*Student name: Anish Niure*

*Student ID: S10086062*

*Advanced System Security - Report Assignment*

# Current Threats to Cyberspace

**Executive summary:**

Information and communication technology has become the essential part in this contemporary world. Cyberspace is taken as the one giant term of collection of all the interconnected digital technologies for the online communications. It is the outcome of the hard research and development in the cyberspace from which the modern civilization is blessed with an opportunity to sense the possibilities from those digital means. Conversely, these digital means can be compromised by different threat vectors which can be devastating for the users. Any individual or the organizations has economic, reputational, and legal consequences from a cyber breach.  We keep hearing, 'No device or mechanisms are hundred percent secure' that means with the advancement in the technology, the threats activities have also been growing profoundly, even the present cyberspace experiences many threats, which is due to inappropriate way of controlling the data and protocols used while communication. The safest means now, can be undeniable vulnerability next minute, which shows speed and exercise in the cyber today.

The purpose of this report is also to highlight the current threats that are unembittering to the cyberworld, mechanisms to identify those threats, using tools and implementation of techniques to mitigate those threats, further investigating the attack and mitigation techniques.

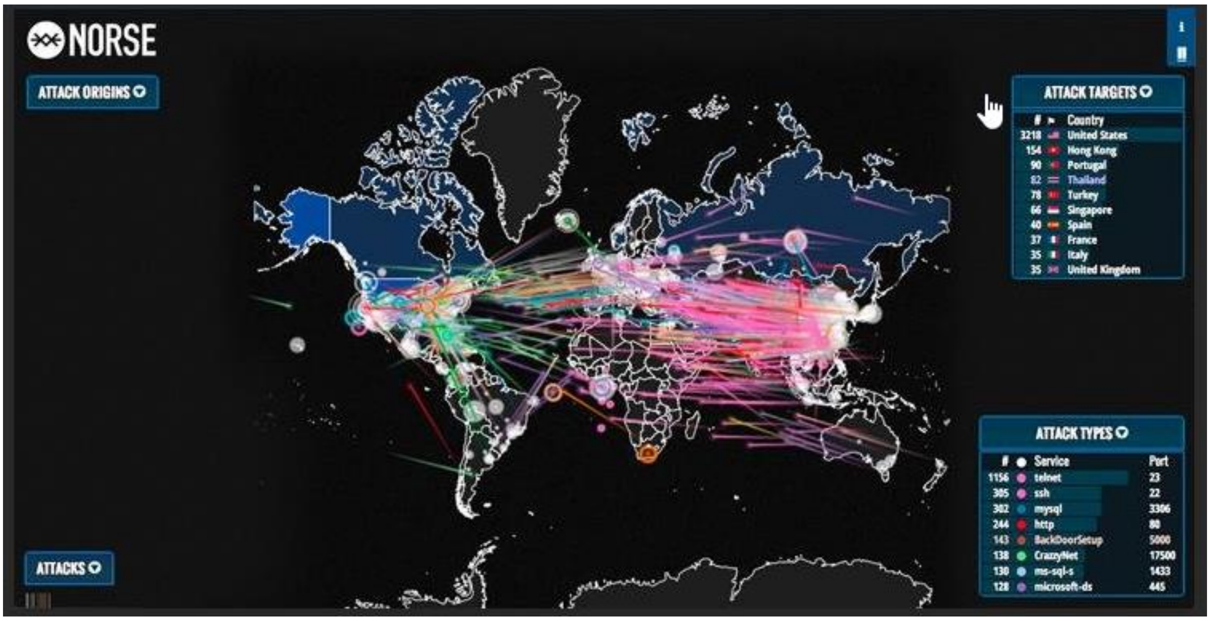
This report is written for the academic purpose as the assessment for system securities, in which I have investigate different types of cyber threats prevailing in the present condition, from which I expect, the readers will get mindful information about the cyberspace and evolving risks and can also analyse different Threats. The information is collected from different sources, reports, which I have clearly referenced and anyone willing to go in depth for the chosen term can visit the related references.

Thank you!

# Table of Contents

# Introduction

Cyberspace is the concept which describes a widespread global interconnected computer network to facilitate online communication, which largely consists of the artifacts/source based on or dependent on computer and communications technologies, information about using, storing, handling, and processing the information of those artifacts used and the interconnections between them. Further, the relation to the use of the global Internet/cyberspace for diverse purpose, example the commerce to entertainment, has created the pretty conformist and one-dimensional relation to what could exit, in an individual's level and social level, which are always evolving, and being more diverse in the years to come [1] [2].The dependence on IT, antisocial behaviours of mankind -dominating others for self-gains, and inevitability having vulnerabilities lots of cyber threats occur in the cyberspace, daily. [3]NORSE believes, we can view real-time attacks occurring around the globe that gathers critical threat intelligence on these attacks, live, and can be helpful to determine hostile activities in the cyberspace and maintaining security for the enterprises working with them.



ATTACK TARGETS

| # | Country |
|---|---|
| 3218 | United States |
| 154 | Hong Kong |
| 90 | Portugal |
| 82 | Thailand |
| 78 | Turkey |
| 66 | Singapore |
| 40 | Spain |
| 37 | France |
| 35 | Italy |
| 35 | United Kingdom |

ATTACK TYPES

| # | ● | Service | Port |
|---|---|---|---|
| 1156 | ● | telnet | 23 |
| 305 | ● | ssh | 22 |
| 302 | ● | mysql | 3306 |
| 244 | ● | http | 80 |
| 143 | ● | BackDoorSetup | 5000 |
| 138 | ● | CrazzyNet | 17500 |
| 130 | ● | ms-sql-s | 1433 |
| 128 | ● | microsoft-ds | 445 |

**Fig: Norse, real-time intrusions.**

Although, there are different types of attacks, an attacker can use to intrude to other network and devices unauthorizedly, which are mostly done by compromising target network, injecting malwares, social engineering, and are done to gather information or to compromise the accessibility of the service. In this report, as well, we will talk about some current threats in the world. The data shows about 67% financial institutions faced some type of intrusion, in which 26% were destructive in the past few years. They believe more sophisticated attacks are performed by the attackers. 25% of the of the organizations experienced malware attacks in which most are the financial offices. Also, web attacks were 46%, 28% access attacks, final and least DDOS attack with 8%. For the response to that 69% financial organisations had planned to increase their security by spending 10% more, in 2019. The security techniques include the protection of digital devices, data, ensuring only the right person has access the data in right time [4].

## Security Threats

Cybersecurity threats helps to analyse the risk after the cyberattack, which are the intentional and malicious efforts by any organizations or an individual to breach the systems of another organization or individual, which can be impossible for every organization to prepare for all of them. MITRE mentions, Threat Assessment and Remediation Analysis (TARA) provides clear Tactics, techniques, and Procedure (TTP) analysis which is developed by them [4]. Also, there are many cybersecurity frameworks which are the structures, containing processes, practices, and technologies which anyone can use to maintain secure network from intruders. ISO IEC 27001/ISO 27002, NIST Cyber security Framework are some top frameworks [5].

### Current and major threats

Cybersecurity threats can be taken from different angles, basically, threats appear in weak system because anyone with the simple knowledge (script kiddies) in computers can be the threats for them, whereas strong mechanisms can be deployed to reduce the attack surface physically and virtually, which also reduces the risks. Secure organisations not only test their network but also monitors and controls the traffic and data that is approaching and exceeding the network, with proper risk assessments techniques like Disaster Recovery Management, disaster recovery service (DRaaS) [6]. Malware and ransomware attack, social engineering attacks, Software Supply chain attacks, Distributed Denial of Service (DDoS attack), password attack and other types of attacks commonly used network attacks [4]. Nonetheless, zero-day attacks; the attacks which the attacker uses in the target for the first time, form which developers are unaware with are also evolving dramatically in the trends of past few years. I will briefly describe the trend of higher threats of attacks like Ransomeware and Malware attack, social engineering attack and zero-day attack briefly.

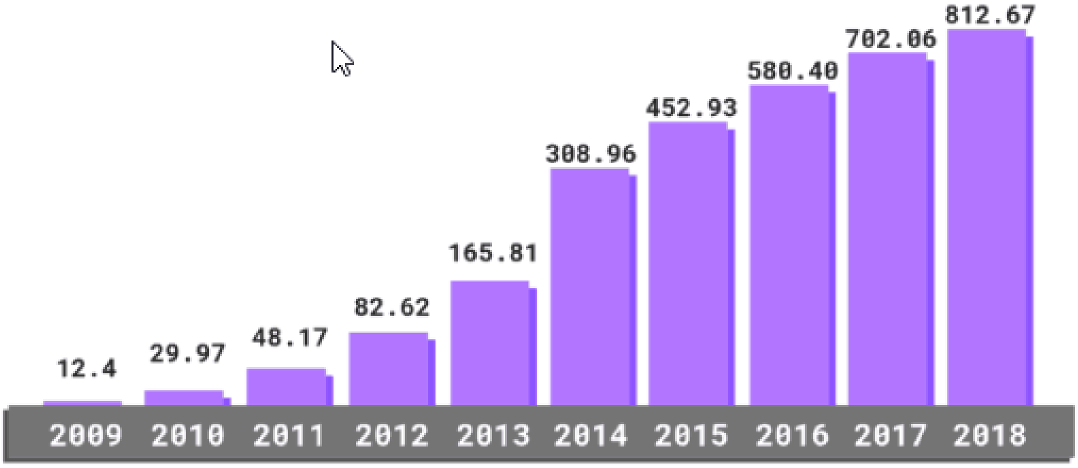
## Ransomware and Malware attacks

Ransomware attack is a form of Malware attack, in which attacker injects the malware to target computer using phishing, suing virus, trojans and other techniques and encrypts all the data and insist to provide to the key only after the ransom is paid. There are different types of Malware attacks which includes trojan virus, Ransomware, worms, Spyware, botnets and so many.

Malware, especially ransomware, is leading the serious problems for the organizations. Not only these types of attacks are increasing but also the rate of the ransom which the victim must pay has also been increased [8]. Wannacry [9] ransomware is an example of popular Ransomware.

The average ransomware payment was increased by 82%, where largest demand was $100 million. Ransomware attacks increased 41% in 2019 with 205,000 businesses lose their files. In that 20% victims were small to mid-sized businesses, with average of 645 employees in a company.

Likewise, the malware attack in 2009 was 12.4 million which increased to 812.67 million in 2018. Mostly the malwares are delivered by email and 98% malware targets Android devices. Almost 45% of all malwares is Trojans. Virus, Worms, and botnets are other types of malwares. It was predicted after 2021, a business will be victimized every 11 seconds, and the cost will rose to $20 billion, which is 57 times in 2015 [8].



Total Malware Infection Growth Rate (In Millions)

[4]

### Social Engineering attacks

Social engineering is an access attack in which malicious actor attempts to lure individuals or employees to perform malicious actions or try to access the confidential information. Phishing, Spear phishing, tailgating, baiting, pretexting are common ways to perform social engineering attacks [10].

In 2020, United State record phishing as the most common cybercrime. Social engineering alone, compromise 70% of data breaches and 96% of them uses email, also there are more than two million phishing websites. Up to 2022 an average organization was facing 700 social engineering threats per year. In covid pandemic about 47% employees fall for the phishing scams[11]. SaaS companies and webmail providers and financial institutions are highly targeted for social engineering attacks, which is 34.7% and 18% respectively [4].

### Zero-day attacks

The data from 'purplesec' shows 28 number of zero-day attack were recorded in 2011, which hit the peak of 41 in 2013, which then dramatically reduced to 34 for next three years and kept fluctuating after 2017 between 29 – 40 numbers and hit the peak ever with 66 numbers recorded in 2021 [7].

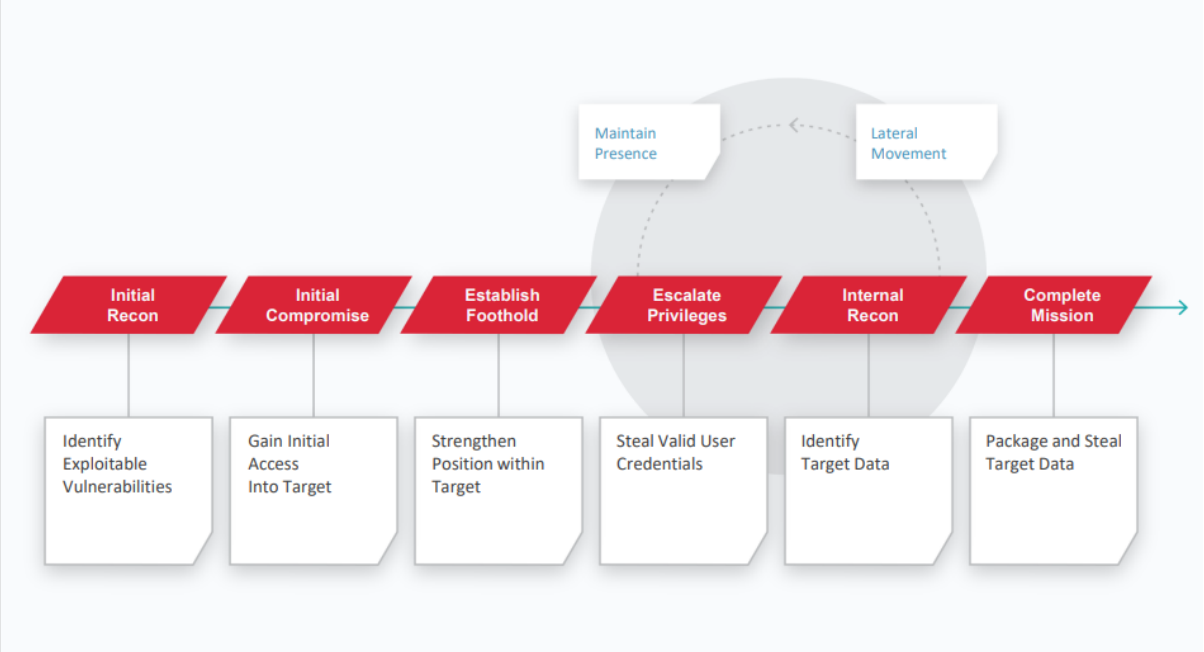
Let's have a look detailly into some of these attacks and the statistics in the past years. Zero-day attack responsible for about 42% of all attacks in 2021, Also in 2019, 80% successful attacks were from this attack. Memory Corruption 67%, Logic/Design Flaw 14%, Information Leaks 5% were common types of zero-day attacks exploits [4].

| **Year** | **2011** | | **2012** | **2013** | **2014** | **2015** | **2016** | **2017** | **2018** | **2019** | **2020** |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **Total zero-day attacks** | 28 | | 25 | 41 | 34 | 35 | 34 | 40 | 31 | 29 | 66 |

## Use of tools and Implementation of techniques

Different tools are used to conduct different types of tools, one can use their own tools and methods to conduct an attack, however ISSAF, OWASP, NIST these are some well known methodologies using the tools [12]. Blackhat are the unethical hackers, who penetrate other's network for the self-gains and for revenge, whereas white hat are the ethical hackers who are legal and are to penetrate the network with legal written consent of the organization. Greyhat, brown hat, hacktivists, script-kiddies are types of hackers [13]. Every attack can be done in certain phases which has the create a cycle, I will briefly describe the types of tools used to perform above mentioned attacks.

## Attack lifecycle


Maintain Presence
Lateral Movement
Initial Recon
Initial Compromise
Establish Foothold
Escalate Privileges
Internal Recon
Complete Mission
Identify Exploitable Vulnerabilities
Gain Initial Access Into Target
Strengthen Position within Target
Steal Valid User Credentials
Identify Target Data
Package and Steal Target Data

[14] fig Attack life cycle.

**Reconnaissance:**

In this stage attacker, attacker collects the publicly available information about the company. Web browser, social medias are the main source for the initial reconnaissance. Emails, messaging handling and contact information. Tools like aquatone and Datasploit can be used for initial recon. For the Advance Persistent Threat different types of attacks like above described can be done in different stages for fully compromise the network.

**Intrusion:**

Social Engineering attacks can give fast and easy completion of this phase. Phishing, spear phishing attacks, watering hole attacks using the information from previous stage can be done in this phase. Phishing attacks can be done by luring any employees to click to the malicious emails, websites to inject the codes to their devices. Watering hole can be done by infecting the services any organization use. Spear phishing is done for the targeted person, whaling is to go after chief employees in an organization. More than 80% security incidents reported were phishing, out of which 65% was spear phishing attack [15]. Ransomware attacks can be conducted injecting the malware from phishing. Tools such as TOR, ZeroNet and I2P are most frequently used for staging coordinated ransomware attacks [16].

**Infection:**

Initial backdoor can is established by the malware, trojans are known as the backdoor malware, which an attacker can use to use remotely to connect to targeted machine. Metasploit can be useful to create backdoor. Zero-day attack code can be executed in this phase, bypassing the security. Operating system vulnerabilities code to exploit them are zero-day code which has no previous signature can bypass the firewalls. Further, internal reconnaissance is not to determine the services and software the organization is using. Nmap, Nessus, Burpsuite, nikto, etc can be used.

**Credential theft:**

Different social engineering and malwares along with brute forcing can bring luck in this phase. Gaining passwords using malwares like key-loggers, spywares, botnets and social engineering techniques like phishing, shoulder surfing can be used for getting the passwords. Default and weak passwords can be easily cracked using brute forcing. Hashcat, john the ripper is used to crack the password, where as hydra can be useful for brute forcing. Gaining administrative credential is main aim of attacker.

**Lateral Movement**

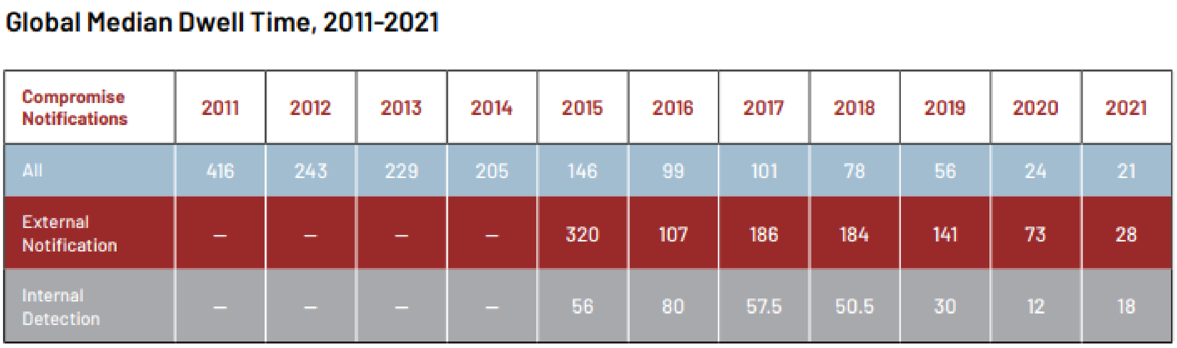
One compromised device can give lead for the other devices in an organization, which allows persistence to the attacker over different devices which is termed as 'pivoting'.

**Data Exfiltration**

An advance persistence threat (APTs) is to collect information that could be damaging to the company. Hacktivism, extortion attack is seen in these phases. Saudi Aramco is an example of cyber extrusion attack and asked for the ransom of about $50 Million [17].

**Persistence**

The longer the attacker undetected inside the network the more damage he can cause, which can be achieved by persistency. Attacker must keep moving back and forward phase to maintain persistence in another network. The average dwell time in 2021 was 21 compared to 24 days in 2020.



Global Median Dwell Time, 2011-2021

| Compromise Notifications | 2011 | 2012 | 2013 | 2014 | 2015 | 2016 | 2017 | 2018 | 2019 | 2020 | 2021 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| All | 416 | 243 | 229 | 205 | 146 | 99 | 101 | 78 | 56 | 24 | 21 |
| External Notification | – | – | – | – | 320 | 107 | 186 | 184 | 141 | 73 | 28 |
| Internal Detection | – | – | – | – | 56 | 80 | 57.5 | 50.5 | 30 | 12 | 18 |

Fig: Global Dwell time in 2011 to 2021 [14]

Overall, it shows different attack techniques can be used to achieve advance persistence threat. In different stage of an attack different tools were useful. For the desired attacks performed by different person varies depending on the skills, knowledge they used. APT can be achieved following frameworks properly with advance technical knowledge, to cause greater harm to an organization..

## Mitigation techniques

As we have already discussed, there is no way to get 100 percent guaranteed secure system, however we can reduce the attack surface in any system. Many systems approach the technologies like defence in depth, secure Architecture, security policies access control, found to be incredibly effective. Nonetheless, organizations should have some Disaster Recovery Management to minimize the risk of an attack.. Despite of these factors, confidentiality, integrity, and Accessibility (CIA)triad is a common model basic for developing security systems. Basic techniques such as Antivirus, IPS/IDS, VPN, Firewalls, ESA/WSA with proper authentication, secure ports and protocols, updated software's, encryption with secure authentication, are common techniques for overall protection and maintain compliance, however different threats should be handled and can be mitigated differently.

If we consider the threats, I have described they are done using different processes and targeted to different resources. Malware attacks are mostly done in end devices, Zero-days in ISO or operating systems, and social engineering are targeted to staffs, or individuals.

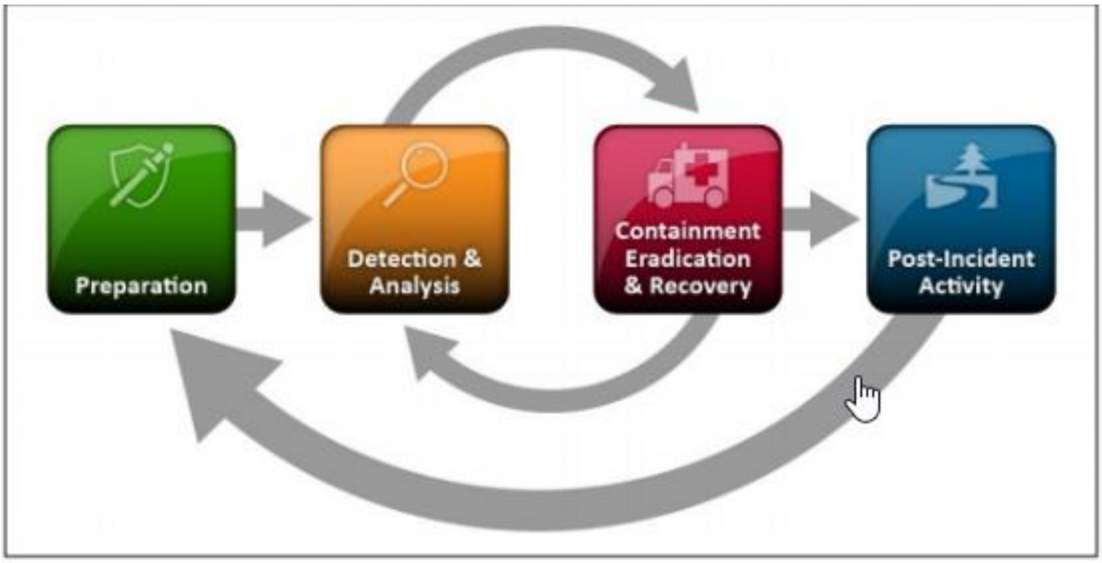
Mitigating Social Engineering: such types of attacks can be mitigated raising the awareness, trainings, and implementing the security policies to the users/members about using the resources and dealing with the suspicious activities (mails, weblinks). The social Engineering Toolkit [18] (SET) can be use by the white hats and other security professionals to test their network against social engineering. The data shows, 45% of employees were unaware of phishing, and only 27% of companies were providing social engineering awareness training in 2022 [11].

Mitigating Zero-day attack: The attacker launches the exploit to the vulnerability, from which any software and anti-virus vendors are unaware, which makes zero-days more likely to succeed. However, vulnerability scanning, patch management, Inputting validation and sanitizing websites, application can reduce the zero-day attacks [19]. Security professors should be updated or close with security organizations such as CERT, SANS, MITRE, (ISC)2 and many more for latest threats, news, and secure mechanisms. Oracle virtual box 5.2.20 and older, had unpatched zero day disclosed by Russian security researcher sergey Zelenyuk [20], which shows vulnerability scanning and patching are helpful to mitigate zero-day attack.

Mitigating Malware attacks: Antivirus software, firewalls are highly recommended techniques to mitigate malware attacks, malware contains the malicious signature which these devices or software detects which filters and drops. Overall, Malware are injected in a system using phishing techniques using emails and websites containing malware, can be minimized using awareness, and secure Architecture and backups. Further, prevention and treatment of malware being spread is crucial. Cisco suggests the response to the worm can be done in four phases:

- **Containment** – It is the phase to limit the spread of worm to areas that are already affected. Segmentation and compartmentalization of network using the ACLs and firewalls.
- **Inoculation** – Along with containment, patching the uninfected systems should be done.
- **Quarantine** - Tracking down to infected machines from containment and isolating these systems disconnecting, blocking, or removing them.
- **Treatment** - This involves actively disinfecting infected systems, propagation of worms is terminated, modified files or settings are removed, and vulnerability is patched.
  [21].

**NIST Incident response lifecycle.**



[22]

Implementation of NIST 800-171 requirements is a good way to mitigate risk and minimize data loss and crucial for maintaining compliance and continuity of the business. Redline is also a great tool for monitoring and reporting the incidence.

## Conclusion:

The crusade between the morality and immorality is a long and on-going process in cybersecurity as well. The struggle for protecting and exploiting the technology has really helped for the advancement of cyberspace. In this report as well, we evaluate the modern threats, the way they are performed, and the ways to minimize and mitigate those threats. We briefly analysed different types of threats, which are executed in different ways whose purpose were different, and nonetheless mitigating techniques were different which I believe has provided different angles and approach for related incident. The data presented shows the enormity and analyse risk in practical world for each attack vector. Further, from the attacking cycle we evaluated different attacks can be performed to achieve the advance persistence threat, and from the Incidence response lifecycle we overviewed the process to mitigate already exploited devices. In conclusion, I believe the system security approach should be initiate from deploying to destroying any system, because we must keep in mind, attacker may only be successful one time, but defenders must be successful every time.

# References

[1] Techopedia, “What does Cyberspace Mean?,” 2022 05 2022. [Online]. Available: https://www.techopedia.com/definition/2493/cyberspace.

[2] wikipedia, “Cyberspace,,” 2 06 2022. [Online]. Available: https://en.wikipedia.org/wiki/Cyberspace.

[3] NORSE, “New Norse Live Attack Map Opens Window Into Global Cyber Attacks In Real Time,” [Online].

[4] purplesec.us, “cybersecurity-statics,” 2022. [Online]. Available: https://purplesec.us/resources/cyber-security-statistics/#ZeroDay.

[5] O. Cassetto, “21 Top Cybersecurity Threats and How Threat Intelligence Can Help,” exabeam, 01 06 2022. [Online]. Available: https://www.exabeam.com/information-security/cyber-security-threat/#MITRE.

[6] G. Mutune, 09 01 2019. [Online]. Available: https://cyberexperts.com/cybersecurity-frameworks/#:~:text=%2023%20Top%20Cybersecurity%20Frameworks%20%201%20ISO,the%20SOC%202%20framework.%20The%20framework’s...%20More%20.

[7] hystax, “7 reasons why your business needs disaster recovery as a service,” 17 03 2021. [Online]. Available: https://hystax.com/7-reasons-why-your-business-needs-disaster-recovery-as-a-service/#:~:text=Disaster%20Recovery%20as%20a%20Service%20%28DRaaS%29%20main%20benefits,6%20Accessibility.%20...%207%20External%20IT%20expertise.%20.

[8] Packetlabs, “Cybersecurity Statistics for 2021,” 03 08 2021. [Online]. Available: https://www.packetlabs.net/posts/cybersecurity-statistics-2021/#:~:text=In%202021%3A%2085%25%20of%20breaches%20involved%20a%20human,engineering%20was%20observed%20in%20over%2035%25%20of%20incidents.

[9] wikipedia, “WannaCry ransomware attack,” [Online]. Available: https://en.wikipedia.org/wiki/WannaCry_ransomware_attack.

[10] cisco, “Principles of Network security,” [Online]. Available: https://hacc.hawaii.gov/wp-content/uploads/2020/05/CyOps-Presentation.pdf.

[11] N. Galov, “17+ Sinister Social Engineering Statistics for 2022,” 14 04 2022. [Online]. Available: https://webtribunal.net/blog/social-engineering-statistics/#gref.

[12] D. Gkoutzamanis, “Five Penetration Testing Frameworks and Methodologies,” 4 05 2020. [Online]. Available: https://cisotimes.com/five-top-penetration-testing-frameworks-and-methodologies/.

[13] malwarebytes, “Hacking definition: What is hacking?,” [Online]. Available: https://www.malwarebytes.com/hacker.

[14] D. Seth, “Incidence response,” Boxhill, 2022.

[15] soanning, “Cyberattacks 2021: Phishing, Ransomware and data Breach Statics,” spanning cloud apps, 2021. [Online]. Available: https://spanning.com/blog/cyberattacks-2021-phishing-ransomware-data-breach-statistics/#:~:text=According%20to%20CISCO's%202021,14%20malicious%20emails%20every%20year..

[16] blackfog, “Anonymous Ransomware Attack Tools,” 22 06 2021. [Online]. Available: https://www.blackfog.com/anonymous-ransomware-attack-tools/#:~:text=TOR%2C%20ZeroNet%2C%20and%20I2P%20are,for%20staging%20coordinated%20ransomware%20attacks..

[17] Purplesec, “Saudi Aramco $50 Million Data Breach Explained | Breach Report,” 05 08 2021. [Online]. Available: https://www.youtube.com/watch?v=CYritZGDC2I&t=20s.

[18] TrustedSec, “THE SOCIAL-ENGINEER TOOLKIT (SET),” [Online]. Available: https://www.trustedsec.com/tools/the-social-engineer-toolkit-set/.

[19] imperva, “Zero-day (0day) exploit,” [Online]. Available: https://www.imperva.com/learn/application-security/zero-day-exploit/.

[20] L. Constantin, “Zero-Day Exploit Published for VM Escape Flaw in VirtualBox,” 08 11 2018. [Online]. Available: https://securityboulevard.com/2018/11/zero-day-exploit-published-for-vm-escape-flaw-in-virtualbox/.

[21] Cisco, “What Is a Worm?,” [Online]. Available: https://www.cisco.com/c/en/us/products/security/what-is-a-worm.html.

[22] P. B. A. W. P. D. G. D. L. Marianne swanson, “NIST Special Publication 800-34 Rev. 1,” NIST, 2010.