won a prize, or ask for an immediate update to your accounts. Ignore these scare tactics to reduce the risk of being tricked into a malicious download.
- Find a well-reviewed, high-quality security suite that can help identify rogue software before it's installed. The top choices will halt installations if they note any threats.

We never think our security software could be a threat. Unfortunately, hackers play on this false sense of security with rogue software. Many people have never even heard of this threat, which makes it even more deadly.

If you're adequately informed, it's easy to protect yourself from rogue threats. Follow smart guidelines to reduce the risk of infection, and find a security solution that you can genuinely trust.

✓ Malware

Malware (short for "malicious software") is a file or code, typically delivered over a network, that infects, explores, steals or conducts virtually any behavior an attacker wants. And because malware comes in so many variants, there are numerous methods to infect computer systems. Though varied in type and capabilities, malware usually has one of the following objectives:

- Provide remote control for an attacker to use an infected machine.
- Send spam from the infected machine to unsuspecting targets.
- Investigate the infected user's local network.
- Steal sensitive data.

- **Types of Malware**

Malware is an inclusive term for all types of malicious software. Malware examples, malware attack definitions and methods for spreading malware include:

Adware – While some forms of adware may be considered legitimate, others make unauthorized access to computer systems and greatly disrupt users.

Botnets

Short for "robot network," these are networks of infected computers under the control of single attacking parties using command-and-control servers. Botnets are highly versatile and adaptable, able to maintain resilience through redundant servers and by using infected computers to relay traffic. Botnets are often the armies behind today's distributed denial-of-service (DDoS) attacks.

Cryptojacking – is malicious cryptomining (the process of using computing power to verify transactions on a blockchain network and earning cryptocurrency for providing that service) that happens when cybercriminals hack into both business and personal computers, laptops, and mobile devices to install software.

Malvertising – Malvertising is a portmanteau of "malware + advertising" describing the practice of online advertising to spread malware. It typically involves injecting malicious code or malware-laden advertisements into legitimate online advertising networks and webpages.

Polymorphic malware – Any of the above types of malware with the capacity to "morph" regularly, altering the appearance of the code while retaining the algorithm within. The alteration of the surface appearance of the software subverts detection via traditional virus signatures.

Ransomware – Is a criminal business model that uses malicious software to hold valuable files, data or information for ransom. Victims of a ransomware attack may have their operations severely degraded or shut down entirely.

Remote Administration Tools (RATs) – Software that allows a remote operator to control a system. These tools were originally built for legitimate use, but are now used by threat actors. RATs enable administrative control, allowing an attacker to do almost anything on an infected computer. They are difficult to detect, as they don't typically show up in lists of running programs or tasks, and their actions are often mistaken for the actions of legitimate programs.

Rootkits – Programs that provide privileged (root-level) access to a computer. Rootkits vary and hide themselves in the operating system.

Spyware – Malware that collects information about the usage of the infected computer and communicates it back to the attacker. The term includes botnets, adware, backdoor behavior, keyloggers, data theft and net-worms.

Trojans Malware – Malware disguised in what appears to be legitimate software. Once activated, malware Trojans will conduct whatever action they have been programmed to carry out. Unlike viruses and worms, Trojans do not replicate or reproduce through infection. "Trojan" alludes to the mythological story of Greek soldiers hidden inside a wooden horse that was given to the enemy city of Troy.

Virus Malware – Programs that copy themselves throughout a computer or network. Malware viruses piggyback on existing programs and can only be activated when a user opens the program. At their worst, viruses can corrupt or delete data, use the user's email to spread, or erase everything on a hard disk.

Worm Malware – Self-replicating viruses that exploit security vulnerabilities to automatically spread themselves across computers and networks. Unlike many viruses, malware worms do not attach to existing programs or alter files. They typically go unnoticed until replication reaches a scale that consumes significant system resources or network bandwidth.

➢ Types of Malware Attacks

Malware also uses a variety of methods to spread itself to other computer systems beyond an initial attack vector. Malware attack definitions can include:

- Email attachments containing malicious code can be opened, and therefore executed by unsuspecting users. If those emails are forwarded, the malware can spread even deeper into an organization, further compromising a network.

- File servers, such as those based on common Internet file system (SMB/CIFS) and network file system (NFS), can enable malware to spread quickly as users access and download infected files.
- File-sharing software can allow malware to replicate itself onto removable media and then on to computer systems and networks.
- Peer to peer (P2P) file sharing can introduce malware by sharing files as seemingly harmless as music or pictures.
- Remotely exploitable vulnerabilities can enable a hacker to access systems regardless of geographic location with little or no need for involvement by a computer user.

Learn how to use Palo Alto Networks next-generation threat prevention features and WildFire® cloud-based threat analysis service to protect your network from all types of malware, both known and unknown.

How to Prevent Malware

A variety of security solutions are used to detect and prevent malware. These include firewalls, next-generation firewalls, network intrusion prevention systems (IPS), deep packet inspection (DPI) capabilities, unified threat management systems, antivirus and anti-spam gateways, virtual private networks, content filtering and data leak prevention systems. In order to prevent malware, all security solutions should be tested using a wide range of malware-based attacks to ensure they are working properly. A robust, up-to-date library of malware signatures must be used to ensure testing is completed against the latest attacks

The Cortex XDR agent combines multiple methods of prevention at critical phases within the attack lifecycle to halt the execution of malicious programs and stop the exploitation of legitimate applications, regardless of operating system, the endpoint’s online or offline status, and whether it is connected to an organization’s network or roaming. Because the Cortex XDR agent does not depend on signatures, it can prevent zero-day malware and unknown exploits through a combination of prevention methods.

- **Malware Detection**

  Advanced malware analysis and detection tools exist such as firewalls, Intrusion Prevention Systems (IPS), and sandboxing solutions. Some malware types are easier to detect, such as ransomware, which makes itself known immediately upon encrypting your files. Other malware like spyware, may remain on a target system silently to allow an adversary to maintain access to the system. Regardless of the malware type or malware meaning, its detectability or the person deploying it, the intent of malware use is always malicious.

  When you enable behavioral threat protection in your endpoint security policy, the Cortex XDR agent can also continuously monitor endpoint activity for malicious event chains identified by Palo Alto Networks.

- **Malware Removal**

  Antivirus software can remove most standard infection types and many options exist for off-the-shelf solutions. Cortex XDR enables remediation on the endpoint following an alert or investigation giving administrators the option to begin a variety of mitigation steps starting with isolating endpoints by disabling all network access on compromised endpoints except for traffic to the Cortex XDR console, terminating processes to stop any running malware from continuing to perform malicious activity on the endpoint, and blocking additional executions, before quarantining malicious files and removing them from their working directories if the Cortex XDR agent has not already done so.

- **Malware Protection**

  To protect your organization against malware, you need a holistic, enterprise-wide malware protection strategy. Commodity threats are exploits that are less sophisticated and more easily detected and prevented using a combination of antivirus, anti-spyware, and vulnerability protection features along with URL filtering and Application identification capabilities on the firewall.

- ✓ **Ransomware**

Ransomware is a malware designed to deny a user or organization access to files on their computer. By encrypting these files and demanding a ransom payment for the decryption key, cyberattackers place organizations in a position where paying the ransom is the easiest and cheapest way to regain access to their files. Some variants have added additional functionality – such as data theft – to provide further incentive for ransomware victims to pay the ransom.

Ransomware has quickly become the most prominent and visible type of malware. Recent Ransomware attacks have impacted hospitals' ability to provide crucial services, crippled public services in cities, and caused significant damage to various organizations.

- ➢ **Ransomware variants**

Dozens of ransomware variants exist, each with its own unique characteristics. However, some ransomware groups have been more prolific and successful than others, making them stand out from the crowd.

Ryuk

Ryuk is an example of a very targeted ransomware variant. It is commonly delivered via spear phishing emails or by using compromised user credentials to log into enterprise systems using the Remote Desktop Protocol (RDP). Once a system is infected, Ryuk encrypts certain types of files (avoiding those crucial to a computer's operation), then presents a ransom demand.

Ryuk is well-known as one of the most expensive types of ransomware in existence. Ryuk demands ransoms that average over $1 million. As a result, the cybercriminals behind Ryuk primarily focus on enterprises that have the resources necessary to meet their demands.

Maze

The Maze ransomware is famous for being the first ransomware variant to combine file encryption and data theft. When targets started refusing to pay ransoms, Maze began collecting sensitive data from victims' computers before encrypting it. If the ransom demands were not met, this data would be publicly exposed or sold to the highest bidder. The potential for an expensive data breach was used as additional incentive to pay up.

The group behind the Maze ransomware has officially ended its operations. However, this does not mean that the threat of ransomware has been reduced. Some Maze affiliates have transitioned to using the Egregor ransomware, and the Egregor, Maze, and Sekhmet variants are believed to have a common source.

REvil (Sodinokibi)

The REvil group (also known as Sodinokibi) is another ransomware variant that targets large organizations.

REvil is one of the most well-known ransomware families on the net. The ransomware group, which has been operated by the Russian-speaking REvil group since 2019, has been responsible for many big breaches such as 'Kaseya' and 'JBS'

It has competed with Ryuk over the last several years for the title of the most expensive ransomware variant. REvil is known to have demanded $800,000 ransom payments.

While REvil began as a traditional ransomware variant, it has evolved over time- They are using the Double Extortion technique- to steal data from businesses while also encrypting the files. This means that, in addition to demanding a ransom to decrypt data, attackers might threaten to release the stolen data if a second payment is not made.

Lockbit

LockBit is a data encryption malware in operation since September 2019 and a recent Ransomware-as-a-Service (RaaS). This piece of ransomware was developed to encrypt large organizations rapidly as a way of preventing its detection quickly by security appliances and IT/SOC teams.

DearCry

In March 2021, Microsoft released patches for four vulnerabilities within Microsoft Exchange servers. DearCry is a new ransomware variant designed to take advantage of four recently disclosed vulnerabilities in Microsoft Exchange

The DearCry ransomware encrypts certain types of files. Once the encryption is finished, DearCry will show a ransom message instructing users to send an email to the ransomware operators in order to learn how to decrypt their files.

Lapsus$

Lapsus$ is a South American ransomware gang that has been linked to cyberattacks on some high-profile targets. The cyber gang is known for extortion, threatening the release of sensitive information, if demands by its victims aren't made. The group has boasted breaking into Nvidia, Samsung, Ubisoft and others. The group uses stolen source code to disguise malware files as trustworthy.

- **Working process**

In order to be successful, ransomware needs to gain access to a target system, encrypt the files there, and demand a ransom from the victim. While the implementation details vary from one ransomware variant to another, all share the same core three stages

Step-1:

Infection and Distribution Vectors

Ransomware, like any malware, can gain access to an organization's systems in a number of different ways. However, ransomware operators tend to prefer a few specific infection vectors.

One of these is phishing emails. A malicious email may contain a link to a website hosting a malicious download or an attachment that has downloader functionality built in. If the email recipient falls for the phish, then the ransomware is downloaded and executed on their computer.

Another popular ransomware infection vector takes advantage of services such as the Remote Desktop Protocol (RDP). With RDP, an attacker who has stolen or guessed an employee's login credentials can use them to authenticate to and remotely access a computer within the enterprise network. With this access, the attacker can directly download the malware and execute it on the machine under their control.

Others may attempt to infect systems directly, like how WannaCry exploited the EternalBlue vulnerability. Most ransomware variants have multiple infection vectors.

Step-2:

Data Encryption

After ransomware has gained access to a system, it can begin encrypting its files. Since encryption functionality is built into an operating system, this simply involves accessing files, encrypting them with an attacker-controlled key, and replacing the originals with the encrypted versions. Most ransomware variants are cautious in their selection of files to encrypt to ensure system stability. Some variants will also take steps to delete backup and shadow copies of files to make recovery without the decryption key more difficult.

Step-3:

Ransom Demand

Once file encryption is complete, the ransomware is prepared to make a ransom demand. Different ransomware variants implement this in numerous ways, but it is not uncommon to have a display background changed to a ransom note or text files placed in each encrypted directory containing the ransom note. Typically, these notes demand a set amount of cryptocurrency in exchange for access to the victim's files. If the ransom is paid, the ransomware operator will either provide a copy of the private key used to protect the symmetric encryption key or a copy of the symmetric encryption key itself. This information can be entered into a decryptor program (also provided by the cybercriminal) that can use it to reverse the encryption and restore access to the user's files.

While these three core steps exist in all ransomware variants, different ransomware can include different implementations or additional steps. For example, ransomware variants like Maze perform files scanning, registry information, and data theft before data encryption, and the WannaCry ransomware scans for other vulnerable devices to infect and encrypt.

Protection

Proper preparation can dramatically decrease the cost and impact of a ransomware attack. Taking the following best practices can reduce an organization's exposure to ransomware and minimize its impacts:

- **Cyber Awareness Training and Education:** Ransomware is often spread using phishing emails. Training users on how to identify and avoid potential ransomware attacks is crucial. As many of the current cyber-attacks start with a targeted email that does not even contain malware, but only a socially-engineered message that encourages the user to click on a malicious link, user education is often considered as one of the most important defenses an organization can deploy.

- **Continuous data backups:** Ransomware's definition says that it is malware designed to make it so that paying a ransom is the only way to restore access to the encrypted data. Automated, protected data backups enable an organization to recover from an attack with a minimum of data loss and without paying a ransom. Maintaining regular backups of data as a routine process is a very important practice to prevent losing data, and to be able to recover it in the event of corruption or disk hardware malfunction. Functional backups can also help organizations to recover from ransomware attacks.

- **Patching:** Patching is a critical component in defending against ransomware attacks as cyber-criminals will often look for the latest uncovered exploits in the patches made available and then target systems that are not yet patched. As such, it is critical that organizations ensure that all systems have the latest patches applied to them, as this reduces the number of potential vulnerabilities within the business for an attacker to exploit.

- **User Authentication:** Accessing services like RDP with stolen user credentials is a favorite technique of ransomware attackers. The use of strong user authentication can make it harder for an attacker to make use of a guessed or stolen password

✓ Phishing attacks

Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message. The recipient is then tricked into clicking a malicious link, which can lead to the installation of malware, the freezing of the system as part of a ransomware attack or the revealing of sensitive information.

An attack can have devastating results. For individuals, this includes unauthorized purchases, the stealing of funds, or identify theft.

Moreover, phishing is often used to gain a foothold in corporate or governmental networks as a part of a larger attack, such as an advanced persistent threat (APT) event. In this latter scenario, employees are compromised in order to bypass security perimeters, distribute malware inside a closed environment, or gain privileged access to secured data.

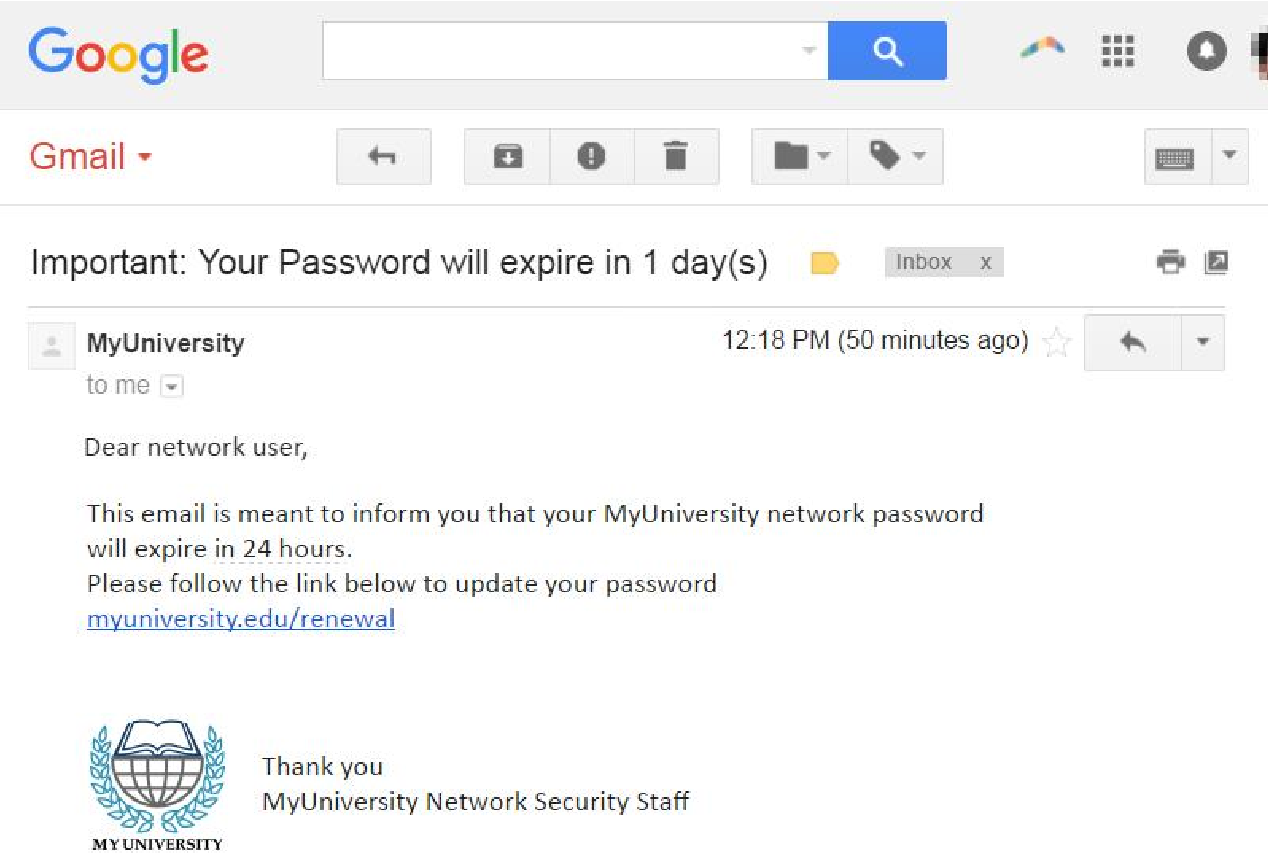
An organization succumbing to such an attack typically sustains severe financial losses in addition to declining market share, reputation, and consumer trust. Depending on scope, a phishing attempt might escalate into a security incident from which a business will have a difficult time recovering.

➢ Example

The following illustrates a common phishing scam attempt:

A spoofed email ostensibly from myuniversity.edu is mass-distributed to as many faculty members as possible.

The email claims that the user's password is about to expire. Instructions are given to go to myuniversity.edu/renewal to renew their password within 24 hours.



Important: Your Password will expire in 1 day(s)

MyUniversity

to me

12:18 PM (50 minutes ago)

Dear network user,

This email is meant to inform you that your MyUniversity network password will expire in 24 hours.
Please follow the link below to update your password
myuniversity.edu/renewal

Thank you
MyUniversity Network Security Staff

Several things can occur by clicking the link. For example:

The user is redirected to myuniversity.edurenewal.com, a bogus page appearing exactly like the real renewal page, where both new and existing passwords are requested. The attacker, monitoring the page, hijacks the original password to gain access to secured areas on the university network.

The user is sent to the actual password renewal page. However, while being redirected, a malicious script activates in the background to hijack the user's session cookie. This results in a reflected XSS attack, giving the perpetrator privileged access to the university network.

- **Phishing technique**

Email phishing scams

Email phishing is a numbers game. An attacker sending out thousands of fraudulent messages can net significant information and sums of money, even if only a small percentage of recipients fall for the scam. As seen above, there are some techniques attackers use to increase their success rates.

For one, they will go to great lengths in designing phishing messages to mimic actual emails from a spoofed organization. Using the same phrasing, typefaces, logos, and signatures makes the messages appear legitimate.

In addition, attackers will usually try to push users into action by creating a sense of urgency. For example, as previously shown, an email could threaten account expiration and place the recipient on a timer. Applying such pressure causes the user to be less diligent and more prone to error.

Lastly, links inside messages resemble their legitimate counterparts, but typically have a misspelled domain name or extra subdomains. In the above example, the myuniversity.edu/renewal URL was changed to myuniversity.edurenewal.com. Similarities between the two addresses offer the impression of a secure link, making the recipient less aware that an attack is taking place.

Spear phishing

Spear phishing targets a specific person or enterprise, as opposed to random application users. It's a more in-depth version of phishing that requires special knowledge about an organization, including its power structure.

An attack might play out as follows:

A perpetrator researches names of employees within an organization's marketing department and gains access to the latest project invoices.

Posing as the marketing director, the attacker emails a departmental project manager (PM) using a subject line that reads, Updated invoice for Q3 campaigns. The text, style, and included logo duplicate the organization’s standard email template.

A link in the email redirects to a password-protected internal document, which is in actuality a spoofed version of a stolen invoice.

The PM is requested to log in to view the document. The attacker steals his credentials, gaining full access to sensitive areas within the organization’s network.

By providing an attacker with valid login credentials, spear phishing is an effective method for executing the first stage of an APT.

- **Prevention**

Phishing attack protection requires steps be taken by both users and enterprises.

For users, vigilance is key. A spoofed message often contains subtle mistakes that expose its true identity. These can include spelling mistakes or changes to domain names, as seen in the earlier URL example. Users should also stop and think about why they’re even receiving such an email.

For enterprises, a number of steps can be taken to mitigate both phishing and spear phishing attacks:

- Two-factor authentication (2FA) is the most effective method for countering phishing attacks, as it adds an extra verification layer when logging in to sensitive applications. 2FA relies on users having two things: something they know, such as a password and user name, and something they have, such as their smartphones. Even when employees are compromised, 2FA prevents the use of their compromised credentials, since these alone are insufficient to gain entry.

- In addition to using 2FA, organizations should enforce strict password management policies. For example, employees should be required to frequently change their passwords and to not be allowed to reuse a password for multiple applications.

- Educational campaigns can also help diminish the threat of phishing attacks by enforcing secure practices, such as not clicking on external email links.

✓ Viruses

A computer virus is a malicious piece of computer code designed to spread from device to device. A subset of malware, these self-copying threats are usually designed to damage a device or steal data.

Think of a biological virus – the kind that makes you sick. It's persistently nasty, keeps you from functioning normally, and often requires something powerful to get rid of it. A computer virus is very similar. Designed to replicate relentlessly, computer viruses infect your programs and files, alter the way your computer operates or stop it from working altogether.

➢ How a computer get affected

Even if you're careful, you can pick up computer viruses through normal Web activities like:

1. Sharing music, files, or photos with other users
2. Visiting an infected website
3. Opening spam email or an email attachment
4. Downloading free games, toolbars, media players and other system utilities
5. Installing mainstream software applications without thoroughly reading license agreements

➢ How computer virus spread

Viruses can be spread several ways, including via networks, discs, email attachments or external storage devices like USB sticks. Since connections between devices were once far more limited than today, early computer viruses were commonly spread through infected floppy disks.

Today, links between internet-enabled devices are for common, providing ample opportunities for viruses to spread. According to the U.S. Cybersecurity and Infrastructure Security Agency, infected email attachments are the most common means of circulating computer viruses. Most, but not all, computer viruses require a user to take some form of action, like enabling "macros" or clicking a link, to spread.

Symptoms of virus attack

Your computer may be infected if you recognize any of these malware symptoms:

- Slow computer performance
- Erratic computer behavior
- Unexplained data loss
- Frequent computer crashes

How can be removed

Antiviruses have made great progress in being able to identify and prevent the spread of computer viruses. When a device does become infected, though, installing an antivirus solution is still your best bet for removing it. Once installed, most software will conduct a "scan" for the malicious program. Once located, the antivirus will present options for its removal. If this is not something that can be done automatically, some security vendors offer a technician's assistance in removing the virus free of charge.

Protection

When you arm yourself with information and resources, you're wiser about computer security threats and less vulnerable to threat tactics. Take these steps to safeguard your PC with the best computer virus protection:

- Use antivirus protection and a firewall
- Get antispyware software
- Always keep your antivirus protection and antispyware software up-to-date
- Update your operating system regularly
- Increase your browser security settings
- Avoid questionable Websites
- Only download software from sites you trust.
- Carefully evaluate free software and file-sharing applications before downloading them.
- Don't open messages from unknown senders
- Immediately delete messages you suspect to be spam

An unprotected computer is like an open door for computer viruses. Firewalls monitor Internet traffic in and out of your computer and hide your PC from online scammers looking for easy targets. Products like Webroot Internet Security Complete and Webroot Antivirus provide complete protection from the two most dangerous threats on the Internet – spyware and computer viruses. They prevent viruses from entering your computer, stand guard at every possible entrance of your computer and fend off any computer virus that tries to open, even the most damaging and devious strains.

While free antivirus downloads are available, they just can't offer the computer virus help you need to keep up with the continuous onslaught of new strains. Previously undetected forms of polymorphic malware can often do the most damage, so it’s critical to have up-to-the-minute, guaranteed antivirus protection.

Comparison between Distance vector routing and Routing Information Protocol (RIP)

Most routing protocols fall into one of two classes: distance vector or link state. The basics of distance vector routing protocols are examined here; the next section covers link state routing protocols. Distance vector algorithms are based on the work done of R. E. Bellman,1 L. R. Ford, and D. R. Fulkerson2 and for this reason occasionally are referred to as Bellman-Ford or Ford-Fulkerson algorithms.

The name distance vector is derived from the fact that routes are advertised as vectors of (distance, direction), where distance is defined in terms of a metric and direction is defined in terms of the next-hop router. For example, "Destination A is a distance of 5 hops away, in the direction of next-hop router X." As that statement implies, each router learns routes from its neighboring routers' perspectives and then advertises the routes from its own perspective. Because each router depends on its neighbors for information, which the neighbors in turn may have learned from their neighbors, and so on, distance vector routing is sometimes facetiously referred to as "routing by rumor."

Distance vector routing protocols include the following:

- Routing Information Protocol (RIP) for IP
- Xerox Networking System's XNS RIP
- Novell's IPX RIP
- Cisco's Internet Gateway Routing Protocol (IGRP)
- DEC's DNA Phase IV
- AppleTalk's Routing Table Maintenance Protocol (RTMP)

Common Characteristics of DVR:

A typical distance vector routing protocol uses a routing algorithm in which routers periodically send routing updates to all neighbors by broadcasting their entire route tables.

The preceding statement contains a lot of information. Following sections consider it in more detail.

Periodic Updates

Periodic updates means that at the end of a certain time period, updates will be transmitted. This period typically ranges from 10 seconds for AppleTalk's RTMP to 90 seconds for Cisco's IGRP. At issue here is the fact that if updates are sent too frequently, congestion may occur; if updates are sent too infrequently, convergence time may be unacceptably high.

- **Neighbors**

  In the context of routers, neighbors always means routers sharing a common data link. A distance vector routing protocol sends its updates to neighboring routers4 and depends on them to pass the update information along to their neighbors. For this reason, distance vector routing is said to use hop-by-hop updates.

- **Broadcast Updates**

  When a router first becomes active on a network, how does it find other routers and how does it announce its own presence? Several methods are available. The simplest is to send the updates to the broadcast address (in the case of IP, 255.255.255.255). Neighboring routers speaking the same routing protocol will hear the broadcasts and take appropriate action. Hosts and other devices uninterested in the routing updates will simply drop the packets.

- **Full Routing Table Updates**

  Most distance vector routing protocols take the very simple approach of telling their neighbors everything they know by broadcasting their entire route table, with some exceptions that are covered in following sections. Neighbors receiving these updates glean the information they need and discard everything else.

So DVR includes the RIP (Routing information protocol). Basically, RIP is not different from DVR. It is a part of distance vector routing. Let's discuss about RIP.

Routing Information Protocol (RIP) is a dynamic routing protocol that uses hop count as a routing metric to find the best path between the source and the destination network. It is a distance-vector routing protocol that has an AD value of 120 and works on the Network layer of the OSI model. RIP uses port number 520.

Hop Count

Hop count is the number of routers occurring in between the source and destination network. The path with the lowest hop count is considered as the best route to reach a network and therefore placed in the routing table. RIP prevents routing loops by limiting the number of hops allowed in a path from source and destination. The maximum hop count allowed for RIP is 15 and a hop count of 16 is considered as network unreachable.

Features of RIP

RIP uses a modified hop count as a way to determine network distance. Modified reflects the fact that network engineers can assign paths a higher cost. By default, if a router's neighbor owns a destination network and can deliver packets directly to the destination network without using any other routers, that route has one hop. In network management terminology, this is described as a cost of one.

RIP allows only 15 hops in a path. If a packet can't reach a destination in 15 hops, the destination is considered unreachable. Paths can be assigned a higher cost (as if they involved extra hops) if the enterprise wants to limit or discourage their use. For example, a satellite backup link might be assigned a cost of 10 to force traffic to follow other routes when available.

Advantages

- Feasible configuration
- Easy to understand
- Predominantly loop free
- Guaranteed to support almost all routers
- Promotes load balancing

Additionally, RIP is preferred over static routes due to its simple configuration and the fact that it does not require an update every time the topology changes. Unfortunately, the disadvantage of RIP is its increased network and processing overhead when compared to static routing.

Other disadvantages include:

- Not always loop free
- Only equal-cost load balancing is supported
- Pinhole congestion can occur
- Bandwidth intensive and inefficient
- Large networks lead to slow convergence

Limitations

While utilizing RIP, users may run into various limitations. For example, the Routing Information Protocol results in increased network traffic due to the checks and updates it performs on neighboring routers every 30 seconds. Furthermore, since RIP only updates neighboring routers, updates for non-neighboring routers can be forgotten since the information is not immediately accessible.

Another limitation of RIP is the enforcement of a maximum hop count of 15. As a result, remote routers in large networks may not be able to be accessed or reached. Furthermore, the closest path may not be the shortest path. This is because RIP does not take various factors into consideration when calculating the shortest path.

How to avoid man- in- the- middle attack

Man-in-the-middle attacks (MITM) are a common type of cyber security attack that allows attackers to eavesdrop on the communication between two targets. The attack takes place in between two legitimately communicating hosts, allowing the attacker to “listen” to a conversation they should normally not be able to listen to, hence the name “man-in-the-middle.”

Here’s an analogy: Alice and Bob are having a conversation; Eve wants to eavesdrop on the conversation but also remain transparent. Eve could tell Alice that she was Bob and tell Bob that she was Alice. This would lead Alice to believe she's speaking to Bob, while actually revealing her part of the conversation to Eve. Eve could then gather information from this, alter the response, and pass the message along to Bob (who thinks he's talking to Alice). As a result, Eve is able to transparently hijack their conversation.

- **Avoid technique:**

  Strong WEP/WAP Encryption on Access Points

  Having a strong encryption mechanism on wireless access points prevents unwanted users from joining your network just by being nearby. A weak encryption mechanism can allow an attacker to brute-force his way into a network and begin man-in-the-middle attacking. The stronger the encryption implementation, the safer.

  Strong Router Login Credentials

  It's essential to make sure your default router login is changed. Not just your Wi-Fi password, but your router login credentials. If an attacker finds your router login credentials, they can change your DNS servers to their malicious servers. Or even worse, infect your router with malicious software.

  Virtual Private Network

  VPNs can be used to create a secure environment for sensitive information within a local area network. They use key-based encryption to create a subnet for secure communication. This way, even if an attacker happens to get on a network that is shared, he will not be able to decipher the traffic in the VPN.

  Force HTTPS

  HTTPS can be used to securely communicate over HTTP using public-private key exchange. This prevents an attacker from having any use of the data he may be sniffing. Websites should only use HTTPS and not provide HTTP alternatives. Users can install browser plugins to enforce always using HTTPS on requests.

  Public Key Pair Based Authentication

  Man-in-the-middle attacks typically involve spoofing something or another. Public key pair based authentication like RSA can be used in various layers of the stack to help ensure whether the things you are communicating with are actually the things you want to be communicating with.