

Task 'Cyberattack Case File Origins Methods and Mitigation' Unit 1

Cyberattack Report

INTRODUCTION	2
PURPOSE OF THE REPORT	3
SCOPE	4
OVERVIEW OF CYBERATTACKS AND GENERAL DESCRIPTION	4
TABLE 1: MITRE ATT&CK ALIGNED CRITICALITY RATING	5
1. PHISHING ORIGIN & HISTORY	7
1.1. How the Phishing Attack Works	7
1.2. Phishing Best Practice Mitigation Strategies	7
1.3. Modern Protection Tools & Techniques	7
2. SQL INJECTION ORIGIN & HISTORY	7
2.1 How the SQL Injection Attack Works	8
2.2. SQL Injection Best Practice Mitigation Strategies	8
2.3. Modern Protection Tools & Techniques	8
3. RANSOMWARE ORIGIN & HISTORY	8
3.1. How the Ransomware Attack Works	9
	1

Task ‘Cyberattack Case File Origins Methods and Mitigation’ Unit 1

3.2. Ransomware Best Practice Mitigation Strategies	9
3.3. Modern Protection Tools & Techniques	9
4. DENIAL-OF-SERVICE (DOS) ORIGIN & HISTORY	9
4.1. How the DoS Attack Works	9
6.2 DoS Best Practice Mitigation Strategies	10
6.3. Modern Protection Tools & Techniques	10
7. MAN-IN-THE-MIDDLE (MITM) ORIGIN & HISTORY	10
7.1. How the MitM Attack Works	10
7.2. MitM Best Practice Mitigation Strategies	11
7.3. Modern Protection Tools & Techniques	11
8. CROSS-SITE SCRIPTING (XSS) ORIGIN & HISTORY	11
8.1. How the XSS Attack Works	11
8.2. XSS Best Practice Mitigation Strategies	12
8.3. Modern Protection Tools & Techniques	12
CONCLUSION	12
REFERENCES	13

Introduction

As cyberattacks continue to evolve in scale, sophistication, and impact this brings significant threat to the digital infrastructures. Organizations are increasingly relying

Task 'Cyberattack Case File Origins Methods and Mitigation' Unit 1

on interconnected systems, cloud services, and web applications, which expands the attack vector available to adversaries, cybercriminals exploit technical vulnerabilities, human error, and inadequate security controls to compromise confidentiality, integrity, and availability of information systems, Breaches and service are continually being disrupted, and demonstrates that cyber threats are no longer isolated technical issues but critical business and societal risks. Understanding how adversaries plan and execute cyberattacks, also, how such can be mitigated, is therefore essential for developing resiliency in the many environments where these operate. This report examines six widely encountered cyberattacks to provide structured insight into their origins, mechanisms, and defense strategies.

Purpose of the Report

The purpose of this report is to examine a number of chosen cyberattack types; Phishing, SQL Injection, Ransomware, Denial-of-Service (DoS), Man-in-the-Middle (MitM), and Cross-Site Scripting (XSS) and to enhance understanding of their technical operation, historical context, and real-world impact, by applying a structured investigation framework, the report aims to bridge theoretical cybersecurity concepts with practical defensive measures used in contemporary organizations. This report seeks to also identify best-practice mitigation strategies and modern protection techniques that are aligned with current industry practices. This includes examining preventive detective and corrective controls, monitoring solutions, and automated defense mechanisms that address risk. Through analysis of attack type, criticality and impact, this report could help enabling informed decision-making regarding cybersecurity prioritization. Ultimately, the findings support the development of robust

Task 'Cyberattack Case File Origins Methods and Mitigation' Unit 1

security postures capable of addressing both technical vulnerabilities and human-centric threats in real-world operational environments.

(Antelada Toledano, 2024).

Scope

The scope of this report covers the set of cyber threats that affect many enterprise IT systems, web applications, cloud platforms, networks and critical infrastructure. It focuses on attacks that exploit both technical weaknesses and user behavior across organizational environments. The report does not focus on any specific incident but instead reviews commonly used by adversaries to attack companies and individuals on a regular basis. The analysis includes six attack types that are frequently observed in real-world cybersecurity incidents. Each attack is examined through origin, execution method, and mitigation strategies and emphasizing defensive measures that are applicable for organizations operating in connected digital ecosystems to leverage and increase protection.

(Kaczmarczyk, 2024).

Overview of Cyberattacks and General Description

A cyberattack is an attempt to deliberately, disrupt, damage, or gain unauthorized access to digital systems, data, or networks. Phishing is very effective social engineering designed to exploit human trust through deceptive communication. SQL

Task 'Cyberattack Case File Origins Methods and Mitigation' Unit 1

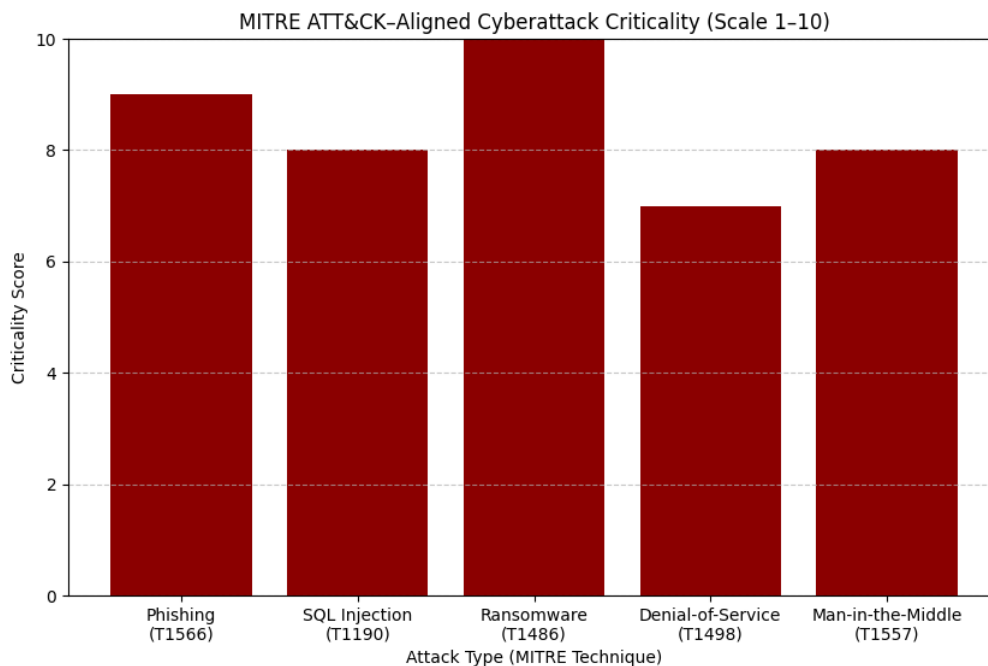
Injection and XSS target insecure web applications. Ransomwares encrypt systems to extort victims. DoS attacks are designed and aim to disrupt legitimate service availability through traffic excess and overloading. MitM attacks intercept transmissions of private connections between two or more trusted parties. Each attack type presents unique set of risks but collectively threatens organizational confidentiality, integrity, and availability. As digital dependence increases, these cyber threats represent critical operational and financial risks to organizations worldwide.

(Kaczmarczyk, 2024)

Attack Type	ATT&CK Tactics Involved	MITRE-Criticality (1–10)	Justification
Phishing	Initial Access, Credential Access, Execution	9	Phishing (T1566) is the most common Initial Access vector and enables multiple downstream ATT&CK techniques, including privilege escalation and lateral movement.
SQL Injection	Initial Access, Persistence, Collection	8	Maps to Exploit Public-Facing Application (T1190); high data breach risk but limited lateral impact compared to ransomware.
Ransomware	Impact, Execution, Lateral Movement	10	Strongly aligned with Impact (T1486 – Data Encrypted for Impact); causes operational shutdowns and is often the final stage of multi-tactic campaigns.
Denial-of-Service (DoS)	Impact	7	Mapped to Network Denial of Service (T1498); disrupts availability but usually does not result in persistent compromise or data loss.
Man-in-the-Middle (MitM)	Credential Access, Collection	8	Associated with Adversary-in-the-Middle (T1557); high risk for credential theft and session hijacking, especially on insecure networks.

Table 1: MITRE ATT&CK Aligned Criticality Rating Table

Task 'Cyberattack Case File Origins Methods and Mitigation' Unit 1



Picture 1: MITRE ATT&CK Aligned Criticality Rating Visualization

The criticality ratings assigned to each cyberattack type is based on the MITRE ATT&CK framework which is used to classify adversary behavior according to tactics, techniques, and their potential operational impact on targeted systems.

(MITRE Corporation, 2025).

Ransomware has the highest impact due to operational shutdowns and financial loss. Phishing remains a primary entry vector. XSS, while serious, typically has localized impact compared to systemic attacks.

Task 'Cyberattack Case File Origins Methods and Mitigation' Unit 1

1. Phishing Origin & History

Phishing emerged in the mid-1990s targeting AOL users. A notable number of targeted attacks had been emerging since the 2010s, where phishing enabled attackers to compromise high-profile business accounts.]

1.1. How the Phishing Attack Works

Attackers send deceptive emails or messages impersonating trusted entities to trick users into revealing credentials or installing malware, exploiting lack of user awareness and weak email authentication.

1.2. Phishing Best Practice Mitigation Strategies

Mitigation measures include, in between: user security awareness training and email authentication protocols such as SPF, DKIM, and DMARC can help to reduce the risk from spoofed communications.

1.3. *Modern Protection Tools & Techniques*

AI-driven email filtering, Secure Email Gateways (SEGs), phishing simulation platforms, and Zero Trust policies are widely used to detect and prevent phishing attacks.

(Panda, 2025).

2. SQL Injection Origin & History

SQL Injection was identified in the late 1990s. A 1998 event mentioned in the Phrack magazine and related to Microsoft SQL server seemed to be injected due to queries that enabled unauthorized data extraction.

Task 'Cyberattack Case File Origins Methods and Mitigation' Unit 1

(Horner and Hyslip, 2017).

2.1 How the SQL Injection Attack Works

Attackers insert malicious SQL code into input fields, exploiting improper input validation to manipulate backend databases and retrieve or modify sensitive data.

(Horner and Hyslip, 2017).

2.2. SQL Injection Best Practice Mitigation Strategies

Prepared statements, parameterized queries, awareness and strict input validation significantly reduce SQL injection vulnerabilities.

(Boateng, 2025)

2.3. Modern Protection Tools & Techniques

Web Application Firewalls (WAFs), automated code scanning tools, in addition it depends on the code and platform, many methods are developed to prevent SQL injection attacks, for instance the OWASP is a very well-known and effective source for such.

(Boateng, 2025; OWASP Foundation 2024)

3. Ransomware Origin & History

Ransomware gained prominence with CryptoLocker in 2014. The 2017 WannaCry attack severely disrupted global healthcare and industrial systems.

(Humayun, et al. 2021)

Task 'Cyberattack Case File Origins Methods and Mitigation' Unit 1

3.1. How the Ransomware Attack Works

Ransomware infiltrates systems via phishing, vulnerabilities and weak backups, encrypting data, and demands payment usually in Bitcoins for the decryption.

(Humayun, et al. 2021)

3.2. Ransomware Best Practice Mitigation Strategies

Regular offline and immutable backups, timely patch management, and network segmentation are essential to limit ransomware spread and recovery time.

3.3. Modern Protection Tools & Techniques

Endpoint Detection and Response (EDR), User Awareness, User behavior-based malware detection, and automated incident response platforms are key modern ransomware defenses.

4. Denial-of-Service (DoS) Origin & History

DoS attacks emerged in 1999. The attack leveraged using tools like trinoo (or trin00) and tribe flood network (or TFN) and using UDP flooding attacked services with malicious intent.

(CERT Incident Notes, 1999).

4.1. How the DoS Attack Works

Attackers overwhelm servers or networks with excessive traffic, exploiting limited bandwidth and resource capacity to deny legitimate user access.

Task 'Cyberattack Case File Origins Methods and Mitigation' Unit 1

(Arafat, et al., 2015)

6.2 DoS Best Practice Mitigation Strategies

Traffic filtering, rate limiting, reverse proxy and redundant infrastructure help reduce the impact of DoS and some DDoS attacks.

(Arafat, et al., 2015)

6.3. Modern Protection Tools & Techniques

While today DDoS attacks present a much higher threat than DoS attacks, a similar approach such as Cloud-based DoS and DDoS protection services, CDN, network behavior analytics, and automated traffic scrubbing are widely adopted defensive solutions in addition to the above mitigation strategies are being used for protection against both DoS and DDoS attacks.

7. Man-in-the-Middle (MitM) Origin & History

MitM attacks have existed since early networking. One very early, notable case involved public Wi-Fi that was documented; reproducible break of WEP, Fluhrer–Mantin–Shamir (FMS) Attack in 2001. Targeting weaknesses in key scheduling of the RC4 algorithm

(Fluhrer, et al, 2001)

7.1. How the MitM Attack Works

MitM Attack comes in many forms, the main characteristic of such attack is where attackers intercept communications between parties, exploiting unsecure channels, weak encryption, or compromised certificates to gain unauthorized access to data.

Task 'Cyberattack Case File Origins Methods and Mitigation' Unit 1

(Rajendran, 2023)

7.2. MitM Best Practice Mitigation Strategies

End-to-end encryption, secure Wi-Fi configurations, and TLS/SSL certificates validation reduce MitM attack risks. Secure WIFI, awareness and monitoring for suspicious activity are few important mitigation measures.

(Rajendran, 2023)

7.3. Modern Protection Tools & Techniques

TLS enforcement, VPN usage, intrusion detection systems, WPA2, WPA3, WPA Enterprise encryption, and Zero Trust Network Access (ZTNA) frameworks mitigate MitM threats.

(Rajendran, 2023)

8. Cross-Site Scripting (XSS) Origin & History

XSS vulnerabilities were identified in early web applications by Microsoft security engineers back in 1999.

(Hannousse, et al, 2024).

8.1. How the XSS Attack Works

XSS attacks can be leveraged using different methods, usually, attackers inject malicious scripts into a browser's web pages viewed by users, exploiting poor input validation and more developed techniques.

Task 'Cyberattack Case File Origins Methods and Mitigation' Unit 1

(Hannousse, et al, 2024).

8.2. XSS Best Practice Mitigation Strategies

Input validation, output encoding, awareness, secure coding and Content Security Policy (CSP) implementation reduce risks from XSS.

(Hannousse, et al, 2024).

8.3. Modern Protection Tools & Techniques

Modern defenses include WAFs, secure coding frameworks such as the OWASP guidelines, automated vulnerability scanners, and browser-level security controls.

Conclusion

This report has investigated six major cyberthreats types that continue to pose few substantial risks to many organizations these days. By analyzing their origins, execution methods, and real-world impacts, it is clear that both technical vulnerabilities and human factors are contributing to the success of such attacks. Effective mitigation is essential. for instance, layered security approach combining, user awareness, secure system design, advanced detection technologies and more modern tools such as AI-driven monitoring, Zero Trust frameworks, and automated response systems play a crucial role in reducing cyber risk. As cyber threats evolve, organizations must continuously adapt their security strategies to maintain resilience and protect critical assets.

(Antelada Toledano, 2024).

Task 'Cyberattack Case File Origins Methods and Mitigation' Unit 1

References

- Arafat, M.Y., Alam, M.M. and Alam, M.F., (2015). A practical approach and mitigation techniques on application layer DDoS attack in web server. *International Journal of Computer Applications*, 131(1), pp.13-20.
- Antelada Toledano, S. (2024) *Critical Infrastructure Security*. May 2024 ed. Birmingham: Packt Publishing.
- Boateng, F., (2025). *SQL Injection Techniques and Mitigation Strategies: a study using OWASP Mutillidae II*.
- Center, C.C., (1999). CERT incident note IN-99-07 distributed denial of service tools. *CERT Coordination Center, Pittsburgh, Incident Note IN-99-07*, http://www.cert.org/incident_notes/IN-99-07.html.
- Fluhrer, S., Mantin, I. and Shamir, A., (2001), August. Weaknesses in the key scheduling algorithm of RC4. In *International Workshop on Selected Areas in Cryptography* (pp. 1-24). Berlin, Heidelberg: Springer Berlin Heidelberg.
- Hannousse, A., Yahiouche, S. and Nait-Hamoud, M.C., 2024. Twenty-two years since revealing cross-site scripting attacks: a systematic mapping and a comprehensive survey. *Computer Science Review*, 52, p.100634.
- Horner, M. & Hyslip, T. (2017) *SQL Injection: The Longest Running Sequel in Programming History*. *The journal of digital forensics, security and law*. [Online] 12 (2), 97–107.
- Humayun, M. et al. (2021) *Internet of things and ransomware: Evolution, mitigation and prevention*. *Egyptian informatics journal*. [Online] 22 (1), 105–117. Available at: https://essex.primo.exlibrisgroup.com/permalink/44UOES_INST/o3t9un/cdi_d

Task 'Cyberattack Case File Origins Methods and Mitigation' Unit 1

oaj_primary_oai_doi.org/article/a78e9db11fc44a2a909b0549018d2529

[Accessed 30 January 2026]

- Kaczmarczyk, B., 2024. Cyberattacks/incidents and responding to them.
- MITRE Corporation (2025) MITRE ATT&CK® Framework. Available at: <https://attack.mitre.org/> [Accessed 30 January 2026]
- Panda, S.P., (2025). The Evolution and Defense Against Social Engineering and Phishing Attacks. International Journal of Science and Research (IJSR).
- OWASP Foundation (2023) Secure Coding Practices Quick Reference Guide. Available at: <https://owasp.org/www-project-secure-coding-practices-quick-reference-guide/> [Accessed 31 January 2026].
- Rajendran, H.H., (2023). Enhance MITM attack detection with response time in Secure web communication (Doctoral dissertation, Dublin, National College of Ireland).