CYBER security

Ransomware Analysis: Petya

Salvatore Di Salvo

Staffordshire University: London Digital Institute

Table of Contents

[Abstract: 4](#_Toc135256667)

[Introduction: 5](#_Toc135256668)

[Petya’s Attack Vectors: 5](#_Toc135256669)

[Phishing emails: 5](#_Toc135256670)

[Drive-by downloads: 5](#_Toc135256671)

[Watering Hole Attacks: 6](#_Toc135256672)

[Social Engineering: 6](#_Toc135256673)

[Evidence of Petya’s Presence: 6](#_Toc135256674)

[Encrypted files: 6](#_Toc135256675)

[Ransom note: 7](#_Toc135256676)

[System modifications: 8](#_Toc135256677)

[Network propagation: 8](#_Toc135256678)

[Threats to Data: 8](#_Toc135256679)

[Overview: 8](#_Toc135256680)

[Petya’s Encryption/Decryption Algorithm and it’s effect on data: 9](#_Toc135256681)

[Introduction: 9](#_Toc135256682)

[The mechanics of Petya’s encryption/decryption: 9](#_Toc135256683)

[Overall impact on data: 10](#_Toc135256684)

[Effects on Organizations and Individuals: 11](#_Toc135256685)

[Threats to Systems: 11](#_Toc135256686)

[File encryption: 11](#_Toc135256687)

[Public key cryptography: 11](#_Toc135256688)

[System tampering: 11](#_Toc135256689)

[Malware evolution: 11](#_Toc135256690)

[Ransom demand: 12](#_Toc135256691)

[Conclusion: 12](#_Toc135256692)

[Threats to Networks: 12](#_Toc135256693)

[Network Propagation: 12](#_Toc135256694)

[Exploitation of Weak Authentication Mechanism: 13](#_Toc135256695)

[Effects on Organizations and Individuals: 13](#_Toc135256696)

[Disaster Recovery: 13](#_Toc135256697)

[The Significance of a Disaster Recovery Plan: 13](#_Toc135256698)

[Disaster Recovery Plan: 14](#_Toc135256699)

[Risk Prevention: 15](#_Toc135256700)

[Why Risk Prevention is Vital: 15](#_Toc135256701)

[Risk Prevention Plan: 15](#_Toc135256702)

[Executive Summary: 16](#_Toc135256703)

[References: 17](#_Toc135256704)

Table of Figures

[Figure 1 - An example of a phishing email; many phishing emails will often encourage individuals to download attachment’s under the guise of free software’s/games/media. 4](#_Toc135256342)

[Figure 2 - An example of classic scams on websites which promises free software/media/games. It's common for people to upload a variety of malware to compromise people's devices and networks. 5](#_Toc135256343)

[Figure 3 - Petya has completely encrypted the files of the device and has shut down all functionality, leaving the user with a ransom note encouraging them to 'press a key' 6](#_Toc135256344)

[Figure 4 - Petya's ransom note instructing the user to visit an '.onion' website on TOR (the 'dark web') and pay the ransom in order to de-crypt the user's files. 6](#_Toc135256345)

[Figure 5 - The process of Petya encrypting the device. This message is purposely designed with the Window's aesthetic to influence users to not switch off their PC's and halt the encryption. 7](#_Toc135256346)

[Figure 6 - Petya is encrypting the device 8](#_Toc135256347)

[Figure 7 - An image of the ransom note, it is configured to simply reject incorrect redemption codes, or de-crypt the device once the correct redemption code has been entered. 11](#_Toc135256348)

# Abstract:

With the increased frequency of cyber threats, knowing the complexities of ransomware has become crucial for protecting critical data, systems, and networks. This scholarly paper delves into the Petya ransomware version, digging into its complex transmission mechanisms, possible hazards to data security, system vulnerabilities, and network consequences. A practical experiment was also carried out to get practical insights into Petya's behaviour and impact by purposefully infecting a virtual machine environment.

To provide a comprehensive understanding of Petya, the research methodology included a thorough assessment of current literature, scholarly publications, technical reports, and case studies. The research focused on its distinct traits, such as the methods by which it spreads and the encryption techniques used to hold victims' data hostage.

Petya typically uses social engineering techniques, spam emails, malicious attachments, and software flaws to obtain early access to a targeted machine, according to the research. Once inside, it uses complex encryption algorithms to make crucial data unavailable and demands a ransom to be paid for its release. Petya also exhibited the potential to spread within a network, infecting additional systems by exploiting network vulnerabilities and lax security controls. (Aidan, J. S., Verma, H. K., & Awasthi, L. K., 2017,)

The study investigated the considerable concerns Petya poses to data integrity, confidentiality, and availability, in addition to analysing its propagation processes. The encryption capabilities of the ransomware were discovered to be quite advanced, making data recovery extremely difficult without the decryption key. The potential financial and reputational ramifications of Petya infection for individuals, organisations, and institutions highlight the significance of proactive security measures.

A controlled experiment was carried out in a virtual machine environment to increase the research's practical usefulness. The experiment attempted to study Petya's behaviour, influence on system performance, and interaction with current security mechanisms by purposefully infecting the virtual machine with it. The experiment gave researchers personal knowledge of the ransomware's evasion strategies, communication with command-and-control servers, and ability to proliferate and encrypt data within the virtual environment.

Furthermore, the study dug into the crucial areas of risk prevention and disaster recovery. It investigated proactive ways to reduce the danger of Petya infections, including as regular patching and updates, network segmentation, tight access restrictions, and user awareness training. Furthermore, the research looked into the implementation of advanced endpoint protection solutions, intrusion detection and prevention systems, and comprehensive backup and recovery processes to reduce the impact of data loss and system downtime.

The findings contribute to the realm of cybersecurity by allowing organisations to establish effective risk prevention strategies and put in place comprehensive disaster recovery plans in the face of Petya and other ransomware threats. Organisations may proactively protect their key assets, improve their security posture, and maintain continuity of operations in the event of an attack by completely understanding the spread methods, data threats, and risk prevention strategies connected with Petya.

# Introduction:

A careful and methodical investigator has been tasked with researching the ransomware known as Petya. Petya, a well-known kind of ransomware, has been wreaking havoc in the cyber world with its complex attack routes and destructive effects on both individual machines and entire networks (Fayi, S. Y. A., 2018). This essay will go into the depths of Petya, investigating its vectors, proof of its presence on devices, the damage it may cause, and presenting a full disaster recovery strategy and risk prevention techniques to reduce its destructive impacts. This essay aims to shed light on the inner workings of Petya and provide insights into effective remedies against this harmful software through rigorous investigation and analysis.

# Petya’s Attack Vectors:

## Phishing emails:

Petya may be spread by phishing emails containing malicious attachments or links. These emails are frequently designed to deceive people into clicking on a link or opening an attachment, which then causes the malware to download and execute. The emails may appear legitimate, typically impersonating well-known organisations or individuals, and may contain urgent or appealing material designed to entice recipients to act without thoroughly validating the email's validity.

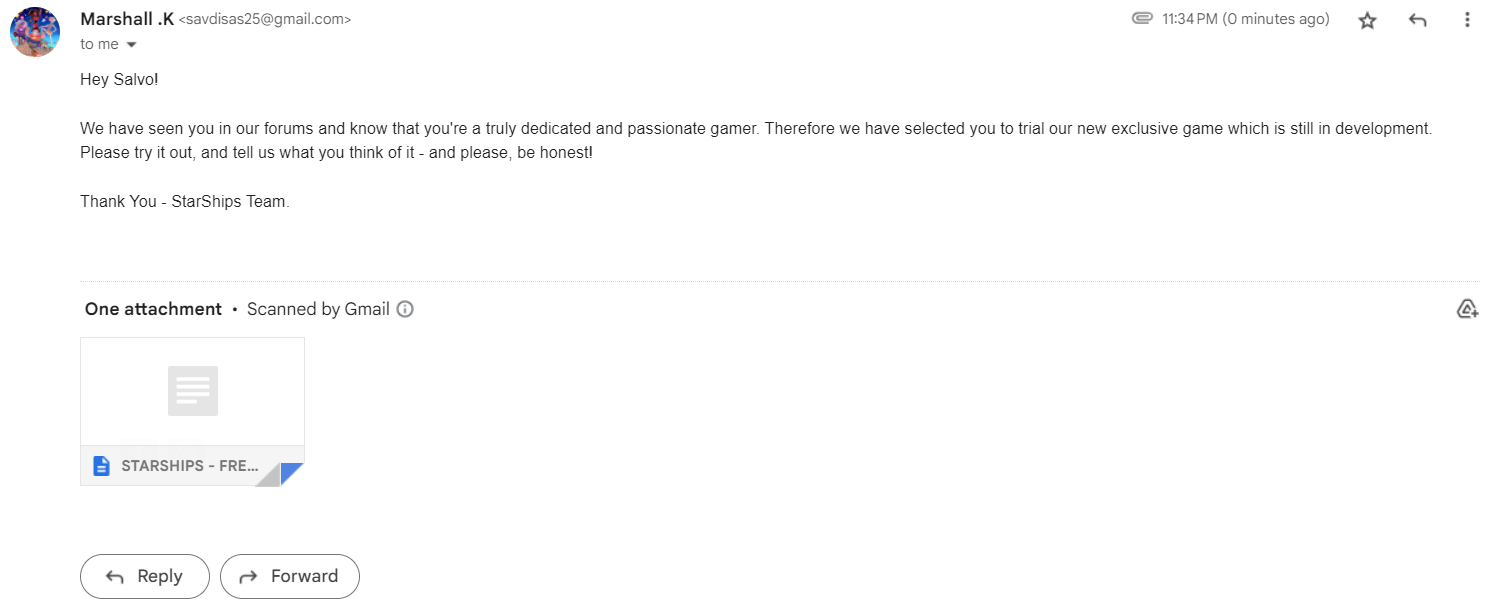


Figure - An example of a phishing email; many phishing emails will often encourage individuals to download attachment’s under the guise of free software’s/games/media.

## Drive-by downloads:

Petya can also be distributed via hijacked websites, where visitors unintentionally download malware via drive-by downloads. When users visit a website that has been infiltrated by hackers, the malware is immediately downloaded and run without the user's knowledge or agreement. Drive-by downloads can start the infection process by exploiting vulnerabilities in web browsers, plugins, or other software.

## Watering Hole Attacks:

Petya also employs watering hole assaults, in which malware is installed on websites frequented by the targeted persons or organisations. Attackers hack these websites, insert malware into legitimate web content, and then wait for selected victims to visit them and become infected.

## Social Engineering:

Petya may also utilise social engineering techniques to lure users into downloading and running the malware, such as social media posts, bogus software updates, or misleading internet adverts. These approaches take use of human behaviour and trust to trick users into unknowingly installing malware on their devices.

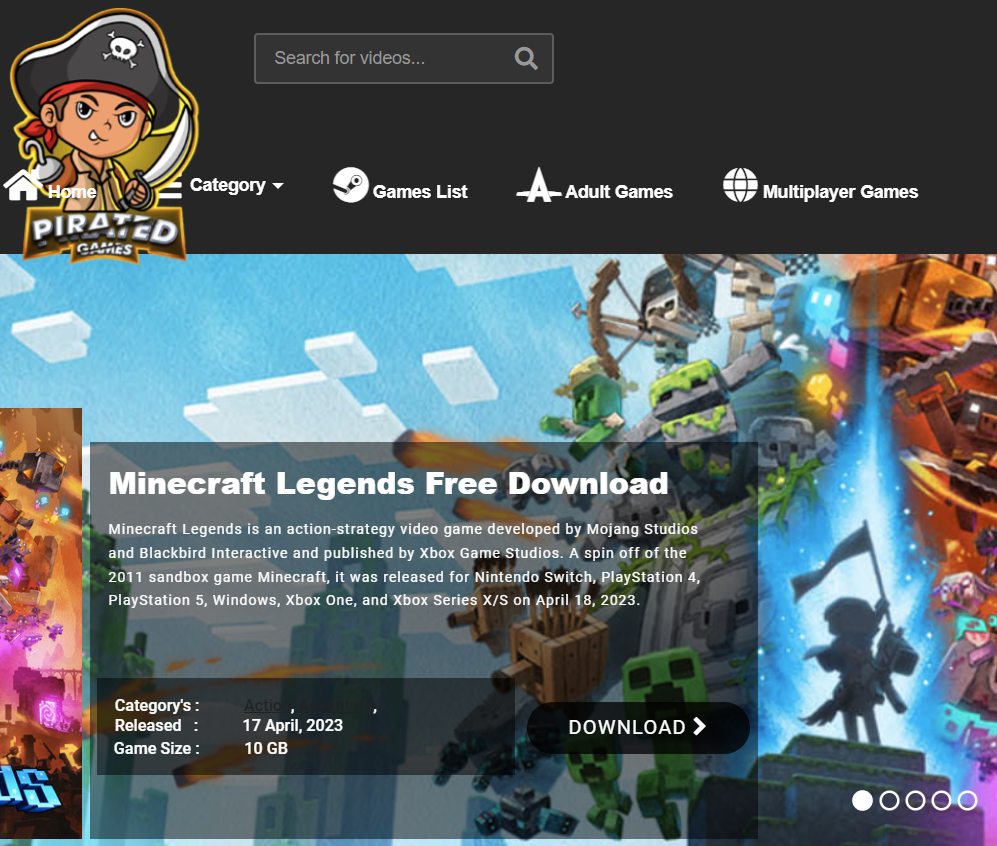


Figure - An example of classic scams on websites which promises free software/media/games. It's common for people to upload a variety of malware to compromise people's devices and networks.

# Evidence of Petya’s Presence:

## Encrypted files:

The encryption of files on the infected machine is one of the key indicators of Petya's presence. The malware encrypts files with specified file extensions, such as.doc,.docx,.xlsx,.pptx,.txt,.jpg,.png, and so on, and appends a unique extension to the encrypted files, such as.encrypted or.encrypted1. As a result, the files become unavailable and unusable until decrypted with the appropriate key.

## Ransom note:

Since Petya is a Ransomware, a ransom note will be explicitly available on the affected device. The ransom note will have instructions on how to pay the ransom and acquire the decryption key. The ransom note can be shown as a pop-up window, a desktop text file, or as a wallpaper replacement. The ransom note frequently comprises threats and instructions from the attackers, indicating Petya's presence on the system. (Petrenko, A. S., Petrenko, S. A., et al., 2018)

A red and black flag with a skull and crossbones

Description automatically generated with medium confidence

Figure - Petya has completely encrypted the files of the device and has shut down all functionality, leaving the user with a ransom note encouraging them to 'press a key'

A picture containing text, screenshot, font, design

Description automatically generated

Figure - Petya's ransom note instructing the user to visit an '.onion' website on TOR (the 'dark web') and pay the ransom in order to de-crypt the user's files.

## System modifications:

To ensure its persistence on the infected system, Petya encrypts the Master File Table (MFT), a database used by Windows to keep track of the location of files on the hard drive. The system becomes unbootable after the MFT is encrypted, and the user is presented with a ransom message.. It may also conduct numerous system alterations such as disabling critical services, editing registry entries, or changing system configurations. These changes can be discovered using system logs, registry changes, or other forensic analysis techniques, proving the malware's presence and activity on the system.

A picture containing text, screenshot, design

Description automatically generated

Figure - The process of Petya encrypting the device. This message is purposely designed with the Window's aesthetic to influence users to not switch off their PC's and halt the encryption.

## Network propagation:

Petya's ability to spread quickly can also leave traces of its presence in network logs and traffic analysis. Malware may display strange network behaviours such as scanning for susceptible systems, brute-forcing passwords, or establishing suspicious network connections, which can be detected by network monitoring and analysis.

# Threats to Data:

## Overview:

Petya's primary goal is to encrypt files on the infected machine and demand a ransom for their release. This can have serious ramifications for businesses and individuals, leading in data loss, operational disruptions, and financial losses. Without the decryption key, which is only delivered upon payment of the ransom, the encrypted data become unavailable. However, paying the ransom does not guarantee that the encrypted data would be recovered, as cybercriminals may not keep their promises. Furthermore, the encryption and decryption processes of ransomware such as Petya can jeopardise data integrity. Data may be compromised or altered during the encryption and decryption processes, potentially resulting in data integrity issues. This can have major ramifications, particularly when working with sensitive or essential data that must be accurate and reliable.

## Petya’s Encryption/Decryption Algorithm and it’s effect on data:

### Introduction:

Petya encrypts files on the infected machine using a combination of symmetric and asymmetric cryptography. The files are encrypted using symmetric cryptography, which uses the same key for both encryption and decryption, while asymmetric cryptography, which uses a pair of public and private keys, is used to securely exchange the symmetric key between the victim's system and the attacker's server. (Aidan, J. S., & Garg, U, 2018)

### The mechanics of Petya’s encryption/decryption:

Petya ransomware has a two-stage encryption technique, the first of which encrypts the Master File Table (MFT). The MFT is a critical component of the Windows file system that keeps information on all the files and folders on the hard disc, such as file names, sizes, and locations.

Petya replaces the original MFT with a malicious one to encrypt it. The new MFT is a bogus table containing random data, rendering the hard drive's files inaccessible. Petya then uses a symmetric encryption technique, often AES-128 or AES-256, to encrypt the new MFT and generates a unique encryption key. (Watson, F. C., CISM, C., & ECSA, A., 2017))

A black screen with white text

Description automatically generated with low confidence

Figure - Petya is encrypting the device

The encryption key is subsequently encrypted and kept on the perpetrators' server using an asymmetric encryption algorithm, generally RSA-2048. The system becomes unbootable when the MFT is encrypted, and the user is confronted with a ransom message demanding money for the decryption key. It is impossible to access any of the files on the hard drive without the decryption key, rendering the system inoperable. Because the encryption utilised is highly secure, recovering the encrypted MFT without the decryption key is also quite difficult.

Specifically, Petya begins the encryption process by employing the Advanced Encryption Standard (AES), a widely utilised symmetric encryption method noted for its security and efficiency. AES works with fixed-size data blocks (128 bits) and key lengths of 128, 192, or 256 bits. For each infected system, Petya produces a unique AES key, which is used to encrypt the victim's files. Depending on the Petya type, the files are often encrypted with AES-128, AES-192, or AES-256.

After the files are encrypted with AES, Petya encrypts the AES key with asymmetric cryptography, specifically the RSA-2048 technique. RSA is a popular asymmetric encryption technology that makes use of a pair of public and private keys. Data is encrypted using the public key, and decrypted using the private key. The attacker's public key is used to encrypt the AES key in the case of Petya, and the encrypted AES key is delivered to the attacker's server for safekeeping. (Mohurle, S., & Patil, M., 2017)

Petya's usage of AES for file encryption assures that the files are safely scrambled and cannot be easily decoded without the appropriate AES key. AES is a powerful encryption technique that is extensively used and trusted in a wide range of applications. The use of RSA-2048 for asymmetric encryption, on the other hand, adds an extra degree of security to the encryption key used in the ransomware attack. However, with such a thorough and ‘messy’ encryption, data integrity can be compromised since the data is susceptible to undesired edits or even complete loss. (Kok, S. H., Abdullah, A., Jhanjhi, N. Z., et al., 2019)

### Overall impact on data:

The use of AES and RSA-2048 in Petya has important consequences for data security. The encryption method effectively encrypts the victim's files, rendering them inaccessible without the decryption key. As a result, the victim's data is effectively kept hostage, and the files cannot be viewed or utilised until the ransom is paid and the attacker provides the decryption key. As previously said, this might result in the loss of crucial data for organisations and people. (Richardson, R., & North, M. M., 2017)

Additionally, using RSA-2048 for asymmetric encryption adds another degree of complexity to the decryption process. RSA-2048 is a computationally demanding method, and decrypting the AES key requires the attacker's private key. This can considerably slow down decryption and make it more difficult for victims to recover their data without paying the ransom.

## Effects on Organizations and Individuals:

It can also have a significant influence on organisations and individuals. The financial and operational disruptions caused by ransomware attacks can be disastrous for businesses. The loss of essential data can cause business activities to be disrupted, resulting in; financial losses because of potential manufacturing delays, product or service delivery delays, and revenue loss, reputational damage, and possibly legal and regulatory ramifications. Ransom fees, incident response, and recovery efforts can all add up quickly. Personal data loss, such as images, papers, and other digital assets, can be catastrophic for individuals. It could also render individuals vulnerable to identity theft or financial fraud if their data is succumbs to the wrong hands. The emotional and financial consequences of losing important data may be irreversible, causing anguish and difficulty. (Huang, D. Y., Aliapoulios, M. M., Li, V. G., Invernizzi, L., et al., 2018)

# Threats to Systems:

## File encryption:

As expressed prior, Petya employs the AES (Advanced Encryption Standard) technique. Because AES is a symmetric encryption method, it uses the same key for both encryption and decryption. Petya generates a one-of-a-kind key for each victim's machine, which is then used to encrypt files on local drives and network shares. Once encrypted, the files are rendered inaccessible without the associated decryption key, thus keeping them away from the user.

## Public key cryptography:

In addition to AES, Petya employs the RSA-2048 (Rivest-Shamir-Adleman) asymmetric encryption method. For encryption and decryption, asymmetric encryption employs a pair of keys, a public key and a private key. Petya encrypts the AES key used to encrypt the victim's data with the RSA-2048 technique. Using the victim's public key, the encrypted AES key is then transferred to the attacker's server. This makes decrypting the encrypted files extremely impossible without the accompanying private key, which is held by the attacker.

## System tampering:

Petya may also interfere with system settings and configurations, putting system security at risk. To ensure its permanence on the infected system, it may stop vital services, modify registry entries, and change system configurations. These system-level manipulation actions can cause system instability, lower performance, and extended downtime, resulting in operational interruptions and financial losses for the organisations involved.

## Malware evolution:

Petya, like other malware, is continually evolving, with hackers creating new types and versions. These variations may feature enhanced encryption, evasion, and propagation methods, making them even more difficult to detect and combat. Petya's dynamic nature necessitates continual updates to defences and mitigation measures in order to properly protect systems against this threat.

## Ransom demand:

The ransom demand made by Petya to victims has the greatest impact on systems. After encrypting the data, Petya shows a ransom message on the victim's system, demanding bitcoin payment for the release of the decryption key. The ransom amount varies, but it is frequently placed at a large figure, putting financial burden on the afflicted organisations. Failure to pay the ransom may result in irreversible data loss, emphasising Petya's negative influence on systems.

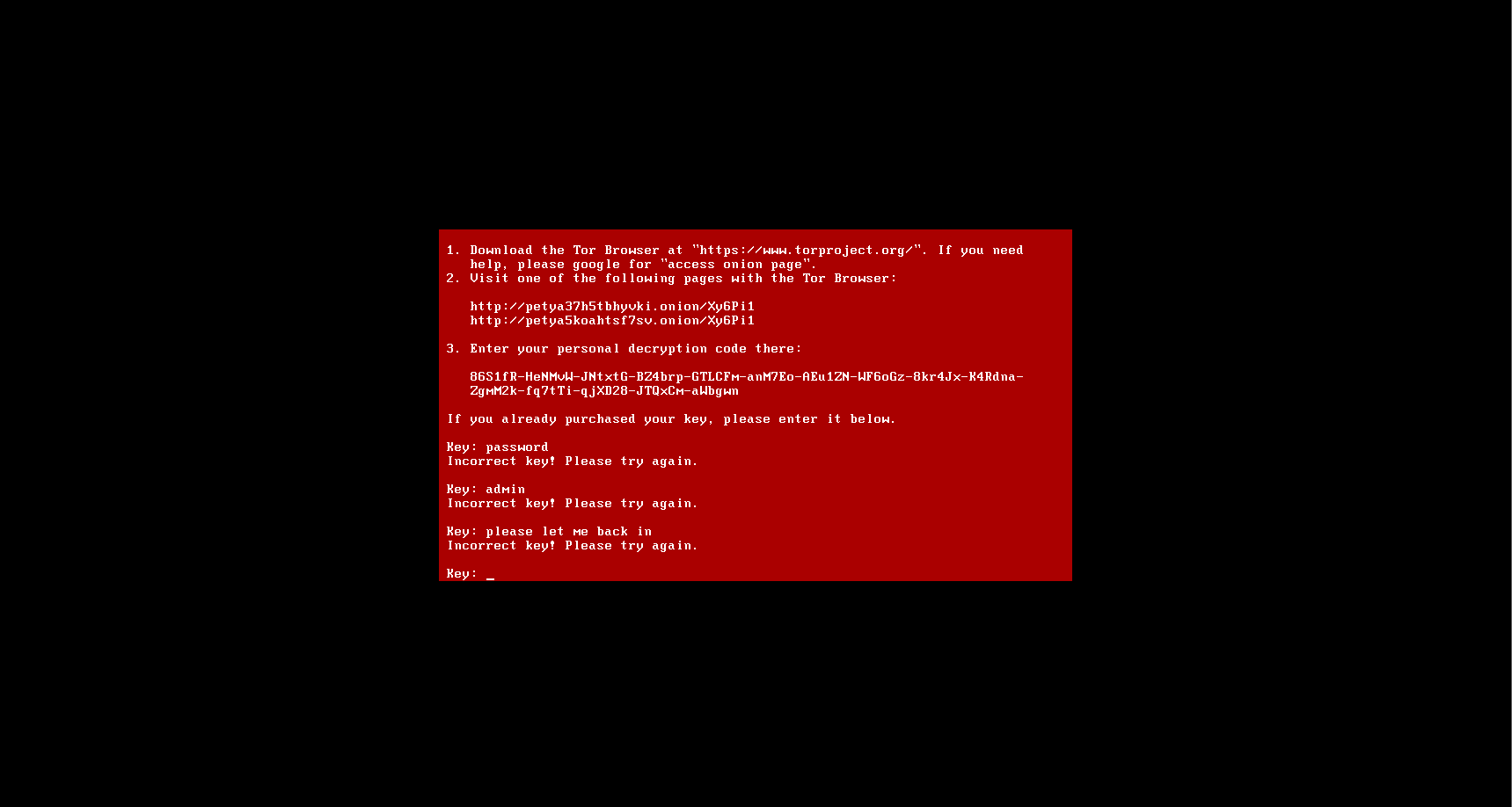


Figure - An image of the ransom note, it is configured to simply reject incorrect redemption codes, or de-crypt the device once the correct redemption code has been entered.

## Conclusion:

To summarise, Petya has a significant and multifaceted impact on systems, including file encryption, the use of public key cryptography, quick dissemination, system tampering, changing versions, and ransom demands. To protect against the risks and hazards posed by Petya to system security, organisations must establish robust cybersecurity measures such as regular software upgrades, effective access controls, network segmentation, and employee awareness training.

# Threats to Networks:

## Network Propagation:

Petya is capable of rapidly spreading across networks by exploiting weaknesses in unpatched computers or via insecure Remote Desktop Protocol (RDP) connections. Once it has gained access to a single system, it can spread laterally, infecting additional network-connected devices. This rapid propagation has the potential to cause massive data encryption and network disruption.

Petya has the potential to cause network infrastructure disruption by focusing on critical network components such as routers, switches, and servers. It can severely impair network connectivity and management by encrypting or rendering critical system files inoperable, resulting in extensive downtime and financial losses.

Petya may encrypt not only local files but also network shares and shared drives that are available to connected devices. This poses a significant concern because it has the potential to encrypt key data kept on central servers, rendering it unavailable to many users and disrupting the organization's operations.

## Exploitation of Weak Authentication Mechanism:

Petya can take advantage of weak or default credentials, especially in the event of insecure RDP connections. Petya can acquire unauthorised network access through brute force attacks or the use of freely available tools, weakening system security and allowing the ransomware to spread further. (Oz, H., Aris, A., Levi, A., & Uluagac, A. S., 2022)

## Effects on Organizations and Individuals:

Petya ransomware poses substantial financial risks to businesses. The ransom demands might be enormous, asking victims to pay a large sum of money in cryptocurrency in order to acquire the decryption key. Furthermore, the costs of downtime, data recovery, and remediation operations can be significant, affecting an organization's bottom line.

Petya ransomware can have a severe impact on an organization's operations. Network-wide encryption and the resulting inaccessibility of important systems and data can result in extended downtime, reduced productivity, missed deadlines, and a loss of customer trust. Restoring operations following an attack necessitates significant resources and time, worsening the impact on business continuity.

# Disaster Recovery:

## The Significance of a Disaster Recovery Plan:

A disaster recovery plan is critical for any organisation because it lays out the procedures and processes that must be followed in the case of a disaster. The plan lays the groundwork for responding to and recovering from a variety of calamities, including cyberattacks, natural disasters, power outages, and equipment failures (Toigo, J., 2002). A comprehensive disaster recovery plan can reduce the impact of a disaster on an organization's operations, data, and reputation. It can also ensure that important company functions are swiftly and effectively restored, reducing downtime and financial losses. (Fallara, P., 2004))

## Disaster Recovery Plan:

|  |
| --- |
| 1. Detection and Containment:  1.1 Incident Response:  - Define Petya ransomware attack signs and methods for prompt detection.  - To avoid further infection, isolate the affected system(s) by unplugging them from the network.  - Notify the appropriate stakeholders, such as IT, security teams, and management.  1.2 Damage Assessment: Identify affected systems, networks, and data and assess the degree of the infection.  - Determine the relevance of essential systems and data to corporate operations and prioritise their recovery.  2. Recovery Strategy:  2.1 Backup Restoration: - Identify and validate the integrity of the most recent backup that was not affected by the ransomware attack.  - Restore essential systems and data to a separate, isolated environment from the clean backup.  2.2 System Rebuild: - Rebuild infected computers by reimaging or reinstalling the operating system and any required applications from reputable sources.  - Before connecting systems to the network, ensure that all security patches and upgrades have been deployed.  2.3 Data Recovery: If applicable, decrypt and retrieve encrypted data using available decryption tools.  - If necessary, use professional data recovery services to recover data from encrypted or damaged systems.  3. Network Infrastructure Restoration:  3.1  Network examination and Remediation: Perform a complete examination of the network infrastructure to detect potential vulnerabilities and backdoor access points.  - Patch vulnerabilities, update firmware, and reconfigure network devices in accordance with best practises.  3.2 Network Segmentation: Use network segmentation to isolate important systems and limit ransomware lateral movement in the case of subsequent attacks.  - Establish access controls to limit network communication and prevent unauthorised access.  4. Post-Recovery Protocol:  4.1 System Hardening: - Implement strong security measures such as firewall setups, intrusion detection systems, and endpoint protection solutions.  - Implement strong password policies, multi-factor authentication, and frequent employee security awareness training  4.2 Testing and Validation: - Test restored systems, applications, and network infrastructure thoroughly to guarantee adequate operation and security.  - Test the efficacy of the disaster recovery plan using simulated ransomware attack scenarios.  4.3 Learnings and Documentation:  - Record the incident response and recovery process, including critical observations, problems encountered, and recommended changes.  - Examine the lessons learned and revise the disaster recovery plan as needed. |

(Rouhanizadeh, B., Kermanshachi, S., & Nipa, T. J., 2020)

Figure 8 – A comprehensive step-by-step disaster-recovery protocol.

# Risk Prevention:

## Why Risk Prevention is Vital:

Preventing a Petya ransomware attack requires a comprehensive risk prevention plan that incorporates various security measures. It’s undeniable that trying to purge Petya from a device and restore the device to it’s original state is significantly difficult, hence why it’s imperative to delegate appropriate time and effort into risk prevention.

## Risk Prevention Plan:

* Routinely update software: Make sure that all software, including the operating system and apps, is routinely updated with the most recent security patches to avoid vulnerabilities that fraudsters can exploit.
* Implement strong passwords: Make sure that all accounts, including administrator accounts, have strong, difficult-to-guess passwords. Implement a password policy that demands password changes on a regular basis.
* Implement multi-factor authentication for all accounts, which adds an extra layer of protection and makes it more difficult for fraudsters to get unauthorised access.
* Train staff on how to recognise and prevent phishing emails and other social engineering techniques used by thieves to disseminate malware. This training should also include how to detect and report unusual network activities.
* Implement access controls: Limit access to sensitive data and systems by implementing access restrictions. Allow access only to personnel who need it for their job duties.
* Install and routinely update antivirus software: To identify and prevent malware, including ransomware, install and frequently update antivirus software on all systems.
* Use backup and disaster recovery solutions: Backup all data on a regular basis and develop a disaster recovery strategy to guarantee that data can be retrieved promptly in the case of a ransomware attack.
* Implement network segmentation: Segment the network to isolate essential systems and data from the rest of the network. This makes malware spreading to vital systems more challenging.
* Use advanced threat detection solutions: To identify and respond to attacks in real time, use advanced threat detection solutions such as intrusion detection systems and security information and event management (SIEM) systems.

(Barker, W. C., Scarfone, K., Fisher, W., & Souppaya, M., 2021)

(Profile, A. C. F., 2022)

# Executive Summary:

In summary, this essay gives a thorough examination of the Petya virus, concentrating on its vectors, proof of presence, and possible damage to devices and networks. The disaster recovery plan and risk prevention techniques established are critical tools for assisting organisations and individuals in successfully responding to and mitigating the risks connected with Petya attacks. Organisations/individuals may improve their preparation, reduce the effect of attacks, and assure the continuation of their operations and data security by employing these steps.

# References:

Aidan, J. S., Verma, H. K., & Awasthi, L. K. (2017, December). Comprehensive survey on petya ransomware attack. In *2017 International Conference on Next Generation Computing and Information Systems (ICNGCIS)* (pp. 122-125). IEEE.

Fayi, S. Y. A. (2018). What Petya/NotPetya ransomware is and what its remidiations are. In *Information Technology-New Generations: 15th International Conference on Information Technology* (pp. 93-100). Springer International Publishing.

Petrenko, A. S., Petrenko, S. A., Makoveichuk, K. A., & Chetyrbok, P. V. (2018, January). Protection model of PCS of subway from attacks type «wanna cry»,«petya» and «bad rabbit» IoT. In *2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)* (pp. 945-949). IEEE.

Aidan, J. S., & Garg, U. (2018, December). Advanced Petya ransomware and mitigation strategies. In *2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC)* (pp. 23-28). IEEE.

Watson, F. C., CISM, C., & ECSA, A. (2017). Petya/NotPetya Why It Is Nastier Than WannaCry and Why We Should Care. *ISACA Journal*, *6*, 1-6.

Mohurle, S., & Patil, M. (2017). A brief study of wannacry threat: Ransomware attack 2017. *International Journal of Advanced Research in Computer Science*, *8*(5), 1938-1940.

Richardson, R., & North, M. M. (2017). Ransomware: Evolution, mitigation and prevention. *International Management Review*, *13*(1), 10.

Huang, D. Y., Aliapoulios, M. M., Li, V. G., Invernizzi, L., Bursztein, E., McRoberts, K., ... & McCoy, D. (2018, May). Tracking ransomware end-to-end. In *2018 IEEE Symposium on Security and Privacy (SP)* (pp. 618-631). IEEE.

Kok, S. H., Abdullah, A., Jhanjhi, N. Z., & Supramaniam, M. (2019). Prevention of crypto-ransomware using a pre-encryption detection algorithm. *Computers*, *8*(4), 79.

Oz, H., Aris, A., Levi, A., & Uluagac, A. S. (2022). A survey on ransomware: Evolution, taxonomy, and defense solutions. *ACM Computing Surveys (CSUR)*, *54*(11s), 1-37.

Toigo, J. (2002). *Disaster recovery planning: Preparing for the unthinkable*. Prentice Hall Professional Technical Reference.

Fallara, P. (2004). Disaster recovery planning. *IEEE potentials*, *23*(5), 42-44.

Rouhanizadeh, B., Kermanshachi, S., & Nipa, T. J. (2020). Exploratory analysis of barriers to effective post-disaster recovery. *International Journal of Disaster Risk Reduction*, *50*, 101735.

Barker, W. C., Scarfone, K., Fisher, W., & Souppaya, M. (2021). Cybersecurity Framework Profile for Ransomware Risk Management. *National Institute of Standards and Technology*.

Profile, A. C. F. (2022). Ransomware Risk Management.