



INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Future Trends And Threats In Cyber Crime And Scams

Dr Naveen Kumar Sharma^{#1}, Mr. Abhishek Kumar Singh^{#2}, Priyanshu Vatsaya^{#3}, Pulkit Asthana^{#4}, Adarsh Tiwari^{#5}

Intellectual Institute of Management and Technology(IIMT) Greater Noida Uttar Pradesh

Abstract- The term cyber security is often employed interchangeably with the term protection of information. This paper argues that while cyber security and information protection are significantly similar, these two terms are not completely comparable. In addition, the paper argues that cyber security stretches beyond conventional information security definitions to include not only the protection of information data, but also that of other properties, including the individual himself. In information protection, reference to the human factor is generally linked to human's role(s) in the process of protection. In cyber security this aspect has a further element, namely, humans as possible targets of cyber-attacks or even engaging unknowingly in a cyber assault. This additional aspect has ethical consequences for society as a whole, as it may be seen as a social obligation to protect such marginalized groups, for example children.

KEYWORDS- Cyber Security, Cyber Attack, Malware, SQL Injection, Supply chain

INTRODUCTION

An effective cybersecurity method has numerous layers of defense spread across the networks, computers, programs, or information's that one aims to keep non-toxic. In a society, the processes, the people and tools must all accompaniment one alternative to generate a real defence on or after cyberattacks. In the intricate tapestry of our digital age, where information flows seamlessly across interconnected networks, the significance of cybersecurity cannot be overstated. This introduction delves into the multifaceted realm of

cybersecurity, exploring the persistent threats, evolving attack landscapes, preventive strategies, and the looming challenges that shape the future of safeguarding our digital world .

Consumers must appreciate and obey with basic information's security ethics like selecting strong passwords, actuality wary of accessories in email, and back-up up data. Learn extra around basic cybersecurity values. Implementing cyber security has software, hardware and human components. Antivirus software and firewalls can help prevent unauthorized access to private data. Governments, businesses and individuals are all potential targets, and the consequences of cyberattacks can be severe, ranging from financial losses and reputational damage to the compromise of sensitive information and even national security risks like CovidLock, ransomware, 2020.

Cybersecurity is the frontline defense against an array of threats that constantly evolve with technological advancements. Malware, phishing, ransomware, and sophisticated hacking techniques pose persistent dangers to the confidentiality, integrity, and availability of data. As technology continues to shape our digital future, the resilience of cybersecurity practices remains pivotal in preserving the trust and security of our interconnected world.

Threats of Cyber Security

This figure shows the types of cyber security threats-



Figure 1: Types of threats
Here are some threats which we explaining :-

1. Malware Attacks

Malware is an abbreviation of “malicious software”, which includes viruses, worms, trojans, spyware, and ransomware, and is the most common type of cyberattack. Malware infiltrates a system, usually via a link on an untrusted website or email or an unwanted software download. It deploys on the target system, collects sensitive data, manipulates and blocks access to network components, and may destroy data or shut down the system altogether.

This is the case of malware attack:-

CovidLock, ransomware, 2020

Fear in relation to coronavirus (COVID-19) has been widely exploited by cybercriminals. CovidLock ransomware is an example. This type of ransomware infects victims via malicious files promising to offer more information about the disease.[3]

3. Supply Chain Attacks

Supply chain attacks are a new type of threat to software developers and vendors. Its purpose is

The problem is that, once installed, CovidLock encrypts data from Android devices and denies data access to victims. To be granted access, you must pay a ransom of USD 100 per device.

2. Phishing

The attacker sends emails pretending to come from a trusted source. Phishing often involves sending fraudulent emails to as many users as possible, but can also be more targeted. For example, “spear phishing” personalizes the email to target a specific user, while “whaling” takes this a step further by targeting high-value individuals such as CEOs. [4]

This is the case of Phishing:-

□ Facebook and Google (2013-15)□

Between 2013 and 2015, Facebook and Google were tricked out of \$100 million due to an extended phishing campaign. The phisher took advantage of the fact that both companies used Quanta, a Taiwanbased company, as a vendor. The attacker sent a series of fake invoices to the company that impersonated Quanta, which both Facebook and Google paid.[5]

Eventually, the scam was discovered, and Facebook and Google took action through the US legal system. The attacker was arrested and extradited from Lithuania, and, as a result of the legal proceedings, Facebook and Google were able to recover \$49.7 million of the \$100 million stolen from them.

to infect legitimate applications and distribute malware via source code, build processes or software update mechanisms.[6]

This is the case of Supply Chain attacks:-

SolarWinds (2020)□

In December 2020, the network management software company SolarWinds got hacked, resulting in a widespread breach of multiple government agencies and private companies. A total of 18,000 customers and businesses got impacted. The attack was traced back to a malicious software update added to SolarWinds' Orion software, demonstrating the importance of secure software updates in the supply chain.[7]

4. SQL Injection

An attacker enters an SQL query into an end user input channel, such as a web form or comment field. A vulnerable application will send the attacker's data to the database, and will execute any SQL commands that have been injected into the query. Most web applications use databases based on Structured Query Language (SQL), making them vulnerable to SQL injection. A new variant on this attack is NoSQL attacks, targeted against databases that do not use a relational data structure.[8]

This is the case of SQL Injection: -

7-Eleven breach□

A team of attackers used SQL injection to penetrate corporate systems at several companies, primarily the 7-Eleven retail chain, stealing 130 million credit card numbers.

ATTACKS OF CYBER SECURITY

Cyber-attack is a big issue in the cyber world that needs to be focus because of the effect on the critical infrastructure and data. The growth of technology is accompanied by cyber security threats or "cyber-attacks" which threaten users security when using such techniques.

Cyber threats and attacks are difficult to identify and prevention. So users are not accepting the new technology due to the frequently cyberattacks less security of data. A cyber-attack is when someone gain or attempts to gain unauthorized access to a computer maliciously. [1]

5. Password Attacks

Techniques such as brute-force attacks, credential stuffing, or password spraying to gain unauthorized access by exploiting weak or compromised passwords.

This is the case of Password Attacks: -

Ticketmaster□

At the very beginning of 2021, Ticketmaster pleaded guilty to a charge of repeatedly and illegally accessing competitors' computers. Ticketmaster admitted that an employee who previously worked for a rival company handed over to Ticketmaster executives confidential internal documents that he'd kept from his former employer, as well as the login credentials for multiple corporate accounts that the rival company used to manage ticket presales. The employee even demonstrated—at a division wide summit attended by other Ticketmaster employees—how to hack into an account at the rival company.[9] Ticketmaster was charged with violations of the Computer Fraud and Abuse Act, computer intrusion for commercial advantage or private financial gain, computer intrusion in furtherance of fraud, wire fraud conspiracy, and wire fraud. As part of a deferred prosecution agreement, the ticket sales company had to pay a \$10 million fine to resolve these charges.[10]

Untargeted attacks- Un-targeted attacks in attackers indiscriminately target as users and services possible. They find the vulnerabilities of the service or network.

They encouraging the visits of fake website and give the good offers. The customers click on the links on the email to enter their information. dummy website or compromising a legitimate one in order to exploit visiting user's information.

Ransom ware: It includes spread disk encrypting extortion malware. Scanning: Attacking wide swathes of the Internet at random.

Targeted attacks- Targeted attacks in attackers, attack on the targeted users in the cyber world.

Spear-phishing Sending links of malicious software and advertisement via emails to targeted individuals that could contain for downloads malicious software. [2]

It is deliver a DDOS (Distributed Denial of Service) attack Subverting the supply chain. To attack on network or software being delivered to the organization In general attackers will, in the first instance use tools and techniques to probe your systems for an exploiting vulnerability of the service. [3]

This figure which shows attack:-

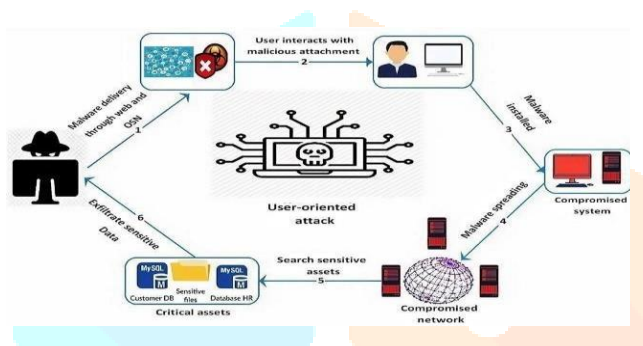


Table 1 shows some of main types of malware attacks are:-[4]

S.No	Malware Types	Description
1.	Viruses	A piece of code injects itself into an application
2.	Worms	hat exploits software vulnerabilities and backdoors to gain access to an operating system.
3.	Trojans	Malicious code or software that poses as an hiding in apps or games.
4.	Ransomware	A user is denied access to their own systems or data.
5.	Spyware	A malicious actor gains access to an unsuspecting user's data, including sensitive information such as passwords and payment details.

Figure 2 which shows about Cyber Security attacks work.[2]

Some attacks of Cyber Security are:-

A. Malware Attacks

Malware is an abbreviation of “malicious software”, which includes [viruses](#), worms, trojans, spyware, and ransomware, and is the most common type of [cyberattack](#). Malware infiltrates a system, usually via a link on an untrusted website or email or an unwanted software download. It deploys on the target system, collects sensitive data, manipulates and blocks [access](#) to network components, and may destroy data or shut down the system altogether.[4]

B. Supply Chain Attack

Supply chain attacks are a new type of threat to software developers and vendors. Its purpose to infect legitimate applications and distribute malware via source code, build processes or software update mechanisms.

Compromise of build tools or development pipelines

Compromise of code signing procedures or developer accounts

Malicious code sent as automated updates to hardware or firmware components

Malicious code pre-installed on physical devices

C. Social Engineering Attack

Social engineering involves tricking users into providing an entry point for malware. The victim provides sensitive information or unwittingly installs malware on their device, because the attacker poses as a legitimate actor.

Table 2 some of the main types of social engineering attacks[5]

S.No	Types	Description
1.	Phishing	The attacker sends emails pretending to come from a trusted source.
2.	Vishing	The imposter uses the phone to trick the target into disclosing sensitive data or grant access to the target system.
3.	Smishing	The attacker uses text messages as the means deceiving the

Table 1 shows some of main types of malware attacks are:[6]

S.No	Types	Description
1.	SQL Injection	An attacker enters a SQL query into an end user input channel
2.	Code Injection	An attacker can inject code into an application if it is vulnerable

PREVENTION FROM THREATS AND ATTACKS

1. Train our staff

One of the most common ways cyber criminals get access to your data is through your employees.

They'll send fraudulent emails impersonating someone in your organisation and will either ask for personal details or for access to certain files. Links often seem legitimate to an untrained eye and it's easy to fall into the trap. This is why employee awareness is vital.

One of the most efficient ways to protect against cyber-attacks and all types of data breaches is to train your employees on cyber-

		victim.
--	--	---------

D. Injection Attacks

Injection attacks exploit a variety of vulnerabilities to directly insert malicious input into the code of a web application. Successful attacks may expose sensitive information, execute a DoS attack or compromise the entire system.

attack prevention and inform them of current cyber-attacks.[4]

They need to:

Check links before clicking them Check email addresses from the received email ([have a look here on how to check it](#))

Use common sense before sending sensitive information. If a request seems odd, it probably is. It's better to check via a phone call with the person in question before actioning the "request".

2. Keep your software and systems fully up to date

Often cyber attacks happen because your systems or software aren't fully up to date, leaving weaknesses. So cybercriminals exploit these weaknesses to gain access to your network. Once they are in – it's often too late to take preventative action.

To counteract this, it's smart to invest in a patch management_system that with manage all software and system updates, keeping your system resilient and up to date.[1]

3.Install a Firewall

There are so many different types of sophisticated data breaches and new ones

surface every day and even make comebacks.

Putting your network behind a firewall is one of the most effective ways to defend yourself from

4. Backup your data

In the event of a disaster (often a cyber attack) you must have your data backed up to avoid serious downtime, loss of data and serious financial loss.

5. Passwords

Having the same password setup for everything can be dangerous. Once a hacker figures out your password, they now have access to everything in your system and any application you use. Having different passwords setup for every application you use is a real benefit to your security, and changing them often will maintain a high level of protection against external and internal threats. [3]



Prevention: If you were to secure your network, prevention would be using the firewall, security software and end user use the antivirus software. You are doing everything possible to keep the threat out.

Detection: You want to be sure you detect when such failures happen. Everyday update the security software as well as hardware.

any cyber attack. A firewall system will block any brute force attacks made on your network and/or systems before it can do any damage, something we can help you with. [2]

Fig 3 It shows how prevention work prevention[8]

The parameters for prevention from Cyber security attack and threats are as follows:

Identify threats.

Identify vulnerabilities.

Access risk explore

Establish contingency plan.

Respond to cyber security accident.

Establish contingency plan.



FIG 4 PARAMETERS OF CYBERSECURITY [8]

Results and Analysis

Secure the System There are basic three methods to secure the system from outsider threat and attack.

Reaction: Detecting the failure has little value if you do not have the ability to respond. If anything it's happen so your security software warn. [1]

Preventing from Attack and Threats

Recovering from Viruses, Worms, and Trojan Horses
 Avoiding Social Engineering and Networking Attacks
 Avoiding the Pitfalls of Online Trading

Using Caution with USB Drives
 Securing Wireless Networks

Preventing from Email and communication [2]

Using Caution with Email Attachments
 Reducing Spam
 Using Caution with Digital Signatures
 Using Instant Messaging and Chat Rooms Safely
 Staying safe on social Network Sites

Safe Browsing [3]

Evaluating Your Web Browser's Security Settings
 Shopping Safely Online
 Web Site Certificates
 Bluetooth Technology [4].

Future Work

ahead becomes pivotal for a safer online environment. Organizations are finding themselves under the pressure of being forced to react quickly to the dynamically increasing number of cybersecurity threats. Since the attackers have been using an attack life cycle, organizations have also been forced to come up with a vulnerability management life cycle. The vulnerability management life cycle is designed to counter the efforts made by the attackers in the quickest and most effective way. This chapter has discussed the vulnerability management life cycle in terms of the vulnerability management strategy. It has gone through the steps of asset inventory creation, the management of information flow, the assessment of risks, assessment of vulnerabilities, reporting and remediation.

The future aim for cybersecurity involves a proactive and adaptive approach to counter emerging threats in the evolving digital landscape.[4] The field of advanced threat detection in cybersecurity and scam prevention is dynamic and continuously evolving as cyber threats become more sophisticated. To work in this area is likely to focus on advanced threat detection by learning models for anomaly detection and behaviour analysis to identify subtle and complex patterns indicative of advanced threats. Enhancing threat intelligence capabilities to provide more context around indicators of compromise, allowing organizations to understand potential impact of threats.[1]

CONCLUSION

In the ever-connected digital landscape, safeguarding against cyber threats and scams is paramount. Vigilance and awareness serve as our first line of defense. By staying informed, adopting secure practices, and fostering a culture of cyber resilience, we can collectively mitigate risks. Cybersecurity is a shared responsibility, and as technology evolves, our commitment to staying one step

REFERENCES

1. S. Huda et al., "A Malicious Threat Detection Model for Cloud Assisted Internet of Things (Cot)...", Journal of Parallel and Distributed Computing, 2018.
2. Xiao, Z. et al., "Malware Detection based on Deep Learning of Behavior Graphs", Mathematical Problems in Engineering, 2019.
3. G.D.L.T. Parra et al., "Detecting Internet of Things attacks using Distributed Deep Learning", Journal of Network and Computer Applications, 2020.
4. Facebook and Google Phishing Case Report (2013–2015) – Legal and Cybersecurity Incident Records.
5. SolarWinds Supply Chain Attack Report, U.S. Cybersecurity Infrastructure and Security Agency (CISA), 2021.

6. SQL Injection and 7-Eleven Breach – U.S. Department of Justice Records, 2009.
7. Ticketmaster Legal Settlement Press Release, U.S. Department of Justice, 2021.
8. NIST Special Publication 800-61, “Computer Security Incident Handling Guide”, National Institute of Standards and Technology.
9. OWASP (Open Web Application Security Project) – Top 10 Cybersecurity Threats.
10. ENISA Threat Landscape Report 2023 – European Union Agency for Cybersecurity.

