**Sure trust organization**

**Domain : Cyber security**

**Trainer : Mr. Himaneesh sir**

**Done by :**

**K.SAI JAYANTH**

**Definition of Ransomware:**

Ransomware is a type of malicious software (malware) that aims to encrypt files or lock computer systems and make them inaccessible to users. The perpetrators then demand payment, usually in cryptocurrencies such as Bitcoin, in return for restoring access or providing a decryption key. Ransomware attacks can target individuals, companies, or even entire networks, often with the aim of extorting victims.

**How ransomware works**:

**Delivery:** Ransomware is usually distributed via phishing emails, malicious attachments, or infected websites. Cybercriminals use social engineering techniques to trick users into clicking on links or downloading malicious files.

**Infiltration:** Once the user interacts with the malicious content, the ransomware gets activated and starts infiltrating the system. Some advanced ransomware strains can exploit software vulnerabilities to gain access.

**Encryption:** Ransomware encrypts files on the infected system, making them inaccessible. It uses strong encryption algorithms that are difficult to crack without the decryption key in attackers' possession.

**Ransom notes:** After encryption, a ransom note is usually displayed on the victim's screen. This notice informs the user that their files are encrypted, provides instructions on how to pay the ransom, and includes a deadline. The notice often warns against attempting to recover files without paying.

**Ransom payment:** Cybercriminals often demand payments in cryptocurrencies to make transactions more difficult to trace. Victims are instructed to send the ransom to a specific wallet address. Payment does not always guarantee that attackers will provide the decryption key or fully restore access.

**Propagation:**  In some cases, ransomware is designed to spread laterally across networks, infecting other connected systems. This can lead to more widespread damage and increase the ransom demands for larger organizations.

**Multiplication:** In some cases, ransomware is designed to spread laterally across networks and infect other connected systems. This can cause greater damage and increase ransom demands for larger organizations.

**Avoid detection:** Some ransomware variants use tactics to evade detection by security software, such as: B. the use of encryption techniques, changing their code or storing them in memory instead of on the hard drive.

**Development:** Ransomware tactics evolve over time as cybercriminals adapt to security measures. These include the use of more sophisticated encryption methods, evasion techniques, and sometimes even double extortion, where attackers threaten to reveal sensitive data if the ransom is not paid.

**Prevention and damage control:** prevention and mitigation strategies include regular data backups, updating software, implementing strict security practices, using trusted antivirus software, and educating users about the risks of phishing and suspicious links. Regularly updating and patching software is essential to close vulnerabilities that can be exploited by ransomware.

Some of the biggest ransomware attacks in history are listed below as:

1. ExPetr / NotPetya

* Type of Attack: Ransomware (A wiper exploiting an SMB vulnerability)
* Year: 2017 Attackers: Likely Russian-sponsored threat actors Target
* Company: Various, but severely impacted Maersk and Merck
* Monetary Impact: Estimated $10 billion

2. WannaCry

* Type of Attack: Ransomware (vulnerability in SMB protocol)
* Year: 2017
* Attackers: Believed to be the Lazarus Group
* Target Company: Multiple (global attack); Microsoft Windows users
* Monetary Impact: Estimated $4 billion.

3. Gand Crab

* Type of Attack: Ransomware-as-a-service (RaaS) (phishing, exploit kits)
* Year: 2018-2019 Attackers: Unknown, operators announced
* 'retirement' in 2019 Target Company: Various, including businesses and individuals (PCs using MS Windows)
* Monetary Impact: Estimated to have extorted over $2 billion from victims

4.Locky

* Type of Attack: Ransomware (phishing emails distributing a macro in a Word document)
* Year: 2016 - 2018 Attackers: Unknown, possibly the Dridex hackers (aka Evil Corp or TA505)
* Target Company: Various (predominantly healthcare providers in the US, Canada, France, Japan, Korea, and Thailand)
* Monetary Impact: Estimated at $1 billion.

5.Ryuk

* Type of Attack: Ransomware (initial compromise, usually Trick Bot infection)
* Year: 2018-present Attackers: Unclear, possibly various groups using the Ryuk malware or Wizard Spider (Russia)
* Target Company: Various, mostly healthcare and municipalities.
* Monetary Impact: Some sources claim they've made over $150 million; individual ransom demands reported from 15 to 500 Bitcoin.

**WANNACRY RANSOMWARE ATTACK**

The WannaCry ransomware attack, which occurred in May 2017, was a global cybersecurity incident that affected hundreds of thousands of computers in more than 150 countries. The attack targeted computers running Microsoft Windows operating systems, encrypting their files and demanding a ransom payment in Bitcoin for their release. Here's a detailed explanation of the WannaCry attack:

**1. Spread:** WannaCry exploited a vulnerability in the Microsoft Windows operating system called Eternal Blue. This vulnerability was part of the Windows Server Message Blocking (SMB) protocol. The Eternal Blue exploit was developed by the USA National Security Agency (NSA) but was leaked by a group called Shadow Brokers. The exploit allowed the malware to spread quickly across networks.

Worm-like Behaviour: WannaCry had worm-like abilities that allowed it to automatically spread within a network. Once a system was infected, the malware attempted to spread to other vulnerable systems by scanning and exploiting the same SMB vulnerability.

**2.Encryption and Ransom:** WannaCry encrypted files on infected computers and made them inaccessible to users. The encryption used in WannaCry was based on the AES (Advanced Encryption Standard) algorithm.

Ransom note: After encrypting the files, the ransomware displayed a ransom note on the desktop of the infected computer. The note demanded a ransom payment in Bitcoin and threatened to permanently delete the decryption key if the payment was not made within a certain period.

**3.Impact:** The rapid spread of WannaCry had a global impact, affecting organizations in various sectors, including healthcare, finance, telecommunications and government agencies. Critical infrastructure disruption: Some of the most severe impacts have been seen in organizations operating critical infrastructure, such as the National Health Service (NHS) in the United Kingdom. Hospitals and health centres had to divert resources to deal with the attack, causing disruptions in patient care**.**

**4. Answer and solution:** Microsoft had released a security patch (MS17-010) to fix the SMB vulnerability two months before the WannaCry attack. Organizations that installed the patch were not vulnerable to the exploit. However, many organizations were slow to roll out updates, leading to widespread infections. Kill Switch Discovery: A security researcher named Marcus Hutchins accidentally discovered a “kill switch” in the malware code. By registering a specific domain named in the ransomware code, he was able to stop the spread of WannaCry. This discovery gave companies time to deploy patches and resolve infections.

**5. Findings:** The WannaCry attack demonstrated the importance of quickly applying security patches to software systems. Many infected systems were running outdated and unpatched versions of the Windows operating system. Global Collaboration: The incident highlighted the need for global cybersecurity collaboration. This raised awareness of the potential of cyber tools developed by nation states for use in criminal activities.

Following the WannaCry attack, there was an increased focus on cybersecurity best practices, collaboration between researchers and security organizations, and efforts to improve overall cyber resilience. The incident was a wake-up call for many companies to prioritize cybersecurity and regularly update and patch their systems to defend against new threats.

**GandCrab ransomware attack**

**Introduction to GandCrab**: GandCrab is a notorious ransomware strain that emerged in early 2018. Known for its Ransomware-as-a-Service (RaaS) model, it has been one of the most widespread and constantly evolving threats in the cyber landscape.

**1. Initial infection vector :** GandCrab was primarily distributed via phishing emails and exploit kits. Cybercriminals used social engineering techniques to trick users into opening malicious attachments or clicking on infected links. The ransomware payload was often hidden in seemingly innocuous files or documents.

**2. Exploitation of software vulnerabilities:** In some cases, GandCrab exploited software vulnerabilities to gain access to systems. Exploits that target vulnerabilities in software or operating systems, if not addressed quickly, provide an entry point for ransomware.

**3. Encryption method:** After a successful infiltration, GandCrab encrypted files on the victim's system using a combination of RSA and Salsa20 algorithms. It targeted a wide range of file types and made them inaccessible to the user. The ransomware then displayed a ransom note and demanded payment in cryptocurrencies, usually Dash or Bitcoin, in exchange for the decryption key.

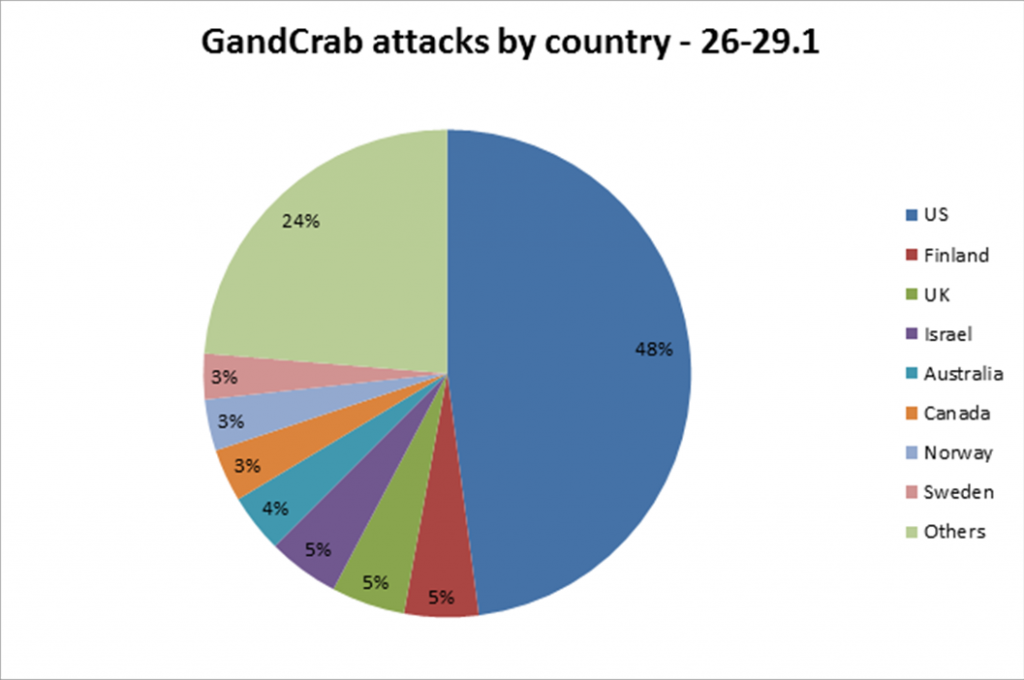
**4.Further development and version updates**: GandCrab has undergone several version updates, with each iteration bringing improvements in evasion techniques and encryption algorithms. The threat actors behind GandCrab have continually adapted security measures, making it difficult for cybersecurity experts to develop universal decryption tools.

**5. Monetization through ransom payments:** victims were redirected to a Tor-based payment portal where they could pay the ransom. The attackers set specific deadlines and failure to meet them often led to an increase in the ransom amount. The RaaS model allowed partners to use the GandCrab platform and developers received a percentage of each ransom payment.

**6. Response from the security and law enforcement community:** The cybersecurity community, in collaboration with law enforcement agencies, worked actively to disrupt GandCrab's operations. The researchers analysed the ransomware infrastructure, tracked command and control servers, and collaborated to develop decryption tools.

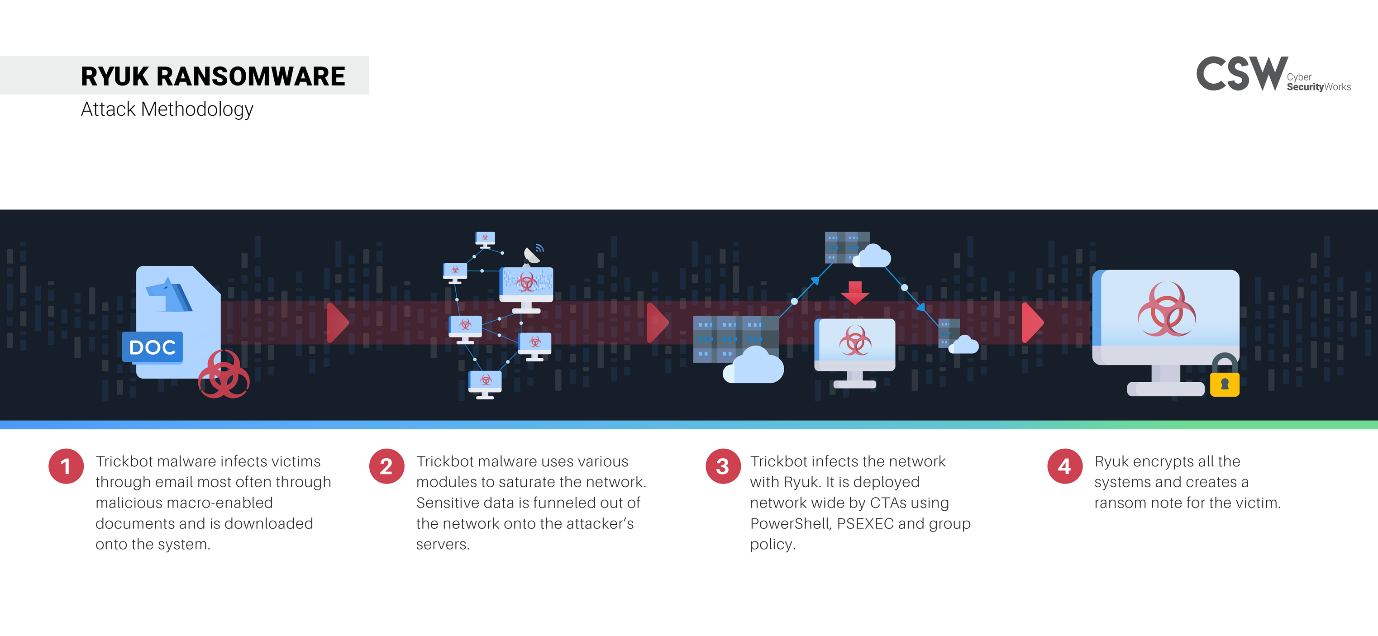
**7.Decryption solutions:** Over time, researchers and security organizations have successfully developed decryption tools for specific versions of GandCrab. These tools allowed victims to recover their files without paying the ransom, dealing a major blow to ransomware operations.

**8. Decommissioning and retirement:** In June 2019, the makers of GandCrab announced the “withdrawal” of the ransomware. This decision was likely influenced by the increasing effectiveness of decryption tools, law enforcement efforts, and increased awareness within the cybersecurity community.



Emphasizes the importance of timely software updates, robust cybersecurity practices, and collaborative efforts between the security industry and law enforcement to counter evolving threats. While GandCrab is no longer actively spreading, its legacy is a reminder of the ongoing need for vigilance and collaboration in the face of complex cyber threats.

**RYUK RANSOMWARE ATTACK**



**1. Introduction to Ryuk:–** Ryuk is a sophisticated and targeted ransomware variant that emerged in August 2019. It has gained notoriety for its specific attacks against high-profile organizations, particularly those in the corporate and healthcare sectors.

**2. First infection vector:–** Ryuk is often transferred by exploiting system vulnerabilities .This is usually associated with initial compromises enabled by other malware such as TrickBot or Emotet. These precursor strains of malware serve as entry points for Ryuk operators.

**3. Precursor malware involvement:–** TrickBot and Emotet are often involved in Ryuk campaigns. These malware strains are typically distributed via phishing emails that use social engineering techniques to trick users into opening malicious attachments or clicking on malicious links.

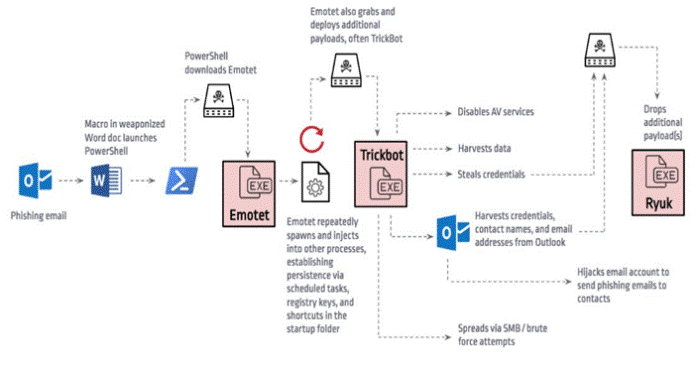
**4. Lateral movement and network propagation:-** Once on the network, Ryuk uses advanced lateral movement and network propagation techniques. It scans valuable targets such as servers and critical infrastructure before starting the encryption process. Ryuk operators are known to carefully select high-value targets to maximize ransom payments.

**5.Encryption process:–** Ryuk uses a combination of RSA and AES encryption algorithms to encrypt files on compromised systems. The encryption process is quick and targeted, focusing on critical files and databases that are essential to the functioning of the victim's organization.

**6. Ransom demand and message**:– Once Ryuk is encrypted, he leaves behind a ransom note, usually called “RyukReadMe.txt,” which contains instructions on how to contact the attackers and pay the ransom. Communication often takes place via a Tor-based payment portal.

**7. Custom Ransom Demands:–** Ryuk operators adjust ransom demands based on the size and perceived financial strength of the victim organization. Ransom demands are typically made in Bitcoin and the amounts can be large, ranging from hundreds of thousands to millions of dollars.

**8.Avoid discovery:–** Ryuk is designed to prevent detection by security tools. Techniques such as code obfuscation, anti-scan measures, and the use of legitimate system management tools are often used to navigate the network without triggering alarms.

****

**9. Reduction measures:–** Containing a Ryuk attack requires a combination of proactive measures and incident response. This includes regularly updating and patching systems, using network segmentation, implementing effective email security solutions, and educating users about the dangers of phishing.

**10. Law Enforcement and Cybersecurity Response:-** Law enforcement agencies, cybersecurity companies and researchers are actively collaborating to track Ryuk's operations. Over time, security researchers have developed decryption tools for some Ryuk variants, giving victims the ability to recover their files without paying a ransom.

**11. Quest Challenges:-** It's difficult to attribute Ryuk's attacks since the Operators are often good at covering their tracks. However, some suspect that Ryuk is connected to threat groups in Russia or other Eastern European countries. While Ryuk remains a persistent threat, ongoing efforts in cybersecurity research and international cooperation have helped mitigate its impact and provide victims with alternative options for recovery. However, the dynamic nature of ransomware threats highlights the ongoing need to remain vigilant and update cybersecurity practices.

**MEASURES TO TAKE AGAINST RANSOMWARE ATTACKS**

Mitigating the risk of ransomware attacks involves a combination of proactive measures, cybersecurity best practices, and user awareness. Here are some key measures to help avoid ransomware attacks:

**1. Regular Data Backups:**

Regularly back up critical data and ensure that backups are stored in an isolated environment. This allows for quick recovery without paying ransom in case of an attack.

**2. Update and Patch Systems:**

Keep operating systems, software, and applications up to date with the latest security patches. Regularly update antivirus and anti-malware software to protect against known vulnerabilities.

**3. Network Segmentation:**

- Implement network segmentation to restrict lateral movement of malware within the network. This can limit the impact of a potential ransomware infection.

**4. User Education:**

Educate users about the risks of phishing emails, malicious attachments, and links. Training programs can help users recognize and avoid suspicious content.

**5. Email Security:**

Use email filtering solutions to detect and block phishing emails. Implement Sender Policy Framework (SPF) and Domain-based Message Authentication, Reporting, and Conformance (DMARC) to authenticate email sources.

**6. Application Whitelisting:**

Employ application whitelisting to allow only approved programs to run on a system. This helps prevent the execution of unauthorized and potentially malicious applications.

**7. Endpoint Protection:**

- Utilize robust endpoint protection solutions that include anti-malware, anti-ransomware, and behaviour analysis features. Ensure that these solutions are regularly updated.

**8. Multi-Factor Authentication (MFA):**

- Implement multi-factor authentication to add an extra layer of security, making it more difficult for unauthorized users to access systems.

**9. Vulnerability Management:**

Conduct regular vulnerability assessments and promptly address identified weaknesses. This includes both external and internal vulnerabilities that could be exploited by attackers.

**10. Incident Response Plan:**

- Develop and regularly update an incident response plan that outlines the steps to be taken in the event of a ransomware attack. This plan should include communication strategies, contact information, and procedures for isolating affected systems.

**11. Security Awareness Training:**

Train employees on cybersecurity best practices, emphasizing the importance of not clicking on suspicious links, downloading unknown attachments, or providing sensitive information in response to unsolicited requests.

**12. Limit User Privileges:**

Restrict user privileges to the minimum required for their job functions. This can prevent ransomware from spreading laterally within the network.

**13. Network and Web Filtering:**

Implement network and web filtering to block access to known malicious websites and prevent users from inadvertently visiting compromised sites.

**14. Regular Security Audits:**

Conduct regular security audits to assess the effectiveness of security measures and identify areas for improvement.

**15. Collaborate and Share Threat Intelligence:**

Stay informed about the latest threats by collaborating with industry peers and sharing threat intelligence. This can help organizations anticipate and prepare for emerging ransomware threats.

By combining these measures, organizations can significantly reduce the risk of falling victim to ransomware attacks and enhance their overall cybersecurity posture.